



siteVIEW APEX

Distributed Monitoring Software

User Manual

For siteVIEW APEX

Document #: 050-015-0110

Revision: R04

NOVEMBER 2017

TASC Systems Inc. • Langley, BC • Canada

Disclaimer

TASC Systems Inc. will not be held responsible for any damages, direct or indirect, arising from the use of our materials or from any other causes. Any liability whatsoever is hereby expressly limited to replacement or repair of defective materials.

This manual contains proprietary information that is the intellectual property of TASC Systems Inc. Reproduction, disclosure, modification or distribution, wholly or in part, without prior written permission from TASC Systems Inc., is strictly prohibited.

TASC Systems is continuously working to improve system performance and expand product capabilities. Specifications and features contained within this document are subject to change and will be revised in the next edition of the manual.

For additional copies of this publication contact:

TASC Systems Inc.	Tel: 604-455-2000
9415 – 202 Street	Fax: 604-888-2712
Langley, BC V1M 4B5	info@tascsystems.com
Canada	www.tascsystems.com

Document: 050-015-0110 R04

Copyright 2015 TASC Systems Inc., Langley, BC Canada

PREFACE

This document describes the installation and operation of TASC Systems' siteVIEW APEX distributed monitoring software applications.

Hardware and software described in this document is subject to ongoing development and improvement. Consequently, there may be minor discrepancies between the information in this document and the performance and design of the hardware and software.

The siteVIEW APEX system is designed for flexibility of use and installation and is therefore highly configurable and should only be installed by an appropriately trained technician.

The user should ascertain that this product is suitable for the intended application. TASC Systems Inc. accepts no responsibility, liability, for misuse, or damage resulting from the inappropriate use of the product described herein.



Before connecting any equipment to siteVIEW APEX, it is advised to read this manual in its entirety.

TABLE OF CONTENTS

PREFACE	4
INDEX OF FIGURES	13
INDEX OF TABLES	19
RELATED DOCUMENTS	20
REVISION HISTORY	21
1. PRODUCT DESCRIPTION	22
1.1. GENERAL DESCRIPTION	22
1.2. INSTALLATION REQUIREMENTS	23
1.2.1. <i>siteVIEW APEX Data Manager Requirements</i>	23
1.2.2. <i>siteVIEW APEX TASC Communication Server Requirements</i>	23
1.2.3. <i>siteVIEW APEX Summit Communication Server Requirements</i>	23
1.2.4. <i>siteVIEW APEX SNMP Communication Server Requirements</i>	23
1.2.5. <i>siteVIEW APEX Alarm Notification Manager Requirements</i>	23
1.2.6. <i>siteVIEW APEX Client (User Interface) Requirements</i>	23
1.3. SITEVIEW APEX KEY FEATURES	24
2. INTRODUCTION	25
2.1. SOFTWARE ARCHITECTURE	25
3. SOFTWARE CONFIGURATION	27
3.1. INSTALLING THE SYSTEM	27
3.1.1. <i>Distributed Installations of siteVIEW Components</i>	28
3.2. SITEVIEW APEX LICENSE REGISTRATION	29
3.2.1. <i>Managing the siteVIEW APEX License</i>	30
3.3. CONFIGURING THE DATA MANAGER	34
3.4. CONFIGURING THE TASC COMMUNICATION SERVER	36
3.5. CONFIGURING THE SUMMIT COMMUNICATION SERVER	38
3.6. CONFIGURING THE SNMP COMMUNICATION SERVER	40

3.6.1. Setting the Local SNMP Listening Port	40
3.7. CONFIGURING THE ALARM NOTIFICATION MANAGER.....	42
3.8. STARTING THE SITEVIEW APEX CLIENT (USER INTERFACE)	43
3.8.1. Logging In to siteVIEW	43
3.8.2. Password Recovery.....	45
3.9. REDUNDANT DATA MANAGER	46
3.9.1. System Architecture	46
3.9.2. Installation and Configuration	48
3.9.3. System Operation.....	49
3.9.4. System Considerations	52
4. THE GRAPHICAL CLIENT (USER INTERFACE).....	53
4.1. SITE NAVIGATION TREE.....	54
4.2. MAIN MENU.....	54
4.3. TOOL BAR	55
4.4. ALARM PANEL	55
4.5. SITE PANEL	56
4.6. PANEL COMPONENTS	58
4.7. STATUS BAR.....	58
4.8. COMMUNICATION PANEL	59
4.9. BANDWIDTH METER	60
5. USER ADMINISTRATION.....	61
5.1. MANAGING USER ACCOUNTS.....	61
5.1.1. Managing Users using Apex Authentication.....	62
5.1.2. Managing Users using LDAP-Compatible Authentication.....	64
6. SYSTEM CONFIGURATION	68
6.1. TASC COMMUNICATION SERVERS.....	69
6.1.1. TASC Communication Server Ports.....	70
6.1.2. TASC Communication Server Devices	74

6.2.	SUMMIT COMMUNICATION SERVERS	82
6.2.1.	<i>Summit Communication Server Ports</i>	83
6.2.2.	<i>Summit Communication Server Devices.....</i>	84
6.3.	SNMP COMMUNICATION SERVERS	87
6.3.1.	<i>SNMP Communication Server Ports</i>	87
6.3.2.	<i>SNMP Communication Server Devices</i>	88
6.4.	SITE PANEL	90
6.4.1.	<i>Background Properties.....</i>	90
6.4.2.	<i>Panel Control Property Form.....</i>	91
6.4.3.	<i>Panel Control Types.....</i>	93
6.4.4.	<i>Format String</i>	103
6.4.5.	<i>Adding Controls to a Panel.....</i>	105
6.4.6.	<i>Panel Import and Export</i>	107
6.5.	ALARM CONDITIONS	108
6.5.1.	<i>Alarm Condition States.....</i>	108
6.5.2.	<i>Configuring an Alarm Condition.....</i>	109
6.5.2.1.	<i>Analog and Temperature Sensor Alarm Conditions.....</i>	111
6.5.1.	<i>Alarm Management.....</i>	112
6.5.1.1.	<i>Show Cleared Alarms</i>	112
6.5.1.2.	<i>Clear All Reported Alarms</i>	112
6.5.1.3.	<i>Clear a Selected Alarm</i>	113
6.5.1.4.	<i>Acknowledge a Selected Alarm</i>	114
6.5.1.5.	<i>Clear All Alarms for a Device</i>	114
6.5.1.6.	<i>Clear All Ceased Alarms.....</i>	115
6.5.2.	<i>Alarm Specific Reporting Options.....</i>	115
6.5.3.	<i>Global Alarm Notification Settings.....</i>	118
6.6.	AUTOMATED POLLING.....	125
6.7.	SITE MAPPING.....	127
6.8.	USER ACCESS	129

7. MONITORING AND CONTROLLING DEVICES.....	130
7.1. MONITORING DEVICES	130
7.1.1. TASC Remote Platforms and Summit Devices	130
7.1.1. Ping Devices	131
7.1.2. SNMP Agent Devices	131
7.2. ALARM HANDLING	132
7.3. MANUALLY POLLING THE DEVICES IN THE NETWORK	134
8. LOGGING	135
8.1. SITEVIEW APEX LOGGING	136
8.2. DEVICE LOGGING.....	136
8.3. LOG VIEWER PROPERTIES	137
8.3.1. Log Archiving.....	137
9. SYSTEM ARCHIVE AND RESTORE	139
9.1. AUTOMATED ARCHIVE.....	139
9.2. MANUAL ARCHIVE & RESTORE	139
10. TROUBLESHOOTING.....	141
10.1. EVENT VIEWER	141
10.2. TASC COMMUNICATION SERVER LOG FILES.....	141
10.2.1. Message Transaction Log Files.....	141
10.2.1. Port Transactions Log Files.....	142
10.3. SOLUTIONS TO PROBLEMS	144
APPENDIX A. TASC HARDWARE & FIRMWARE	147
A.1. OVERVIEW.....	147
A.2. CONFIGURATION UTILITIES	147
A.3. ANALOG INPUTS	147
A.3.1. Jumper Configuration	147
A.3.2. User Ranges	149

APPENDIX B. TASC SITECOMMANDER CONFIGURATION	151
B.1. DESCRIPTION.....	151
B.2. GENERAL.....	152
B.3. STARTUP OPTIONS	153
B.4. COMMUNICATION	153
B.5. CONTACT INPUTS	155
B.6. ANALOG INPUTS	156
B.7. TEMPERATURE INPUTS.....	158
B.8. OUTPUTS	159
B.9. DEVICE LOGGING – CONFIGURATION.....	160
B.10. DEVICE LOGGING – DOWNLOADING TO SITEVIEW	161
APPENDIX C. TASC SITEPORTAL LITE CONFIGURATION	164
C.1. DESCRIPTION.....	164
C.2. GENERAL.....	165
C.3. CALL & MODEM CONTROL	165
C.3.1. Call Control.....	165
C.3.2. Device Modem Parameters.....	166
C.4. CONTACT INPUTS	167
C.5. ANALOG INPUTS	168
C.6. TEMPERATURE INPUTS.....	170
C.7. OUTPUTS	172
C.8. SITE INFORMATION	173
C.9. PERIPHERALS.....	174
C.10. PERIPHERAL PASS-THROUGH IN SITEVIEW	174
APPENDIX D. TASC SITERSM CONFIGURATION.....	177
D.1. DESCRIPTION.....	178
D.2. GENERAL.....	178
D.3. COMMUNICATION SETTINGS	179
D.4. CONTACT INPUTS	180

D.5. ANALOG INPUTS	180
D.6. TEMPERATURE INPUTS.....	183
D.7. OUTPUTS	184
APPENDIX E. SUMMIT CONFIGURATION	185
E.1. DESCRIPTION.....	185
E.2. GENERAL.....	186
E.3. COMMUNICATION SETTINGS	187
APPENDIX F. PING DEVICE CONFIGURATION	188
F.1. ADDING PING DEVICES	188
F.2. USING PING DEVICES	189
<i>F.2.1. Understanding Ping Transactions</i>	<i>189</i>
<i>F.2.2. Generating Ping Transactions.....</i>	<i>190</i>
<i>F.2.3. Monitoring Ping Devices Transactions.....</i>	<i>190</i>
<i>F.2.4. Reviewing Ping Device Transactions.....</i>	<i>191</i>
APPENDIX G. SNMP AGENT DEVICE CONFIGURATION	192
G.1. MANAGING SNMP COMMUNICATION	192
<i>G.1.1. Monitoring SNMP Traps.....</i>	<i>192</i>
<i>G.1.2. Connecting the SNMP Communication Server to siteVIEW APEX.....</i>	<i>194</i>
<i>G.1.3. Minimizing the SNMP Communication Server</i>	<i>195</i>
<i>G.1.4. Log Files for the SNMP Communication Server.....</i>	<i>195</i>
G.2. MANAGING SNMP AGENT DEVICES	196
<i>G.2.1. Defining SNMP Agent Devices.....</i>	<i>196</i>
<i>G.2.2. Adding SNMP Agent Devices.....</i>	<i>201</i>
<i>G.2.3. Monitoring SNMP Agent Devices.....</i>	<i>202</i>
APPENDIX H. SITEVIEW TO DEVICE COMMUNICATIONS.....	204
H.1. SITEVIEW APEX TO SITERSM COMMUNICATION MANAGEMENT	204
<i>F.1.1. Overview.....</i>	<i>204</i>
<i>F.1.2. Selecting TASC Serial, CPR Serial and Ethernet Devices</i>	<i>204</i>

F.1.3. Differences between TASC Serial, CPR Serial and IP Devices.....	206
F.1.4. Communication Alarms.....	207
F.1.5. Communication Logging System.....	208
F.1.6. Communication State Icons.....	210
H.2. SITEVIEW APEX COMMUNICATION VIA LANTRONIX CPR PORTS.....	213
F.2.1. Lantronix CPR Overview	213
F.2.2. siteRSM Tunnel Settings.....	215
F.2.3. Lantronix CPR Settings	217
H.3. SITEVIEW APEX COMMUNICATION VIA ETHERNET PORTS	218
F.3.1. Adding Ethernet Devices	218
F.3.2. Using Ethernet Devices.....	219
F.3.2.1. Understanding Ethernet Device Transactions.....	219
F.3.2.2. Generating IP Device Transactions.....	220
F.3.2.3. Monitoring TASC Ethernet Device Transactions.....	220
F.3.2.4. Reviewing Ethernet Device Transactions	221
H.4. MIGRATING TASC SERIAL OR CPR SERIAL DEVICES TO ETHERNET DEVICES.....	222
H.4.1. Adjusting siteRSM IP Settings.....	222
H.4.2. Creating the IP Device	227
H.4.3. Migrating siteVIEW-specific Data	228
H.4.4. Testing and Finalizing Migration.....	230
APPENDIX I. SITEVIEW APEX PANEL DESIGN	231
I.1. PANEL DESIGN GUIDELINES.....	231
I.1.1. Panel Image Size	231
I.1.2. Panel Image Layout.....	232
I.1.3. Panel Sub-Groups.....	232
I.1.4. HMI Standards	233
I.1.5. Panel Image Design Tools	234
I.2. PANEL ICONS.....	235
I.2.1. Icon Usage.....	235

I.2.2.	<i>Icon Design Tools</i>	235
I.3.	SITEVIEW APEX CONTROL GUIDELINES	236
I.3.1.	<i>siteVIEW APEX Control Usage</i>	236
I.3.2.	<i>Contact Input Controls</i>	237
I.3.3.	<i>Contact Outputs Controls</i>	237
I.3.4.	<i>Analog Input Controls</i>	237
I.3.5.	<i>Temperature Controls</i>	237
I.4.	STANDARD SITEVIEW APEX ICON SETS.....	238
APPENDIX J.	SITEVIEW APEX ADMINISTRATION.....	239
J.1.	SITEVIEW APEX DEPLOYMENT	239
J.1.1.	<i>Device Planning</i>	239
J.1.2.	<i>System Communication/Network Design</i>	239
J.1.3.	<i>siteVIEW APEX Client (User Interface) Design</i>	239
J.1.4.	<i>siteVIEW APEX I/O Properties Refinement</i>	240
J.1.5.	<i>siteVIEW APEX User Account Management</i>	240
J.1.6.	<i>siteVIEW APEX Notification and Alarming Definition</i>	240
J.1.7.	<i>siteVIEW APEX Communication Optimization</i>	240
J.1.8.	<i>Operational Preparedness</i>	240

INDEX OF FIGURES

Figure 1 – siteVIEW APEX Software Architecture	25
Figure 2 – Data Manager Utility – License Management tab.....	30
Figure 3 – Data Manager Utility – Extend the License Trial Evaluation	31
Figure 4 – Data Manager Utility – Activate a Module	31
Figure 5 – Data Manager Utility – Activated Module.....	32
Figure 6 – Data Manager Utility – Deactivate a Module	33
Figure 7 – Data Manager Utility – Deactivated Module	33
Figure 8 – Data Manager Utility – Configuration Tab.....	34
Figure 9 – Data Manager Utility – Activity Tab	35
Figure 10 – TASC Communication Server Configuration Tool	36
Figure 10 – Summit Communication Server Configuration Utility	38
Figure 11 – SNMP Communication Server Connected to siteVIEW APEX Data Handler	40
Figure 12 – SNMP Communication Server Select SNMP Listening Port.....	41
Figure 13 – Alarm Notification Manager Configuration Tool.....	42
Figure 14 – siteVIEW APEX Client Desktop Shortcut Icon	43
Figure 15 - Client - Sign In.....	43
Figure 16 - Client - Not Connected to Data Manager	44
Figure 17 - Data Manager Connection Form.....	44
Figure 18 - Redundant Data Manager - System Architecture	46
Figure 19 - Redundant Data Manager - Location of Primary Server	48
Figure 20 - Redundant Data Manager - Connection to Primary Server	49
Figure 21 - Redundant Data Manager - Redundant Data Manager Status	50
Figure 22 - Redundant Data Manager - Assume Role as System Manager	51
Figure 23 - Redundant Data Manager - Connected to Redundant Status.....	51
Figure 24 - Redundant Data Manager - Recovery of Main Data Manager	52
Figure 25 - siteVIEW APEX Client (User Interface)	53
Figure 26 - Toolbar Buttons.....	55
Figure 27 - Alarm Panel Components.....	55

Figure 28 – Site Panel	57
Figure 29 - Status Bar Components.....	58
Figure 30 - Communication Panel	59
Figure 31 - Outputs Update Communication.....	60
Figure 32 – Bandwidth Meter.....	60
Figure 33 - User Access - User Administration	62
Figure 34 - User Access - Changing Your Password	63
Figure 35 - User Access - Current Users.....	63
Figure 36 - User Access - LDAP System Architecture	64
Figure 37 - User Access - LDAP Active Directory Groups	65
Figure 38 - User Access - Enabling LDAP Services	65
Figure 39 - User Access - LDAP Services Enabled	66
Figure 40 - User Access - Login Using LDAP Credentials	66
Figure 41 - Edit Menu	68
Figure 42 – TASC Communication Server Level Context Menu	68
Figure 43 – TASC Communication Server in siteVIEW APEX Network Tree	69
Figure 44 – TASC Communication Server Details	69
Figure 45 – Connection Wizard – Serial Details	70
Figure 46 – Connection Wizard – Ethernet Details.....	71
Figure 47 – Connection Wizard – Timings	71
Figure 48 – Connection Wizard – Identification.....	72
Figure 49 - Connection Details.....	73
Figure 50 – COM Port Panel Component.....	73
Figure 51 – Device Monitoring Wizard – Details (TASC Remote Platforms)	75
Figure 52 – Device Monitoring Wizard - Identification.....	76
Figure 53 – Ethernet Device Connection Details.....	77
Figure 54 – Device Details – Temperature Units Selection	78
Figure 55 – Device Details – Analog Formula Configuration	79
Figure 56 – Formula Configuration Form	80
Figure 57 – Device Monitoring Wizard – Details (Ping Device)	81

Figure 43 – Summit Communication Server in siteVIEW APEX Network Tree	82
Figure 44 – Summit Communication Server Details	82
Figure 45 – Summit Connection Wizard	83
Figure 46 – Connection Wizard – Ethernet Details.....	83
Figure 49 - Connection Details.....	84
Figure 51 – Device Monitoring Wizard – Details (Summit Devices)	85
Figure 52 – Device Monitoring Wizard - Identification.....	85
Figure 53 – Ethernet Device Connection Details.....	86
Figure 58 – SNMP Communication Server in siteVIEW APEX Network Tree.....	87
Figure 59 – SNMP Communication Server Details	87
Figure 60 – Connection Wizard – Identification.....	88
Figure 61 – Device Monitoring Wizard – Details (Ping Device)	89
Figure 62 - Background Properties.....	91
Figure 63 – Selecting Multiple Panel Controls with the Mouse	92
Figure 64 – Multiple Panel Controls Selected	92
Figure 65 – Panel Control Display Properties	93
Figure 66 - Boolean Styles of Panel Controls	95
Figure 67 - Boolean Element Properties.....	96
Figure 68 – Analog Boolean Control Properties.....	97
Figure 69 - Boolean Control On Condition.....	97
Figure 70 - Knob Styles of Panel Controls.....	98
Figure 71 - Knob Properties.....	99
Figure 72 - Slide Styles of Panel Controls	101
Figure 73 - Slide Style Properties	102
Figure 74 - Display Style of Panel Controls	102
Figure 75 - Display Style Properties	103
Figure 76 - Celsius to Fahrenheit Conversion	104
Figure 77 - Adding Text to Format String	105
Figure 78 - Adding I/O to a Panel.....	106
Figure 79 - Panel Control Properties	107

Figure 80 – siteVIEW APEX Alarm Condition States	108
Figure 81 - Alarm Configuration Form.....	110
Figure 82 – Alarm Management	112
Figure 83 – Alarm Management	112
Figure 84 – Alarm Management	113
Figure 85 – Alarm Management	114
Figure 86 – Alarm Management	114
Figure 87 – Alarm Management	115
Figure 88 – Alarm Sound	116
Figure 89 –Text to Speech	117
Figure 90 - Alarm Recipients	118
Figure 91 – Notification Configuration – Display Settings	119
Figure 92 – Notification Configuration – Email.....	120
Figure 93 – Default Email Message Editor	121
Figure 94 – Notification Configuration – Pager Settings.....	122
Figure 95 – Notification Configuration – FleetSync Settings.....	123
Figure 96 – Notification Configuration – SNMP Settings	124
Figure 97 - Polling Configuration Form	125
Figure 98 - Site Mapping Configuration Form.....	127
Figure 99 – User Access Configuration	129
Figure 100 - Site Panel Example for a TASC Remote Platform	131
Figure 101 - Alarm Pop-Up Notification	132
Figure 102 - Alarm Details Form	133
Figure 103 - Manual Poll Options	134
Figure 104 - siteVIEW APEX Log Viewer	135
Figure 105 - siteVIEW APEX Log Viewer - Options	138
Figure 106 – Automated System Archive	139
Figure 107 – Manual System Archive & Restore.....	140
Figure 108 – Sample Message Transaction Log File	142
Figure 109 – Sample Port Transaction Log File	143

Figure 110 - Photo of Analog Jumpers	148
Figure 111 - External Resistor Network.....	150
Figure 112 - Device Properties.....	151
Figure 113 - Device Properties - General.....	152
Figure 114 - Device Properties - Startup Options.....	153
Figure 115 - Device Properties - Communication.....	154
Figure 116 - Device Properties - FFSK Communication.....	155
Figure 117 - Device Properties - Contact Inputs.....	156
Figure 118 - Device Properties - Analog Inputs.....	157
Figure 119 - Device Properties - Temperature Inputs	159
Figure 120 - Device Properties - Outputs	160
Figure 121 - Device Properties - Device Logging	161
Figure 122 - Device Data Logger	162
Figure 123 - Device Details - Description.....	164
Figure 124 - Device Details - General	165
Figure 125 - Device Details – Call & Modem Control	166
Figure 126 - Device Properties – Contact Inputs.....	168
Figure 127 - Device Properties – Analog Inputs	169
Figure 128 - Device Properties – Temperature Inputs.....	170
Figure 129 - Device Properties – Outputs.....	172
Figure 130 - Device Properties – Site Information	173
Figure 131 - Device Properties – Peripherals.....	174
Figure 132 – Starting Peripheral Pass-through	175
Figure 133 – Peripheral Pass-through Connection Waiting	176
Figure 134 - Device Details - Description.....	178
Figure 135 - Device Details - General	178
Figure 136 - Device Details – Communication	179
Figure 137 - Device Properties – Contact Inputs.....	180
Figure 138 - Device Properties – Analog Inputs	182
Figure 139 - Device Properties – Temperature Inputs.....	183

Figure 140 - Device Properties – Outputs.....	184
Figure 134 - Device Details - Description.....	185
Figure 135 - Device Details - General	186
Figure 135 - Device Details - Communication	187
Figure 141 - Ping Device - Add Device.....	189
Figure 142 - Ping Device - Non-Responsive Alarms.....	190
Figure 143 - siteVIEW APEX - SNMP Communication Server	192
Figure 144 - siteVIEW APEX - SNMP Communication Server - Listen Settings	193
Figure 145 - siteVIEW APEX - SNMP Communication Server - Incoming Traps	193
Figure 146 - siteVIEW APEX - SNMP Communication Server - Detailed Trap Information.....	194
Figure 147 – siteVIEW APEX - SNMP Communication Server -Configuration File Settings	194
Figure 148 - siteVIEW APEX - SNMP Communication Server - Log Files	195
Figure 149 – siteVIEW APEX MIB Translator Utility	197
Figure 150 – siteVIEW APEX MIB Translator Utility – Load MIBs	198
Figure 151 - siteVIEW APEX MIB Translator Utility- Confirm OIDs.....	199
Figure 152 - siteVIEW APEX MIB Translator Utility - MIB Translator Options.....	200
Figure 153 - siteVIEW APEX – Monitoring SNMP Agent Devices in siteVIEW APEX Client	202
Figure 154 - siteVIEW APEX – Monitoring SNMP Agent Devices in siteVIEW APEX History.....	203
Figure 155 – Communication Alarms – Non-Responsive Alarms	207
Figure 156 – Communication Logging System – Transmit Receive Log Files.....	208
Figure 157 – Communication Logging System – TASC Communication Server Log File	209
Figure 158 – siteVIEW APEX to siteRSM Connections	213
Figure 159 – Connection Management – Device Status Poll	214
Figure 160 – siteRSM Tunnel Settings – XPort Pro.....	215
Figure 161 – siteRSM Tunnel Settings - XPort.....	216
Figure 162 – siteRSM Tunnel Settings.....	218
Figure 163 - Ethernet Port Communication - Add Device.....	219
Figure 164 - Ethernet Port Communication - Monitoring Port Health.....	221
Figure 165 - Migrating to Ethernet - siteRSM Config Logon Screen	222
Figure 166 - Migrating to Ethernet - Telnet Config	223

Figure 167 - Migrating to Ethernet - Select Channel	224
Figure 168 - Migrating to Ethernet - Flush Mode	225
Figure 169 - Migrating to Ethernet - Save Config	226
Figure 170 - Migrating to Ethernet - Create Ethernet Port	227
Figure 171 - Migrating to Ethernet - Add Device	227
Figure 172 - Migrating to Ethernet - Export Panel	228
Figure 173 - Migrating to Ethernet - Import Panel	229
Figure 174 - Migrating to Ethernet - Update Formulas	229
Figure 175 - Migrating to Ethernet - Adjust Scheduled Polls	230
Figure 176 – Sample Panel Layout	233
Figure 177 – Default siteVIEW APEX Controls	236
Figure 178 – Standard siteVIEW APEX Icon Set	238

INDEX OF TABLES

Table 1 – Login Security Level Matrix.....	61
Table 2 – Recommended Communication Timing Parameters	72
Table 3 - Device Properties – Analog Jumper Configuration	148
Table 4 - Device Properties – Analog Jumper Ranges	149
Table 5 - Device Properties – Suggested External Resistor Network Values.....	150

RELATED DOCUMENTS

- [siteCOMMANDER User Manual \(050-015-0002\)](#)
- [sitePORTAL Lite User Manual \(050-015-0012\)](#)
- [siteRSM User Manual \(050-015-0052\)](#)
- [siteVIEW APEX MOBILE User Manual](#)
- [Summit User Manual \(050-015-0112\)](#)

REVISION HISTORY

Revision	Date	Changes
050-015-0110 R01	March 2015	<ul style="list-style-type: none">Initial release of the siteVIEW APEX Manual
050-015-0110 R02	May 2015	<ul style="list-style-type: none">Updated for siteVIEW APEX v3.1 (Copy Protection System)
050-015-0110 R03	August 2016	<ul style="list-style-type: none">Updated to include information on Redundant Server and LDAP re-introduction
050-015-0110 R04	November 2017	<ul style="list-style-type: none">Updated to include information on Summit Communication Service

1. PRODUCT DESCRIPTION

1.1. GENERAL DESCRIPTION

TASC siteVIEW APEX is a distributed monitoring software package designed to work in conjunction with TASC hardware monitoring products. Currently siteVIEW APEX supports the following monitored elements:

- Using the TASC Communication Server: siteCOMMANDER, sitePORTAL lite, siteRSM and the ability to ping third party IP based network devices
- Using the Summit Communication Server: Summit devices
- Using the SNMP Communication Server: SNMP (agent) devices

siteVIEW APEX is built with an easy to use graphical user interface (GUI) that provides visibility into a network of devices. This simplifies the task of site monitoring by centralizing all site information and communication into a single software package.

siteVIEW APEX allows for multiple simultaneous client connections to the siteVIEW APEX data warehouse. With this ability, it is possible to setup a group of operators or dispatchers, in one or multiple locations, to supervise and control devices in the network.

siteVIEW APEX Components:

- Data Manager
 - Data Warehouse
 - Logging Interface
- Device Communication Services
 - TASC Communication Service
 - Summit Communication Service
 - SNMP Communication Server
- Alarm Notification Handler
- Client (User Interface)
 - Graphical Client User Interface
 - Log Viewer

1.2. Installation Requirements

1.2.1. siteVIEW APEX Data Manager Requirements

- Microsoft Windows 7, 8, 8.1, Server
- Microsoft .NET Framework 3.5 or later

1.2.2. siteVIEW APEX TASC Communication Server Requirements

- Microsoft Windows 7, 8, 8.1, Server
- Microsoft .NET Framework 3.5 or later

1.2.3. siteVIEW APEX Summit Communication Server Requirements

- Microsoft Windows 7, 8, 8.1, Server
- Microsoft .NET Framework 3.5 or later

1.2.4. siteVIEW APEX SNMP Communication Server Requirements

- Microsoft Windows 7, 8, 8.1, Server
- Microsoft .NET Framework 3.5 or later

1.2.5. siteVIEW APEX Alarm Notification Manager Requirements

- Microsoft Windows 7, 8, 8.1, Server
- Microsoft .NET Framework 3.5 or later

1.2.6. siteVIEW APEX Client (User Interface) Requirements

- Microsoft Windows 7, 8, 8.1, Server
- Microsoft .NET Framework 3.5 or later
- Microsoft DirectX 9.0 or later

1.3. siteVIEW APEX Key Features

N-Tier Software Architecture

SNMP Manager and Agent Functionality

Device Configuration and Monitoring

Various Alarm Reporting Options

Multi – Protocol Communication Routing

Scheduled Polling and Log Retrieval

Site-to-Site Output Mapping

Custom Panel Backgrounds

Drag and Drop Site Panel Controls

Site Grouping

Kenwood FleetSync™ Protocol Integration

Simple Licensing Scheme

2. INTRODUCTION

2.1. Software Architecture

siteVIEW APEX is based on an N-Tier software model with several components that are responsible for different components of the system. There is a central *Data Manager* service that manages access to the data that is stored in the Data Warehouse and several services that connect to each other.

The siteVIEW APEX Logging Interface is installed with the *Data Manager* and provides access to the siteVIEW logs. The log viewer is installed with the siteVIEW APEX Client (User Interface) and it connects to the logging interface.

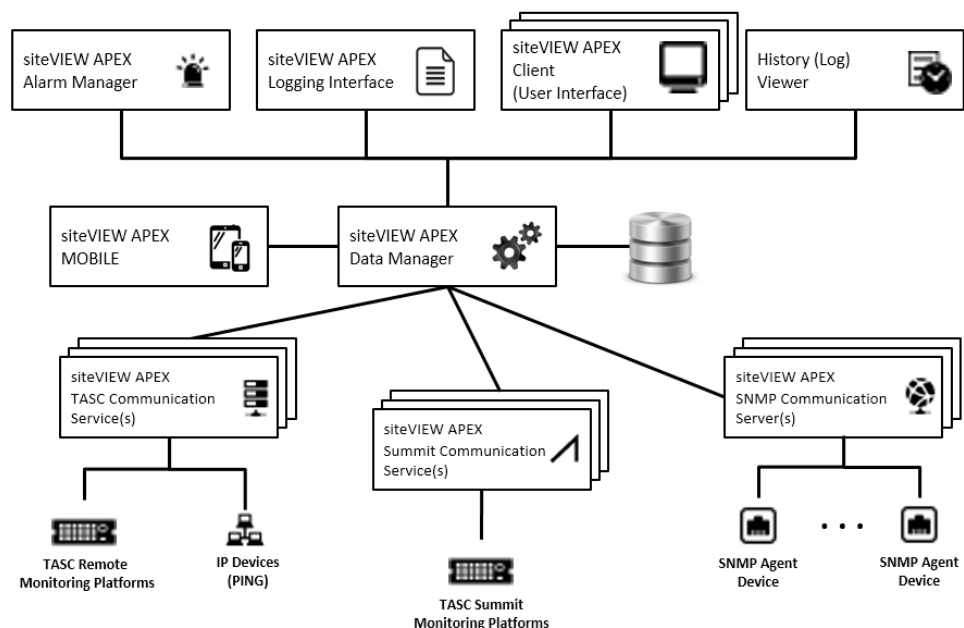


Figure 1 – siteVIEW APEX Software Architecture

The *Alarm Notification Manager* provides services for notifying recipients of alarms via email or pager notifications.

One or more TASC Communication Server(s) clients handle communication with one or more sites through communication ports on the PC. Each *TASC Communication Server* communicates with a set of TASC Remote Monitoring platforms and/or IP (Ping) devices and then forwards the received data on to the *Data Manager* where the data is then interpreted and stored in the *Data Warehouse*. Multiple *TASC Communication Servers* can be connected to the same *Data Manager* at the same time.

One or more Summit Communication Server(s) clients handle communication with one or more set of Summit devices. Each *Summit Communication Server* communicates with a set of Summit devices and then forwards the received data on to the *Data Manager* where the data is then interpreted and stored in the *Data Warehouse*. Multiple *Summit Communication Servers* can be connected to the same *Data Manager* at the same time.

One or more SNMP Communication Server(s) clients handle communication with one or more set of SNMP agent devices. Each *SNMP Communication Server* communicates with a set of SNMP Agent devices and then forwards the received data on to the *Data Manager* where the data is then interpreted and stored in the *Data Warehouse*. Multiple *SNMP Communication Servers* can be connected to the same *Data Manager* at the same time.

The siteVIEW APEX Client connects to the *Data Manager* and requests the stored information and displays it in an organized manner. Multiple user interfaces can be connected to the *Data Manager* at the same time and can view information for any *TASC Communication Servers* connected to the *Data Manager*.

Each application is installed using its own installation program. All four applications can be installed on the same computer or on separate computers. There can be only one *Data Manager* and *Alarm Notification Manager* active for each system, but there can be several *TASC Communication Servers*, *SNMP Communication Servers* and user interfaces installed on several computers.

siteVIEW APEX MOBILE interface can be installed to allow client access for mobile devices. Please refer to the siteVIEW APEX MOBILE User Manual for more information.

3. SOFTWARE CONFIGURATION

3.1. Installing the System

The entire siteVIEW APEX system can be installed on a single computer, or each component can reside on different computers connected via network.

1. Start by installing the *Data Manager* and configure the *Data Manager*. See [Configuring the Data Manager](#).
2. Install the siteVIEW APEX client application and configure it to connect to the *Data Manager*. See [Starting the siteVIEW APEX Client](#), of this manual. Several client applications may be installed on different computers and used simultaneously to connect to the *Data Manager*.
3. Install a *TASC Communication Server* and configure it so that it can connect to the *Data Manager*. See [Configuring the TASC Communication Server](#). Several *TASC Communication Servers* running on different computers can be configured within the system.
4. Install a *Summit Communication Server* and configure it so that it can connect to the *Data Manager*. See [Configuring the Summit Communication Server](#). Several *Summit Communication Servers* running on different computers can be configured within the system.
5. Install a *SNMP Communication Server* and configure it so that it can connect to the *Data Manager*. See [Configuring the SNMP Communication Server](#). Several *SNMP Communication Servers* running on different computers can be configured within the system.



Currently the *SNMP Communication Server* is installed by simply copying the release directory to a suitable location and running the SnmpCommServer.exe application.

For convenience, you may consider locating it in the same directory as the other siteVIEW APEX components.

6. Install an *Alarm Notification Manager* and configure it so that it can connect to the *Data Manager*. See [Configuring the Alarm Notification Manager](#). Only one *Alarm Notification Manager* is needed in the system.
7. Using the siteVIEW APEX client application, configure communication ports, devices, alarm conditions & notification, users, site mapping, automated polling, panels and more.

3.1.1. Distributed Installations of siteVIEW Components

If siteVIEW APEX software components are to be installed as a distributed system over multiple platforms and networks to balance load and/or manage system architecture, the following considerations are recommended:

- The firewall mechanism for each platform, either Windows or other third-party, must allow the siteVIEW APEX specific ports. For example, if you are using port 11003 to connect the siteVIEW APEX client from one platform to a Data Manager on another platform, both platforms should permit port 11003 usage.
- If the platforms are distributed over different networks and/or accessible via public IP address, it may be necessary to configure your system's router to port-forward to the internal platform's connection.

3.2. siteVIEW APEX License Registration

siteVIEW APEX utilizes a key-based copy protection system to manage licensing for software functionality.

Software functionality is partitioned into modules:

- siteVIEW APEX Core Module – enables the core infrastructure of siteVIEW APEX including general operation and alarm management.
- TASC and Ping Devices Module – enables the TASC and Summit Communication Service(s). The TASC Communication Service interfaces with TASC remote terminal units – sitePORTAL Lite, siteCOMMANDER, siteRSM – and Ping devices. The Summit Communication Service interfaces with Summit devices.
- SNMP Agent Devices Module – enables the SNMP Communication Server(s). The SNMP Communication Server interfaces with SNMP agent devices.
- Other Software Modules – enables various (future) software modules provided by siteVIEW APEX

Upon initial install, siteVIEW APEX provides all modules on a trial basis. Users must activate the modules before the expiration date to retain software functionality of these modules.

Keys are used to activate individual modules. These keys are provided as part of your purchase. Once activated the modules provide full software functionality for the life of your system.

There are two methods for activation, web activation and manual activation. Web activation can be performed through the Data Manager Utility. Manual activation is only recommended if Internet access is not available. Contact TASC Systems technical support to perform manual activation.

The activation process registers the module's key within TASC Systems registration system and within the siteVIEWAPEX.lic file.



The siteVIEWAPEX.lic file holds the activation information for the siteVIEW APEX system. This file will only work on the server on which it was activated on. It cannot be moved to another system.

By default, siteVIEW APEX provides the ability to have 10 user clients.

3.2.1. Managing the siteVIEW APEX License

Use the siteVIEW APEX Data Manager Utility's License Management tab to manage the siteVIEW APEX modules. The License Management tab shows the status of each module and provides multiple options for management.

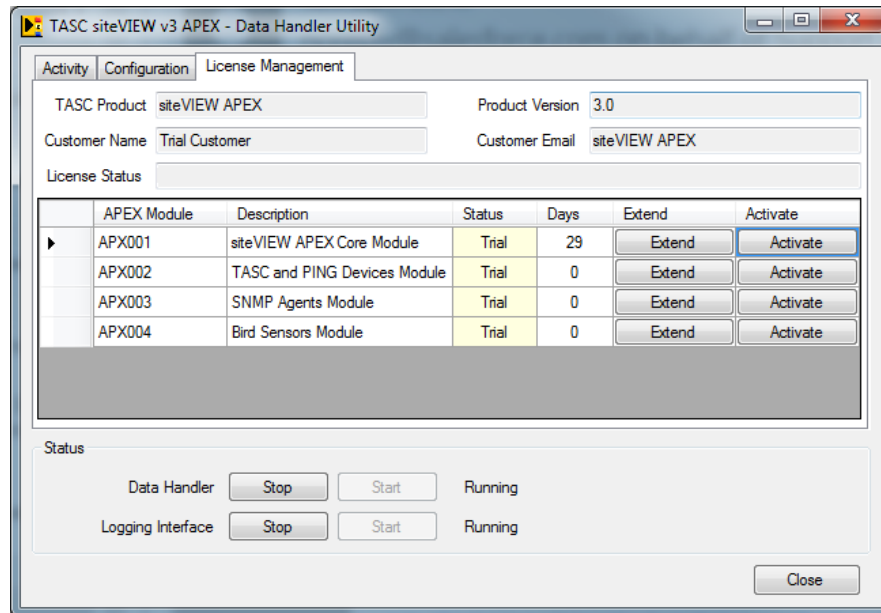


Figure 2 – Data Manager Utility – License Management tab

Extending the License Trial Evaluation

For trial customers, if you need to extend the trial of siteVIEW APEX to continue evaluation, please contact TASC Systems technical support for trial extension key(s).

Upon receiving the trial extension key, use the Extend button for the siteVIEW APEX Core Module to enter the key. Additional days will be provided for all siteVIEW APEX modules once the key is registered.

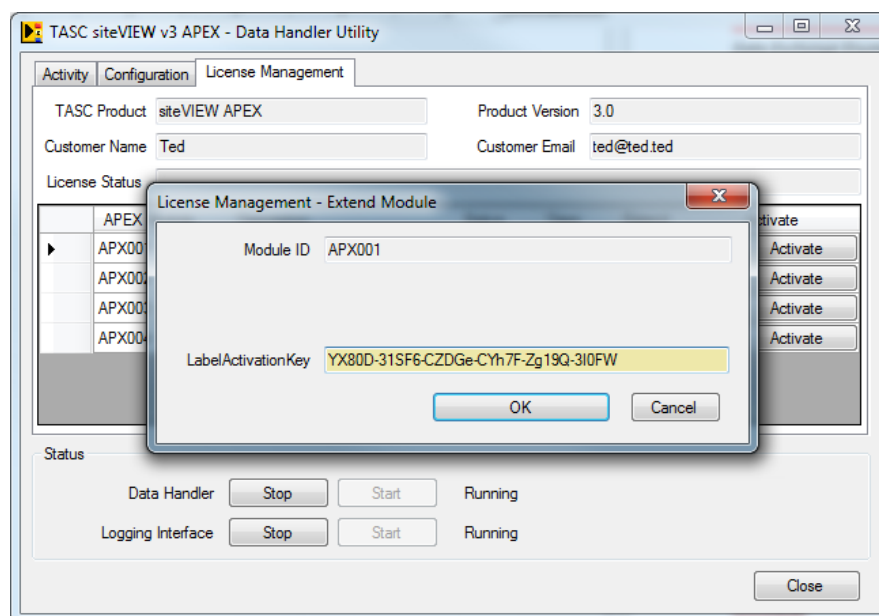


Figure 3 – Data Manager Utility – Extend the License Trial Evaluation

Activating Modules

To activate a module, use the Activate button for the module and enter the company, company email and the key provided for this module. This information will be registered within TASC Systems license activation server.

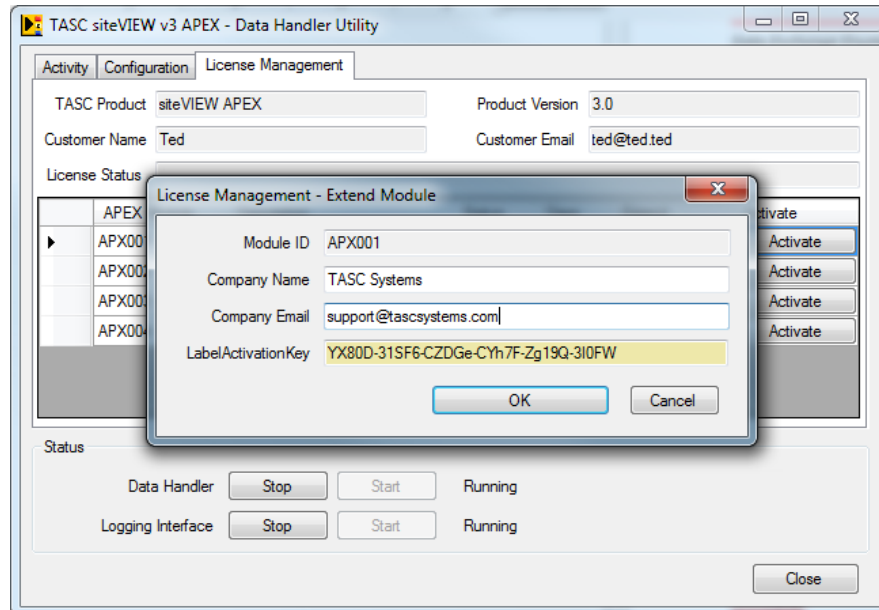


Figure 4 – Data Manager Utility – Activate a Module



The activation process can take up to 30 seconds. Any issues or errors will be reported in the License Status text area.

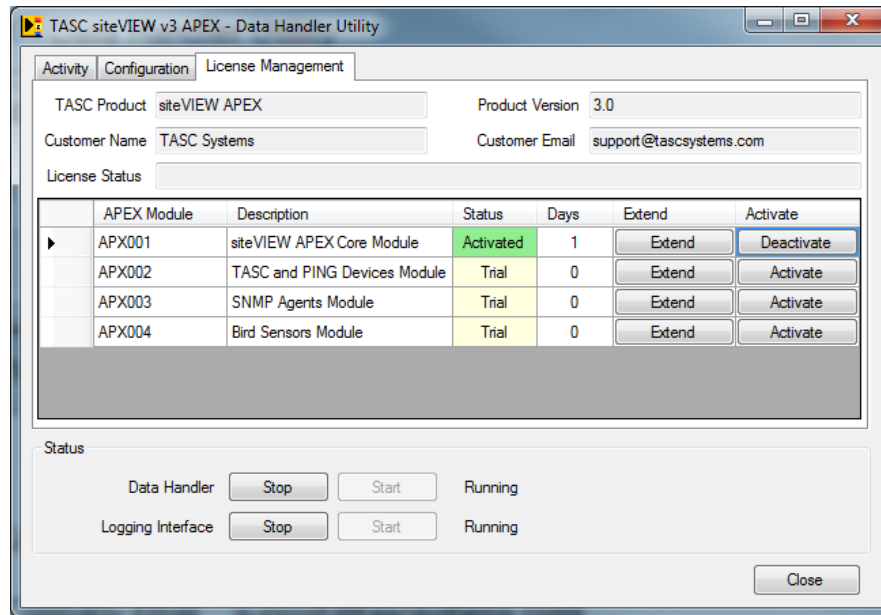


Figure 5 – Data Manager Utility – Activated Module

Once activated, the module will show as activated and is fully functional for the life of your siteVIEW APEX system.

The activation process also ties the siteVIEWAPEX.lic file to the server on which siteVIEW APEX Data Manager is operating.

Deactivating Modules

Since an activated license is tied to the server on which the Data Manager is running, to move your siteVIEW APEX system to another server, the modules must first be de-activated, then re-activated on the new server.

To deactivate a module, use the Deactivate button for the module.

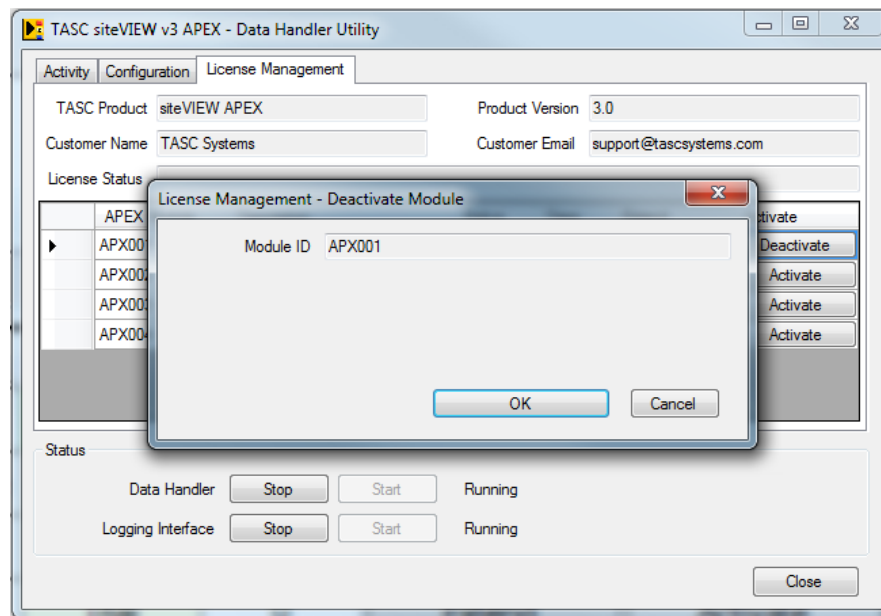


Figure 6 – Data Manager Utility – Deactivate a Module



The deactivation process can take up to 30 seconds. Any issues or errors will be reported in the License Status text area.

Once deactivated, the module will show as deactivated and the key is ready to be used on another system.

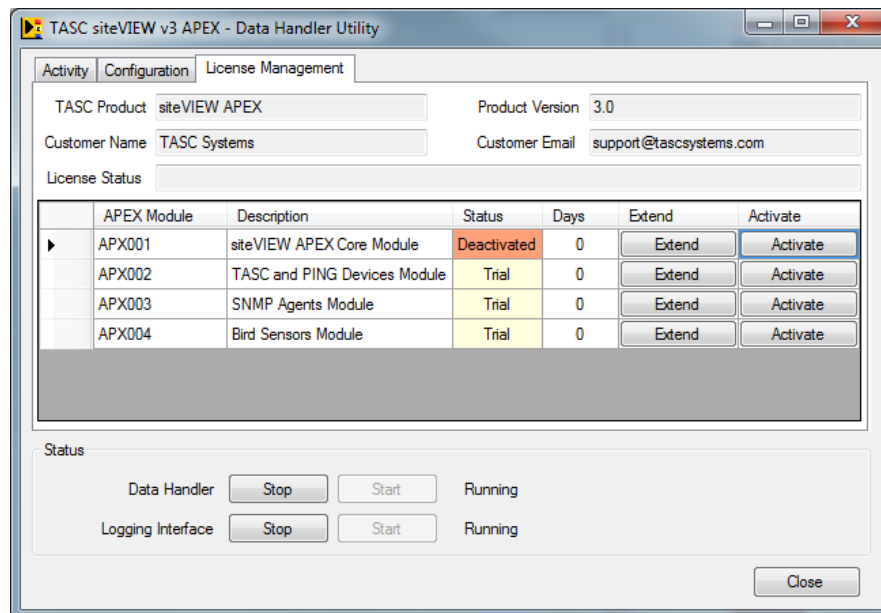


Figure 7 – Data Manager Utility – Deactivated Module

3.3. Configuring the Data Manager

By default the *Data Manager* is configured to monitor incoming client connections on port 11003. The *Logging Interface* installs with the *Data Manager* and it is configured to monitor incoming *Log Viewer* connections on port 11006. The default ports can be changed using the *Data Manager Utility* (DataHandlerConfigTool.exe), which can be accessed from the windows start menu at:

Start->Programs->TASC->siteVIEW APEX Data Manager Utility

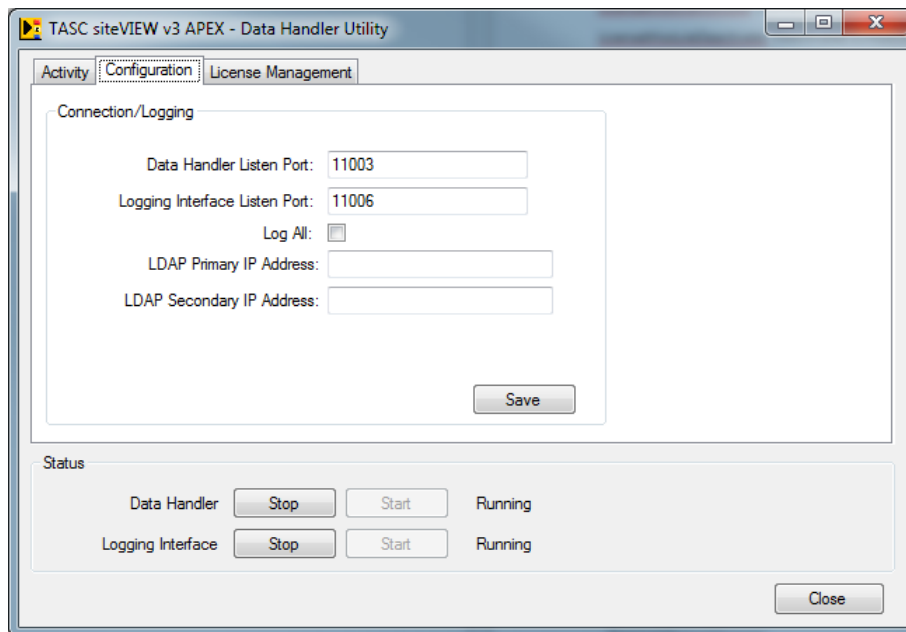


Figure 8 – Data Manager Utility – Configuration Tab

Using the *Data Manager Utility* you can change the port numbers that the *Data Manager* and *Logging Interface* will monitor. Press the save button to save any changes you make and then stop and start the services to get the *Data Manager* and *Logging Interface* to run with the changed settings.

Valid port numbers range from 0 to 65535, but ports numbers 0 to 1024 are reserved for privileged services and designated as well-known ports and should be avoided.

Log All is a feature that when enabled, will log all I/O levels when polling and not just the changes in I/O levels.

Once the changes have been saved and the *Data Manager* or *Logging Interface* services have been restarted, press exit to minimize the *Data Manager Utility* to the

system tray. If you wish to close the *Data Manager Utility* completely, right click on the system tray icon and select exit.

From the activity tab of the *Data Manager Utility*, the system can be monitored for progress while it is loading, or an administrator can check that no updates are waiting to be saved to the database before shutting the *Data Manager* down or restarting the computer.

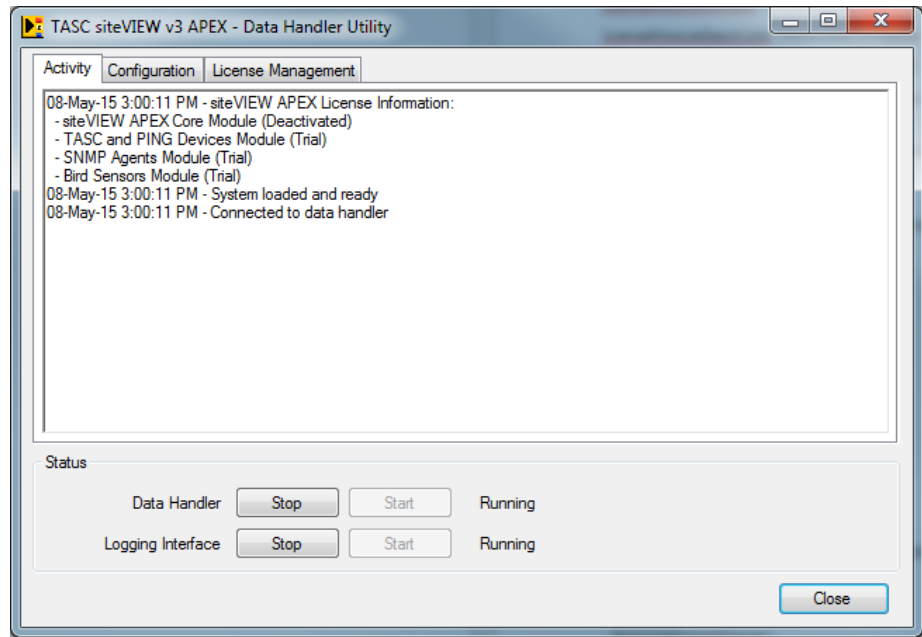


Figure 9 – Data Manager Utility – Activity Tab

When the *Data Manager* runs, it waits for connections from *TASC Communication Servers* and *Clients*. When the *Logging Interface* runs, it waits for connections from client *Log Viewers*. By default, the *Data Manager* and *Logging Interface* services start automatically after the installation and every time the computer is restarted. These services continue to run as a background service even if no user is logged into the computer.

The *Data Manager Utility* is configured from the installation program to start automatically on login to the windows operating system.

3.4. Configuring the TASC Communication Server

Each *TASC Communication Server* must be configured to connect to the *Data Manager* using the *TASC Communication Server Configuration Tool* (CommServiceConfigTool.exe), which can be accessed from the windows start menu at:

Start->Programs->TASC->siteVIEW APEX TASC Communication Server Configuration Tool

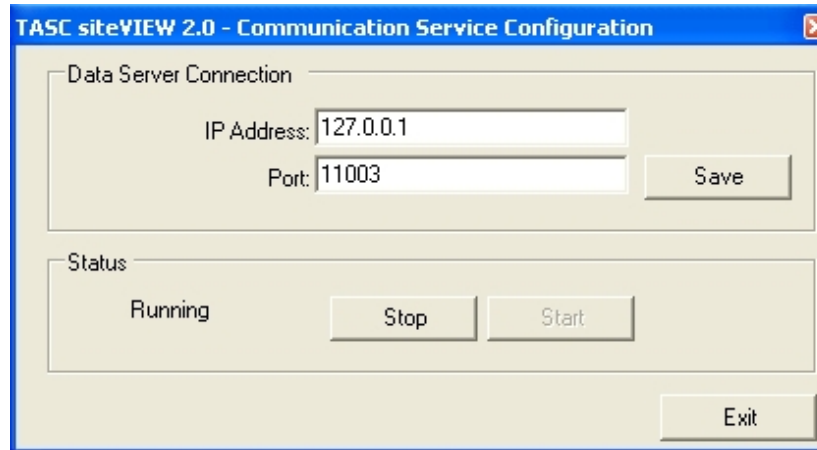


Figure 10 – TASC Communication Server Configuration Tool

Using the configuration tool you can type the IP Address or DNS Name of the computer where the *Data Manager* is installed. Press the save button to save any changes you make and then stop and start the service to get the *TASC Communication Server* to run with the changes.

Once the changes have been saved and the *TASC Communication Server* has been restarted, press exit to close the *TASC Communication Server Configuration Tool*.

The *TASC Communication Server* will automatically connect to the *Data Manager* and monitor ports it has been configured to monitor. By default, the *TASC Communication Server* starts automatically after the installation and every time the computer is restarted. The *TASC Communication Server* continues to run as a background service even if no user is logged into the computer.

You will know if the *TASC Communication Server* has connected successfully by running the siteVIEW APEX Client application and viewing connected *TASC Communication Servers*.



If the *TASC Communication Server* is running on the same machine as the *Data Manager*, the recommended IP Address is localhost (127.0.0.1).

3.5. Configuring the Summit Communication Server

Each *Summit Communication Server* must be configured to connect to the *Data Manager* using the *Summit Communication Server Configuration Utility* (SummitCommServiceConfigTool.exe), which can be accessed from the windows start menu at:

Start->Programs->TASC->siteVIEW APEX Summit Communication Server Configuration Utility

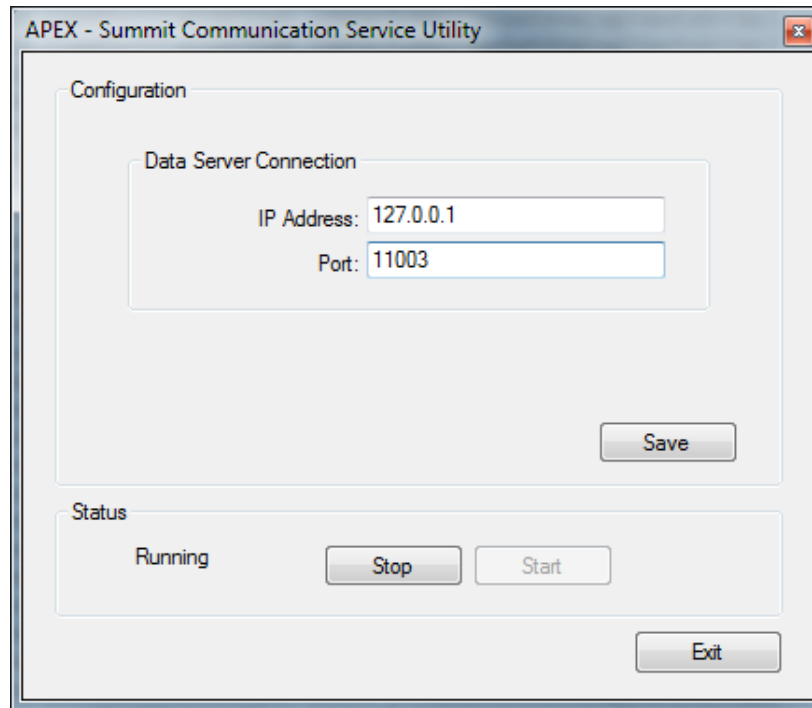


Figure 11 – Summit Communication Server Configuration Utility

Using the configuration utility you can type the IP Address or DNS Name of the computer where the *Data Manager* is installed. Press the save button to save any changes you make and then stop and start the service to get the *Summit Communication Server* to run with the changes.

Once the changes have been saved and the *Summit Communication Server* has been restarted, press exit to close the *Summit Communication Server Configuration Tool*.

The *Summit Communication Server* will automatically connect to the *Data Manager* and monitor ports it has been configured to monitor. By default, the *Summit Communication Server* starts automatically after the installation and every time the computer is restarted. The *Summit Communication Server* continues to run as a background service even if no user is logged into the computer.

You will know if the *Summit Communication Server* has connected successfully by running the siteVIEW APEX Client application and viewing connected *Summit Communication Servers*.



If the *Summit Communication Server* is running on the same machine as the *Data Manager*, the recommended IP Address is localhost (127.0.0.1).

3.6. Configuring the SNMP Communication Server

Each *SNMP Communication Server* must be configured to connect to the *Data Manager*. By default, the SNMP Communication Server will attempt to auto-connect to a Data Manager. You will know if the *SNMP Communication Server* has connected successfully if the indicator to the right of the Start and Stop buttons is green and says “Connected to siteVIEW APEX Data Manager”.

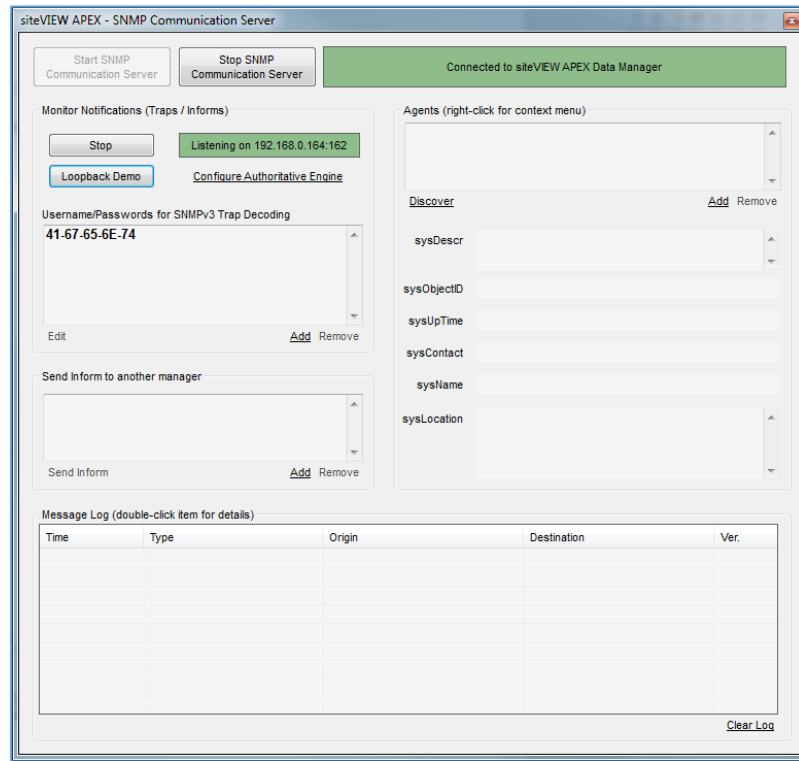


Figure 12 – SNMP Communication Server Connected to siteVIEW APEX Data Handler

3.6.1. Setting the Local SNMP Listening Port

By default, the SNMP Communication Server will begin listening for incoming SNMP messages on the first registered IPv4 address for the PC.

To change the listening port, press the Stop button in the Monitor Notifications, then press Start and select the appropriate listening port.

You will know if the *SNMP Communication Server* is listening if the indicator to the right of the Start and Stop buttons is green and says “Listening on <IP Address:IP Port>”, where IP Address:IP Port is the selected listening port.

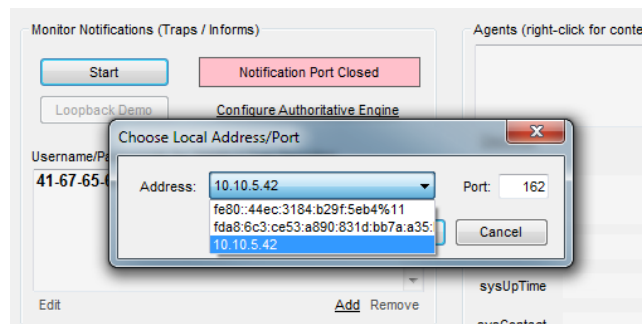


Figure 13 – SNMP Communication Server Select SNMP Listening Port

3.7. Configuring the Alarm Notification Manager

The *Alarm Notification Manager* must be configured to connect to the *Data Manager* using the *Alarm Notification Manager Configuration Tool* (AlarmHandlerConfigTool.exe), which can be accessed from the windows start menu at:

Start->Programs->TASC->Alarm Notification Manager Configuration Tool

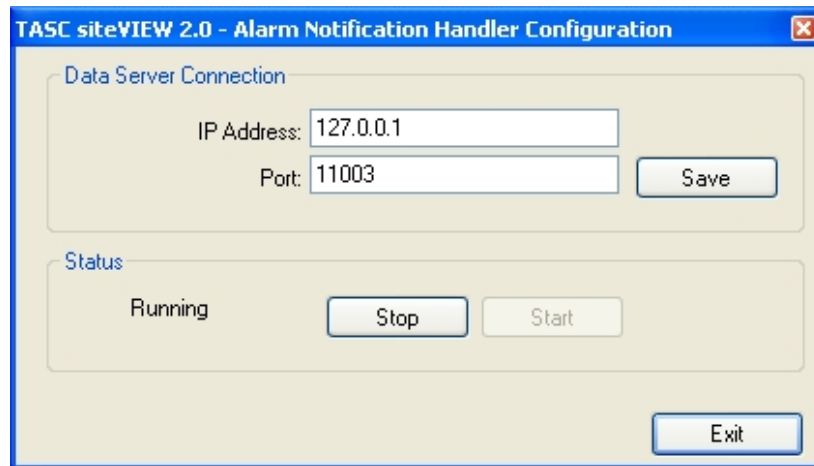


Figure 14 – Alarm Notification Manager Configuration Tool

Using the configuration tool you can type the IP Address or DNS Name of the computer where the *Data Manager* is installed. Press the save button to save any changes you make and then stop and start the service to get the *Alarm Notification Manager* to run with the changes.

Once the changes have been saved and the *Alarm Notification Manager* has been restarted, press exit to close the *Alarm Notification Manager Configuration Tool*.

The *Alarm Notification Manager* will automatically connect to the *Data Manager* and monitor ports it has been configured to monitor. By default, the *Alarm Notification Manager* starts automatically after the installation and every time the computer is restarted. The *Alarm Notification Manager* continues to run as a background service even if no user is logged into the computer.



If the *Alarm Notification Manager* is running on the same machine as the *Data Manager*, the recommended IP Address is localhost (127.0.0.1).

3.8. Starting the siteVIEW APEX Client (User Interface)

3.8.1. Logging In to siteVIEW

To launch the siteVIEW APEX Client, double click on the “siteVIEW APEX User Interface Client” icon that the installation placed on the computer desktop.

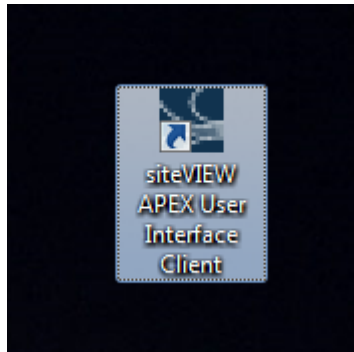


Figure 15 – siteVIEW APEX Client Desktop Shortcut Icon

This can also be accomplished from the Windows start menu, select “Programs->TASC->siteVIEW APEX”.

After launching siteVIEW, one of two things should occur:

If the siteVIEW APEX Client is able to connect to a siteVIEW APEX Data Manager, a *Sign In* form will appear. This is a typical scenario if the Data Manager is installed on the same computer as the user interface, or if the Data Manager Service connection was established previously.



Figure 16 - Client - Sign In

If the host computer exists, but the siteVIEW APEX Client is not able to connect to the siteVIEW APEX Data Manager Service, the siteVIEW APEX Client will launch and at the bottom left corner of the application, the words “Attempting Connection With Server: <servername>” appear, where <servername> is the name of server specified. Then when the connection fails, the words “No Connection” appear. siteVIEW APEX will then continue attempting the connection.

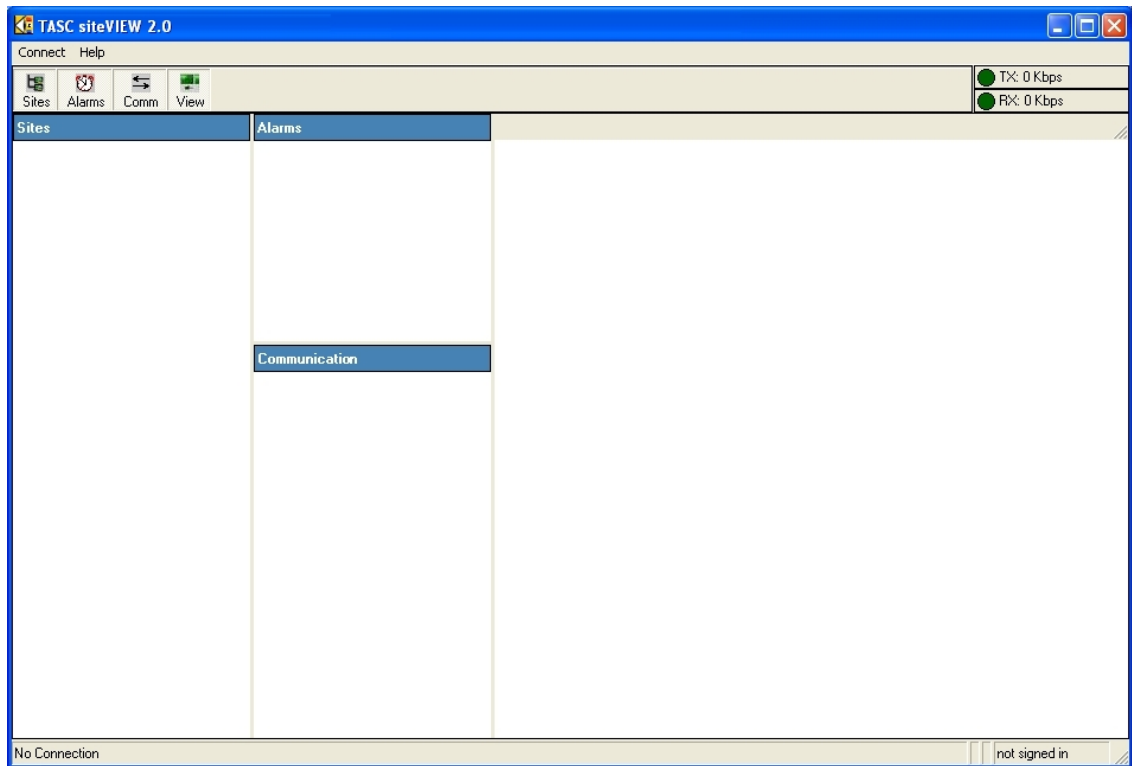


Figure 17 - Client - Not Connected to Data Manager

To connect to the *Data Manager*, select “Connect->Connect to Server” from the main menu and you will be presented with a connection form.

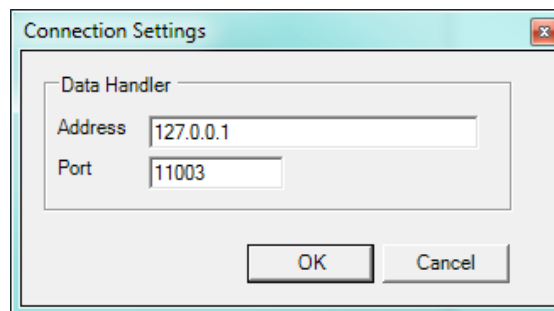


Figure 18 - Data Manager Connection Form

Enter the IP Address or the DNS machine name of the computer where the *Data Manager* is installed. During the client installation, the default *Data Manager* Connection is set up as 127.0.0.1 with port 11003.



If the *siteVIEW APEX Client* is running on the same machine as the *Data Manager*, the recommended IP Address is localhost (127.0.0.1).

Once the *Sign In* form appears, sign in using a valid username and password. When signing in to siteVIEW APEX for the first time, use the username *svadmin* with password *siteview*. The svadmin is an administrator account with full rights to every part of siteVIEW.



Note: To ensure proper security, change the svadmin password during the first sign in

3.8.2. Password Recovery

There is a password-recovery link on the login form, but it only works if a user has setup their email address.

After selecting the password-recovery link, the user specifies the username. An email containing their password information is sent to the user's email account. An administrative user can set the default SMTP server in the notification options form. If the SMTP server is not set, the password-recovery email will fail.

When a user logs in they are reminded to set their email address each time they log in until they set an email address. Admin users can set their email address and the email addresses of other users in the user admin form.

Non-administrative users can set their email address by selecting “Connect->Accounts->Change Email Address” from the main menu.

A message is displayed to the user to tell them if the email was sent or not. The email is then sent to the SMTP server, which may fail to send the email for other reasons.

3.9. Redundant Data Manager

While most typical installations need only run a singular Apex (Data Manager) server, for critical systems, users may consider running a redundant Apex (Data Manager) server. The purpose of the redundant Apex Data Manager server is to take over responsibilities of the system should the main Apex (Data Manager) server go down, thereby limiting any downtime that may result.

3.9.1. System Architecture

A redundant system is best set up using multiple servers, each with specific Apex functionality:

- **Data Manager (Main) Server** – this server acts as the primary system manager and will manage most day-to-day activity. The main system database resides here.
- **Data Manager (Redundant) Server** – this server acts as the back-up to the primary system manager, taking over general system duties if something should happen to the primary system. A synchronized image of the database is managed here.

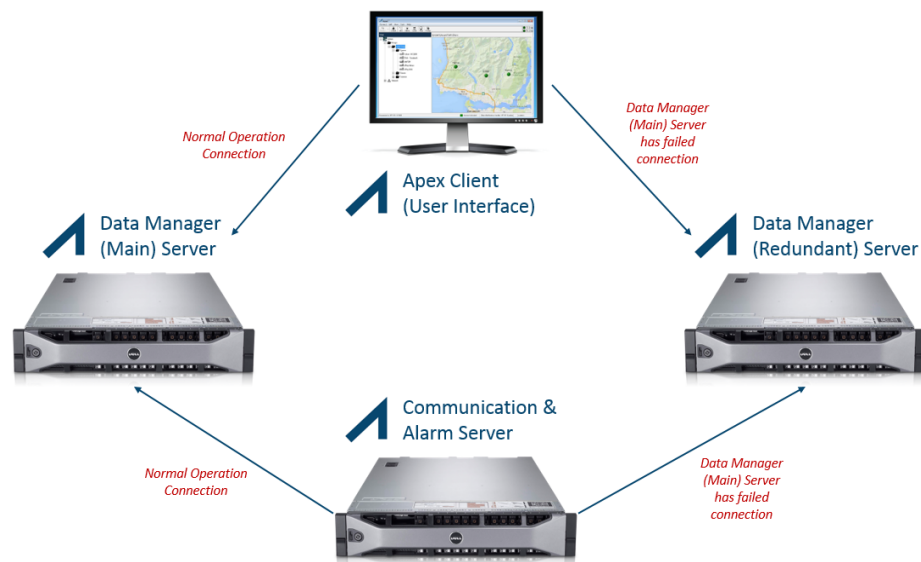


Figure 19 - Redundant Data Manager - System Architecture

- Communication and Alarm Server – this server provide supplementary Apex services. Under normal situations, these services will be report to the primary system manager, but should something happen to the primary system, will automatically connect to the Redundant Server. Upon recovery of the primary system, the services will automatically revert connection back to the primary system.
- Apex clients – one or more clients will normally be connected to the primary system manager, but should something happen to the primary system, will automatically connect to the Redundant Server. Upon recovery of the primary system, the clients will automatically revert connection back to the primary system.

3.9.2. Installation and Configuration

Data Manager (Main) Server

The Apex Data Manager should be installed normally using the provided installation package (MSI file).

Upon installation, the Apex Data Manager should be activated using the software license keys provided at the time of purchase.

This installation will now act as the Data Manager (Main) Server.

Data Manager (Redundant) Server

On a separate OS image/platform than that of the installation of the Data Manager (Main) Server, install another instance of the Apex Data Manager package.

If you have purchased the Redundant Server option, a license file ([ApexRedundantServer.lic](#)) will be provided. After installation, copy this license file to the `C:\Program Files (x86)\TASC\siteVIEW Apex\APEXDataManager` directory.

Either reboot the system or restart the Data Manager to recognize the license file, this will allow the Apex Data Manager to read the license file and re-configure itself to run as a back-up system.

Use the Data Manager Utility to enter the location of the Data Handler (Main) Server:

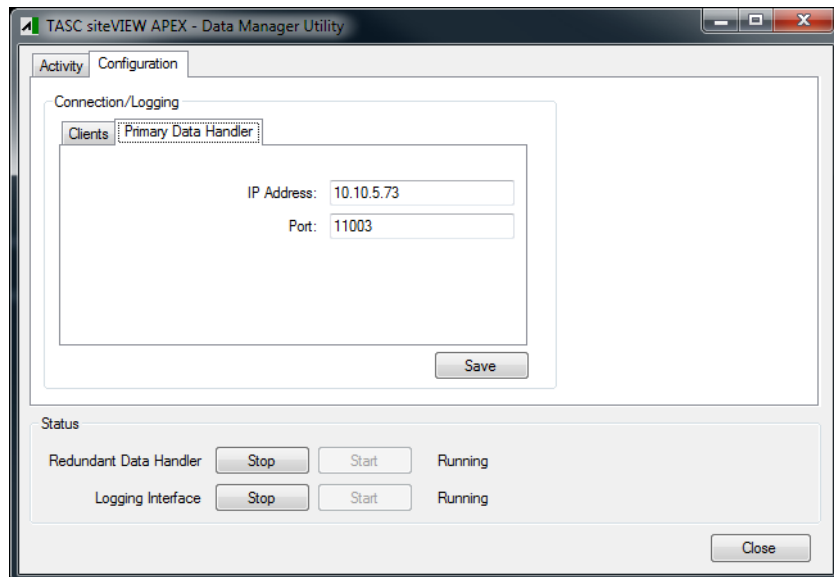


Figure 20 - Redundant Data Manager - Location of Primary Server

Either reboot the system or restart the Data Manager again to recognize the Primary Data Handler location, this will allow this system to connect to the primary system with the new location information.

This installation will now act as the Data Manager (Redundant) Server.



Note: Ensure that the redundant server is visible through the network to the *TASC Communication Servers* and the clients.

3.9.3. System Operation

Start-up of the Apex Data Manager (Main)

Upon system start, all Apex components including the Data Manager (Redundant) Server, the Communication and Alarm Server and all Apex (User Interface) clients connect to the Data Manager (Main) Server using configuration default settings.

Upon successful system start, the Data Manager (Main) Server manages all system activity, including coordination with the Apex Communication Server(s), event annunciation through the Apex Alarm Manager and view capability via the attached Apex (User Interface) clients. Any significant activity is tracked in the Apex system database.

Upon connection, each Apex component is informed about system server configuration, including location of the Data Manager (Redundant) Server, if present. The location of the Data Manager (Redundant) Server is used in case of the primary server failure, each Apex component knows to switch connection to the back-up server.

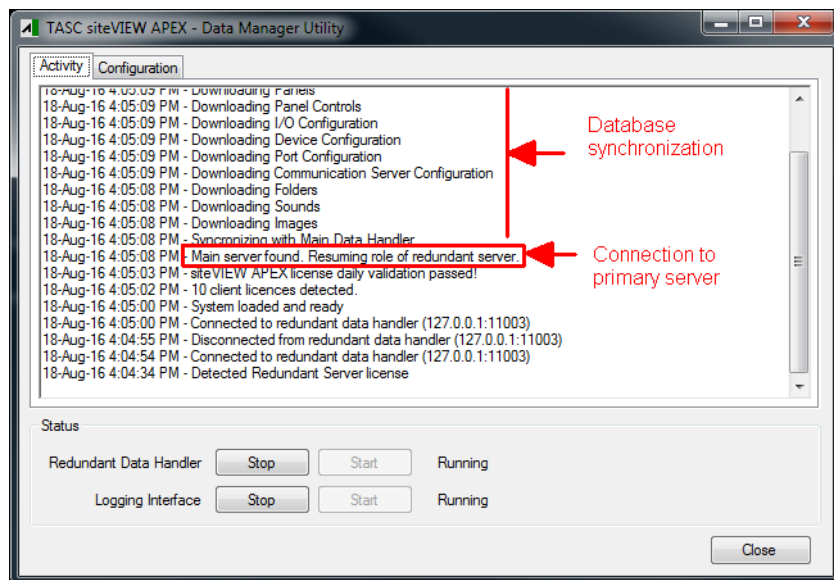


Figure 21 - Redundant Data Manager - Connection to Primary Server

The status bar of the siteVIEW APEX client then shows the location of the connected Data Manager (Main) and the Data Manager (Redundant).

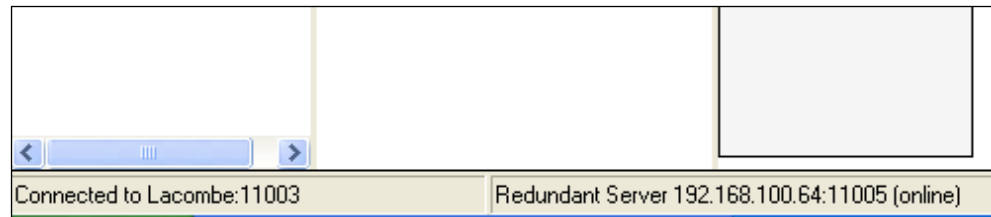


Figure 22 - Redundant Data Manager - Redundant Data Manager Status

Switch to Apex Data Manager (Redundant)

The Data Manager (Main) Server can failover to the Data Manager (Redundant) Server if one or more of these problems arise:

- Power failure
- Network failure which prevents the Data Manager (Redundant) Server to check for the Data Manager (Main) Server's health
- Failure of the hardware platform on which the Data Manager (Main) runs
- Failure of the Data Manager (Main) Server due to a software application issue

Upon a failed connection to a server, the Apex components will connect another server. That is, if the Apex component was previously connected to the primary server, it will attempt connection to the Data Manager (Redundant) Server. But also conversely, if the Apex components were previously connected to the back-up server, they will attempt connection to the Data Manager (Main) Server.

Upon failure of the primary server, the Data Manager (Redundant) Server manages all system activity, including coordination with the Apex Communication Server(s), event annunciation through the Apex Alarm Manager and view capability via the attached Apex (User Interface) clients. Any significant activity is tracked in a back-up version of the Apex system database.

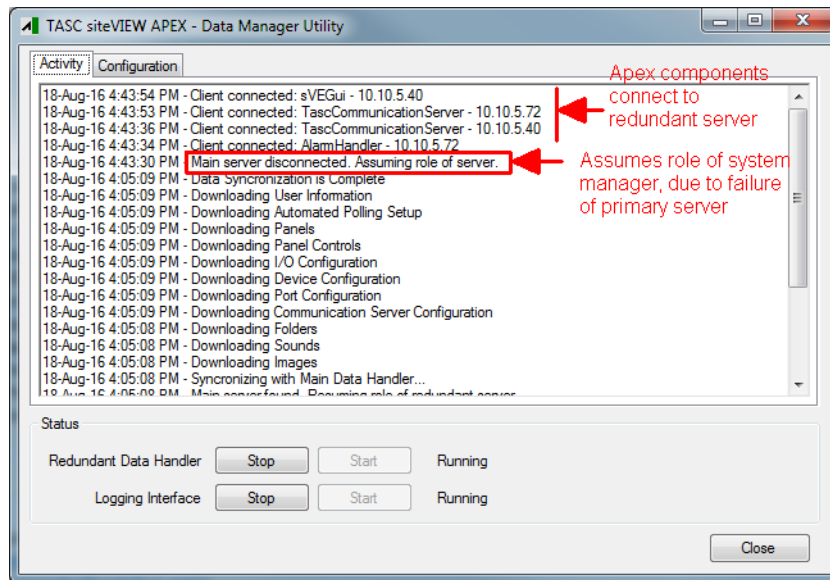


Figure 23 - Redundant Data Manager - Assume Role as System Manager

The status bar indicates when the client is connected to the redundant *Data Manager*.

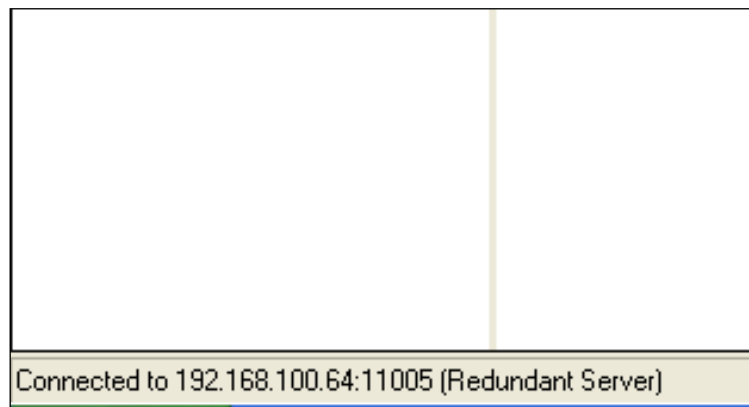


Figure 24 - Redundant Data Manager - Connected to Redundant Status

Recovery of the Apex Data Manager (Main)

Every 5 seconds, the Data Manager (Redundant) Server monitors its connection to the Data Manager (Main) Server, if the Data Manager (Main) Server has recovered, all Apex components are redirected to connect to the recovered Data Manager (Main) Server – essentially returning to normal operation.

Upon recovery, any database changes that were recorded while the primary server was down are forwarded from the Data Manager (Redundant) Server to the Data

Manager (Main) Server, so that all data is synchronized into the primary Apex system database.

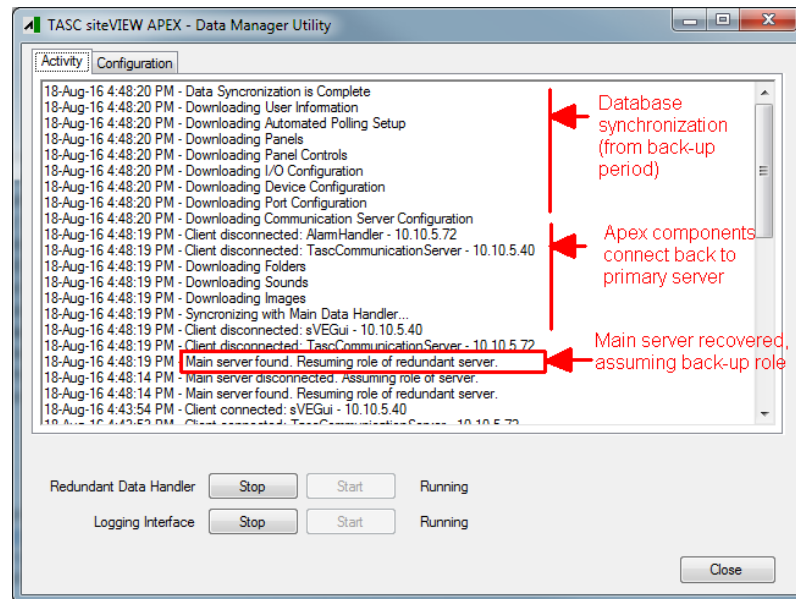


Figure 25 - Redundant Data Manager - Recovery of Main Data Manager

3.9.4. System Considerations

- Start- The Data Manager (Main) Server and Data Manager (Redundant) Server must be on physically two different OS images/platforms.
- While it is possible to install Communication and Alarm services on the same image/platform as either the Data Manager (Main) Server or the Data Manager (Redundant) Server, this is not recommended. To safeguard against the case where there is catastrophic failure of either one of the Data Manager systems, it is best to separate this function to a separate OS image/platform.
- Currently, there is no redundancy offered for communication or alarm services, but it is possible to run duplicate communications or alarm servers.

4. THE GRAPHICAL CLIENT (USER INTERFACE)

The siteVIEW APEX Client (User Interface) is used to view activity and configure the operational parameters of the siteVIEW APEX system. The siteVIEW APEX Client

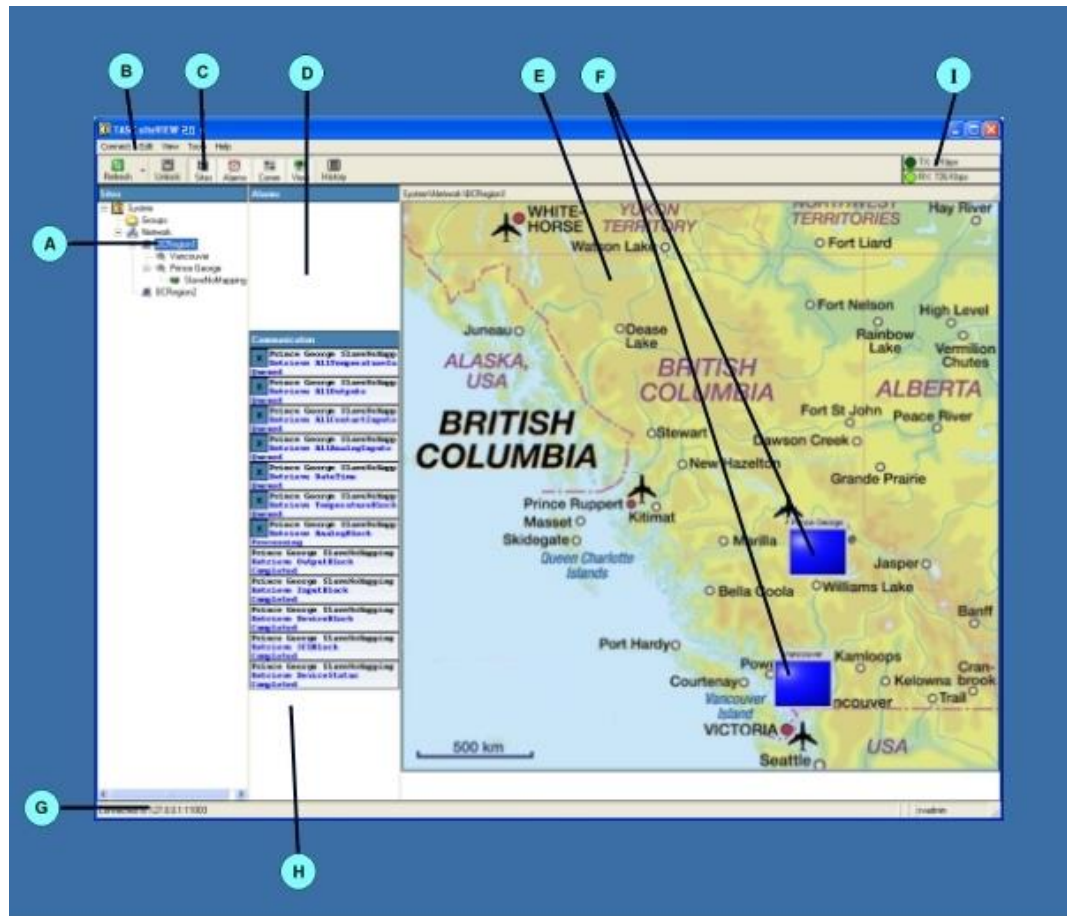


Figure 26 - siteVIEW APEX Client (User Interface)

consists of a main application window that is divided into several sections

- A.** Site Navigation Tree - A tree view of the nodes in a network
- B.** Main Menu – Contains all available menu options
- C.** Toolbar – Quick access to routine functions
- D.** Alarm Panel – Detailed listing of all alarms
- E.** Site Panel – Graphical display of sites or network
- F.** Panel Components – Interactive elements in the network
- G.** Status Bar – Real time program information
- H.** Communication Panel – Listing of network communications
- I.** Bandwidth Meter – Displays network data passed to and from siteVIEW

4.1. Site Navigation Tree

The Site Navigation Tree is a logical representation of a network of monitoring devices (e.g., siteRSM, SNMP devices), which are capable of reporting input and output states to siteVIEW APEX through a communication port (COM or IP port) via the *TASC Communication Server* or *SNMP Communication Server*.

The first level node of the Site Navigation Tree represents the complete siteVIEW APEX system, which contains a 'Groups' node and a 'Network' node.

The Groups node contains custom arranged groups of devices and folders. The "Groups" node's purpose is to arrange devices into custom groupings. Add sub-folders to the "Groups" node and then drag device links into various folders. Right-click on the mouse will provide the additional Cut to Group (for moving to a new group), Copy to Group and Paste to Group options.

The first level nodes of the Network represent *TASC Communication Servers*, *Summit Communication Servers* or *SNMP Communication Servers* that are connected to the *Data Manager*. The second level nodes of the Network represent the monitored communication ports on the *TASC Communication Server*, *Summit Communication Server* or *SNMP Communication Server*. The communication ports are used for monitoring remote devices. The third level of Network represents the physical device.

Right clicking on one of the tree nodes levels (i.e. system, groups, network, server, COM port, device) allows quick access to menu options, by displaying a context menu that pertains to the selected node.

Left clicking on a node updates the site panel to display a graphical representation of all nodes beneath the selected node.

4.2. Main Menu

The main menu allows access to configuration and monitoring of the tree nodes. Some menu items change depending on the node selected, and depending on the user's security rights (See Managing User Accounts, section 5.1, on page 61 of this manual.)

4.3. Tool Bar

The toolbar allows quick access to some menu options

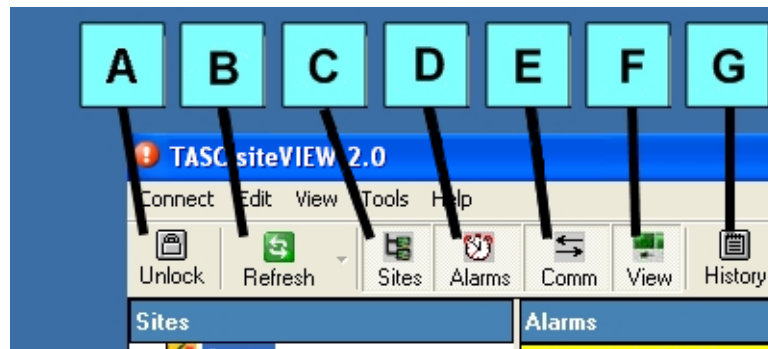


Figure 27 - Toolbar Buttons

- A. Lock/Unlock Site Panel layout
- B. Perform manual poll of the selected portion of the network
- C. Hide/Show Site Navigation Tree
- D. Hide/Show Alarm Panel
- E. Hide/Show Communication Panel
- F. Hide/Show Site Panel
- G. View logs

4.4. Alarm Panel

The alarm panel displays a list of alarms that have not been cleared at the remote site. Each alarm item in the alarm panel has the following information:

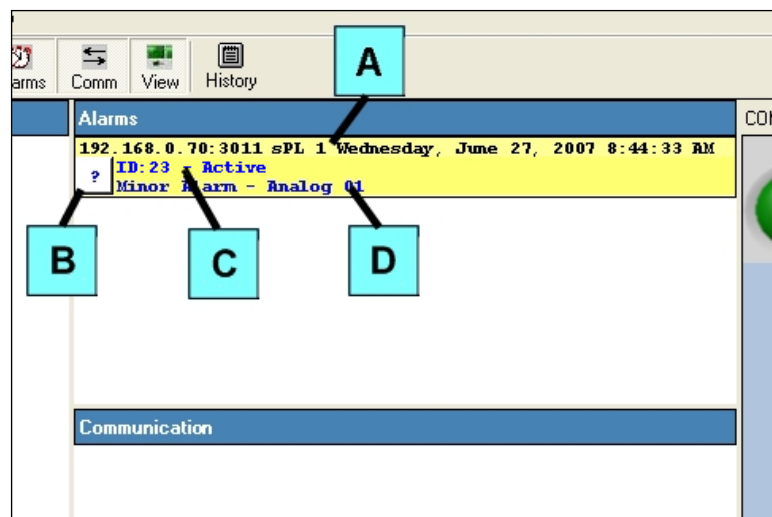


Figure 28 - Alarm Panel Components

- A. Port & device name of the alarm and the last time the alarm status changed
- B. Auto-find button
- C. Alarm ID and status
- D. Alarm severity and the name of the I/O where the alarm condition occurred

The auto-find button appears as a square button with a question mark in the center. Selecting the auto-find button causes the corresponding device node to be selected on the Tree View and for the corresponding panel to be drawn.

Double clicking on an alarm shows more detailed information about the selected alarm and allows the user to acknowledge and clear the alarm.

When an alarm is active and unacknowledged, the alarm will flash a different color depending on the severity of the alarm.

Right-clicking the mouse in the Alarms panel area provides additional contextual options:

- Use the “Clear All Alarms” to clear all ceased alarms
- Access detailed information about the selected alarm
- View a historical summary of alarms within the Log Viewer

4.5. Site Panel

The site panel displays a graphical representation of the currently selected tree node. This provides simplified visibility in networks of monitored devices.

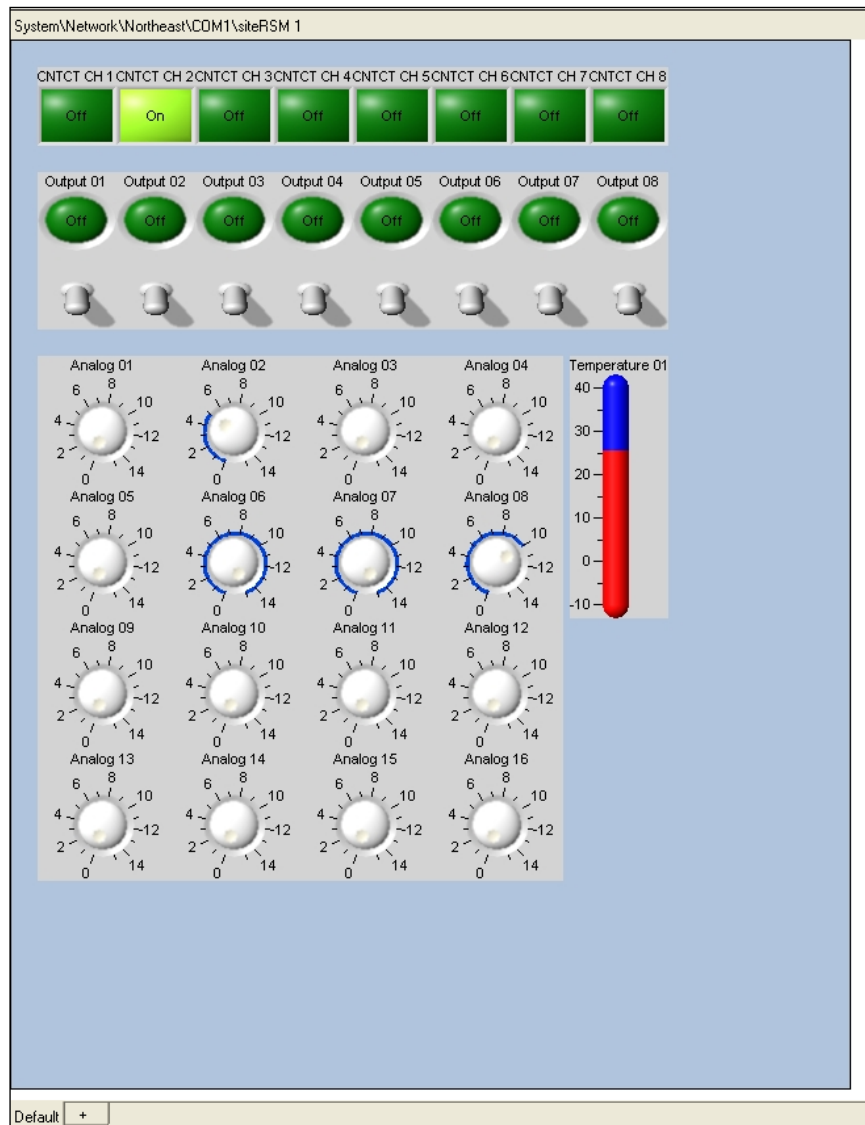


Figure 29 – Site Panel

At the top of the site panel is a status bar that displays the full path name of the selected network tree node.

Device outputs can be controlled from the site panel.

The size, component placement, background image and color of the panel can all be customized. (See Site Panel, section 0, on page 82 for information on customizing the site panel)

When a device's panel is selected, the ability to add more panels is available. A panel selection tab appears on the bottom of the device panel. This feature allows a device to be represented in multiple ways. Press the far right tab with a plus (+) sign on it to add a new panel, or right click on the panel and select the "Insert New Panel" option. From the same menu you can also rename the selected panel or

delete it. If a device only has one panel, it cannot be deleted. The menu options can also be accessed from the main menu by selecting “Edit->Panel”.

4.6. Panel Components

The Site Panel is made up of images, text and panel components. Panel components are interactive elements that allow the operator to navigate as well as monitor and control various areas of their network. Panel components include virtual knobs, buttons, lights, switches, labels, temperature gauges and more.

At a sever node, Panel Components represent the available and configured COM ports that are accessible on the network.

At a COM Port node, panel components represent the available and configured devices accessible on the network.

At a device node, Panel Components represent the specific physical inputs and outputs available to a particular device.

The type, size, color, font and many other configuration options can be customized. (See Panel Control Property Form, section 6.4.2, on page 91 for information on customizing the panel controls)

4.7. Status Bar

The status bar is used to display various messages to the user. The far left of the status bar displays the *Data Manager* connection status and the far right displays the user login status. The center of the status bar shows the online status of the

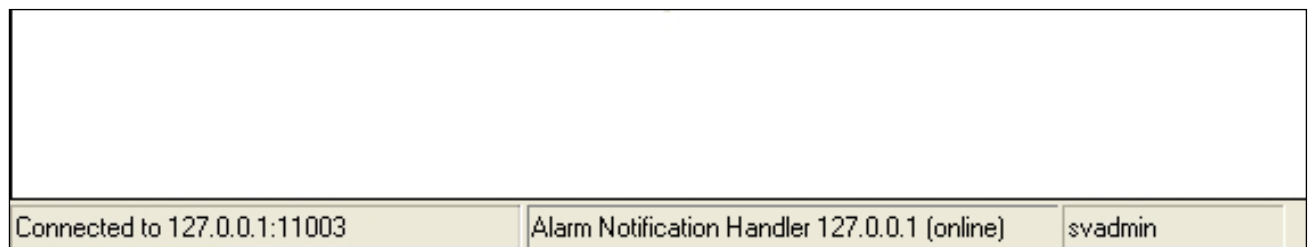


Figure 30 - Status Bar Components

Alarm Notification Manager and if installed, the *Redundant Data Manager*.

4.8. Communication Panel

The communication panel contains recent network communication traffic and the following details pertaining to those transactions:

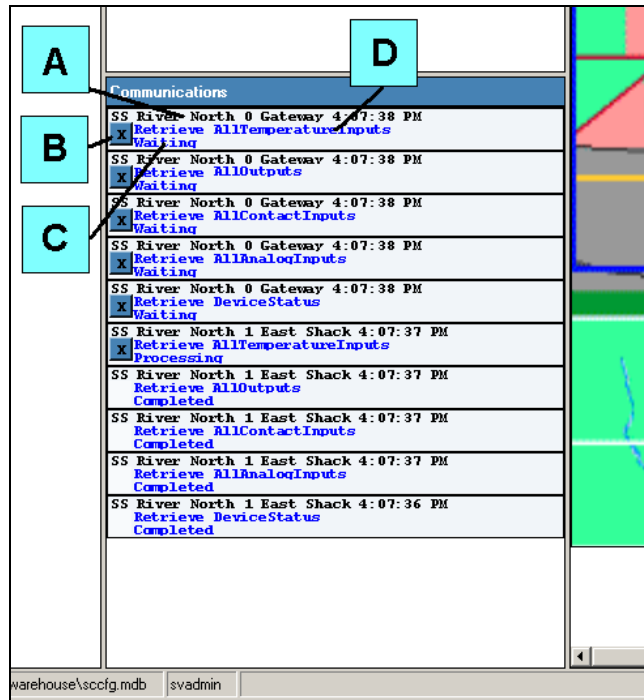


Figure 31 - Communication Panel

- A.** Name of COM port and device the communication pertains to and the time when the communication request occurred
- B.** Cancel transaction button
- C.** Communication transaction status
- D.** Communication transaction command and subcommand

When a new communication transaction is added to the communication panel, any transactions that are older than 8 seconds and are no longer processing, are removed from the communications panel.

Output control traffic is considered a special case. By updating an output a user either turns on or turns off that output. The output that is affected and the state that it is being set to are displayed next to the command and subcommand.

Communication	
SS River North 1 East Shack 8:26:28 AM	Update Outputs - Turn OFF Output 2 Waiting
SS River North 1 East Shack 8:26:25 AM	Update Outputs - Turn ON Output 4 Completed
SS River North 1 East Shack 8:26:24 AM	Update Outputs - Turn ON Output 3 Completed
SS River North 1 East Shack 8:26:22 AM	Update Outputs - Turn ON Output 2 Completed
SS River North 1 East Shack 8:26:14 AM	Update Outputs - Turn OFF Output 2 Completed

Figure 32 - Outputs Update Communication

4.9. Bandwidth Meter

The bandwidth meter shows how much data is being transmitted (TX) and received (RX) by the siteVIEW APEX client. The data is displayed in kilobits per second (kbps) and is updated every second. There are 8192 kilobits in 1 Megabyte (MB).

To see the total amount of data sent or received, hover the mouse pointer over the corresponding label.

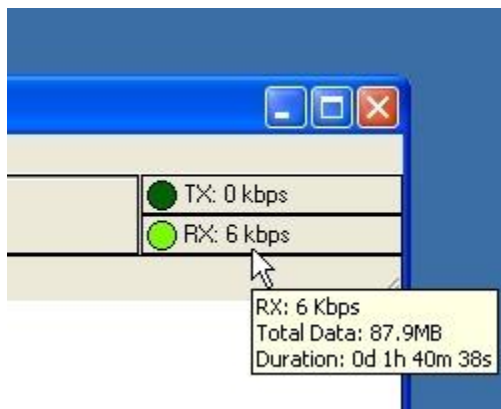


Figure 33 – Bandwidth Meter

5. USER ADMINISTRATION

5.1. Managing User Accounts

Apex provides two methods of managing user accounts:

- Built-in Apex user account management
- LDAP-compatible user account management, which can be used with popular directory management services like Windows Server Active Directory.

For both methods, Apex has three types of defined users:

- Administrators
- General Users
- View Only Users

The following table lists the available security rights and the access associated with each type:

	User Maintenance	Device & System Configuration	Panel Layout	Alarm Control	Manual Polling	Output Control
View Only	None	Read	Read	Read	Read	Read
User	None	Read	Read	Read/ Write	Read/ Write	Read/ Write
Admin	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write	Read/ Write

Table 1 – Login Security Level Matrix

5.1.1. Managing Users using Apex Authentication

Adding Users

To create, modify or delete siteVIEW APEX user accounts open the user administration form, which can be viewed by selecting “Connect->Accounts->User Administration” from the main menu.

Figure 34 - User Access - User Administration

The following tasks may be performed using the user administration form:

- Create new user accounts

- First name, last name and username may be altered

- Security rights may be altered

- User accounts may be enabled or disabled

- The user's password can be set

- User specific alarm notification options may be set, depending on which options are available from within siteVIEW APEX (i.e. email, paging, etc.).

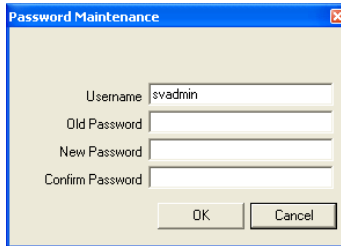
- Existing users may be deleted from the system

- View a history of user login/logout activity

- The user's email address can be set. This is used for password-recovery purposes (If email is enabled in the system the email address can also be used for email notification.)

Changing an Account Password

A user can change their account password through the “Change Password” form by selecting “Connect->Accounts->Change Password.”

A dialog box titled "Password Maintenance" with a blue title bar and a close button. It contains four text input fields: "Username" (pre-filled with "svadmin"), "Old Password", "New Password", and "Confirm Password". At the bottom right are "OK" and "Cancel" buttons.

Username	svadmin
Old Password	
New Password	
Confirm Password	

Figure 35 - User Access - Changing Your Password

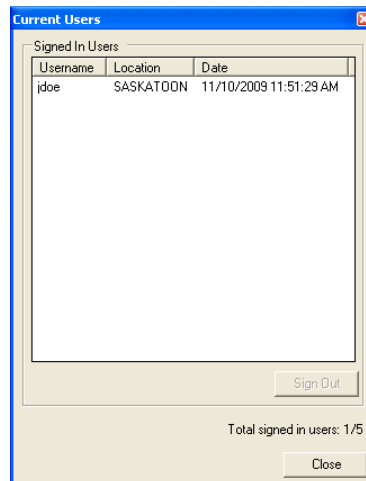
Forced User Sign Out

In the case of a power failure or a system crash/reset, siteVIEW APEX may not get a chance to properly sign users out of the system. Also, there may be times when an operator(s) needs to be forcibly signed out of the system.

In either case, operators may be forced out by anyone who has more security rights than they do. Operators may also sign themselves out. To view users that are currently signed in, type in a valid username and password at the sign in prompt, and select the “Users” button.

This will open the “Current Users” form, with a list of users that are currently signed in, the computer that the user signed in from, and the date and time the he or she signed in.

To sign a user out, select the user from the list of currently signed in users and select “Sign out”.

A dialog box titled "Current Users" with a blue title bar and a close button. It contains a table with the following data:

Username	Location	Date
jdoe	SASKATOON	11/10/2009 11:51:29 AM

Below the table is a "Sign Out" button. At the bottom right, it says "Total signed in users: 1/5" and has a "Close" button.

Username	Location	Date
jdoe	SASKATOON	11/10/2009 11:51:29 AM

Figure 36 - User Access - Current Users

5.1.2. Managing Users using LDAP-Compatible Authentication

While most typical Apex installations use the built-in user authentication services, enterprise installations may consider authenticating Apex users via LDAP (Lightweight directory access protocol) compatible systems like Windows Active Directory. The benefit is that by using LDAP with existing directory management services, Apex user access can be managed and administered consistently using existing in-house policies.

System Architecture

In an enterprise environment, Apex will generally be installed on an independent server and configured to work with an LDAP-compatible directory management system, like Windows Server Active Directory. Once connected, user authentication for Apex can use the same security policies as those defined for the enterprise, allowing a singular mechanism for managing access.

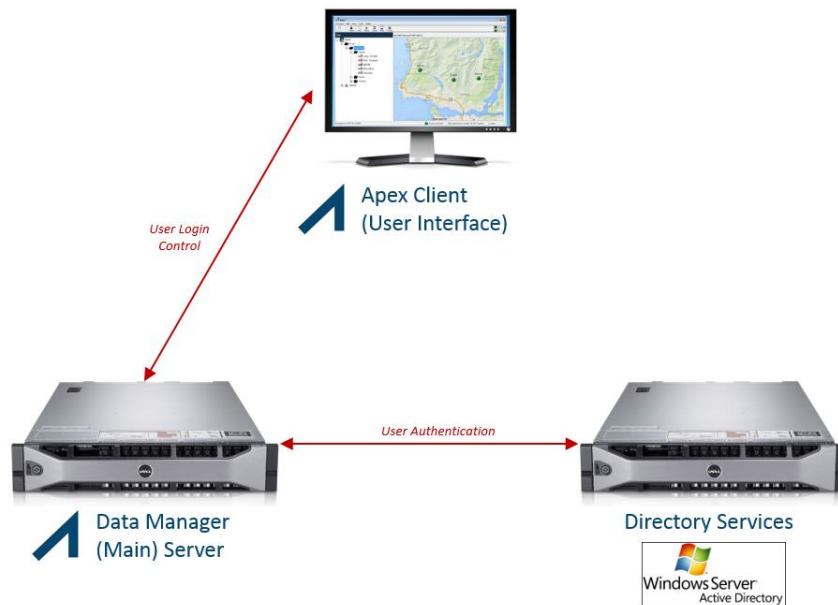


Figure 37 - User Access - LDAP System Architecture

Installation

Directory Services

Before proceeding with Apex installation and user accounts setup, the IT administrator must setup three groups in the directory services (e.g., Active Directory) server for determining user rights. These groups are "siteVIEW ViewOnly", "siteVIEW User", "siteVIEW Administrator".

To begin, a user belonging to the "siteVIEW Administrator" group is required, as the default system administrator. You may consider assigning the username "svadmin" – this is username for the default administrator for the Apex authentication method.

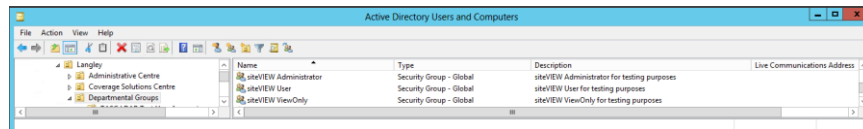


Figure 38 - User Access - LDAP Active Directory Groups

Apex Data Manager

The Apex Data Manager should be installed normally using the provided installation package (MSI file).

Use the Data Manager Utility to enable LDAP services and specify the location of the directory management servers – once complete, press the 'Save' button.

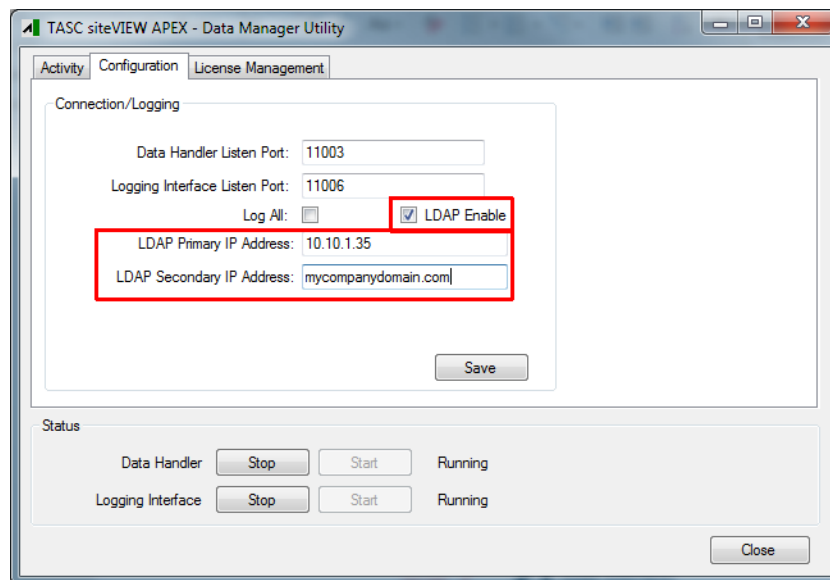


Figure 39 - User Access - Enabling LDAP Services

A restart of the Data Manager will be required to recognize the saved changes. Once restarted, Apex will use LDAP to communicate and authenticate with the specified servers. The Data Manager Utility's Activity log will indicate the selected user authentication method, either 'LDAP services' or 'Apex services', depending what has been configured in previous steps.

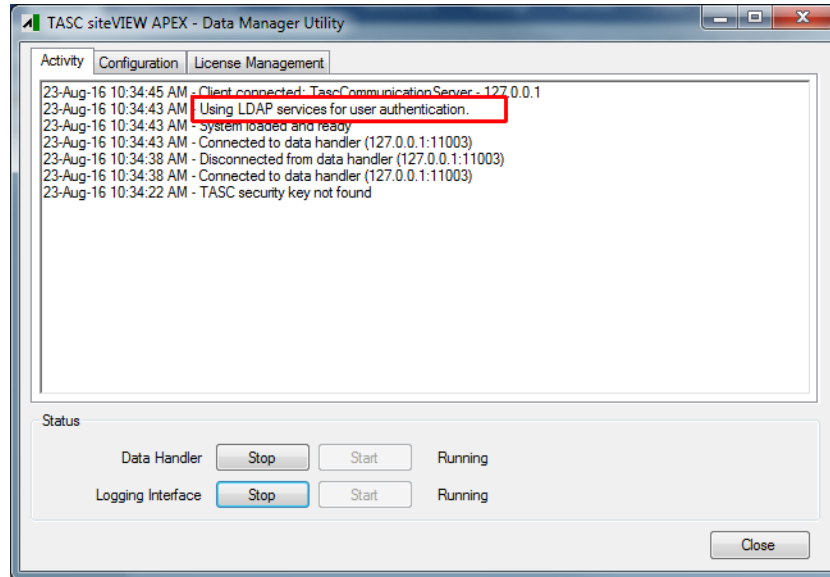


Figure 40 - User Access - LDAP Services Enabled

Operation

Apex Administrator

Only an Apex administrator can manage Apex users. As part of the installation process, a default Apex administrator username (and associated password) must be created by the IT administrator. User administration will be done using this account - to perform any user administration, the administrator must login to the Apex (User Interface) client.

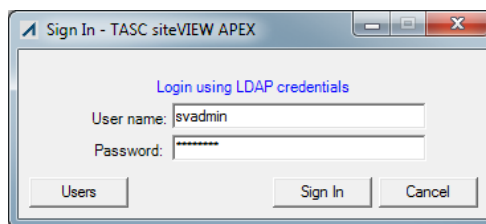


Figure 41 - User Access - Login Using LDAP Credentials

Adding (and Managing) Users

Adding users is a two-step process:

- Users must first be added to the directory services (e.g., Active Directory) server. Normally, all known users are already defined in this context as part of the general IT administration policy. However, if the user is strictly an Apex user without general enterprise privileges, the IT administrator must add this user to the system.
- Once a user has been defined within the directory services, the user can also be added to Apex.

The User Administration configuration dialog (Connect->Accounts->User Administration) is used to manage Apex users. Only Apex administrators will have access to this dialog.

To setup a new account, click on "New" then enter the user name and click "Apply". siteVIEW will then populate the other fields with information from the directory services server. The administrator can enable the account and the email by checking the corresponding boxes.

Upon setting up all users, the administrator can verify individual account information by clicking on the "Verify & Update User Information" tab. The administrator can also verify and update the information of all the users by clicking on the "Verify & Update Users Info" tab.

6. SYSTEM CONFIGURATION

The entire siteVIEW APEX system is represented in two ways: it is represented as a logical tree, which is referred to as the *Site Navigation Tree*, and as a graphical panel, which is referred to as the *Site Panel*. Items in the site navigation tree are referred to as *nodes*.

When a node on the tree is selected, menu options pertaining to that node are accessible through both the main menu, which is located at the top of the Client, and the context sensitive popup menu, which can be accessed by selecting a node with the mouse and then performing a right mouse click. This document will explain how to configure siteVIEW APEX using the main menu, but the same functionality can be accessed using the context specific popup menu.

The Tree View displays a list of *TASC Communication Servers*, the COM ports in use by the *TASC Communication Server* and the devices that are monitored through the COM port(s). Main menu items pertain to the selected node.



Note: Only the administrator users can configure the system.

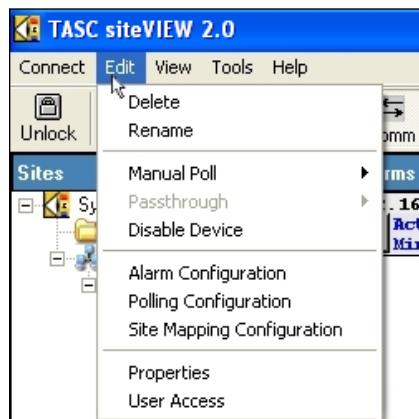


Figure 42 - Edit Menu

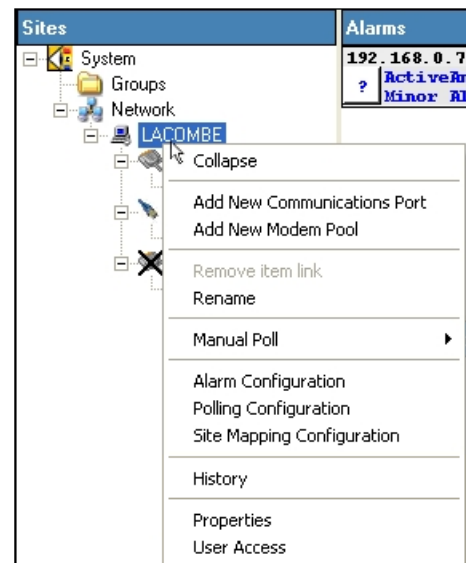


Figure 43 – TASC Communication Server Level Context Menu

6.1. TASC Communication Servers

TASC Communication Servers, which are connected to the system, are visible in the site navigation tree.

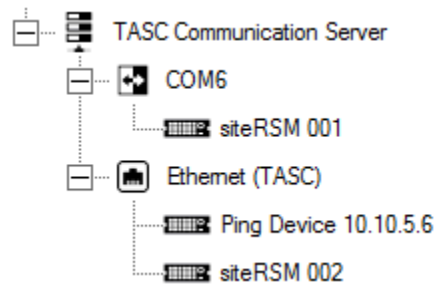


Figure 44 – TASC Communication Server in siteVIEW APEX Network Tree

To view information pertaining to a particular *TASC Communication Server*, select the desired node in the site navigation tree and then select “Edit->Properties” from the main menu. This launches the server details form.

The server details form displays the machine name that the *TASC Communication Server* resides on and its software version.

By default, siteVIEW APEX uses the NetBIOS name of the server for the name of that server node in the site navigation tree. Using the alias field, a system applicable name can be used. The alias and description are the only items on the server details form that can be modified.



Note: Existing archived log files will still contain the old *TASC Communication Server* alias name.

Figure 45 – TASC Communication Server Details

6.1.1. TASC Communication Server Ports

Adding a New TASC Communication Server Port

Each *TASC Communication Server* potentially has available serial and Ethernet communication ports, which can be used to monitor networks of hardware devices.

To add and configure an available communication port for siteVIEW APEX monitoring, select “Edit->Add New Communications Port” from the main menu. This launches the *Connection Wizard*.

In the first stage of the *Connection Wizard* form, select the COM Port type. If the selected type is *Serial* then a list of available serial communication ports will be displayed in the port drop down list. Select the port and protocol, and select “PSTN Modem Port” if the port is an internal PSTN modem or if it is connected to an external PSTN modem.



Figure 46 – Connection Wizard – Serial Details

If the selected COM Port type is *Ethernet* then Ethernet connection will be displayed. The IP Address and Port of the remote Ethernet device will not be needed until the Ethernet devices are added.

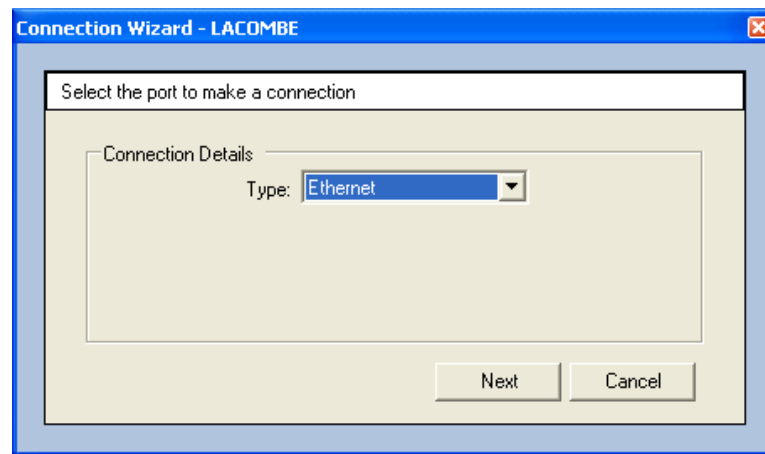


Figure 47 – Connection Wizard – Ethernet Details

After entering the required serial or Ethernet information, select next.

For a serial device, enter the port timing parameters. The *Packet Timeout* is entered in milliseconds and is the maximum amount of time a COM Port should wait for a response after sending out a request. The *Inter-Byte Timeout* is also entered in milliseconds and is the maximum time a COM Port should wait between incoming data bytes before the incoming data is considered complete. The Ethernet timing parameters are entered when you add the device.

If COM Port communication is timing out too often, it may be that the packet timeout is too short. If communication is taking too long to complete, try reducing the packet timeout.

If COM Port communication results in abnormally high communication errors, it may be that the inter-byte timeout is too low. Setting the inter-byte timeout too high also results in the packet timeout taking too long.

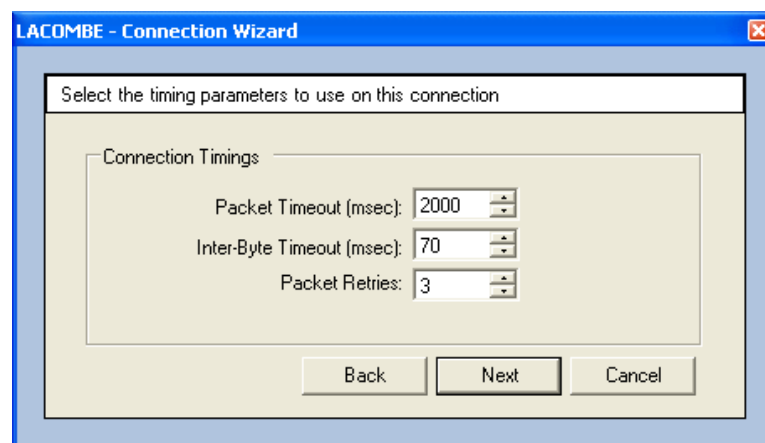


Figure 48 – Connection Wizard – Timings

Change the Packet Retries to specify the number of times a port should retry packets that have no response.

Experiment with the timings until you achieve the fastest and most reliable communication.



As an additional step for optimizing communications, review the [TransmitReceiveCOMxx](#) (where xx is the COM port number) log files found within the CommSvc directory to view retries for a given COM port. Iteratively, using manual Full Refreshes to test communication exchange, adjust the Packet Timeout parameter to minimize retries recorded within the log file.

Defaults: Packet Timeout 2000 msec; Inter-byte Timeout 70 msec; Packet Retries 3.

COM Port Configuration	Packet Timeout (msecs)	Inter-Byte Timeout (msecs)
Ethernet	1000-1500	50-100
Serial	1000-3000	50-200
Serial with PSTN Modem	2000-5000	100-300
Serial with Radio	Depends on the technology used and the number of radio hops.	Depends on the technology used and the number of radio hops.

Table 2 – Recommended Communication Timing Parameters

After selecting the timing parameters, select next. Choose a name for the connection and a description to remind users of useful information about the connection and then select finish to add the COM Port.

Figure 49 – Connection Wizard – Identification

Configuring an Existing Communication Port

To view and change information pertaining to a particular COM port on a *TASC Communication Server*, select the desired COM port node on the Tree View and then select “Edit->Properties” from the main menu. This launches the Connection Details form.

Figure 50 - Connection Details

Select a name for the COM port. The name will be how siteVIEW APEX refers to this communication port throughout the application.



Note: Existing archived log files will still contain the old port name.

The description properties of both the COM port and device detail forms are displayed when a user hovers the mouse above a Site Panel control that represents the COM port or device.

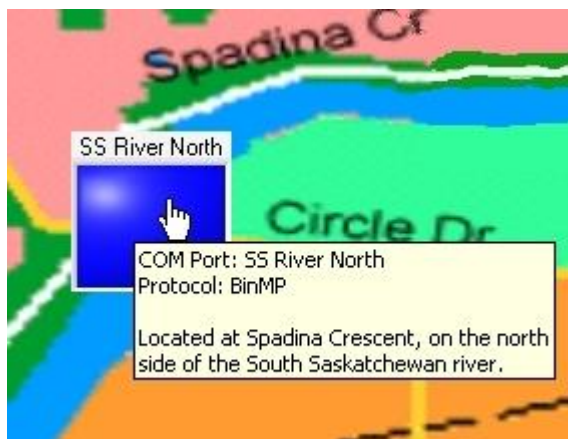


Figure 51 – COM Port Panel Component

Changes can only be made to port settings if the port is offline or by closing the port by disabling monitoring.

For a serial connection, the COM port field contains a list of communication ports available on the *TASC Communication Server*. For an Ethernet connection, the IP Address and Port fields must be specified.

The Protocol drop down field sets the protocol, which is used to communicate on the communication port. By default this protocol is set to BinMP. Other protocols are available as Add-On features from TASC.

Two COM port timeout values exist. The packet timeout is the time the *TASC Communication Server* will wait for a reply after transmitting a communication packet to a device. When the *TASC Communication Server* is receiving a response packet, the packet bytes are received one at a time. The inter-byte timeout is the time in which the *TASC Communication Server* should wait between packet bytes, before deciding the packet has failed.

By increasing the packet timeout and the inter-byte timeout, siteVIEW APEX is more likely to receive a packet. If siteVIEW APEX needs to frequently retry packet transmissions, it is possible that one or both of these timeout values needs to be increased. If siteVIEW APEX frequently encounters communication errors, it is possible that the inter-byte timeout needs to be increased. If these timeout values are too high, siteVIEW APEX communication may seem to take an unusually long time. Achieving the correct balance of timing values ensures that packets are handled efficiently.

6.1.2. TASC Communication Server Devices

Each *TASC Communication Server* COM or Ethernet port is capable of communicating to a network of hardware devices. To add and configure a device for siteVIEW APEX monitoring, first highlight the Port that connects the network of hardware devices to the *TASC Communication Server* and select “Edit->New Device” from the main menu. This launches the *Device Monitoring Wizard*.

Under the Device Type options, two types of devices can be selected:

- TASC Remote Platforms, which include the following models:
 - siteRSM
 - sC (siteCOMMANDER)
 - sPL (sitePORTAL LITE)
- Ping Devices.

TASC Remote Platforms

TASC Remote Devices can be used to monitor remote I/O.

If siteRSM, siteCOMMANDER or sitePORTAL LITE are selected as the Device Type, enter the device type and any addressing information and then select next. The correct addressing information must be selected in order for proper communication to occur.

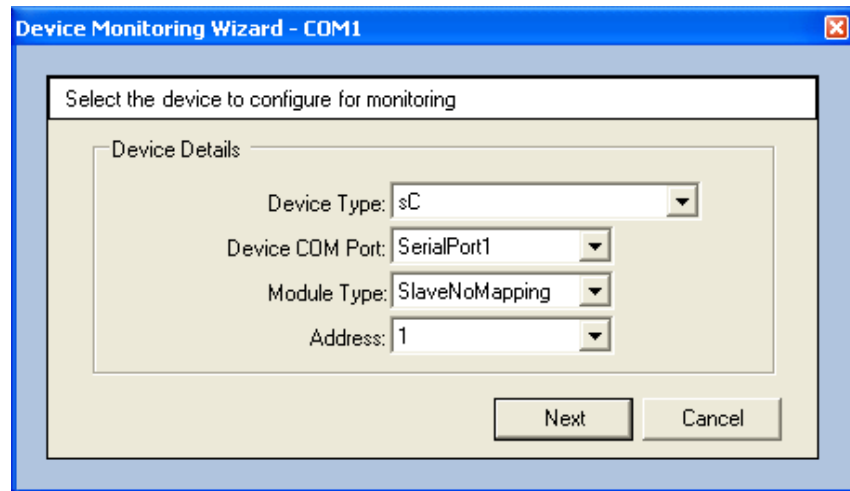


Figure 52 – Device Monitoring Wizard – Details (TASC Remote Platforms)

Next choose the device name and description. The device name will be used by siteVIEW APEX to make reference to the device. The description appears when a user hovers over the Site Panel control that represents the device.

For information about device specific connection parameters, see TASC siteCOMMANDER (see **Appendix B** on page 151), TASC sitePORTAL Lite (see **Appendix C** on page 164), TASC siteRSM device types (see **Appendix D** on page 177) and Ping devices (see Appendix E of this manual).

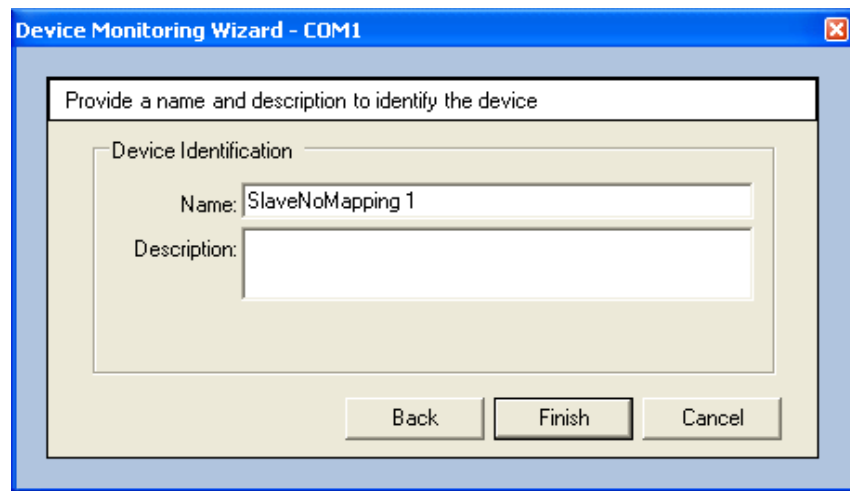


Figure 53 – Device Monitoring Wizard - Identification

After entering the device name and description (optional), select the Finish button to add the device. siteVIEW APEX will then attempt to communicate with the device by polling the device for its status and configuration. If any of the communication is incomplete, an indication of this will be displayed in the site navigation tree, beside the device's name.

siteVIEW APEX will not allow configuration changes to be made on the device until the entire device configuration has been successfully downloaded. From that point on, siteVIEW APEX assumes that it is the only application that has access to the device. If changes are later made to the device using a configuration tool such as the sitePORTAL Configuration Utility (SPCU), siteVIEW's configuration for the device will be out of date and this may result in erroneous data displayed in siteVIEW. To bring siteVIEW APEX back up to date, perform a complete refresh from siteVIEW APEX for the modified device.

Ethernet devices have an additional connection details setup page. In the connection details page enter the IP address, IP port and communication timing parameters.

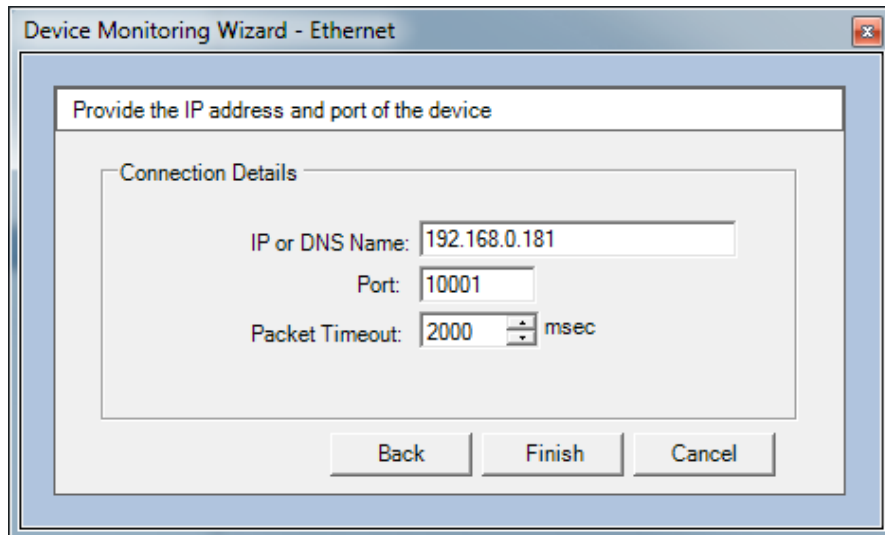


Figure 54 – Ethernet Device Connection Details

After communication with a device has been successfully established, additional device configuration is made available. Selecting “Edit->Properties” from the main menu opens the device details form. The device details form provides the ability to configure a device.

The device details form has multiple tabs. The available tabs differ from device to device depending on the device’s firmware version, the available siteVIEW APEX add-ons, and the type of device.

Device Uploaded Configuration

Currently, siteVIEW APEX supports the TASC siteCOMMANDER (see **Appendix B** on page 151), TASC sitePORTAL Lite (see **Appendix C** on page 164) and the TASC siteRSM device types (see **Appendix D** on page 177)

When changing a device’s name, please note that existing archived log files will still contain the old device name.

The IP address, IP port and timing parameters can be set for Ethernet devices in the communications tab of the device details form.



WARNING: Making configuration changes to a device will cause the device to restart its firmware. As a result the device outputs will turn off. This could unintentionally activate/deactivate equipment located at the remote site without warning. It is the customer’s responsibility to ensure personnel or property is not damaged.

Extra Device Configuration

Some configuration is stored in siteVIEW APEX and not uploaded into the device. The temperature units and the analog formula are extra input configuration parameters that are stored in siteVIEW APEX but are not uploaded to the device.

The temperature units are configurable via the Units selection box on the Temperature Inputs tab of the Device Details form. Available temperature conversions include Celsius, Fahrenheit, Kelvin, Rankine and Réaumur. The default unit value is Celsius.

	1	2	3	4	5	6	7	8	ALL
Enable Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Present	Yes	No	No	No	No	No	No	No	No
Units	Celsius	Celsius	Celsius	Celsius	Celsius	Celsius	Celsius	Celsius	Celsius
Input Qualifier	Celsius	---	---	---	---	---	---	---	---
High Temperature Set Points									
Threshold	24.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	---
Local Output	---	---	---	---	---	---	---	---	---
Low Temperature Set Points									
Threshold	11.5	-55.0	-55.0	-55.0	-55.0	-55.0	-55.0	-55.0	---
Local Output	---	---	---	---	---	---	---	---	---
Hold (secs)	5	1	1	1	1	1	1	1	---

Figure 55 – Device Details – Temperature Units Selection

Similar to the temperature units, the Analog Input formula are configurable via the Formula selection box on the Analog Input tab of the Device Details form. The formula values are configurable through the Formula Configuration form that can be opened by selecting the Edit button that corresponds to the Formula selection box.

Device Details - TASC siteVIEW Enterprise 2.0

Description | General | Communication | Contact Inputs | Analog Inputs | Temperature Inputs | Outputs

Analog Input Configuration

	1	2	3	4	5	6	7	8	ALL
Enable Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Range	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V
Sensor									
Offset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
Input Qualifier	--	8	--	--	--	--	--	--	--

Units: Volts Volts Volts Volts Volts Volts Volts Volts Volts

Formula: -none- -none- -none- -none- -none- -none- -none- -none- -none- Edit

High Threshold Set Points

	1	2	3	4	5	6	7	8	ALL
Threshold	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
Adjusted	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0	10.0
Local Output	--	--	--	--	--	--	--	--	--

Low Threshold Set Points

	1	2	3	4	5	6	7	8	ALL
Threshold	2.7	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5
Adjusted	2.7	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5
Local Output	--	--	--	--	--	--	--	--	--

Hold (secs): 1 1 1 1 1 1 1 1 1

☒ Only upload changed settings

OK Apply Cancel

Figure 56 – Device Details – Analog Formula Configuration

Use the Formula Configuration form to add, remove and update various analog conversions.

The formula Name field is the unique identifier of the formula. The formula name will appear in the Formula selection field.

The formula Units field is an optional field that is displayed in the Log Viewer.

The formula Decimal Places field configures how many decimal places the adjusted value should be rounded.

The formula Equation is used to calculate the value of the analog sensor, where x is the input value. See the Formula Configuration form for a complete list of accepted equation operators and an example of how to use each one.

The Sample field allows the equation to be tested. This value is input into the equation by replacing x and calculating the result. If there are no errors, the result is displayed. If there was an error with the formatting then an error is displayed.

Formula Configuration

Name	Units	Equation	Decimals
Sensor 1	dB	$2x^3 - 2.3x^2 + 4x - 6.234$	2
Sensor 2	dB	$5.64x^4 + 0.54x^3 - 27.9x^2 + 8.35x - 206.234$	2

Name: Units: Decimals:

Equation:

Sample: = 292.27 dB

Operator	Description	Example
x	variable	$\sqrt{x - \ln(2x + 7.45)}$
()	Open & Close Brackets	$x(4+5)$
!	Factorial	$x!$
^	Exponent	$2^{(3 * x)}$
sqrt	Square Root	$\sqrt{x^4}$
*	Multiply	$x * 5$
/	Divide	$x/5$
%	Modulus	$x \% 10$
+	Add	$4.231x + 5.2354$
-	Subtract	$90 - x$
logb	Logarithm (b = base)	$\log_4(x)$
log	Logarithm (base 10)	$\log(x)$
ln	Natural Log	$\ln(25x)$
sec	Secant	$\sec(x)$
sin	Sine	$\sin(35.001x)$
tan	Tangent	$\tan(45.023/x)$
csc	Cosecant	$\csc(x)$
cos	Cosine	$\cos(180) + x$
cot	Cotangent	$\cot(x-25.23)$
abs	Absolute	$\text{abs}(-25 * x)$
pi	3.141592653589793238...	$\pi * x^2$

Figure 57 – Formula Configuration Form

Once an analog formula has been configured it can be selected and applied to any analog input. The analog input's adjusted high and low threshold values will be calculated and displayed. The formula will also be used to calculate the analog value whenever a status is returned from the device and the calculated value will be displayed in the Log Viewer and on any panel controls that represent the analog input.

Ping Devices

Ping devices can be used to validate if an IP device is up and running. siteVIEW APEX be scheduled to ping the Ping device periodically using scheduled polling. If an unresponsive site alarm is setup for the device, the alarm will trigger whenever the site does not respond to a ping.

To add a Ping device, select Ping as the Device Type then select next.

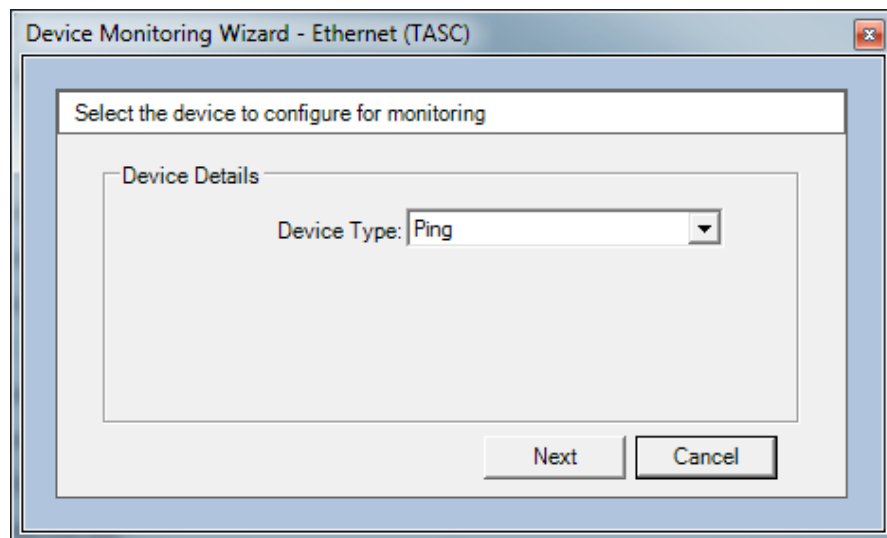


Figure 58 – Device Monitoring Wizard – Details (Ping Device)

Next choose the device name and description. The device name will be used by siteVIEW APEX to make reference to the device. The description appears when a user hovers over the Site Panel control that represents the device.

Ping devices have an additional connection details setup page. In the connection details page enter the IP address, IP port and communication timing parameters.

6.2. Summit Communication Servers

Summit Communication Servers, which are connected to the system, are visible in the site navigation tree.

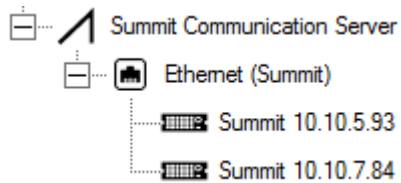


Figure 59 – Summit Communication Server in siteVIEW APEX Network Tree

To view information pertaining to a specific *Summit Communication Server*, select the desired node in the site navigation tree and then select “Edit->Properties” from the main menu. This launches the server details form.

The server details form displays the machine name that the *Summit Communication Server* resides on and its software version.

By default, siteVIEW APEX uses the NetBIOS name of the server for the name of that server node in the site navigation tree. Using the alias field, a system applicable name can be used. The alias and description are the only items on the server details form that can be modified.



Note: Existing archived log files will still contain the old *TASC Communication Server* alias name.

The screenshot shows a dialog box titled 'Summit Handler Details - TASC siteVIEW APEX'. Inside the dialog, there is a tab labeled 'Server'. Below the tab, there is a section titled 'Server Details' containing four input fields: 'Name' (with the value 'GRANDFORKS'), 'Version' (with the value '3.4.0.14'), 'Alias' (with the value 'Summit Communication Server'), and 'Description' (which is empty). At the bottom of the dialog, there are three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 60 – Summit Communication Server Details

6.2.1. Summit Communication Server Ports

Adding a New Summit Communication Server Port

Each *Summit Communication Server* uses an Ethernet connection to monitor a network of Summit devices.

To add and configure an available communication port for siteVIEW APEX monitoring, select “Edit->Add New Communications Port” from the main menu. This launches the *Connection Wizard*.

In the first stage of the *Connection Wizard* form displays the default connection type: Ethernet.

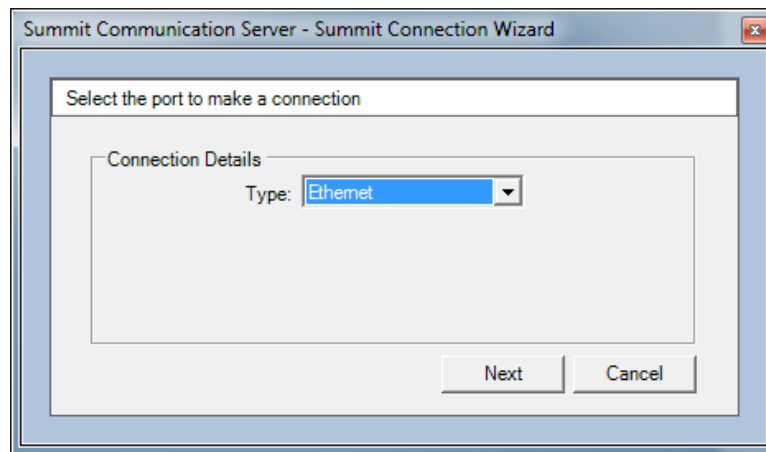


Figure 61 – Summit Connection Wizard

After entering the Ethernet connection’s name and description information, select Finish. The IP Address and Port of the remote Ethernet device will not be needed until the Ethernet devices are added.

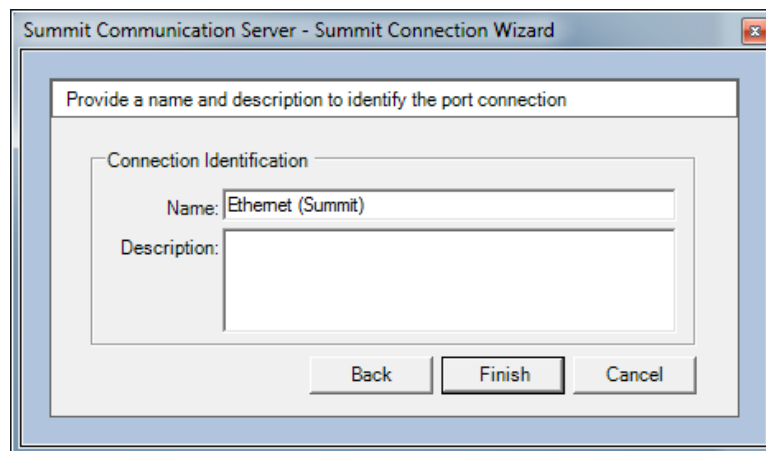
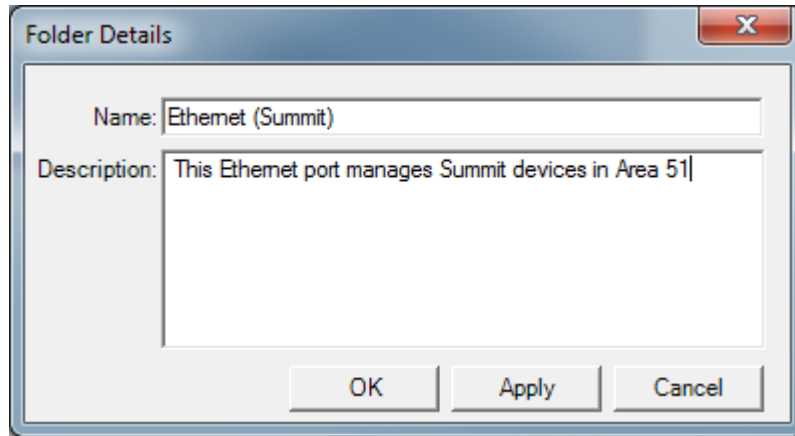


Figure 62 – Connection Wizard – Ethernet Details

Configuring an Existing Communication Port



The screenshot shows a 'Folder Details' dialog box with a title bar containing a close button (X). Inside the dialog, there are two text input fields. The first is labeled 'Name:' and contains the text 'Ethemet (Summit)'. The second is labeled 'Description:' and contains the text 'This Ethemet port manages Summit devices in Area 51'. Below these fields are three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 63 - Connection Details

To view and change information pertaining to an existing Ethernet port on a *Summit Communication Server*, select the desired Ethernet port node on the Tree View and then select “Edit->Properties” from the main menu. This launches the Connection Details form.

Select a name for the Ethernet port. The name will be how siteVIEW APEX refers to this communication port throughout the application.



Note: Existing archived log files will still contain the old port name.

The description properties of both the Ethernet port and device detail forms are displayed when a user hovers the mouse above a Site Panel control that represents the COM port or device.

Changes can only be made to port settings if the port is offline or by closing the port by disabling monitoring.

6.2.2. Summit Communication Server Devices

Each *Summit Communication Server* Ethernet port is capable of communicating to a network of Summit devices. To add and configure a Summit for siteVIEW APEX monitoring, first highlight the Ethernet port that connects the network of hardware devices to the *Summit Communication Server* and select “Edit->Add New Summit Device” from the main menu. This launches the *Device Monitoring Wizard*.

Summit Devices

Summit Devices can be used to monitor remote I/O.

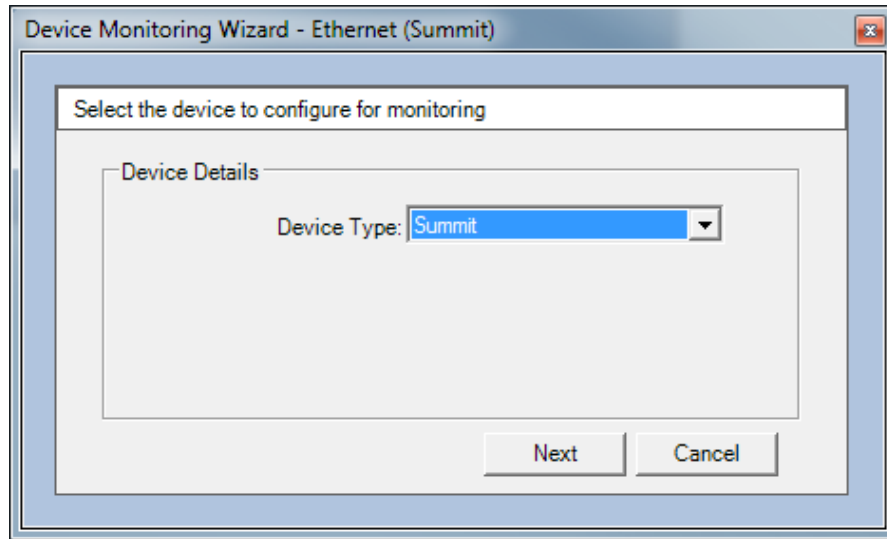


Figure 64 – Device Monitoring Wizard – Details (Summit Devices)

Next choose the device name and description. The device name will be used by siteVIEW APEX to make reference to the device. The description appears when a user hovers over the Site Panel control that represents the device.

For information about device specific connection parameters, see Summit Devices (see **Appendix E**).

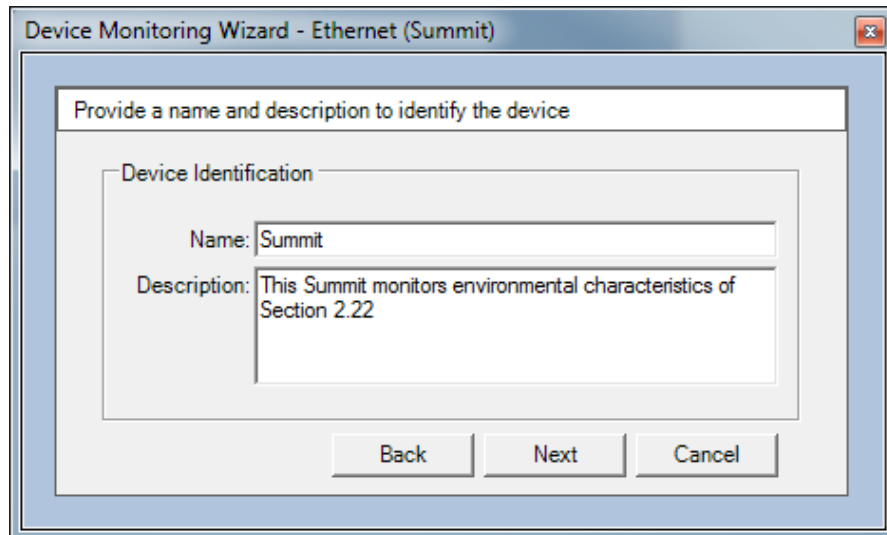


Figure 65 – Device Monitoring Wizard - Identification

After entering the device name and description (optional), Ethernet devices have an additional connection details setup page. In the connection details page enter the IP address and press Finish to add the device.

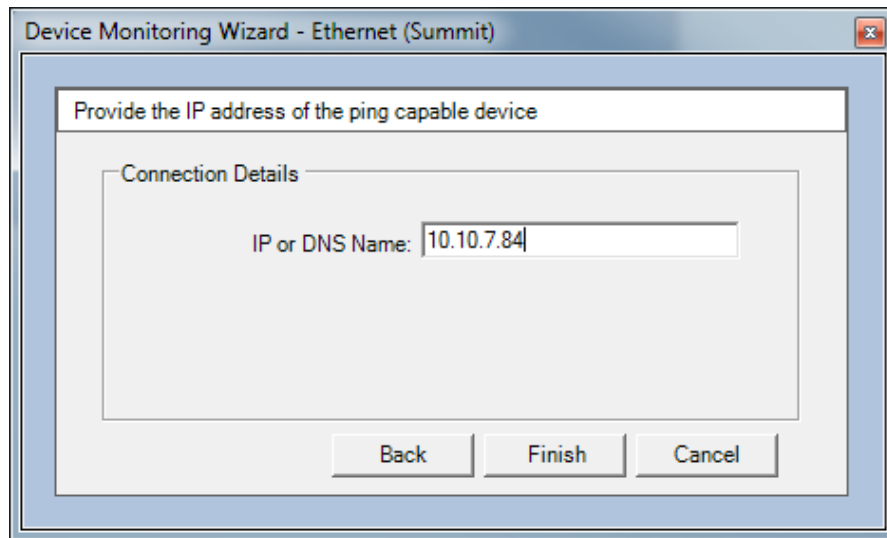


Figure 66 – Ethernet Device Connection Details

After communication with a device has been successfully established, Apex will retrieve I/O information from the Summit.

6.3. SNMP Communication Servers

SNMP Communication Servers, which are connected to the system, are visible in the site navigation tree.

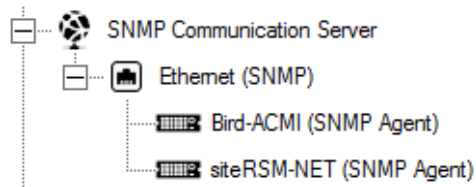


Figure 67 – SNMP Communication Server in siteVIEW APEX Network Tree

To view information pertaining to a particular *SNMP Communication Server*, select the desired node in the site navigation tree and then select “Edit->Properties” from the main menu. This launches the server details form.

The server details form displays the machine name that the *TASC Communication Server* resides on and its software version.

By default, siteVIEW APEX uses the NetBIOS name of the server for the name of that server node in the site navigation tree. Using the alias field, a system applicable name can be used. The alias and description are the only items on the server details form that can be modified.



Note: Existing archived log files will still contain the old *TASC Communication Server* alias name.

Figure 68 – SNMP Communication Server Details

6.3.1. SNMP Communication Server Ports

Each *SNMP Communication Server* uses an Ethernet communication port to monitor SNMP devices. This port can be added by right-clicking on the SNMP

Communication Server and selecting the 'Add New SNMP Communication Port' option. Once selected, press Next to fill in the remaining information.

Choose a name for the connection and a description to remind users of useful information about the connection and then select finish to add the Ethernet communication port.

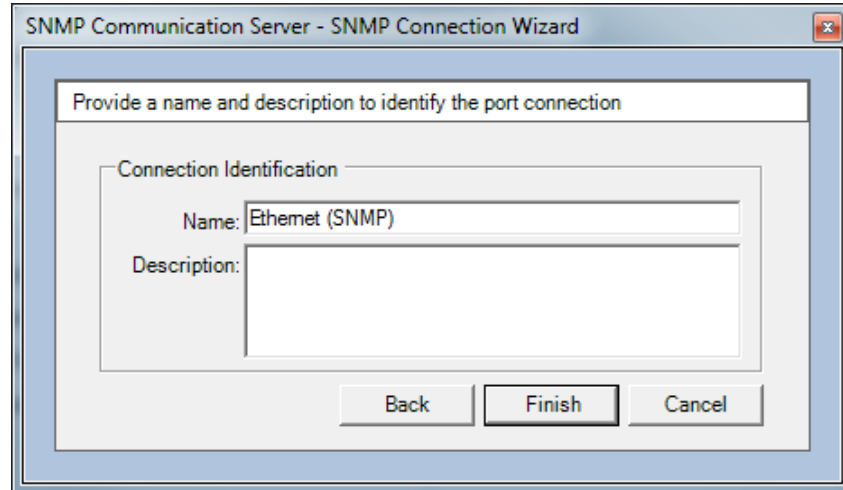


Figure 69 – Connection Wizard – Identification

6.3.2. SNMP Communication Server Devices

siteVIEW APEX can be used to monitor SNMP Agent devices using SNMP Trap messages.

Each *SNMP Communication Server* Ethernet port is capable of communicating to a network of SNMP agent devices. To add and configure a SNMP device for siteVIEW APEX monitoring, first highlight the Ethernet port that connects the network of hardware devices to the *SNMP Communication Server* and select "Edit->New Device" from the main menu. This launches the *Device Monitoring Wizard*.

The Device Monitoring Wizard will contain a list of SNMP devices available. siteVIEW APEX ships with several pre-loaded SNMP devices, however, additional devices may be added by using the siteVIEW APEX MIB File Translator utility (see **Appendix G.2.1** of this manual).

To add a SNMP device, select SNMP Agent as the Device Type and select the SNMP Agent to monitor, then select next.

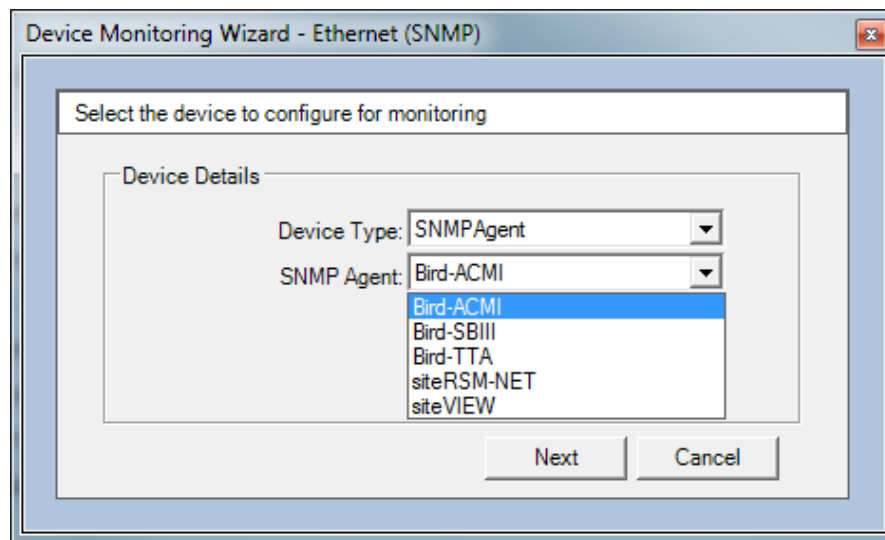


Figure 70 – Device Monitoring Wizard – Details (Ping Device)

Next choose the device name and description. The device name will be used by siteVIEW APEX to make reference to the device. The description appears when a user hovers over the Site Panel control that represents the device.

Finally in the Connection Details page enter the device's IP address and IP port and select the Finish button to add the device to siteVIEW APEX.

6.4. Site Panel

Each node in the site navigation tree has a panel associated with it. The panel contains controls that graphically map out the items available at the server, COM port or device. A server's panel contains controls that represent COM ports, a COM port's panel contains controls that represent devices, and a device's panel contains controls that represent the device's inputs and outputs. Performing a left mouse click on a panel control that represents a COM port or a device causes siteVIEW APEX to display the panel for the selected COM port or device, essentially traversing the Tree View. Performing a left mouse click on a panel control that represents an output can command siteVIEW APEX to turn on or turn off the associated output. Panel controls that represent device inputs serve as visual indicators of the inputs real life state.

A user can modify the layout and appearance of the panel and the panel controls to give more meaning to the panel.

6.4.1. Background Properties

The Site Panel background properties form can be modified in the *Panel Details* form, which is opened by selecting "Edit->Panel->Panel Background" from the main menu. The Panel Details form pertains to the currently displayed panel.

The panel height and width affect the total size of the panel. This can be different from the actual height and width that the user sees. The panel height and width can be set larger or smaller than the actual viewable area of the PC screen.

An image may be set as the panel background by selecting it from the list. When an image is selected, a preview of the image is shown in the picture box above the image list. To add an image to the list, select the Browse button, navigate to the desired image file and select ok. The Rename and Delete buttons rename and delete a selected image on the image list.



It is recommended that background images be less than 256KB in size. Larger images may take longer to load.

The mode setting determines how the background image will be fit into the background.

Color sets the panel background color.

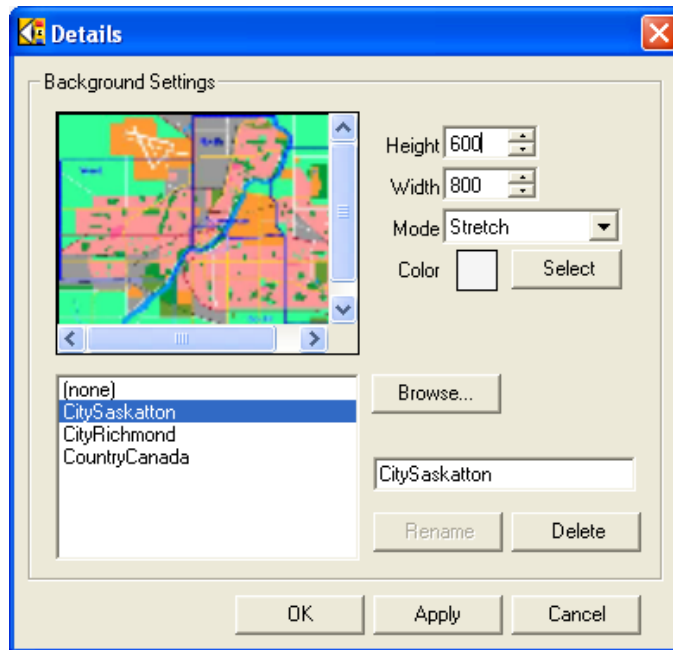


Figure 71 - Background Properties

6.4.2. Panel Control Property Form

There are several types of panel controls. Individual panel controls may be customized to give the control more meaning. Panel controls represent COM port connections to sites, devices, contact inputs, analog inputs, temperature inputs and outputs. In most cases it makes sense to represent sites and devices by a Boolean push button, contact inputs and outputs only have two states and so they are best represented by a visual on or off using a Boolean, and analog and temperature inputs have ranges and are best represented by knobs and slides.

Selecting the “Edit->Panel->Unlock Panel” from the main menu unlocks the currently displayed panel and allows the individual panel controls to be modified. While a panel is unlocked, the normal functionality of the panel controls ceases. Selecting a panel control opens a form that shows the panel control’s display properties. On the top of the panel control display properties form is a drop down field of all the controls that belong to the current panel. This drop down field, along with the previous and next buttons, is used to navigate through the panel controls.

To select multiple panel controls, left click the mouse at some point on the panel, then while holding the left mouse down, drag the mouse over the panel controls you wish to select. Multiple controls can also be selected by hold the keyboard’s Ctrl button down while left clicking panel controls.

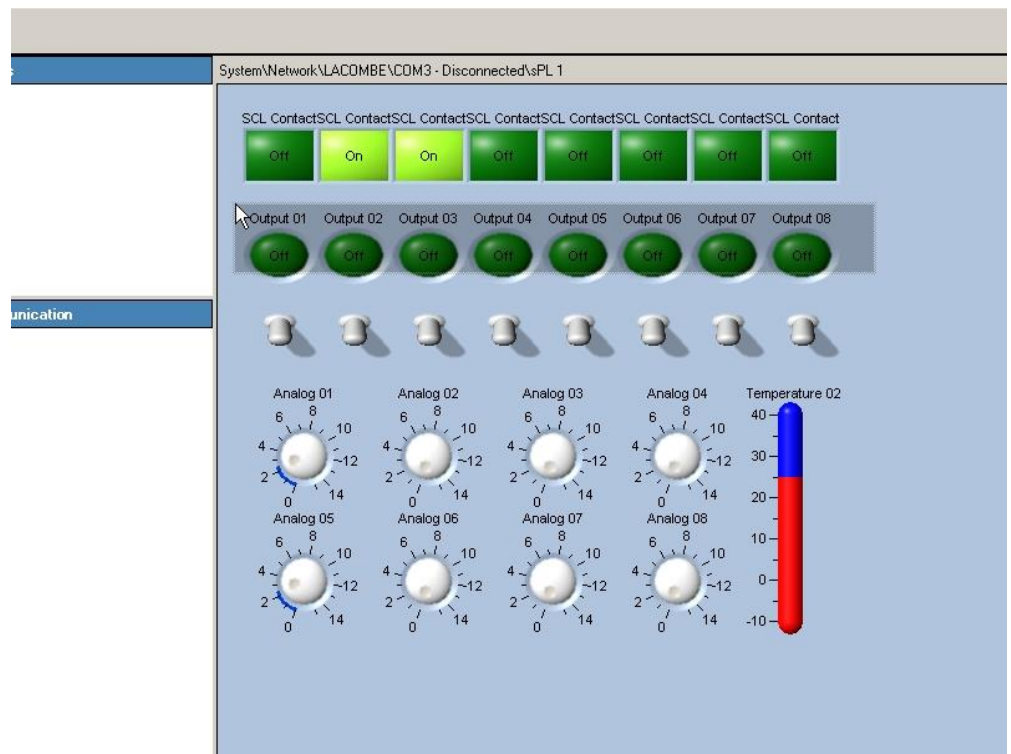


Figure 72 – Selecting Multiple Panel Controls with the Mouse

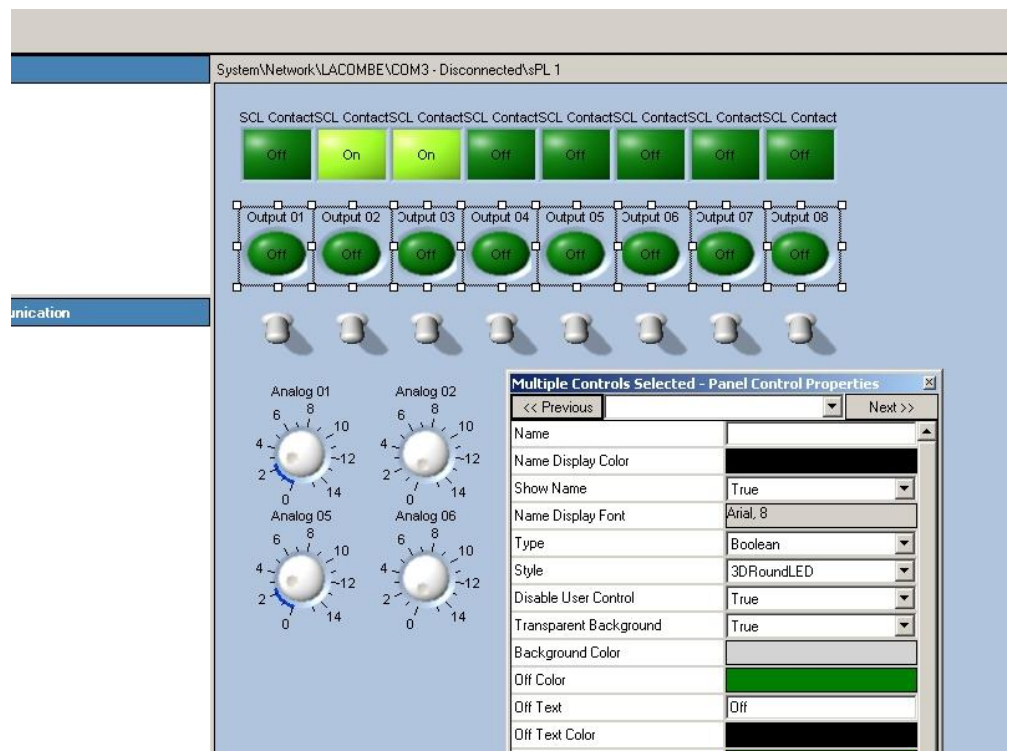


Figure 73 – Multiple Panel Controls Selected

Certain panel control properties are common for all panel control types. Other properties are specific to a control type. The Disable User Control and confirmation properties are only available if the control it represents is an output. When the confirmation property is selected siteVIEW APEX will prompt a user for confirmation if the user turns the output on or off. The Disable User Control option removes user control entirely. An administrator can set these settings accordingly.

The name of the panel control can be changed and shown or hidden using the Panel Control Display Properties form. A panel control can be made visible or hidden, or it can be deleted completely by selecting the delete button. Panel control colors, types and styles are all changed using the panel control display properties form.

Output 5 - Panel Control Properties	
<< Previous	Output 05
Name	Output 05
Name Display Color	
Show Name	True
Name Display Font	Arial, 8
Type	Boolean
Disable User Control	True
Style	3DRoundLED
Transparent Background	True
Background Color	
Off Color	
Off Text	Off
Off Text Color	
On Color	
On Text	On
On Text Color	
Top	100
Left	260
Width	60
Height	60
Visible	True
<div> Delete Close </div>	

Figure 74 – Panel Control Display Properties

6.4.3. Panel Control Types

Four panel control types are available in siteVIEW. The four panel control types are: Boolean, slide, knob and display.

Boolean






















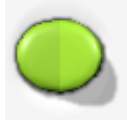





Vertical Toggle (VToggle) 	Horizontal Toggle (HToggle) 	Square LED (SquareLED) 	Square Star LED (SquareStarLED) 
Round LED (RoundLED) 	Round Star LED (RoundStarLED) 	Round Push Button (RoundPushButton) 	Square Push Button (SquarePushButton) 
Vertical 3D Slide (V3dSlide) 	Horizontal 3D Slide (H3dSlide) 	Vertical Slide (VSlide) 	Horizontal Slide (HSlide) 
Toggle On/Off (ToggleOnOff) 	Command OK (CommandOK) 	Bitmap (Bitmap) 	3D Vertical Toggle (3DVToggle) 
3D Square LED (3DSquareLED) 	3D Horizontal Toggle (3DHToggle) 	3D Round LED (3DRoundLED) 	3D Push Button (3DPushButton) 
3D Vertical Rocker (3DVRocker) 	3D Horizontal Rocker (3DHRocker) 	3D Vertical Slide Switch (3DVSlideSwitch) 	3D Horizontal Slide Switch (3DHSlideSwitch) 
3D Toggle On/Off (3DToggleOnOff) 	3D Command OK (3DCommandOK) 	3D Bitmap (3DBitmap) 	

Figure 75 - Boolean Styles of Panel Controls

Boolean control types are used to represent on and off, or are used as buttons. Properties specific to this control type include the off color, off text, off text color,

Output 5 - Panel Control Properties	
<< Previous	Output 05
Name	Output 05
Name Display Color	
Show Name	False
Name Display Font	Arial, 8
Type	Boolean
Confirmation Required	True
Disable User Control	False
Style	3DVToggle
Transparent Background	True
Background Color	
Off Color	
Off Text	
Off Text Color	
On Color	
On Text	
On Text Color	
Top	160
Left	260
Width	60
Height	60
Visible	True
<div> Delete Close </div>	

Figure 76 - Boolean Element Properties

on color, on text and on text color.

When Boolean control types are used to represent analog inputs, an “On Condition” property becomes available for the control. The on condition specifies the conditions when the Boolean control should appear on. When these conditions are not met, the Boolean control will appear off. In Figure 77 – Analog Boolean Control Properties, three Boolean controls are used to represent “Analog 01”. The top Boolean control is set to be on when the analog’s value is above its high threshold. The middle and selected Boolean control is set to appear on when the analog’s value is below the high threshold and above the low threshold. The bottom Boolean control is set to be on when the analog’s value is below the low threshold.

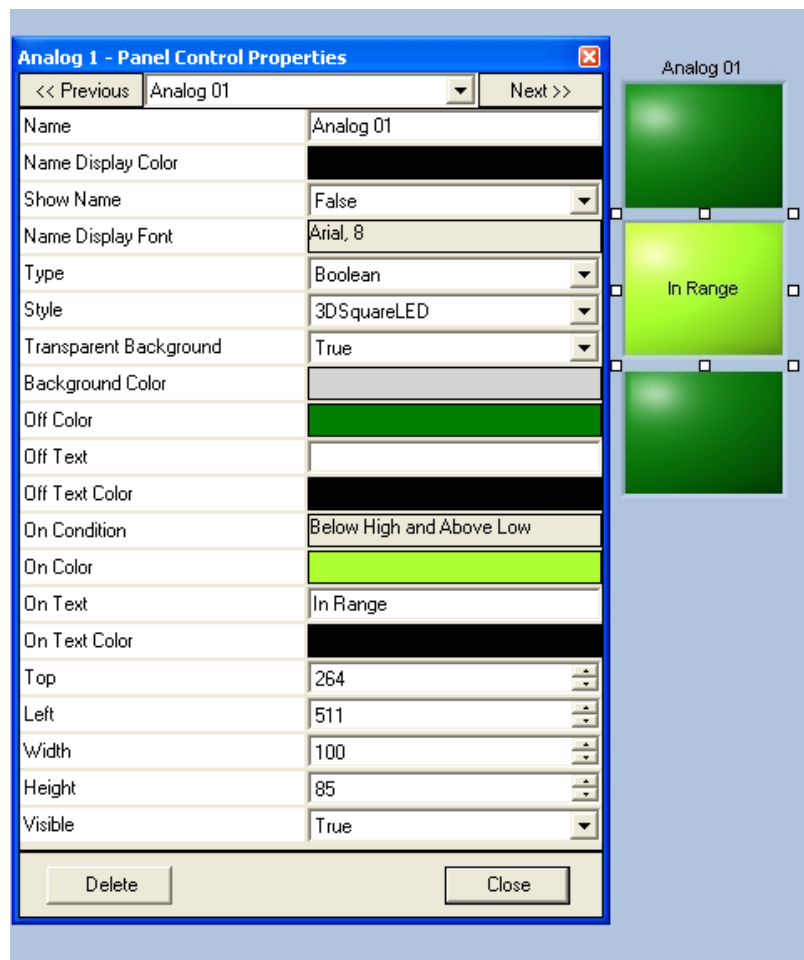


Figure 77 – Analog Boolean Control Properties

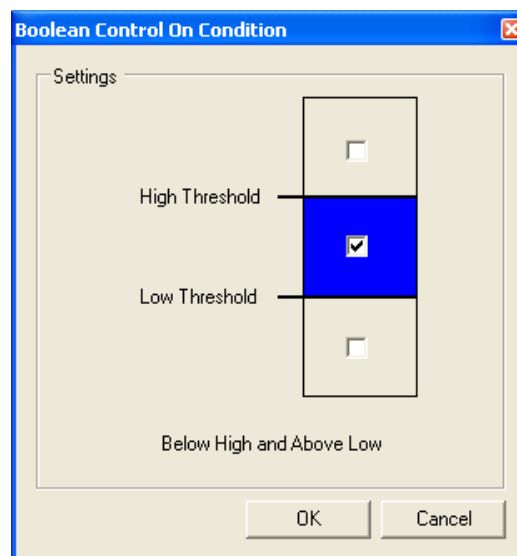


Figure 78 - Boolean Control On Condition

Double clicking on the “On Condition” property’s configuration text opens the Boolean Control On Condition configuration form. Use this form to select when the Boolean control should appear on.

Knob

Knob control types are used to represent a range of values. Properties specific to this control type include the foreground color, format string, axis caption, axis maximum and minimum, axis inversion, and the start and end of the arc of values.

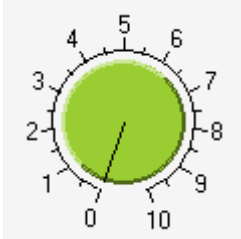


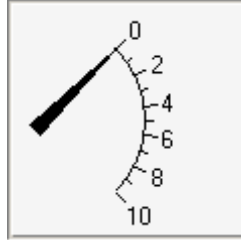



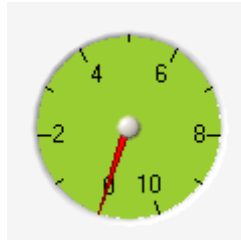


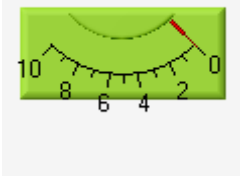

Knob (Knob) 	Dial (Dial) 	Horizontal Top Gauge (HTopGauge) 	Vertical Right Gauge (VRightGauge) 
Horizontal Bottom Gauge (HBottomGauge) 	Vertical Left Gauge (VLeftGauge) 	3D Knob (3DKnob) 	3D Dial (3DDial) 
3D Top Meter (3DTopMeter) 	3D Right Meter (3DRightMeter) 	3D Bottom Meter (3DBottomMeter) 	3D Left Meter (3DLeftMeter) 

Figure 79 - Knob Styles of Panel Controls

The knob control type is represented as an arc.

The format string is discussed in more detail at the end of this section. The axis minimum and maximum specify the minimum and maximum values that the knob will display. The axis can be inverted so that the numeric scale is shown in reverse order. The arc start and end values determine the arc's span. When the arc start and end values are set to -1 a default value is used.

Analog 8 - Panel Control Properties	
<< Previous	Analog 08
Name	Analog 08
Name Display Color	Black
Show Name	True
Name Display Font	Arial, 8
Type	Knob
Style	3DKnob
Transparent Background	True
Background Color	Gray
Foreground Color	White
Format String	%
Arc Start	-1
Arc End	-1
Axis Caption	%
Axis Maximum	15.0
Axis Minimum	0.0
Invert Axis	True
Left/Bottom Ticks	True
Right/Top Ticks	False
Inner Ticks	False
Outer Ticks	True
Major Ticks	True
Minor Ticks	True
Major Tick Color	Black
Minor Tick Color	Black
Tick Spacing	Automatic
Top	340
Left	320
Width	100
Height	100
Visible	True
<div> Delete Close </div>	

Figure 80 - Knob Properties

Slide

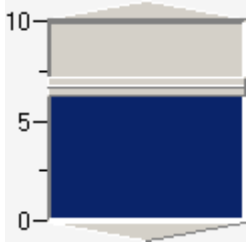
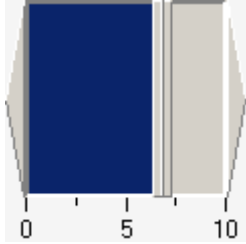
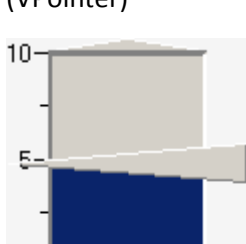
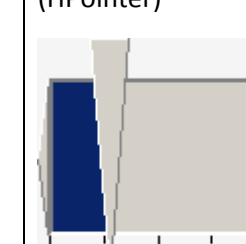
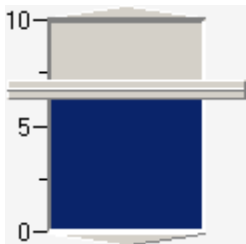
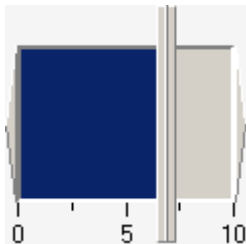

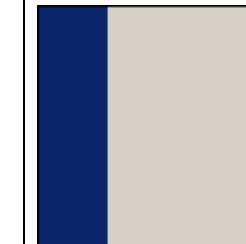
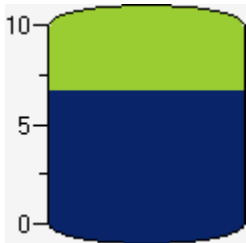
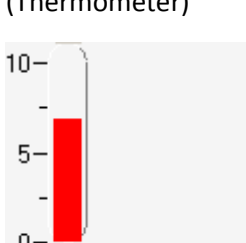
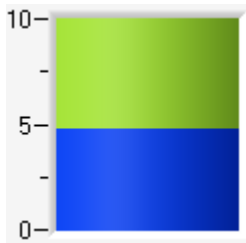
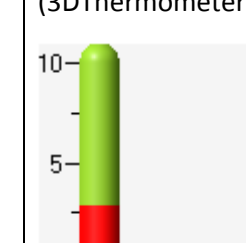
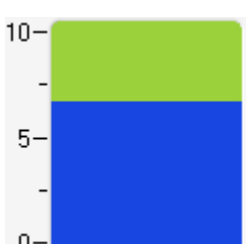
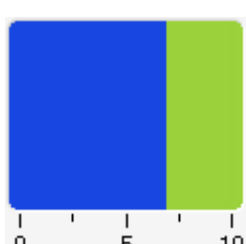
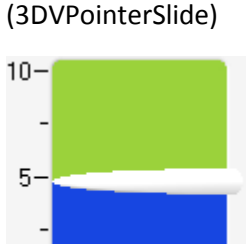
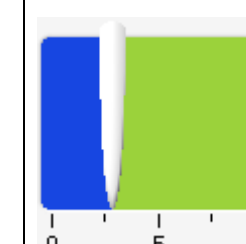




Vertical 1 (V) 	Horizontal 1 (H) 	Vertical Pointer (VPointer) 	Horizontal Pointer (HPointer) 
Vertical 2 (V2) 	Horizontal 2 (H2) 	Vertical Bar (VBar) 	Horizontal Bar (HBar) 
Tank (Tank) 	Thermometer (Thermometer) 	3D Tank (3DTank) 	3D Thermometer (3DThermometer) 
3D Vertical Fill Slide (3DVFillSlide) 	3D Horizontal Fill Slide (3DHFillSlide) 	3D Vertical Pointer Slide (3DVPointerSlide) 	3D Horizontal Pointer Slide (3DHPointerSlide) 
3D Vertical Progress Bar (3DVProgressBar) 	3D Horizontal Progress Bar (3DHProgressBar) 	3D Vertical Graduated Bar (3DVGraduatedBar) 	3D Horizontal Graduated Bar (3DHGraduatedBar) 

Figure 81 - Slide Styles of Panel Controls

Slide control types are like the knob control type since they are also used to represent a range of values. Properties specific to this control type include the fore color, format string, axis caption, axis maximum and minimum, axis inversion. The slide property is represented as a vertical or horizontal line.

The format string is discussed in more detail at the end of this section. The axis minimum and maximum specify the minimum and maximum values that the slide will display. The axis can be inverted so that the numeric scale is shown in reverse order.

Temperature 2 - Panel Control Properties	
<< Previous Temperature 02 Next >>	
Name	Temperature 02
Name Display Color	
Show Name	True
Name Display Font	Arial, 8
Type	Slide
Style	3DHPinterSlide
Transparent Background	False
Background Color	
Foreground Color	
Format String	
Axis Caption	
Axis Maximum	40.0
Axis Minimum	-10.0
Invert Axis	False
Left/Bottom Ticks	True
Right/Top Ticks	False
Inner Ticks	False
Outer Ticks	True
Major Ticks	True
Minor Ticks	True
Major Tick Color	
Minor Tick Color	
Tick Spacing	Automatic
Top	679
Left	162
Width	455
Height	104
Visible	True
<div> Delete Close </div>	

Figure 82 - Slide Style Properties

Display



Figure 83 - Display Style of Panel Controls

Display control types are used to display numeric values using a text string. Properties specific to this control type include the fore color and format string.

The format string is discussed in more detail at the end of this section.

6.4.4. Format String

The format string that is available in the Panel Control Properties form can be used to format the value the user sees.



Note: The format string is limited in its functionality and should only be used to configure the panel control values as they appear on the screen. The values that are produced as a result of the format string do not appear in the Log Viewer or anywhere else in the system. To format the system value of an analog input, configure the Formula value in the Device Properties form (see Extra Device Configuration on page 78).

Analog 7 - Panel Control Properties	
<< Previous Analog 07 Next >>	
Name	Analog 07
Name Display Color	
Show Name	True
Name Display Font	Arial, 8
Type	Display
Background Color	Black
Format String	0.00
Foreground Color	Yellow
Top	237
Left	30
Width	278
Height	100
Visible	True
Delete Close	

Figure 84 - Display Style Properties

The following are examples of the variables and components that can be used to form a Format String.

- . (decimal point) - specifies the beginning of the number within the label. Use # and 0 to the right of the decimal point to specify the precision. If you do not include a decimal point in the format string, a decimal point is assumed to be the first character in the format string
- 0 - specifies the precision to the right of the decimal point. For example, ".#0" always produces two digits to the right of the decimal point, even when given an exact number such as 1.0
- # - specifies the precision to the right of the decimal point. For example, "##" produces up to two digits to the right of the decimal point. Thus, 1.0 produces 1, while 1.025 produces 1.03

e, E - specifies exponential notation. "E" specifies the capital letter, while "e" specifies the lowercase letter

*nn - scales labels. For example, ".*10" prints the value 1.0 as 10

+nn or -nn - offsets labels. For example ".+20" prints the value 1.0 as 21

k - specifies symbolic notation. For the format string ".k", 1.0 prints as 1, 1000 prints as 1k, and .001 prints as 1m

"text" - specifies to add text to the label. For example, '".V"' adds a V to the right of every label. Thus, 1.0 becomes 1 V

\$, % - specifies to print these special characters

The following are two useful format string examples:

Celsius to Fahrenheit Conversion

Note that this conversion is not necessary if your temperature sensor is already set up to use Fahrenheit units, however this example demonstrates how to use the format string.

Using the equation $^{\circ}\text{F} = (1.8) ^{\circ}\text{C} + 32$ to calculate the Fahrenheit value, a format string of `*1.8 +32` would be used and would result in the following:

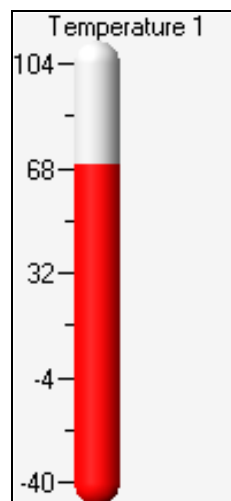


Figure 85 - Celsius to Fahrenheit Conversion

Adding Text

Using the previous example for converting Celsius to Fahrenheit, adding the string "°F" to the format string would become $*1.8 + 32 \text{ "°F"}$ and would result in the following:

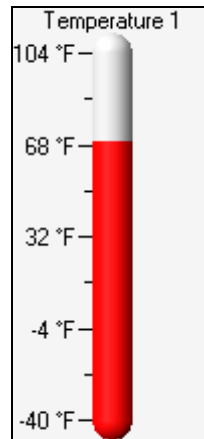


Figure 86 - Adding Text to Format String



Note: To add a degree symbol (°) to your format string, hold the ALT key down and type the number 0176, or refer to the “Character Map” to look for special characters to copy and paste into siteVIEW. The “Character Map” is included with the Microsoft Windows operating system and can be accessed from the windows start menu by selecting “Program→Accessories→System Tools->Character Map”.

Fahrenheit to Celsius Conversion

To convert Fahrenheit to Celsius using the equation $^{\circ}\text{C} = (^{\circ}\text{F} - 32) / 1.8$, the format string would be $-32 * 0.5556$, where 0.5556 is the inverse of 1.8.



Note: There is no division operator available with the format string field. So the user must take the inverse and multiply. Also there must not be any space between the operator and the number, so if you want to add 32, you must write +32, and not + 32. Lastly, you cannot use operators more than once, so you can write $*1.8 + 32$, but if you write $+4.2 * 1.8 + 32$, the first value is ignored.

6.4.5. Adding Controls to a Panel

It may be useful to have multiple components on a panel that represent the same input or output. For example, it may be useful to show an analog or temperature value as a dial or thermometer, and at the same time have a text representation of the same information.

To add controls to a panel, first unlock the panel by selecting “Edit->Site->Unlock Panel” from the main menu. While the Site Panel is unlocked, select “Edit->Site->Add Panel Control” to open the “Add Panel Control” form. Ensure the control is being added to the correct panel, then choose an input or output from the I/O list and select the add button.

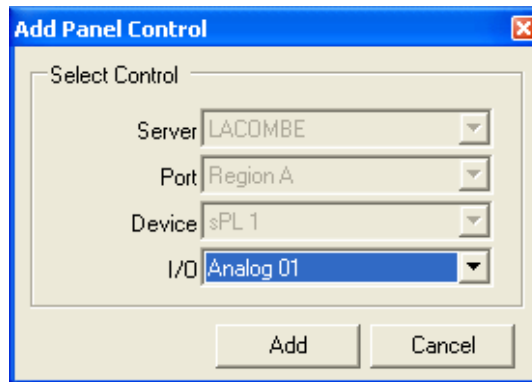


Figure 87 - Adding I/O to a Panel

The new control will appear in the top left corner of the panel. Move the control to the desired location and change the control properties as needed.

It may be useful to have two panel controls representing the same output. By disabling user control on one of the outputs, the disabled control will show the actual device value. Whereas the control that allows user control would be out of sync with the device starting from the time a user changes the output until the device response is received.

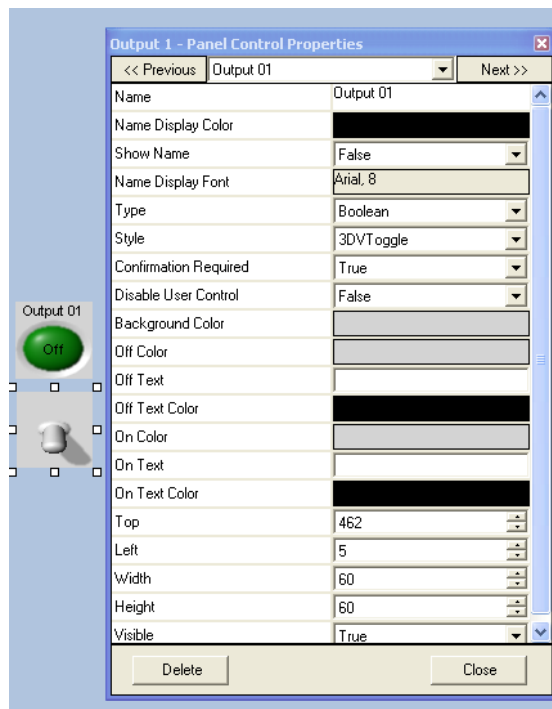


Figure 88 - Panel Control Properties

6.4.6. Panel Import and Export

A panel may be exported to a file and re-imported later into the same panel or into a different panel. If any differences exist between two panels, those differences are ignored. For example, if a panel file that contains a temperature input control is imported into a panel with no temperature input to match, the resulting panel will not contain a temperature input control. The import and export functionality can be accessed by selecting “Edit->Panel->Import Panel” and “Edit->Panel->Export Panel” respectively.

6.5. Alarm Conditions

Alarm conditions can be configured for individual inputs, outputs, or devices.

Alarm conditions can also be configured to alarm when a device is unresponsive.

A user can then manage alarms by taking necessary actions as defined by procedures or the instructions associated with the alarm.

6.5.1. Alarm Condition States

Alarm conditions set boundaries for inputs or outputs, allowing the user to be notified when the value goes outside this boundary. When the value is outside the alarm condition's boundary, the alarm has then been triggered and the user is notified.

Users can acknowledge and clear alarms, hence possible alarm status values are Ceased, CeasedAndAcknowledged, CeasedAndCleared, Active, ActiveAndAcknowledged and ActiveAndCleared.

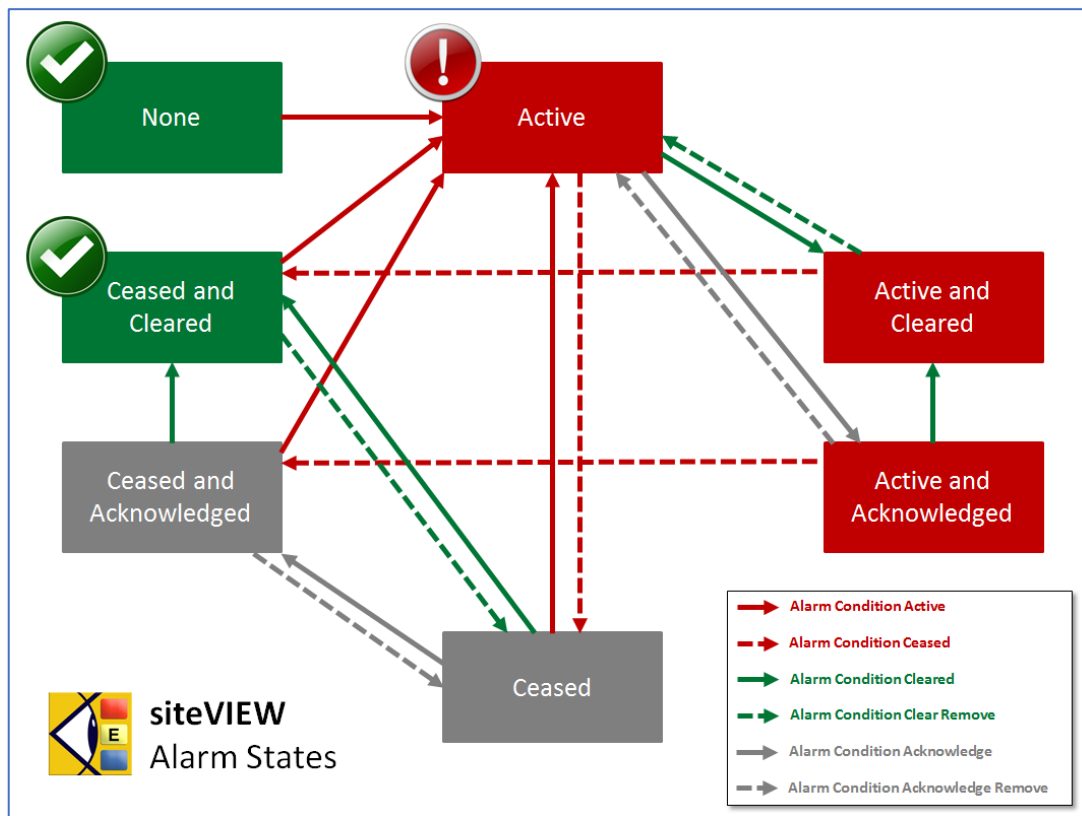


Figure 89 – siteVIEW APEX Alarm Condition States

6.5.2. Configuring an Alarm Condition

To configure an alarm, select a tree node under the “Network” node. Selecting a tree node under the “Groups” node will result in a read only view of configured alarm conditions.

Selecting “Edit->Alarm Configuration” from the main menu opens the alarm configuration form. From this form a user can create new alarm, and delete or modify existing ones.

When creating an alarm, ensure the server, COM port, device and device I/O are selected correctly. Changes made to the alarm configuration form do not take effect until the update button is selected or add is selected while creating a new alarm condition.

The alarm severity is used to place importance and priority on alarms. Three alarm severity options exist: Minor, Major and Critical. Minor alarms are the least severe and Critical alarms are the most severe. The different alarm severities are color coded in the alarm status panel. By default active critical alarms appear red, active major alarms appear orange and active minor alarms appear yellow. Ceased, acknowledged and cleared alarms appear grey in color. These colors are configurable (See Global Alarm Notification Settings, section 6.5.3 on page 118, for information on how to change alarm severity colors).

An alarm can be enabled or disabled by changing the Enabled option.

The type and number fields indicate the input or output the alarm condition applies to.

The alarm conditions for a contact input or an output have only two choices and that is On or Off. In other words an alarm can be set to trigger when the input or output is on or when it is off.

Alarm Configuration

Alarm Properties

Server: COM Site: Device: I/O:

Severity: ☒ Enabled Type: Number:

Is Less Than: Is Greater Than:

Details:

Notification

Server: COM Site: Device: I/O:

ID	Server	COM Site	Device	I/O	Type	Number	Severity	Condition
34	Server1	Prince Ge...	SlaveNoMa...	---	---	---	Minor	Non-Responsive
35	Server1	Prince Ge...	SlaveNoMa...	Output 01	Output	1	Minor	is off
36	Server1	Prince Ge...	SlaveNoMa...	Analog 09	Analog	9	Minor	(value < 0.75 V) or (value ...

Figure 90 - Alarm Configuration Form

The analog or temperature input alarm conditions are based on the low and high thresholds of the device's input, which are configured through the device details form and displayed as read-only fields in the alarm configuration form. When an input's value crosses one of its thresholds, the device then notifies siteVIEW APEX of the change. The alarm can be triggered if the input's values go above a threshold, below a threshold or the threshold change can be ignored.

To configure a non-responsive device alarm, select the desired device and select no I/O. Then whenever the device does not respond to a request from siteVIEW, the alarm will trigger. The non-responsive site alarm does not cease until a successful request/response transaction occurs. A non-responsive device alarm also triggers when the device's port or computer becomes unavailable. Disabling a port or device does not cause a non-responsive device alarm.

The alarm details are useful for providing instructions to the user when the alarm occurs.

The list on the bottom of the alarm configuration form displays alarm conditions. Select an entry from the list to see the alarm condition details. If an alarm condition does not appear on the alarm condition list, ensure the filter is selected correctly.

Alarm Condition for Summit Devices

Unlike other devices, thresholds for Summit devices are configured using Crest, Summit's web configuration interface.

- For Summit Digital Inputs: Thresholds are defined as a change of state. Upon a change of state, events will be sent to Apex. Use the Alarm Configuration form to select the state value that will represent an alarm.
- For Summit Analog Inputs: High and Low threshold values are defined using Crest. Upon a crossing of a threshold value, events will be sent to Apex. Use the Alarm Configuration form to alarm a receipt of the event. Apex does not differentiate high or low events – use Crest to define which crossings are relevant for Apex to alarm on: low only, high only or both.
- For Summit non-responsive alarms: the Summit Communication service “pings” the Summit on a regular basis and will typically recognize a disconnect within 30 seconds. Similarly, the Summit Communication service will continue to “ping” the Summit on a regular basis and will recognize a re-connection within 30 seconds.

6.5.2.1. Analog and Temperature Sensor Alarm Conditions

Unlike Digital Inputs/Outputs and Device (Non-Responsive) alarms, Analog and Temperature sensor alarm conditions can be set configured in multiple ways:

Case	Low Condition Setting	High Condition Setting	Comment
A	LT (Less Than)	GT (Greater Than)	Used for “exclusionary” alarm zones
B	LT	LT	<i>Note: Only High condition is considered</i>
C	LT	Ignore	Single alarm condition
D	GT	GT	<i>Note: Only Low condition is considered</i>
E	GT	LT	Used for “inclusionary” alarm zones
F	GT	Ignore	Single alarm zone
G	Ignore	GT	Single alarm zone
H	Ignore	LT	Single alarm zone
I	Ignore	Ignore	<i>Note: No alarm conditions considered</i>

6.5.1. Alarm Management

Alarms may be managed using siteVIEW APEX interface options.

6.5.1.1. Show Cleared Alarms

Upon startup of siteVIEW, the “Show Cleared Alarms” option, available in the Alarm list, is enabled. This flag determines if Active and Cleared alarms are displayed.

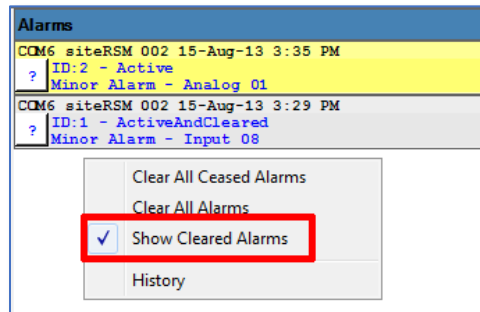


Figure 91 – Alarm Management

Show Cleared Alarms

6.5.1.2. Clear All Reported Alarms

From the Alarm list, use “Clear All Alarms” to clear all active and ceased alarms.

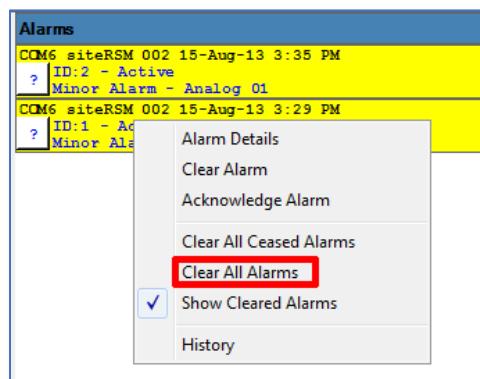


Figure 92 – Alarm Management

Clear All Alarms

6.5.1.3. Clear a Selected Alarm

From the Alarm list, use “Clear Alarm” to clear a specific alarm from the alarm list.

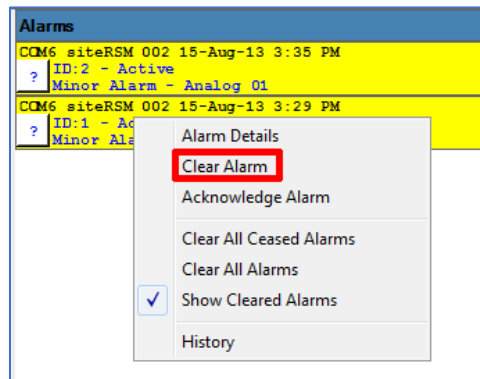


Figure 93 – Alarm Management

Clear a Selected Alarm

6.5.1.4. Acknowledge a Selected Alarm

From the Alarm list, use “Acknowledge Alarm” to acknowledge a specific alarm from the alarm list.

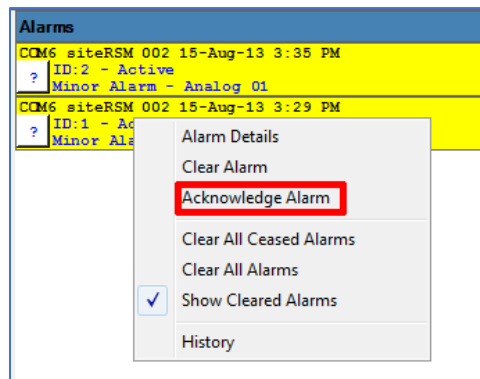


Figure 94 – Alarm Management

Acknowledge a Selected Alarm

6.5.1.5. Clear All Alarms for a Device

From the Sites tree, select a device and use “Clear All Alarms for Device” to clear all active alarms for the selected device.

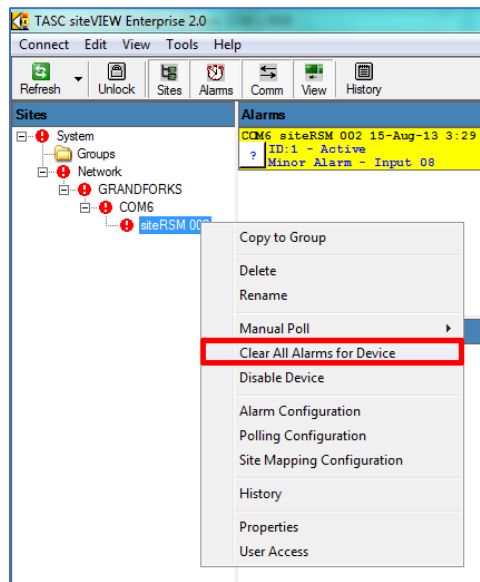


Figure 95 – Alarm Management

Clear All Alarms for a Device

6.5.1.6. Clear All Ceased Alarms

From the Alarm list, use “Clear All Ceased Alarms” to clear all ceased alarms. This will return the alarm condition to “Ceased and Cleared” or normal state.

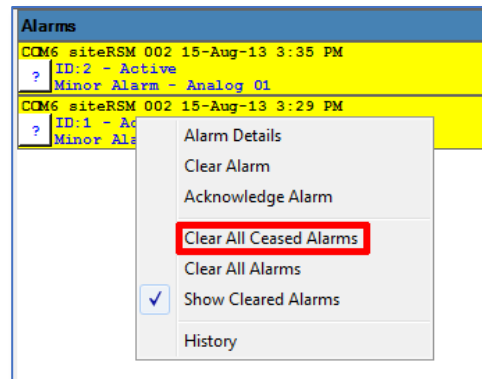


Figure 96 – Alarm Management

Clear All Ceased Alarms

6.5.2. Alarm Specific Reporting Options

Selecting the notification button opens the Alarm Reporting Options form. The alarm condition specific options can be configured from the Alarm Reporting Options form.

Sounds

Selecting the sound tab from the Alarm Reporting Options form allows the selected sound and play interval to be changed. The selected sound file will play on the event the alarm is triggered.

If an alarm is selected the sound interval can be changed. The play interval determines the length of time siteVIEW APEX will wait before replaying the sound file.

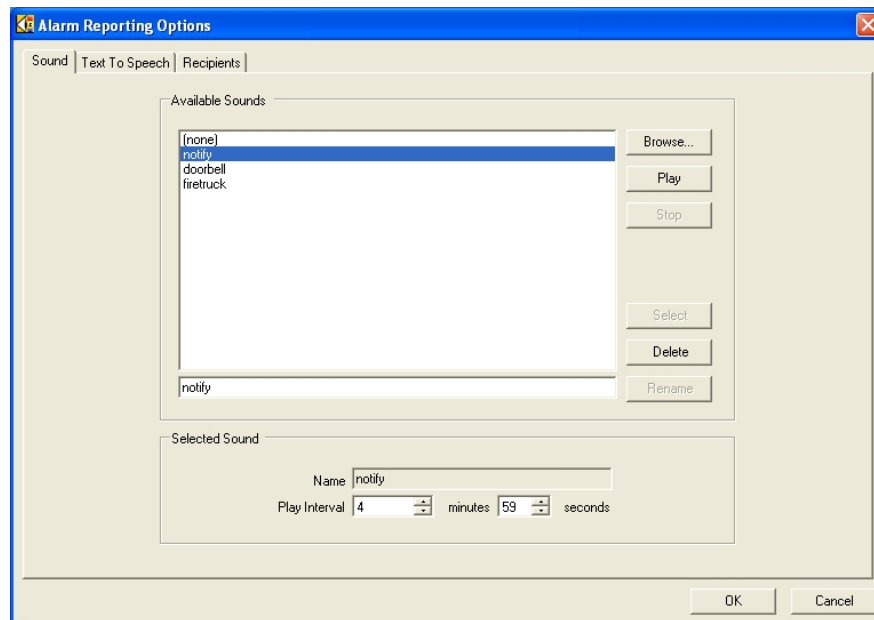


Figure 97 – Alarm Sound

From the sound tab, sound files may be deleted, renamed or sampled, and new sound files may be loaded. siteVIEW APEX is capable of playing most common sound file types including wave (.wav), midi (.mid), mpeg layer 3 (.mp3) and windows media audio (.wma).

Text to Speech

Selecting the “Text To Speech” tab from the Alarm Reporting Options form allows the spoken message and play interval to be changed. The specified text string will be spoken through the client PC’s speakers in the event the alarm is triggered.

The play interval determines the length of time siteVIEW APEX will wait before replaying the message.

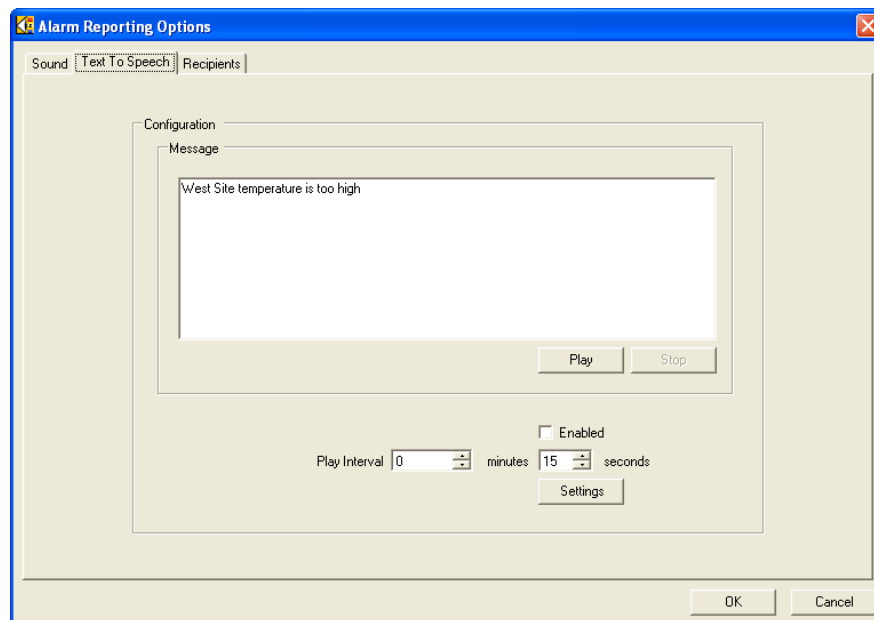


Figure 98 –Text to Speech

Recipients

Recipients are users who receive notification of the alarm. Selecting the “Recipients” tab from the Alarm Reporting Options form allows the selected alarm recipient list to be updated. The selected recipients will be notified when an alarm occurs. The User’s notification options are configured from the “User Administration” form (see Managing User Accounts, section 5.1, on page 61).

If the Notify SNMP Agent is selected, the SNMP Manager will be notified when the alarm occurs. The SNMP Manager is configured within the Global Alarm Notification settings area.

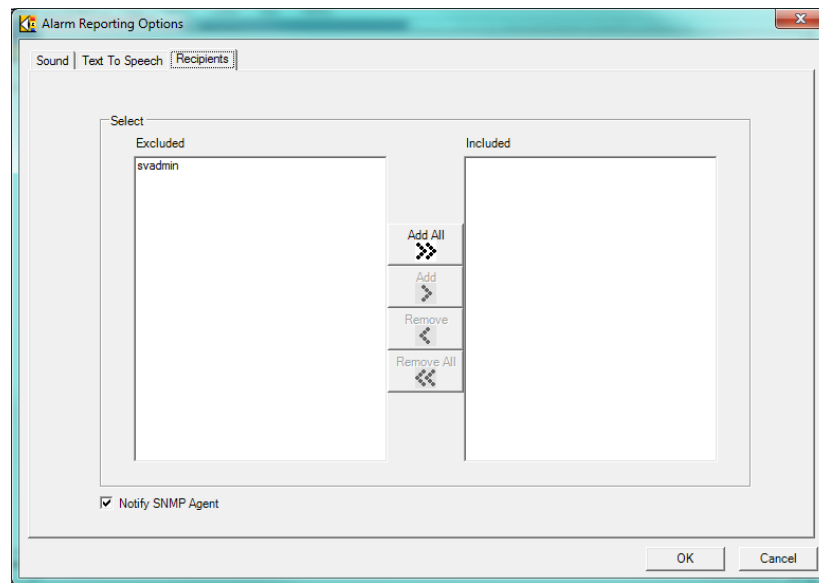


Figure 99 - Alarm Recipients

6.5.3. Global Alarm Notification Settings

By default, when an alarm is cleared, it no longer shows in the alarm panel. However, by selecting "View->Show Cleared Alarms" from the main menu, you may show or hide cleared alarms.

Selecting "Tools-> Notification Settings" from the main menu opens the Notification Configuration Form. From this form, global alarm notification options may be set that apply to all alarm conditions.

Display Settings

Selecting the “Display Settings” tab allows a user to change the alarm panel colors for the different alarm severities.

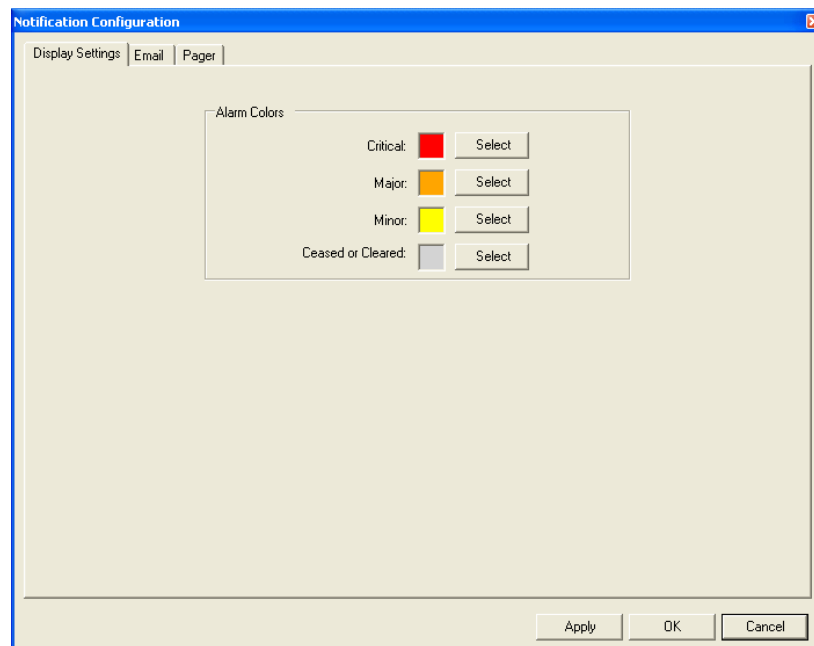


Figure 100 – Notification Configuration – Display Settings

Email

Email alarm notifications are only available if the security key has been configured to allow Email as a siteVIEW APEX option. However, the email page is still available even if email is not enabled in the system for password recovery purposes. Specify an SMTP server that will serve as the default SMTP server during password recovery.

Selecting the “Email” tab allows a user to configure the outgoing email server, the retry interval, the default email message template and the default recipient email addresses. This form also allows the user to test the email reporting system by sending test emails.

Notification Configuration

Display Settings | Email | Pager | FleetSync | SNMP

Outgoing Mail

Server (SMTP): smtp.gmail.com:587

SMTP Account Name: myemail@gmail.com

Password: mygmailpassword ☒ Enable SSL

Name: Recognizable Name

From E-mail: mygmailid@gmail.com

Email Test

To: someoneiknow@gmail.com

This is a test e-mail from TASC siteVIEW 2.0.

Send

Default Recipient Email Addresses

Critical:

Major:

Minor:

Options

Retry Interval: 0 hours 30 minutes

Default email message: Edit

OK Cancel

Figure 101 – Notification Configuration – Email

The outgoing mail SMTP Server is the email server that will be used to send email. This can be any SMTP server that the *Alarm Notification Manager* has access to. If the server resides on the same computer as the *Alarm Notification Manager*, then the server can be set as “localhost” or “127.0.0.1” or even the DNS name of the computer the *Alarm Notification Manager* resides on. A remote server can also be specified.

The outgoing mail name is the sender name that will appear on all out going emails from siteVIEW. A valid *From* email address must also be supplied for the SMTP server to authenticate that the email is being sent from a valid email account.



To use siteVIEW APEX with third party email services which require a secure connection, ensure that *Enable SSL* is selected and the specific port number is appended to the *Server (SMTP)* name.

For example, to use Google’s Gmail service, *Server (SMTP)* would be smtp.gmail.com:587 and the *Enable SSL* option would be checked.

The email test section allows a user to test the outgoing mail configuration by sending a test email to a specified email address.

The default recipient email addresses allows for system wide emails to be sent based on the criticality of the alarm that initiated the email. Each criticality can have one or more email addresses separated by a comma or a semi-colon.

The retry interval indicates how often the email will be resent. The email will continue to be sent to the recipient until the alarm has ceased or been acknowledged or cleared.

Pressing the “Edit” button opens the Notification Message editor. From the Notification Message editor, the siteVIEW APEX alarm notification email can be modified. The left side of the form can be edited and the right side of the form displays an example of what the alarm email will look like. A column of buttons is located down the center of the form. When any of the buttons are pressed, a predefined field tag is inserted into the message. For example, pressing the button labeled “Alarm ID” inserts the alarm id tag into the message in the form of “<ALARM_ID>.” This tag is a placeholder that gets replaced with the actual alarm id

Notification Message

Alarm Notification Message

Subject: siteVIEW Alarm Notification - Alarm ID: <ALARM_ID>

Body: This is an automated email alarm notification from siteVIEW

ALARM INFORMATION

Alarm ID: <ALARM_ID>
 Severity: <SEVERITY>
 Server: <SERVER_NAME>
 Site: <SITE_NAME>
 Device: <DEVICE_NAME>
 I/O Name: <I/O_NAME>
 I/O Type: <I/O_TYPE>
 I/O Number: <I/O_NUMBER>
 Alarm Time: <TIMESTAMP>
 Alarm Reason: <REASON>
 Details: <DETAILS>

<PREVIOUS_STATUS> -> <STATUS>

Alarm ID
 Status
 Previous Status
 Alarm Severity
 Alarm Time
 Alarm Reason
 Alarm Details
 Server Name
 Site Name
 Device Name
 I/O Name
 I/O Type
 I/O Number

Preview

siteVIEW Alarm Notification - Alarm ID: 999999

This is an automated email alarm notification from siteVIEW

ALARM INFORMATION

Alarm ID: 999999
 Severity: Critical
 Server: Server 1
 Site: Eastlake
 Device: Shed
 I/O Name: Room Temp
 I/O Type: Temperature
 I/O Number: 4
 Alarm Time: Tuesday, November 10, 2009 1:30:46 PM
 Alarm Reason: Temperature value is too high
 Details: send technician to investigate

CeasedAndCleared -> Active

OK Cancel

Figure 102 – Default Email Message Editor

before the email is sent.

Pager Settings



Note: Paging is only available if the security key has been configured to allow paging as a siteVIEW APEX option and it is only available as an option in a siteVIEW APEX system.

Selecting the “Pager” tab allows a user to configure the outgoing pager modem line, the retry interval, the numeric paging message and the default recipient pager numbers. This form also allows the user to test the pager reporting system by sending test pages.

The screenshot shows the 'Notification Configuration' dialog box with the 'Pager' tab selected. The dialog has three tabs: 'Display Settings', 'Email', and 'Pager'. The 'Pager' tab contains the following sections:

- Outgoing Calls:** A dropdown menu for 'Modem Line' showing 'Conexant D480 MDC V.92 Modem'.
- Pager Test:** A text field for 'Pager Number' containing '9,6045551515' and a 'Send' button.
- Default Recipient Pager Numbers:** Three stacked text fields for 'Critical:', 'Major:', and 'Minor:'.
- Options:** A 'Retry Interval' section with spinners for '0' hours and '4' minutes, and a 'Numeric Paging Message' text field containing '1234567890'.

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

Figure 103 – Notification Configuration – Pager Settings

The outgoing modem line is the modem line that will be used to send pages. This can be any modem line that is configured on the *Alarm Notification Manager* computer.

The pager test section allows a user to test the outgoing pager configuration by sending a test page to a specified phone number.

The default recipient pager numbers allows for system wide pages to be sent based on the criticality of the alarm that initiated the page. Each criticality can have one or more pager numbers separated by a semi-colon.



Note: Do not use a comma to separate pager numbers, as a comma is used to indicate a pause when dialing a number.

The retry interval indicates how often the page will be resent. The page will continue to be sent to the recipient until the alarm has ceased or been acknowledged or cleared.

FleetSync Settings



Note: FleetSync is only available if the security key has been configured to allow FleetSync as a siteVIEW APEX option and it is only available as an option in a siteVIEW APEX system.

Selecting the “FleetSync” tab allows a user to configure the outgoing FleetSync notification options.

The screenshot shows the 'Notification Configuration' dialog box with the 'FleetSync' tab selected. The dialog has tabs for 'Display Settings', 'Email', 'Pager', 'FleetSync', and 'SNMP'. The 'FleetSync' tab contains two sections: 'Default Recipient Radios' and 'Options'. The 'Default Recipient Radios' section has three text boxes for 'Critical:', 'Major:', and 'Minor:', each with an 'Edit' button to its right. The 'Options' section has a 'Retry Interval' set to 0 hours and 30 minutes, and a 'Default FleetSync message:' field with an 'Edit' button. At the bottom right are 'OK' and 'Cancel' buttons.

Figure 104 – Notification Configuration – FleetSync Settings

SNMP Settings



Note: SNMP is only available if the security key has been configured to allow SNMP as a siteVIEW APEX option and it is only available as an option in a siteVIEW APEX system.

The SNMP notification feature allows siteVIEW APEX to send a SNMP v2 Trap to a SNMP-capable manager – for example, a Network Operations Center software system.

Selecting the “SNMP” tab allows a user to configure the outgoing SNMP notification options.

The screenshot shows a window titled "Notification Configuration" with a tabbed interface. The "SNMP" tab is selected. Inside the window, there are two main sections: "Settings" and "Test Trap". The "Settings" section contains a "Manager" box with "Address" (192.168.0.144) and "Port" (162) fields, and a "MIB" dropdown menu set to "siteView". The "Test Trap" section has a "Send" button. At the bottom right of the window are "OK" and "Cancel" buttons.

Figure 105 – Notification Configuration – SNMP Settings

The SNMP - Settings section defines the SNMP Manager’s location in terms of Address and Port number. Use the MIB dropdown to select the SNMP MIB file to be used.

To test SNMP trap, use the SNMP – Test Trap section’s Send button.

6.6. Automated Polling

Automated Polling is used to check the status of selected devices within the network at scheduled intervals. This is used to ensure that conditions at remote locations remain within acceptable parameters.

To configure polling, select a tree node under the “Network” node. Selecting a tree node under the “Groups” node will result in a read only view of configured polling.

Selecting “Edit->Polling Configuration” from the main menu opens the polling configuration form. From this form a user can create polling schedules, and delete or modify existing ones.

Changes made to the polling configuration form do not take effect until Update is selected after making changes to an existing polling schedule or add is selected while creating a new polling schedule.

Sub Command	Frequency	Start Date	Start Time	End Date	End Time
AllAnalogInputs	every 1 Day	6/20/2007	4:30 PM	none	none
DeviceStatus	every 12 Hours	6/20/2007	4:31 PM	none	none
AllOutputs	every 1 Day	6/20/2007	4:31 PM	none	none
AllContactInputs	every 1 Day	6/20/2007	4:31 PM	none	none
AllTemperatureInputs	every 1 Day	6/20/2007	4:31 PM	none	none

Figure 106 - Polling Configuration Form

A scheduled poll tells siteVIEW APEX to communicate with a device at a specified time. The type of communication depends on the type selected. Available scheduled poll communication types are:

DeviceStatus: retrieves the device status. This ensures that siteVIEW APEX has not lost communication with the device. Also it allows siteVIEW APEX to detect if any device configuration has changed. If a change in device configuration is detected, siteVIEW APEX will automatically download the new configuration settings.

DeviceStatus is also the option to choose for pinging a device. siteVIEW APEX will then ping for the device’s status.

AllContactInputs: retrieves the contact input values.

AllTemperatureInputs: retrieves the temperature input values.

AllOutputs: retrieves the output values.

AllAnalogInputs: retrieves the analog input values.

MinMaxLogCount: retrieves the min/max log count. If the returned value is more than zero, siteVIEW APEX will automatically download and clear the min/max log.

SampleLogCount: retrieves the sample log count. If the returned value is more than zero, siteVIEW APEX will automatically download and clear the sample log.

RealTimeClockRam: retrieves values stored in the real time clock (RTC) random access memory (RAM). The data logger timers are stored in the RTC RAM.

A scheduled poll has an interval. This interval specifies how often the scheduled poll is to occur. An interval of every two hours will cause the scheduled poll to occur every two hours for the selected days, starting from the start date and ending on the end date. The scheduled poll end date can be set to never end by removing the end date option. If the selected interval is in minutes or hours, an end time may be specified. If an end time is specified but no end date is specified, the scheduled poll will occur indefinitely but only between the specified times each day. An end time cannot be specified if the time interval specified is day, week, month or year.

Scheduled polls without the *Enabled* option selected will not occur, but can be re-enabled by selecting the *Enabled* option and then selecting Update.

In order for a scheduled poll to occur, at least one device must be assigned to the scheduled poll. There are two list-boxes in the scheduled poll form, each showing a list of *TASC Communication Servers*, along with the *TASC Communication Server's* COM ports and the devices connected to those COM ports. The Excluded list contains devices that will not be included in this scheduled poll; whereas the Included list contains devices that will all be polled at the scheduled time. After including or excluding devices in the scheduled poll the update button must be selected in order to Update the schedule poll.

Deleting a scheduled poll permanently deletes the scheduled poll for all devices associated with the scheduled poll.

The list on the bottom of the scheduled polling configuration form lists existing scheduled polls. Clicking on an entry in the list shows the schedule details. If a scheduled poll does not appear on the scheduled poll list, ensure the device filtering options are selected correctly.



Polling is not supported for Summit Devices.

6.7. Site Mapping

To configure site mapping, select a tree node under the “Network” node. Selecting a tree node under the “Groups” node will result in a read only view of site mapping.

Selecting “Edit->Site Mapping Configuration” from the main menu opens the site mapping configuration form. From this form a user can map outputs to any other input or output which is monitored by siteVIEW. The site mapping configuration form is also used to delete or modify existing mappings.

Changes made to the site mapping configuration form do not take effect until update is selected after making changes to an existing output mapping or add is selected while creating a new output mapping.

An output mapping tells siteVIEW APEX to turn on or turn off a specified output based on the result of some other input or output in siteVIEW.

Figure 107 - Site Mapping Configuration Form



WARNING: Site Mapping cannot occur if siteVIEW APEX loses its connection to the mapped device. If the target device is unreachable then no output event can occur.

The input condition is specified for a specific server, COM port, device and input or output on that device. When the input or output condition occurs, siteVIEW APEX is then to take the specified output action. An input condition can occur when an input or output is turned on or off, or an input condition can occur when an analog or temperature value is less than or greater than one of its thresholds.

The site mapping condition form allows a user to modify, delete and enable or disable site mappings.

The list on the bottom of the site mapping configuration form displays site mappings. Select an entry from the list to see the site mapping details. If a site mapping does not appear on the site mappings list, ensure the filter is selected correctly.

6.8. User Access

Selecting “Edit->User Access” from the main menu opens the User Access configuration form. The User Access form is only viewable by an administrator. The User Access form allows administrators to restrict access of other users to parts of the system. This way different users can be assigned to different parts of the system and can only see the parts that they are assigned to.

By default, all users have access to different parts of the system and they must be manually denied access to various parts of the system. Administrator users cannot be given restricted access and so they will always have access to all parts of the system.

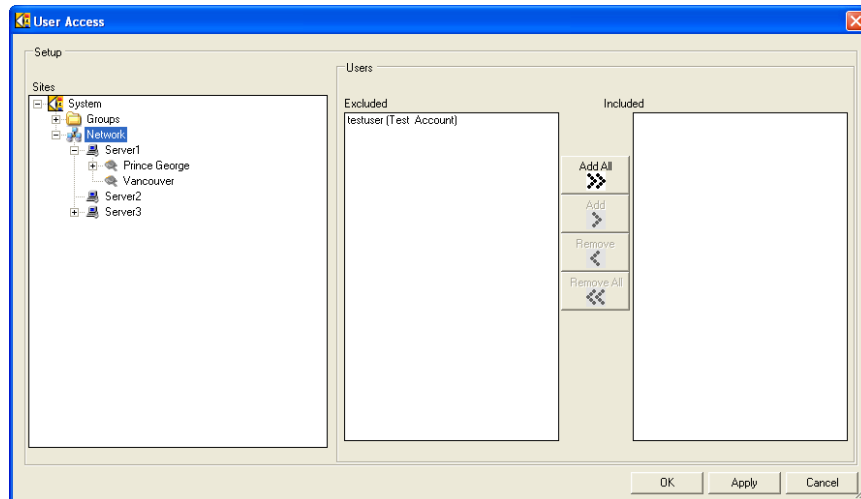


Figure 108 – User Access Configuration

7. MONITORING AND CONTROLLING DEVICES

Once devices are configured they are ready for monitoring and control. Monitoring and control using siteVIEW APEX includes viewing the current status of devices, controlling device outputs and responding to alarms.

siteVIEW APEX does not exit completely when the siteVIEW APEX Client is closed (by selecting the close button in the top right corner of the main application form). Instead siteVIEW APEX Client is minimized to the system tray. To exit the siteVIEW APEX Client completely, select “Connect->Exit siteVIEW” from the main menu.

Once siteVIEW APEX is closed, the *Data Manager*, *TASC Communication Server* and *Alarm Notification Manager* continue to function. Communication with the configured sites, auto polling, site mapping and new status information returned from the device all continue to occur even though the user interface has been closed.



Note: Even though the siteVIEW APEX Client may be closed, monitoring, alarm reporting, scheduled polling and Site Mapping continue to occur.

7.1. Monitoring Devices

7.1.1. TASC Remote Platforms and Summit Devices

siteVIEW APEX can monitor several types of inputs and outputs attached to TASC Remote Platforms. Those inputs and outputs can be represented in different meaningful ways.

Panel control outputs can be turned on and off, but inputs cannot be changed. Outputs may be controlled if the user has the required access rights.



Warning: When controlling outputs, the value displayed on the panel will be different than the actual output value while the command is being sent.

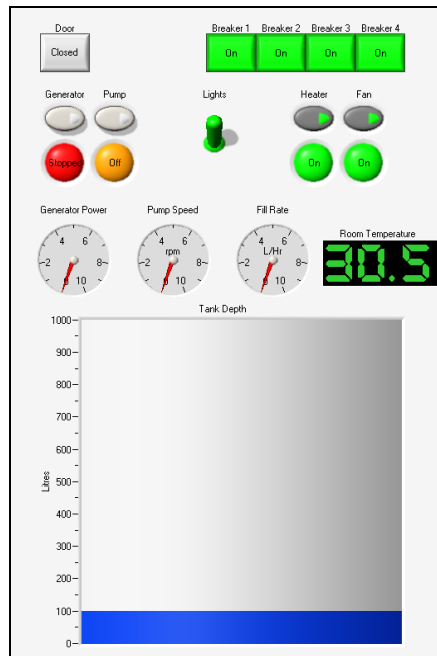


Figure 109 - Site Panel Example for a TASC Remote Platform

7.1.1. Ping Devices

siteVIEW APEX can monitor a set of Ping devices. Since only communication is monitored, no input or output controls are shown on the associated panel display.

To monitor Ping devices, set up a periodic poll. Failure to communication, in the form of an unresponsive status, may mean the device or network is not operating as expected. Use alarms on failed, unresponsive communications to signal failed devices.



Ping devices do not have any associated input or output controls for panel display. To monitor Ping devices, use an unresponsive alarm to signal any communication problems.

7.1.2. SNMP Agent Devices

siteVIEW APEX can monitor a set of SNMP Agent devices. siteVIEW shows an input (by default: in the form of a numeric control) in the display panel for each published Integer OID within the SNMP Agents definition. These inputs are updated by incoming SNMP traps sent to siteVIEW APEX from the SNMP Agent device. Alarms may be set for each SNMP Agent OID input value.



SNMP Agent devices are represented as a list of monitored SNMP Integer OIDs. Incoming SNMP traps from an SNMP Agent are used to update these OIDs. Alarms may be set on any OID.

7.2. Alarm Handling

Alarm conditions pertain to input and output values. When an alarm condition occurs, an alarm is triggered and the siteVIEW APEX user is notified in several ways. Visually, the affected input or output Panel Component will blink on and off, the associated navigation tree node displays an alert icon and an alarm is added to the alarm panel.



WARNING: the 3DCommandOk and 3DToggleOnOff Boolean control styles do not blink during an alarm condition.

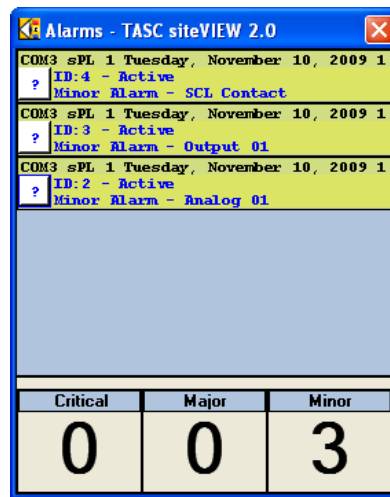


Figure 110 - Alarm Pop-Up Notification

If siteVIEW APEX is minimized when an alarm occurs, the siteVIEW APEX system tray icon will display a blinking alert icon and an alarm pop-up screen is displayed above the siteVIEW APEX system tray icon, in the bottom right area of the screen. The pop-up screen can be displayed manually from the main menu by selecting “View->Show Alarm Pop-up Window.”

If the triggered alarm has a sound file associated to it, the sound file will play while the alarm is active or until the user mutes the alarm sound.

The alarm popup form displays a summary of active alarms. Whereas the alarm panel displays all active and inactive alarms that have not been cleared. Each entry of the alarm popup form and each entry on the alarm panel have a find button with a question mark on it. Selecting the find button navigates the user to the device where the alarm occurred, and the device panel is displayed.

Each alarm entry on the alarm panel and alarm popup displays information about the input or output where the alarm has occurred. Performing a double mouse click on an alarm panel entry displays the alarm details form.

Figure 111 - Alarm Details Form

The Alarm Details form gives details of the alarm location, the time the alarm's status last changed and details about the alarm. The Details field is useful for providing instructions to a user in the event that the alarm is triggered.

If an alarm has a sound file associated to it, selecting the mute button stops the sound from playing until the alarm has been triggered again. The snooze button causes the alarm sound to stop and not resume again until five minutes later. If within those five minutes the alarm condition ceases, the snooze is interrupted and the sound will not occur again until the next time the alarm is triggered.

The status of the alarm is displayed in the status field. A user can change the status of the alarm by selecting an action and then selecting the Set button. Active alarms can be cleared or acknowledged. Acknowledging an alarm causes the alarm to remain in the alarm panel, but all other alarm indications stop. Clearing an alarm removes the alarm from the alarm panel completely. But selecting "View->Show Cleared Alarms" causes cleared alarms to be displayed on the alarm panel as well.

Alarm panel entries have different colors based on the alarm severity and status. Critical alarms appear with a red background, major alarm backgrounds are orange and minor alarm backgrounds are yellow. When an alarm has become inactive or when an alarm is cleared, the alarm panel entry background turns grey. The

background of an active alarm blinks when the alarm is neither acknowledged nor cleared.

7.3. Manually Polling the Devices in the Network

Options exist that allow a user to manually initiate a poll. This allows the operator to retrieve the current status of the selected unit at any time. To perform a manual poll select one of the “Edit->Manual Poll” submenus. Selecting the manual poll button on the tool bar can access the same functionality.

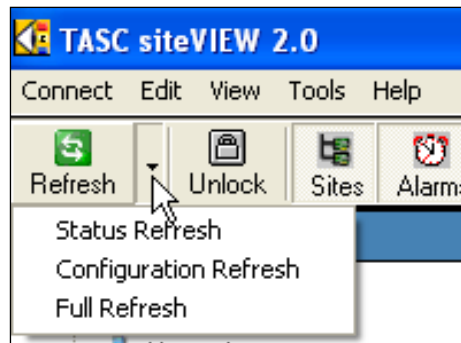


Figure 112 - Manual Poll Options

Selecting “Edit->Manual Poll->Status Refresh” causes siteVIEW APEX to retrieve the status and I/O values of all devices under the currently selected node.

For instance, if a Server node is selected then all COM Ports and their respective devices will be polled.

If a COM Port Node is selected then all devices within that COM Port will be polled.

If a device node is selected then only that particular device will be polled.

A status refresh retrieves a device’s status and I/O values. A configuration refresh retrieves the device’s configuration settings. A full refresh performs the functionality of a status refresh and a configuration refresh combined.

8. LOGGING

Each time an alarm occurs, or an I/O value changes or communication with a device occurs, siteVIEW APEX records the event in a log. This is known as siteVIEW APEX logging.

Some devices also have logging of their own. This kind of logging is referred to as device logging. Device logging is currently only available for the TASC siteCOMMANDER device type and is not visible in systems that are not configured to support siteCOMMANDERS.

The log viewer can be viewed by selecting “View->History” from the main menu or by selecting the history button from the toolbar.

The log viewer connects to the logging interface, which resides on the *Data Manager* computer.

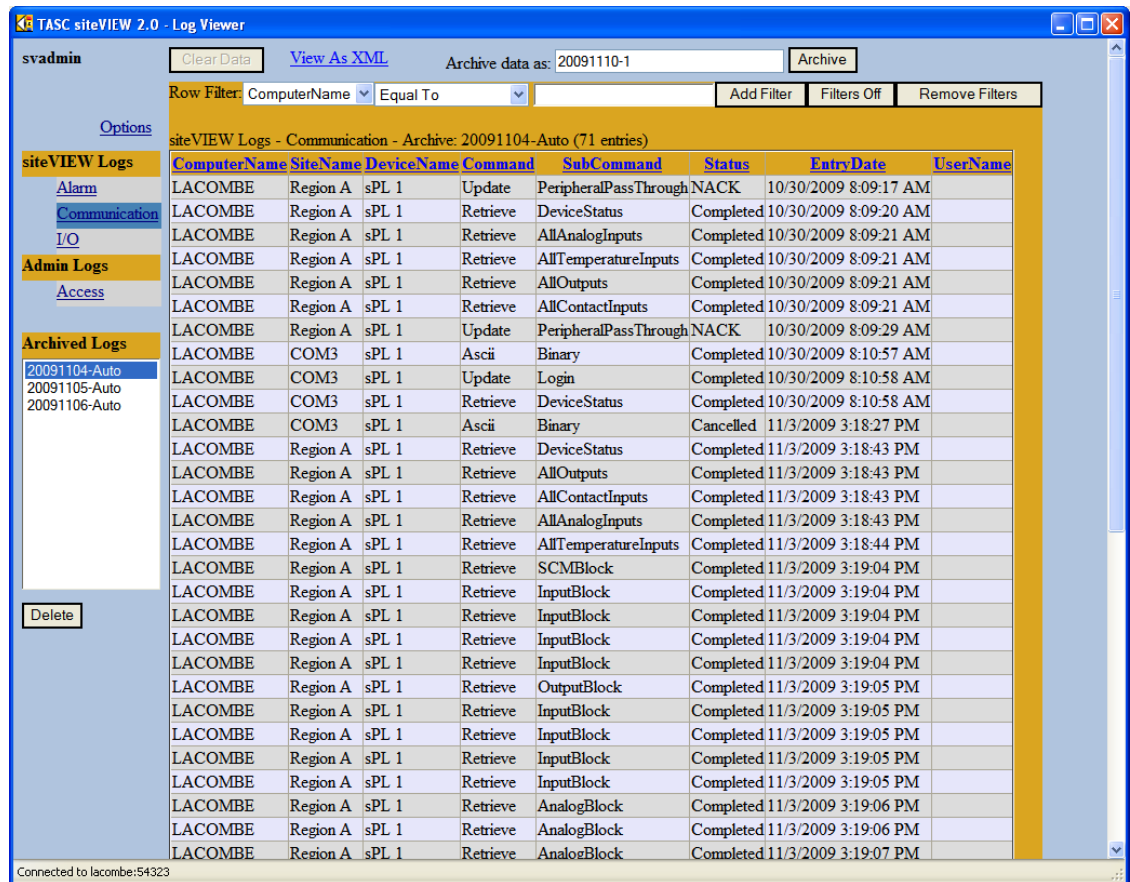


Figure 113 - siteVIEW APEX Log Viewer

The log viewer form displays log entries on the right and a list of log types on the left.

From the menu links of the log viewer form a user can export, clear or refresh log entries. The log data can be filtered and archived, and any data can be exported to xml.

A list of archived logs is shown on the bottom left of the Log Viewer. Select an archived log to view it in the Log Viewer or delete it. Logs are automatically archived to prevent the logs from becoming unmanageably large.

8.1. siteVIEW APEX Logging

Each time an alarm's status changes an entry for the alarm is recorded in the alarms log. The alarm log also contains a field named Username. This field records the user who changed the alarm status. If the Username field is empty, then the alarm status was changed automatically by the system.

Each time communication occurs between siteVIEW APEX and a device, the communication is recorded in the communications log.

Each time an I/O value is returned from a device, an entry is recorded in the I/O values log that indicates this value.

siteVIEW APEX also records each time a user logs in or out of the siteVIEW APEX system in the access log, however, this log can only be viewed by an administrator.

8.2. Device Logging

Device logging is only available for the TASC siteCOMMANDER device.

A siteCOMMANDER may be set up to perform logging locally. If device logging is enabled for a siteCOMMANDER, it can be manually retrieved or automatically retrieved by siteVIEW APEX by setting up an automated poll. To retrieve a device's log manually, select a siteCOMMANDER's device node on the navigation tree and then select "Edit->Data Logger" from the main menu. This will open the device data logger form.

The first time the device data logger form is opened for a device, most of the information will be unavailable. There are two refresh buttons on the device data logger form that allow a user to refresh the logger information. If the data logger is running, the data logger information will constantly change at the device and siteVIEW APEX will not be aware of the changes without performing another refresh.

A user can download the sample log or the min/max log and when the download has completed, siteVIEW APEX automatically clears the log that was downloaded. Or a user can manually clear the log without downloading the values.

The data logger can be stopped and started from the device data logger form. The time the logger was started is displayed in the field labeled start time.

Several timers exist in the device Data Logger form. These values are not stored in the data logger and they cannot be automatically downloaded. The timers are only available for viewing through the device data logger form. The timers display the total accumulated time the carrier operated squelch (COS) was active, if the device is a siteCOMMANDER equipped with the FFSK option, and accumulated time the inputs were on. The last update time displays the last time these values were updated.

8.3. Log Viewer Properties

You can access the *Log Viewer Properties* page by selecting the options link from the *Log Viewer* form.

8.3.1. Log Archiving

By default logs available from the *Log Viewer* are automatically archived every evening at midnight by the *Logging Interface*. The length of time to keep a log entry before archiving is adjustable, as are the auto-delete options.

The log archives are saved to <InstallDir>\data\Archive, where <InstallDir> is the installation path of the *Data Manager* (by default, <InstallDir> is C:\<Program Files>\TASC\siteVIEW APEX \APEXDataManager). The amount of computer hard drive space the *Logging Interface* needs to maintain these archives ranges greatly, depending on the amount of activity in the system and how long the archives are stored, so please monitor these files to make sure the computer does not run out of space.

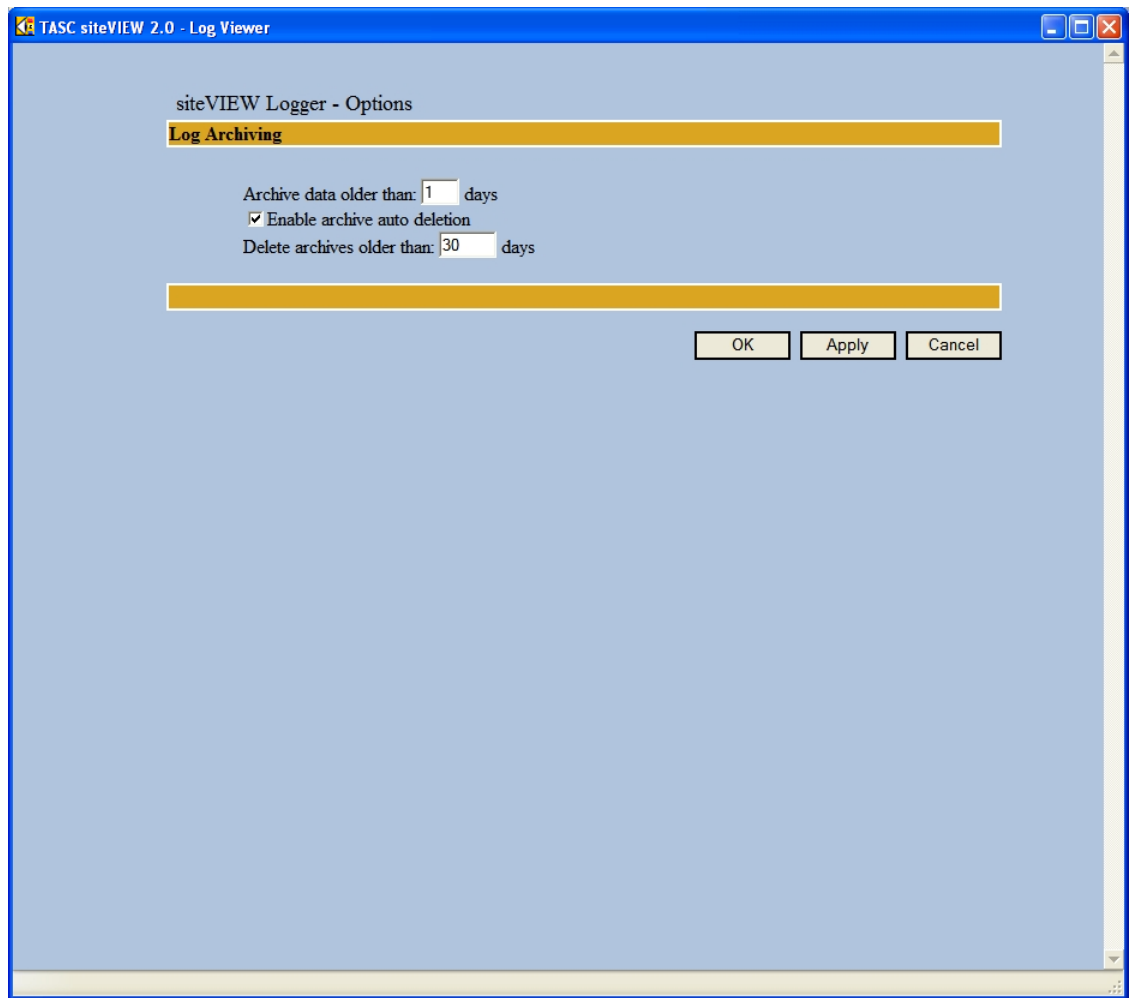


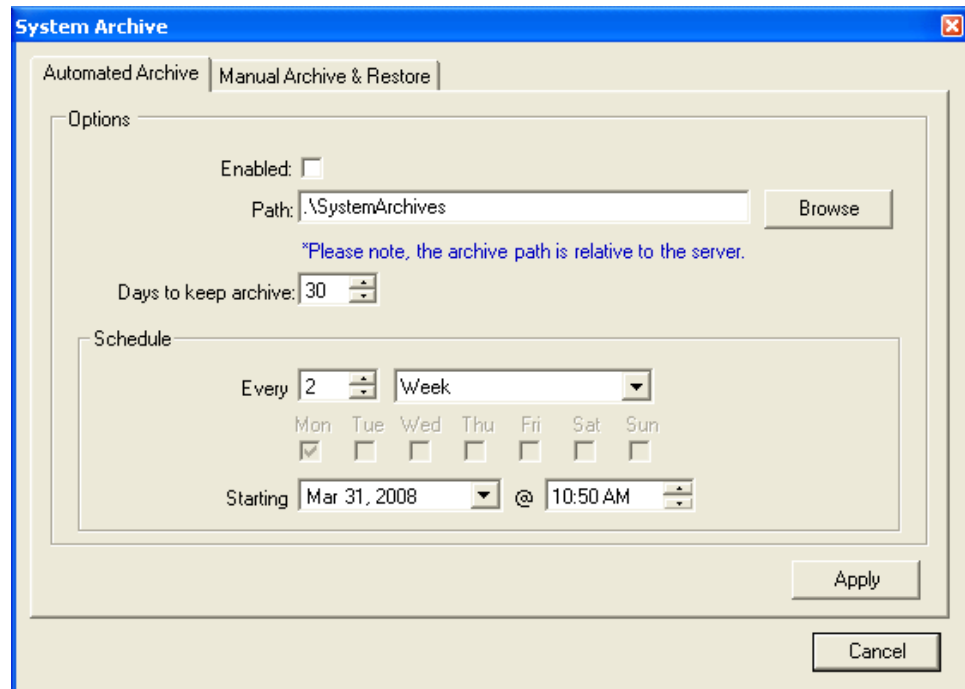
Figure 114 - siteVIEW APEX Log Viewer - Options

9. SYSTEM ARCHIVE AND RESTORE

The stored data and logs can be archived and restored. To access the archive and restore options, select “Tools->System Archive/Restore” from the main menu.

9.1. Automated Archive

To setup automated system archiving, check the enabled checkbox, setup the path on the server where to archive to and set up a schedule.



The screenshot shows the 'System Archive' dialog box with the 'Automated Archive' tab selected. The 'Options' section contains an 'Enabled' checkbox (unchecked), a 'Path' text box with '.\SystemArchives' and a 'Browse' button, and a 'Days to keep archive' spinner box set to 30. A note below the path states: '*Please note, the archive path is relative to the server.' The 'Schedule' section includes an 'Every' spinner box set to 2, a 'Week' dropdown menu, and a row of checkboxes for days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun), with 'Mon' checked. Below this is a 'Starting' date/time field set to 'Mar 31, 2008 @ 10:50 AM'. At the bottom right are 'Apply' and 'Cancel' buttons.

Figure 115 – Automated System Archive

9.2. Manual Archive & Restore

System archives can be archived manually by selecting an archive name and selecting the archive button. The archive will automatically be saved into the default archive directory.

To manually restore a stored system archive, select an available archive from the list and then select restore.

Archives that were stored in previous versions of siteVIEW APEX will be automatically updated to the newer version when the archive is restored.

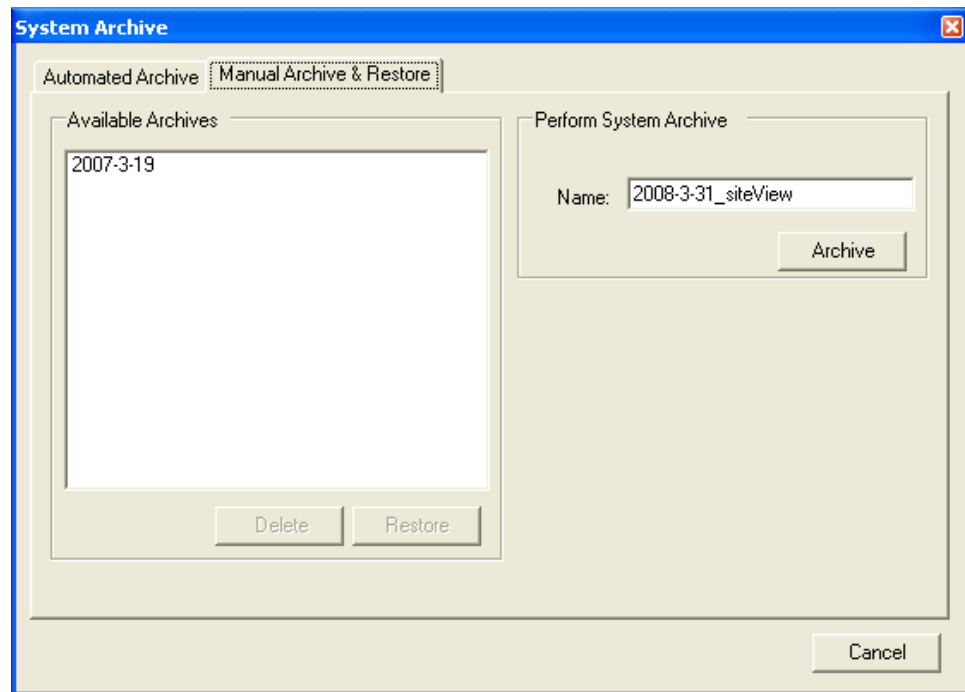


Figure 116 – Manual System Archive & Restore

10. TROUBLESHOOTING

10.1. Event Viewer

TASC siteVIEW APEX uses the Windows operating system's [Event Viewer](#) to track when the *Data Manager* stops and starts. The Event Viewer is also used to track key information such as licenses and add-ons, and to track *Data Manager* application errors.

To access the Windows Event Viewer, select Administrative Tools from the Windows Control Panel. Under administrative tools, select Event Viewer. The TASC siteVIEW APEX event log is specific to TASC siteVIEW APEX.

The Event Viewer can be used to help troubleshoot problems with the security key, notification errors (e.g., email server problems) and *Data Manager* connectivity problems.

10.2. TASC Communication Server Log Files

10.2.1. Message Transaction Log Files

The Message Transaction log file provides high-level operational information for the siteVIEW APEX TASC Communication Server software module, including:

- Message requests and responses from siteVIEW APEX (Data Manager)
- Overall health of all underlying communication ports

By default, the CommunicationService.log file is disabled. To enable the CommunicationService.log file:

- Navigate to the `C:\<Program Files>\TASC\siteVIEW APEX\TASCCommServer` directory
- Use a text editor to edit the `CommunicationService.exe.config` configuration file
- Add the following line before the `</appSettings>` line:
`<add key="CommunicationServiceLogging" value="True" />`
- Save the file

- Use the TASC Communication Server Utility to restart the CommunicationService

```

4:35:56 PM.174,Disconnected from Data Handler Server
2:00:01 PM.643,=====
2:00:01 PM.645,Log File=C:\SVE2Root\Enterprise2\Enterprise2\appSoftware\Bin\CommunicationService\CommunicationService.log [Verbosity=Logs]
2:00:01 PM.645,Connecting to Data Handler Server at 127.0.0.1:11003
2:00:02 PM.896,Connected to Data Handler Server
2:00:03 PM.60,CommSvc->Server [---]: Msg=Update.ClientIdentification
2:00:03 PM.386,Server->CommSvc [---]: Msg=Update.ClientIdentification for Service(2)
2:00:03 PM.391,CommSvc->Server [---]: Msg=Retrieve.SystemSettings
2:00:03 PM.391,CommSvc->Server [---]: Msg=Retrieve.RedundantServerConfig
2:00:03 PM.391,CommSvc->Server [---]: Msg=Retrieve.CommPortConfig
2:00:03 PM.803,Server->CommSvc [---]: Msg=Update.SystemSettings [Server=GRANDFORKS Version=1.0.4813.20928]
2:00:04 PM.16,Server->CommSvc [---]: Msg=Update.CommPortConfig [Port=COM10(COM10) ID1=2 Type=Serial]
2:00:04 PM.184,CommSvc->Server [---]: Msg=Update.ConnectionState for CommPort(2)
2:00:05 PM.201,Server->CommSvc [---]: Msg=Update.CommPortConfig [Port=COM6(COM6) ID1=3 Type=Serial]
2:00:05 PM.206,CommSvc->Server [---]: Msg=Update.CommPortStatus for CommPort(2) is Connected
2:00:13 PM.29,Server->CommSvc [001]: Msg=Update.CommPortTransaction Cmd=Retrieve.DeviceStatus using PortID=2 [Status=Queued]
2:00:13 PM.29,Server->CommSvc [002]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllAnalogInputs using PortID=2 [Status=Queued]
2:00:13 PM.30,Server->CommSvc [003]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllContactInputs using PortID=2 [Status=Queued]
2:00:13 PM.30,Server->CommSvc [004]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllOutputs using PortID=2 [Status=Queued]
2:00:13 PM.30,Server->CommSvc [005]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllTemperatureInputs using PortID=2 [Status=Queued]
2:00:13 PM.30,CommSvc->Server [---]: Msg=Update.TransactionStatus
2:00:13 PM.171,CommSvc->Server [001]: Msg=Update.TransactionStatus
2:00:16 PM.785,CommSvc->Server [001]: Msg=Update.TransactionStatus
2:00:17 PM.45,CommSvc->Server [001]: Msg=Update.CommPortTransaction Cmd=Status.DeviceStatus using PortID=2
2:00:17 PM.60,CommSvc->Server [002]: Msg=Update.TransactionStatus
2:00:17 PM.293,CommSvc->Server [002]: Msg=Update.CommPortTransaction Cmd=Status.AllAnalogInputs using PortID=2

```

Figure 117 – Sample Message Transaction Log File

10.2.1. Port Transactions Log Files

For each COM port, a TransmitReceiveCOMxxx.log file (where xxx is the COM port number) is created in the `C:\<Program Files>\TASC\siteVIEW APEX\TASCCommServer` directory to track communication transactions.

The port transaction log files are created and update automatically. In addition to transactions, the state, availability and the connection status of the port is provided.

```

.. - Monitor: Refresh0 [Port=COM10, State=Unavailable, Avail=False, IsOpen=False]
.. - Monitor: Refresh1 [Port=COM10, State=Unavailable, Avail=True, IsOpen=False]
.. - Monitor: Opening [Port=COM10, State=Unavailable, Avail=True, IsOpen=False]
.. - Monitor: Open OK [Port=COM10, State=Unavailable, Avail=True, IsOpen=True]
.. - Monitor: Opened [Port=COM10, State=ClearToSend, Avail=True, Connection=Connected, ResetPort=False]
.. - Monitor: Change [Port=COM10, State=ClearToSend, Avail=True, Connection=Connected, ResetPort=False]
TX - COM10,255 254 253 252 251 250 249 248 247 246 245 244 243 242 241 240 239 238 237 236 235 234 233 232 231
RX - COM10,10 0 1 0 55 3 15 192 160 0 75
TX - COM10,8 1 0 2 133 0 8 0 103
.. - Monitor: Change [Port=COM10, State=WaitingForReply, Avail=True, Connection=Connected, ResetPort=False]
.. - Monitor: Change [Port=COM10, State=ClearToSend, Avail=True, Connection=Connected, ResetPort=False]
RX - COM10,24 0 1 32 133 2 8 0 161 0 33 2 72 0 88 0 33 2 32 2 48 2 0 0 92

```


 **Retry to open
is successful**

Figure 118 – Sample Port Transaction Log File

10.3. Solutions to Problems

I cannot sign into siteVIEW APEX because there are no licenses available

Look in the event viewer and ensure the *Data Manager* properly detected the key and its licenses.

It may be possible the *Data Manager* is not properly detecting the security key for some reason. Stop the *Data Manager* using the *Data Manager Utility* and then exit the *Data Manager Utility* completely by minimizing it and then closing it once it minimizes to the system tray. Then use the “Safely Remove Hardware” program, which is also located in the system tray to remove the siteVIEW APEX USB Key. Once the key is uninstalled, remove the key manually and then reinsert the key. Make sure the key is inserted completely. The siteVIEW APEX USB Key should then reappear on the list of installed hardware. Then restart the *Data Manager Utility* by selecting “Start->Programs->TASC->Data Manager Utility.” Then using the *Data Manager Utility*, start the *Data Manager*.

Sometimes the siteVIEW APEX USB Key is removed improperly and then the computer must be restarted before the system will properly detect the security key again.

siteVIEW APEX will not detect my key

Ensure the key is properly inserted into an available USB connection on the computer where the *Data Manager* resides. Do not remove the key at any time while the *Data Manager* is running.

If the key is properly inserted and *siteVIEW APEX* still does not detect the key, remove the key and restart the computer. Once the computer has restarted then insert the key and allow the operating system to find and install any drivers it needs. Once the operating system has detecting the key, *siteVIEW APEX* should function properly.

The TASC Communication Server is not running

Use the *TASC Communication Server Configuration Tool* to start the *TASC Communication Server*. Several *TASC Communication Servers* can be installed on different computers and each *TASC Communication Server* is installed with its own configuration tool.

The Alarm Notification Manager is not running

Use the Alarm Notification Manager Configuration Tool to start the Alarm Notification Manager.

I cannot make changes to the system

Ensure the login user you are using has the appropriate rights to access the *siteVIEW APEX* features you wish to use.

siteVIEW APEX is unable to make a connection to a device

Ensure the device addressing is correct, otherwise *siteVIEW APEX* will not be able to connect to the device.

Ensure the device is connected properly.

If using an Ethernet to serial connection to connect to the device, check that the virtual serial communications port is setup properly in the Lantronix CPR Manager application.

siteVIEW APEX tells me the COM port is already in use

Ensure no other applications are using a COM port that *siteVIEW APEX* is expecting to use for monitoring. Once an application is closed and the COM port is freed up again for *siteVIEW APEX* to use, select "Edit->Properties" for the COM port that had difficulties, and then select the refresh button to allow *siteVIEW APEX* to resume monitoring on the COM port.

I cannot connect to the Data Manager

Ensure the *Data Manager* you are trying to connect is visible to the computer you are trying to connect from. Make sure the *Data Manager* listen port is not in use by another program.

The Log Viewer Does not work properly

Using the *Data Manager Utility*, ensure the logging interface service is running and make sure the logging interface listen port is not in use by another program.

APPENDIX A. TASC HARDWARE & FIRMWARE

A.1. Overview

The TASC siteCOMMANDER (sC), sitePORTAL Lite (sPL) and siteRSM (sRSM) all use the same hardware but are different by their application firmware. This common hardware is known as the TASC TRIO.

The TASC TRIO has eight analog inputs, eight contact inputs, eight digital outputs and has room for up to eight temperature sensors.

The siteRSM and sitePORTAL Lite hardware devices are capable of adding digital and analog expansion boards. They are capable of adding a total of 4 digital expansion boards, each with 8 additional contact inputs, allowing for a maximum of 40 contact inputs (32 expansion and 8 on-board). And these boards are capable of adding a total of 2 analog expansion boards, each with 8 additional analog inputs, allowing for a maximum of 24 analog inputs (16 expansion and 8 on-board). How it is packaged will determine the number of expansion inputs.

A.2. Configuration Utilities

TASC devices can be configured using their individual configuration utility, or by using siteVIEW. If the configuration utility is used to configure a device, siteVIEW APEX will be unaware of the change and so siteVIEW's configuration will be out of date for the device. To update siteVIEW APEX perform a complete refresh on the device.

A.3. Analog Inputs

A.3.1. Jumper Configuration

Each analog input may be set to a different range via jumpers J1 to J16 in conjunction with the device's configuration utility. Each analog input has two jumpers noting that the order of jumpers is reversed, i.e. J1 & J2 correspond to the highest analog input.

Analog	Jumper block
8	J1 / J2
7	J3 / J4
6	J5 / J6
5	J7 / J8
4	J9 / J10
3	J11 / J12
2	J13 / J14
1	J15 / J16

Table 3 - Device Properties – Analog Jumper Configuration

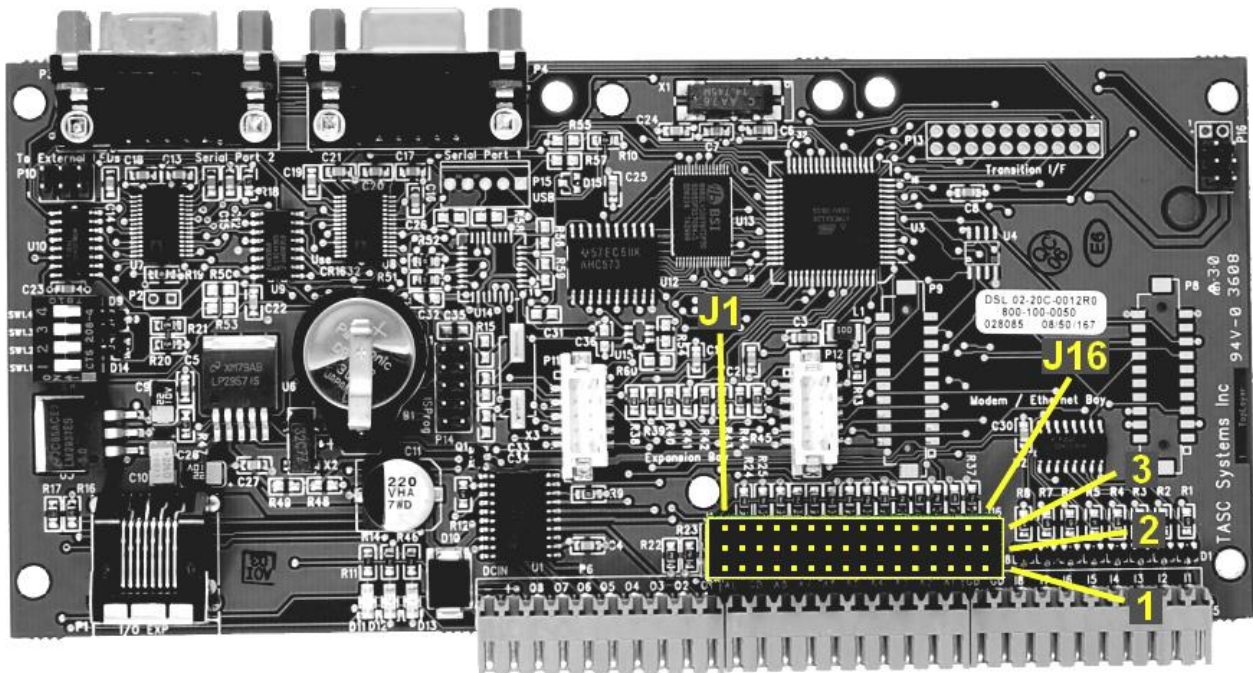


Figure 119 - Photo of Analog Jumpers

Each pair of jumpers configures one of two programmed ranges.

Analog	0-5.0V or User Range	0-25V
1	J16-1 to J16-2 J15 Out	J16-3 to J16-2 J15-1 to J15-2
2	J14-1 to J14-2 J13 Out	J14-3 to J14-2 J13-1 to J13-2
3	J12-1 to J12-2 J11 Out	J12-3 to J12-2 J11-1 to J11-2
4	J10-1 to J10-2 J9 Out	J10-3 to J10-2 J9-1 to J9-2
5	J8-1 to J8-2 J7 Out	J8-3 to J8-2 J7-1 to J7-2
6	J6-1 to J6-2 J5 Out	J6-3 to J6-2 J5-1 to J5-2
7	J4-1 to J4-2 J3 Out	J4-3 to J4-2 J3-1 to J3-2
8	J2-1 to J2-2 J1 Out	J2-3 to J2-2 J1-1 to J1-2

Table 4 - Device Properties – Analog Jumper Ranges

When a range is selected via the jumper block, the corresponding range must also be set in the analog configuration pages for the device.

A 3.2. User Ranges

The user may select one of four external analog ranges by supplying an external ‘potential divider’ resistor network. 1% tolerance resistors should be used. To configure an analog input for an externally supplied resistor network, set the jumpers the same as for 5V.

The following table shows suggested external resistor network values for the user range settings.

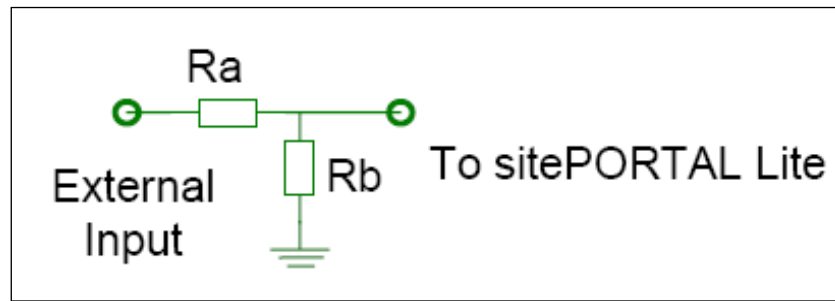


Figure 120 - External Resistor Network

2 x 5V = 10V	4 x 5V = 20V	10 x 5V = 50V	20 x 5V = 100V
$R_a = 10K\Omega$	$R_a = 30K\Omega$	$R_a = 90K\Omega$	$R_a = 190K\Omega$
$R_b = 10K\Omega$	$R_b = 10K\Omega$	$R_b = 10K\Omega$	$R_b = 10K\Omega$

Table 5 - Device Properties – Suggested External Resistor Network Values

APPENDIX B. TASC SITECOMMANDER CONFIGURATION

The TASC siteCOMMANDER is a hardware device that can be used in conjunction with siteVIEW. The device has its own firmware configuration that can be changed either using the siteCOMMANDER Configuration Utility (SCCU) or by using siteVIEW.

Some highlights of the siteCOMMANDER features include:

- Monitoring of 8 built in contact (digital) inputs.
- Monitoring of 8 built in analog inputs.
- Monitoring and control of 8 built in digital outputs.
- Support for adding and monitoring TASC Temperature Sensors.
- Device logging.
- Low power mode.
- Connectivity via RS232 and FFSK.

This section discusses how to change the siteCOMMANDER device settings.

Refer to the siteCOMMANDER User Manual (050-015-0002) for detailed instructions and examples of use of the siteCOMMANDER.

B.1. Description

The description tab contains the name and description of the device, which is used in siteVIEW.

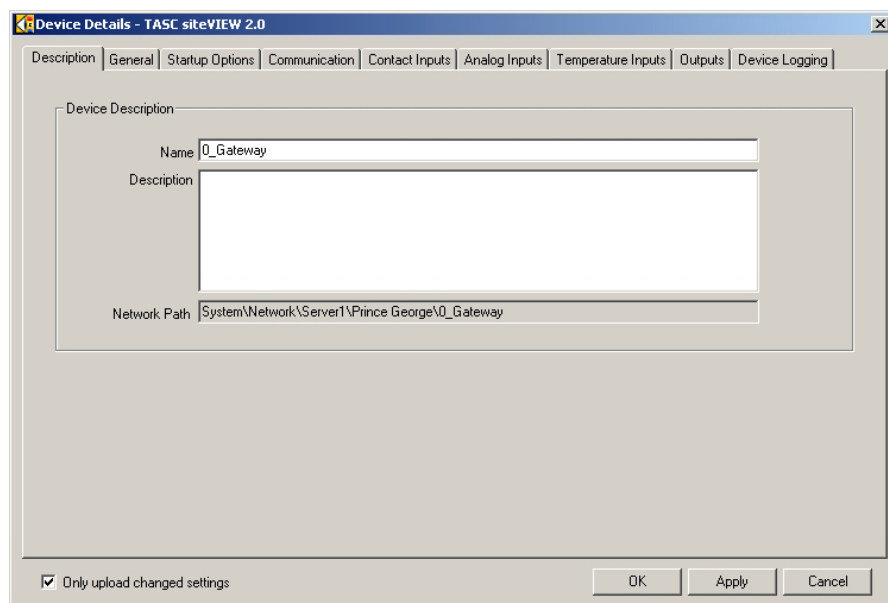


Figure 121 - Device Properties

B.2. General

The general tab contains read-only information about the device such as the device type, the device's internal firmware version, extra device options available and the number of temperature sensors that are attached to the device.

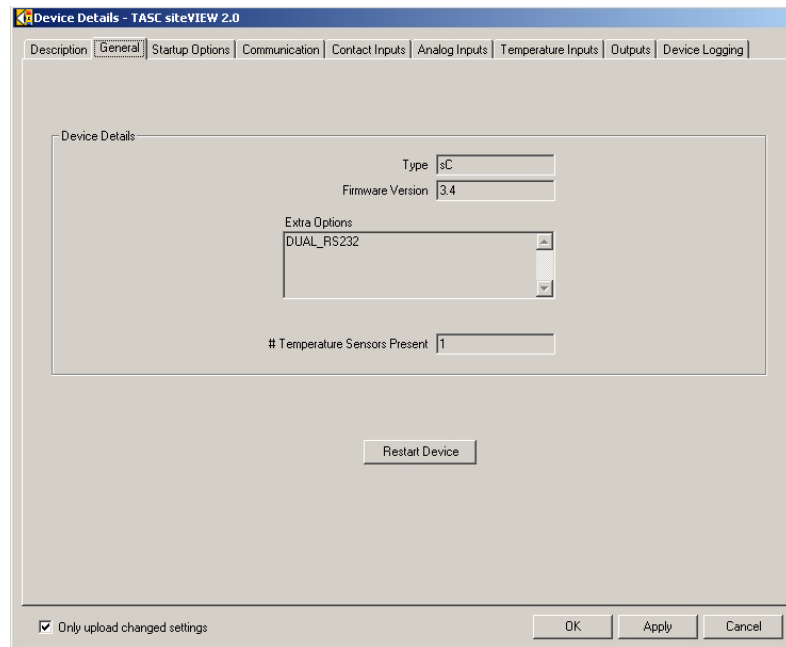


Figure 122 - Device Properties - General

The "Restart Device" button forces the device to reboot the firmware. This is useful if the device is not recognizing a new temperature sensor, because the siteCOMMANDER only scans for new temperature sensors at boot time.

B.3. Startup Options

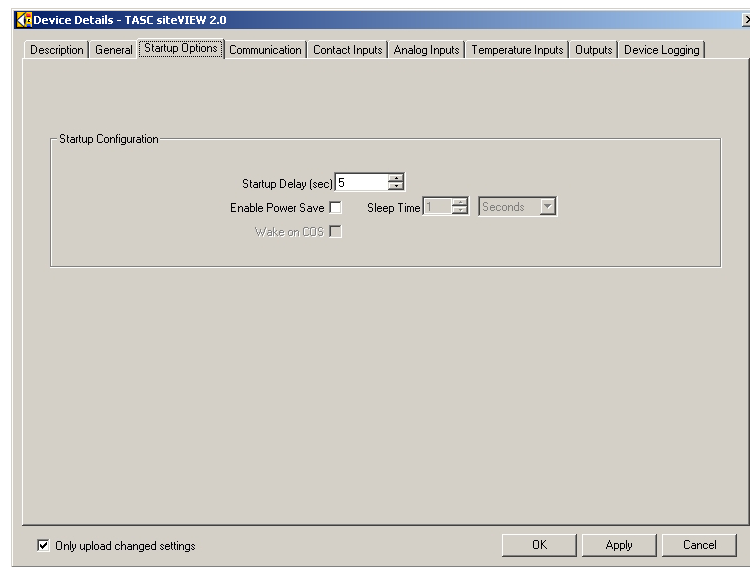


Figure 123 - Device Properties - Startup Options

The startup options tab contains configuration that pertain only to the startup of the device. The startup delay is the length of time in seconds that the device will wait after starting, before it begins monitoring. The enable power save option causes the device to switch into low power mode. When the device is in low power mode, it will have a sleep time. At the end of each sleep interval, the device will wake up and check its status. The wake on COS option causes the device to wake up out of low power mode when it detects a carrier operated squelch from the FFSK module.

B.4. Communication

Making changes to the communication form after the first communication has been established causes the communication configuration to be altered.

The device COM port specifies the COM port the device is to use as its primary COM port.

The module type of the device determines the role of the device. The following is a quick description of each mode:

Gateway: This mode is used on a single device to connect a network of siteCOMMANDERs to the siteVIEW APEX *TASC Communication Server*.

Master: This mode is used in point-to-point or point-to-multipoint applications not involving siteVIEW APEX products

Slave No Mapping: This mode is used for remote devices in siteVIEW APEX and non-siteVIEW APEX applications

Slave Input Mapping: This mode is used strictly for point-to-point or point-to-multipoint applications not involving siteVIEW APEX products

The COM port retry count decides how many times the device should send a message before giving up. The retry timeout determines how long to wait for a response after sending a packet.

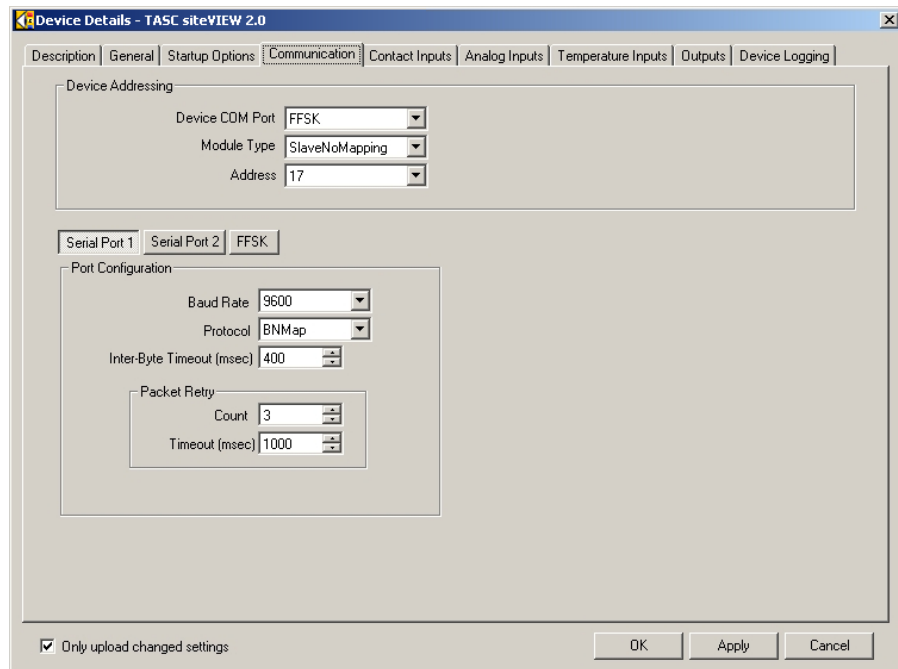


Figure 124 - Device Properties - Communication

Serial port 2 and the FFSK port can only be changed when siteVIEW APEX is in a local connection with the device. This is to ensure that siteVIEW APEX does not lose connectivity with the device it is configuring. To configure serial port 2 and the FFSK port siteVIEW APEX must connect to the device locally.

See Recommended Communication Timing Parameters, Table 2 – Recommended Communication Timing Parameters, on page 61, for recommended timing parameters.

Device Details - TASC siteVIEW 2.0

Description | General | Startup Options | **Communication** | Contact Inputs | Analog Inputs | Temperature Inputs | Outputs | Device Logging

Device Addressing

Device COM Port: FFSK

Module Type: SlaveNoMapping

Address: 17

Serial Port 1 | Serial Port 2 | **FFSK**

Port Configuration

Baud Rate: 2400

Protocol: BinMP

Channel Clear Delay (msec): 150

Packet Retry

Count: 5

Timeout (msec): 1000

Concatenate Packets: ☐

Push To Talk

Delay (msec): 15

Polarity: Low

Output Level: 31

PTT Test

COR/COS/M-SIG

Type: External Sig

Polarity:

Bytes of Preamble: 3

☒ Only upload changed settings

OK Apply Cancel

Figure 125 - Device Properties - FFSK Communication

B.5. Contact Inputs

If *Enable Event* is selected for a contact input, the device will notify siteVIEW APEX whenever the input is turned on or off. The off state specifies if the input is normally in the open state or if it is normally closed. The state that is specified as normal then becomes the off state of the device.

The input mode can be set as normal or toggle. If normal is selected, the input is edged triggered. If toggle is selected, the input is triggered based on levels; the input will alter its state on alternating positive levels.

	1	2	3	4	5	6	7	8	ALL
Enable Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Off State	Open	Open	Open	Open	Open	Open	Closed	Closed	
Input Mode	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal
Hold (secs)	1	1	1	1	1	1	1	1	1
Local Output	---	---	---	---	---	---	---	---	---
Output Delay	0	0	0	0	0	0	0	0	0
Output Action	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal

☒ Only upload changed settings

OK Apply Cancel

Figure 126 - Device Properties - Contact Inputs

By selecting a local output, an input can be set such that when the input is turned on, an output is turned on and when the input is turned off that same output is then turned off.

The hold time specifies the amount of time the input must stay on before the output will be turned on or off. The local output specifies the output to be turned on and off. The output delay indicates how long the device should wait before turning on the local output.

The output action can be normal, set or reset. If the output action is normal, then the output turns on when the input is turn on and the output turns off when the input is turned off. If the output action is set, then the output is turned on when the input is turned on, but the output is unaffected when the input is turned off. Reset causes the output to be turned off when the input is turned on, but is unaffected when the input is turned off.

B.6. Analog Inputs

If enable event is selected for an analog input, the device will notify siteVIEW APEX whenever the input crosses either the low or high threshold voltage.

The range indicates the analog input type that is connected to the device. If this value is not set correctly, siteVIEW APEX may report invalid analog input information.

Various sensors are available that attach to the analog input. If a sensor is connected to an analog input use the sensor drop down list to specify which sensor is present.

The units will change automatically depending on the range and sensor that are selected.

The analog formula and Hi & Low adjusted values allow an analog input to be formatted using an equation (For more information see Extra Device Configuration on page 78).

The offset value allows an analog's value to be adjusted by the specified amount.

By selecting a local output, an analog input is set such that when the input voltage goes above the high threshold, an output is turned on and when the input voltage goes below the high threshold that same output is then turned off. An output can be assigned to both the high and low thresholds and the same output can be used for both or a different output can be used.

Selecting the invert set points option causes the assigned output to turn on when the voltage goes below the high threshold voltage and above the low threshold voltage. The same output turns off when the voltage goes above the high threshold or below the low threshold. Only the low output is used when the set points are inverted.

The hold time specifies the amount of time the analog input must stay above or below the threshold before the output will be turned on or off. The local output specifies the output to be turned on and off. The output delay indicates how long the device should wait before turning on the local output.

The screenshot displays the 'Device Details - TASC siteVIEW Enterprise 2.0' window with the 'Analog Inputs' tab selected. The interface is organized into several sections for configuring 8 individual analog inputs and an 'ALL' option.

- Enable Events:** Checkboxes for each input (1-8) and 'ALL' are present.
- Invert Set Points:** A checkbox for each input and 'ALL'.
- Range:** Dropdown menus for each input, all set to '0-25.0V'.
- Sensor:** Dropdown menus for each input, all set to 'None'.
- Offset:** Numerical input fields for each input, all set to '0.0'.
- Units:** A dropdown menu for each input, all set to 'Volts'.
- Formula:** A dropdown menu for each input, all set to 'None'.
- High Threshold Set Points:**
 - Threshold:** Numerical input fields, all set to '4.0'.
 - Adjusted:** Numerical input fields, all set to '4.0'.
 - Hold (secs):** Numerical input fields, all set to '1'.
 - Local Output:** Dropdown menus, all set to 'None'.
 - Output Delay:** Numerical input fields, all set to '0'.
- Low Threshold Set Points:**
 - Threshold:** Numerical input fields, all set to '2.0'.
 - Adjusted:** Numerical input fields, all set to '2.0'.
 - Hold (secs):** Numerical input fields, all set to '1'.
 - Local Output:** Dropdown menus, all set to 'None'.
 - Output Delay:** Numerical input fields, all set to '0'.

At the bottom, there is a checkbox for 'Only upload changed settings' and buttons for 'OK', 'Apply', and 'Cancel'.

Figure 127 - Device Properties - Analog Inputs

The siteCOMMANDER module cannot accept voltages on its inputs that are negative with respect to ground. Application of negative voltages to the digital and analog inputs will damage the module.

The module provides fixed input ranges of 0-5 VDC and 0-25 VDC depending on jumper settings. Four user ranges of X2, X4, X10 and X20 can also be programmed based on a 5.12 VDC internal reference.

B.7. Temperature Inputs

If enable event is selected for a temperature input, the device will notify siteVIEW APEX whenever the input crosses either the low or high threshold temperature.

The device may have zero to eight temperature sensors present. The present indicator lets the user know which sensor is available for configuration.

The temperature units field specifies which temperature scale to use for calculating values related to the temperature input.

By selecting a local output, a temperature input can be set such that when the input temperature goes above the high threshold, an output is turned on and when the input temperature goes below the low threshold an output is then turned off.

The hold time specifies the amount of time the temperature input must stay above or below the threshold before the output will be turned on or off, and it is also the time before the event will be reported to siteVIEW. The local output specifies the output to be turned on and off. The output delay indicates how long the device should wait before turning on the local output.

Device Details - TASC siteVIEW 2.0

Description | General | Startup Options | Communication | Contact Inputs | Analog Inputs | Temperature Inputs | Outputs | Device Logging

Temperature Input Configuration

	1	2	3	4	5	6	7	8	ALL
Enable Events	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Present	No	Yes	No	No	No	No	No	No	
Units	Celcius	Farenheit	Celcius	Celcius	Celcius	Celcius	Celcius	Celcius	
High Temperature Set Points									
Threshold	40.0	104.0	40.0	40.0	40.0	40.0	40.0	40.0	
Hold (secs)	1	1	1	1	1	1	1	1	1
Local Output	---	---	---	---	---	---	---	---	
Output Delay	0	0	0	0	0	0	0	0	0
Low Temperature Set Points									
Threshold	0.0	32.0	0.0	0.0	0.0	0.0	0.0	0.0	
Hold (secs)	1	1	1	1	1	1	1	1	1
Local Output	---	---	---	---	---	---	---	---	
Output Delay	0	0	0	0	0	0	0	0	0

☒ Only upload changed settings

OK Apply Cancel

Figure 128 - Device Properties - Temperature Inputs

B.8. Outputs

The off state specifies if the output is normally in the open state or if it is normally closed. The state that is specified as normal then becomes the off state of the device.

The output mode can be set as latch or pulse. If *Latch* is selected, when the output is turned on it is left on until the output is turned off again. If pulse is selected, when the output is turned on the output only stays on for the length of times specified by the pulse width.

	1	2	3	4	5	6	7	8	ALL
Off State	Open	Open	Open	Open	Open	Open	Open	Open	Open
Output Mode	Latch	Pulse	Latch	Latch	Latch	Latch	Latch	Latch	
Pulse Width (mS)	0	10	0	0	0	0	0	0	

☒ Only upload changed settings

OK Apply Cancel

Figure 129 - Device Properties - Outputs

B.9. Device Logging – Configuration

The log roll over determines what the device will do when its log file becomes full. If log roll over is enabled, the device will overwrite the oldest log entry to create a new one. If log roll over is not enabled, the device will stop logging when the data logger buffer is full.

Selecting power up run ensures the data logger starts automatically whenever the device starts up.

Figure 130 - Device Properties - Device Logging

The data logger logs sample data at selected intervals and it logs min/max data for selected inputs. The buffer allocation determines how much of the data logger buffer is allocated to each data logger type.

The enabled option determines if the selected input is included when logging. The analog and temperature inputs have a log thresholds option that will cause the data logger to log each time the input's value crosses its high or low threshold.

The input qualifier causes the input value to only be logged when the assigned input qualifier is on. So the input qualifier causes the analog or temperature threshold changes to be ignored if the input qualifier is off. In other words, when an analog or temperature input crosses a threshold, the value will only be logged if the assigned input qualifier is on.

The contact inputs can be logged each time they are turned on or off, or they can be logged as accumulative on times.

B.10. Device Logging – Downloading To siteVIEW

Once device logging configuration has been setup, close the device properties form and open the Device Data Logger form for the selected device, by selecting “Edit->Data Logger” from the main menu.

The Device Data Logger form can be used to stop and start the device logger, download the logs, clear the logs, view the contact input accumulation timers and clear the contact input accumulation timers.

To see the status of the device logger, press the “Refresh” button in the “Data Logger Details” group box. If the data logger is stopped, the start time will be unavailable and the log counts will be empty. Once the data logger is started, the device will begin to store sample and min/max logs based on which inputs the device is configured to log.

Figure 131 - Device Data Logger



Note: The threshold logs are saved and downloaded along with the Min/Max Log.

The device has 9 timers that are stored on the device’s real time clock. If logging of these accumulator timers was enabled for the corresponding contact input then the device will increment the timers for every second that the input is in the on position. These timers are updated even when the device data logger is stopped.

The last update time shows the last time that siteVIEW APEX downloaded these values from the device. Press the “Refresh” button in the “Timers” group box to download the current accumulator timer values.

Selecting the checkbox beside the timer and then pressing the “Clear” button will reset the corresponding timer back to zero.

The maximum accumulator timer values are 16,777,215 seconds (194 days), after which the timer will roll over back to zero.

The COS timer increments on receipt of the externally supplied carrier detect signal via the optional FFSK module. The time that carrier is present (the signal is active), is added to the COS accumulator. The accumulator accuracy is in seconds. To enable tracking of the COS accumulator, select open the Device Properties form, select the Device Logging tab and check the “Log Airtime” box.

For more information on setting up specific logging on specific inputs, see the previous section Device Logging – Configuration.

Manually Downloading Device Logs

Once the sample log or min/max log have a record count greater than zero, press the download button to manually download the data. The data will be downloaded in chunks, so depending on how much data has been stored it could take several packets to download all the data. Once all the data has been downloaded, siteVIEW APEX will automatically clear the log. You may clear the logs manually by pressing the “Clear Log” button for the corresponding log. Stopping and starting the data logger will also clear the log data, but the “Clear Log” button will clear the log without stopping the data logger.

Automatically Downloading Device Logs

To setup automatic downloading of the sample log, create a scheduled poll for the device that checks the sample log count. If the sample log count is greater than zero, siteVIEW APEX will automatically download and clear the sample log. Similarly, to setup automatic downloading of the min/max and threshold logs, create a scheduled poll that checks the min/max log count. If the min/max log count is greater than zero, siteVIEW APEX will automatically download and clear the min/max and threshold logs.

APPENDIX C. TASC SITEPORTAL LITE CONFIGURATION

The TASC sitePORTAL Lite is a hardware device that can be used in conjunction with siteVIEW. The device has its own firmware configuration that can be changed either using the sitePORTAL Configuration Utility (SPCU) or by using siteVIEW.

Some highlights of the sitePORTAL Lite features include:

- Monitoring of 8 built in contact inputs, plus support for adding TASC Contact Input expansion boards.
- Monitoring of 8 built in analog inputs, plus support for adding TASC Analog Input expansion boards.
- Monitoring and control of 8 built in digital outputs.
- Support for adding and monitoring TASC Temperature Sensors.
- 1-2 peripheral pass-through ports.
- Connectivity via TCP/IP, IP Modem, PSTN Modem and RS232.

This section discusses how to change the sitePORTAL Lite device settings.

Refer to the sitePORTAL Lite User Manual (050-015-0012) for detailed instructions and examples of use of the sitePORTAL Lite.

C.1. Description

The description tab contains the name and description of the device, which is used in siteVIEW. As well the device login username and password that siteVIEW APEX will use to connect to the device can be changed on this page.

The screenshot shows a software window titled "Device Details - TASC siteVIEW 2.0". It has a tabbed interface with the "Description" tab selected. Other tabs include "General", "Call & Modem Control", "Contact Inputs", "Analog Inputs", "Temperature Inputs", "Outputs", "Site Information", and "Peripherals".

Under the "Device Description" section, there are three input fields: "Name" (containing "sPL 1"), "Description" (empty), and "Network Path" (containing "System\Network\Server1\Prince George\sPL 1").

Below this is a "Login" section with three input fields: "Username" (containing "sview"), "Password" (containing "****"), and "Retype Password" (containing "****").

At the bottom left, there is a checkbox labeled "Only upload changed settings" which is checked. At the bottom right, there are three buttons: "OK", "Apply", and "Cancel".

Figure 132 - Device Details - Description

C.2. General

The general tab contains read-only information about the device such as the device type, the device's internal firmware version, extra device options available, analog and contact input expansion boards attached to the device and the number of temperature sensors that are attached to the device.

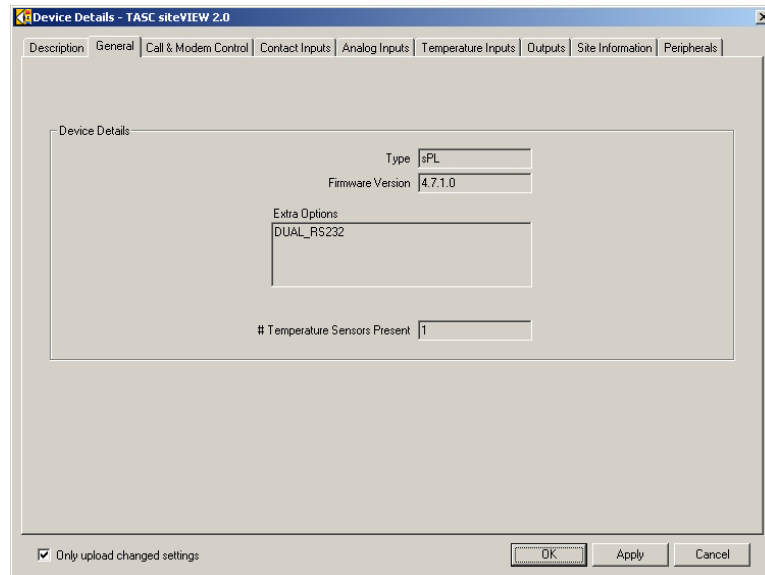


Figure 133 - Device Details - General

C.3. Call & Modem Control

The call & modem control tab is used to configure connection settings.

C.3.1. Call Control

The *Peripheral Inactivity Time* is the length of inactivity in minutes that the sitePORTAL Lite will wait before disconnecting from the peripheral device and returning to regular monitoring mode.

User login Inactivity is the length of inactivity time in minutes the sitePORTAL Lite will wait before disconnecting from siteVIEW.

The *Login Time* is the amount of time in seconds that a remote application has to enter in the login credentials before the sitePORTAL Lite will disconnect the connection. *Attempts* is the number of unsuccessful login tries the remote application has before the sitePORTAL Lite enters a state of hacker guard, where no one can log in for the amount of time specified in the field name Recycle Time.

The *Inter-Byte Timeout* determines how long the com port should wait between incoming bytes before timing out.

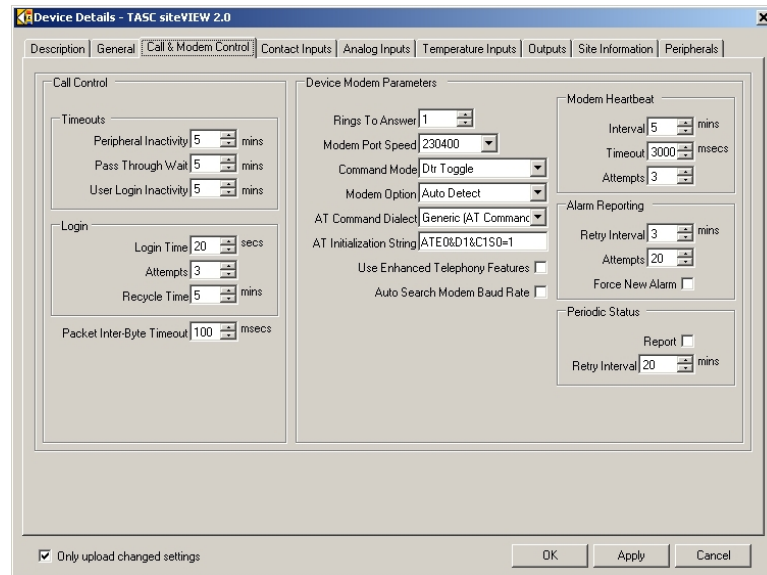


Figure 134 - Device Details – Call & Modem Control

C.3.2. Device Modem Parameters

Rings To Answer specifies the number of rings before a modem will answer a call.

Modem Port Speed is the baud rate that the modem will operate at.

Modem Option is the modem type: no modem, auto detect, internal or external.

AT Command Dialect offers support for a generic modem, but also a few other modem types.

AT Initialization String allows a user to enter a modem initialization string that the sitePORTAL Lite will use when it initializes the modem.

Use Enhanced Telephony Features enables or disables advanced features such as call cadence validation. The sitePORTAL Lite will then only answer calls with a specified ring cadence. The cadence of the ring to answer is set in the Site Phone Number field of the Site Information tab. This is only available if the optional plug in modem TASC PN 800-100-0046 is installed.

The ring cadence must be entered in the following format: [x,y,z], where x is the length in milliseconds of the first ring, y is the length of the pause between rings, and z is the length of the second ring. All times are in milliseconds. The cadence value is surrounded by square brackets, has commas separating cadence values, no

spaces between values, has three values, and all times are integer values. The sitePORTAL Lite will then only answer calls that have the specified ring cadence.

If the cadence value is not entered correctly, or is blank, sitePORTAL Lite will ignore all incoming calls. There is one exception, if the ring cadence is a star character surrounded by square brackets (i.e. [*]), then all calls will be answered.

Auto Search Modem Baud Rate causes the sitePORTAL Lite to attempt to find the baud rate of the incoming connection automatically.

Modem Heartbeat is how often the AT initialization sequence is sent to the modem to make sure it is online. The Timeout is the amount of time the sitePORTAL Lite waits to receive a response from the modem before it retries the initialization and Attempts is the number of retry attempts sitePORTAL Lite performs.

The *Alarm Reporting Retry Interval* is the time in minutes the sitePORTAL Lite will wait since an unsuccessful alarm report before it retries. *Attempts* is the number of unsuccessful alarm report retry attempts the sitePORTAL Lite will attempt before giving up. *Force New Alarm* sets the sitePORTAL Lite to report a new alarm even if previous alarm attempts have failed and are waiting for the retry interval to elapse. If Force New Alarm is not selected, new alarms will wait along with the other alarms.

Periodic Status Report sets the sitePORTAL Lite to periodically report its status to siteVIEW. The *Retry Interval* is how often the sitePORTAL Lite will attempt to report its status.

C.4. Contact Inputs

The sitePORTAL Lite comes with 8 built in contact inputs, but can be expanded with a maximum of 4 TASC digital expansion boards, each with 8 contact inputs, allowing a maximum of 40 contact inputs.

If *Enable Event* is selected for a contact input, the device will notify siteVIEW APEX whenever the input is turned on or off. The off state specifies if the input is normally in the open state or if it is normally closed. The state that is specified as normal then becomes the off state of the device.

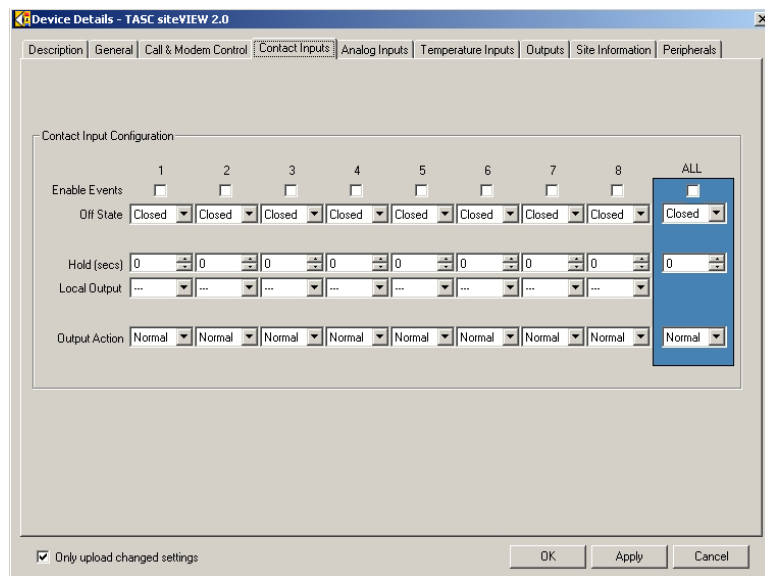


Figure 135 - Device Properties – Contact Inputs

By selecting a local output, an input can be set such that when the input is turned on, an output is turned on and when the input is turned off that same output is then turned off.

The hold time specifies the amount of time the input must stay on before the output will be turned on or off. The local output specifies the output to be turned on and off. The output delay indicates how long the device should wait before turning on the local output.

The output action can be normal, set or reset. If the output action is normal, then the output turns on when the input is turned on and the output turns off when the input is turned off. If the output action is set, then the output is turned on when the input is turned on, but the output is unaffected when the input is turned off. Reset causes the output to be turned off when the input is turned on, but is unaffected when the input is turned off.

C.5. Analog Inputs

The sitePORTAL Lite comes with 8 built in analog inputs, but can be expanded with a maximum of 2 TASC Analog Expansion boards, each with 8 analog inputs, allowing a maximum of 24 analog inputs.

If enable event is selected for an analog input, the device will notify siteVIEW APEX whenever the input crosses either the low or high threshold voltage.

The range indicates the analog input type that is connected to the device. If this value is not set correctly, siteVIEW APEX may report invalid analog input information.

Various sensors are available that attach to the analog input. If a sensor is connected to an analog input, use the sensor drop down list to specify which sensor is present.

The units will change automatically depending on the range and sensor that are selected.

The analog formula and Hi & Low adjusted values allow an analog input to be formatted using an equation (For more information see Extra Device Configuration on page 78).

The offset value allows an analog's value to be adjusted by the specified amount.

The input qualifier causes the analog threshold changes to be ignored if the input qualifier is off. In other words, when an analog input crosses a threshold, the value will only be reported to siteVIEW APEX if the assigned input qualifier is on.



Inputs 1 through 8 should be used if the analog has a hold time of 1 second (default hold time). Inputs greater than 8 should be used as qualifiers only if the analog hold time is greater than 2 seconds.

By selecting a local output, an analog input can be set such that when the input voltage goes above the high threshold, an output is turned on and when the input voltage goes below the low threshold that same output is then turned off.

Figure 136 - Device Properties – Analog Inputs

The hold time specifies the amount of time the analog input must stay above or below the threshold before the output will be turned on or off. The local output

specifies the output to be turned on and off. The output delay indicates how long the device should wait before turning on the local output. The output action offers several conditions for when the local output will turn on or off based on the analog voltage.

The sitePORTAL Lite module cannot accept voltages on its inputs that are negative with respect to ground. Application of negative voltages to the digital and analog inputs will damage the module.

The module provides fixed input ranges of 0-5 VDC and 0-25 VDC depending on jumper settings. Four user ranges of X2, X4, X10 and X20 can also be programmed based on a 5.12 VDC internal reference.

C.6. Temperature Inputs

If *Enable Event* is selected for a temperature input, the device will notify siteVIEW APEX whenever the input crosses either the low or high threshold temperature.

Figure 137 - Device Properties – Temperature Inputs

The device may have zero to eight temperature sensors present. The present indicator lets the user know which sensor is available for configuration.

The temperature units field specifies which temperature scale to use for calculating values related to the temperature input.

The input qualifier causes the temperature threshold changes to be ignored if the input qualifier is off. In other words, when a temperature input crosses a threshold, the value will only be reported to siteVIEW APEX if the assigned input qualifier is on.



Inputs 1 through 8 should be used if the analog has a hold time of 1 second (default hold time). Inputs greater than 8 should be used as qualifiers only if the analog hold time is greater than 2 seconds.

The hold time specifies the amount of time the temperature input must stay above or below the threshold before the event is reported to siteVIEW.

C.7. Outputs

The off state specifies if the output is normally in the open state or if it is normally closed. The state that is specified as normal then becomes the off state of the device.

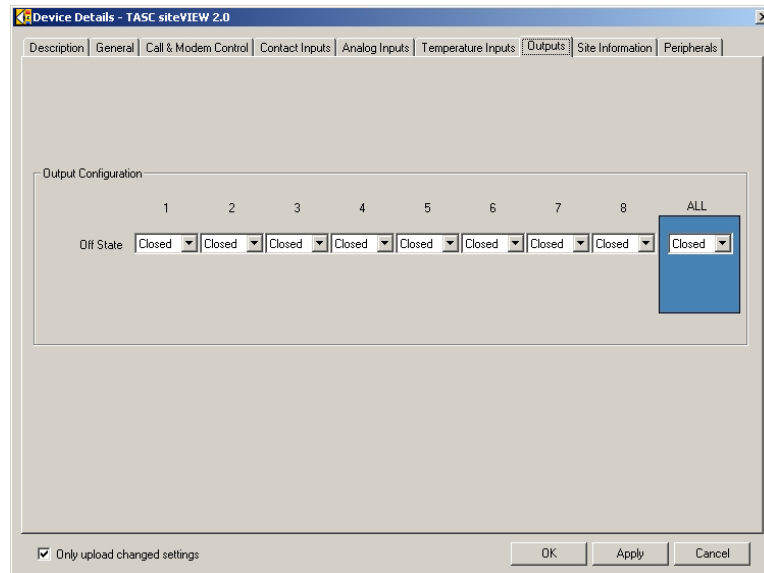
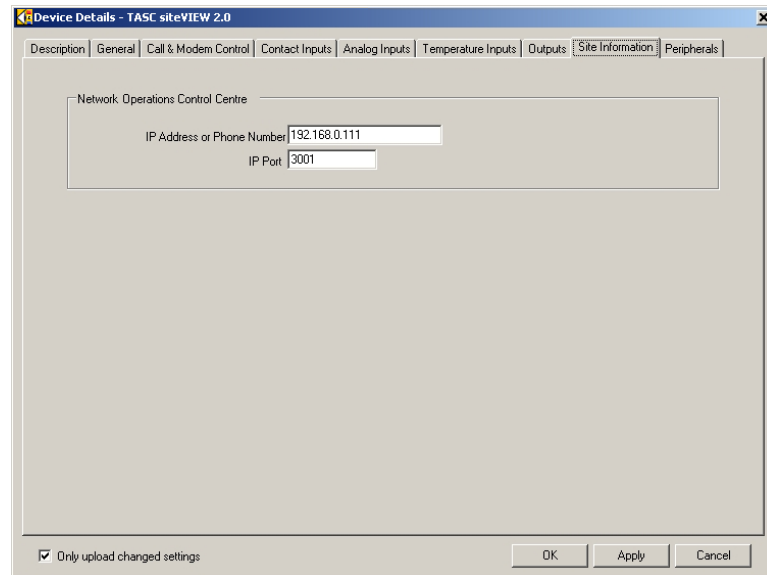


Figure 138 - Device Properties – Outputs

C.8. Site Information

When an I/O event occurs, the sitePORTAL Lite will attempt to report the event to siteVIEW. The Network Operations Control Center information must be supplied in order for the sitePORTAL Lite to properly know how to connect to siteVIEW. Enter the IP Address and IP Port if the device is connected to siteVIEW APEX via Ethernet, or supply the phone number if the device is connected via a PSTN modem.



The screenshot shows a window titled "Device Details - TASC siteVIEW 2.0". It has a tabbed interface with the following tabs: Description, General, Call & Modem Control, Contact Inputs, Analog Inputs, Temperature Inputs, Outputs, Site Information (selected), and Peripherals. The "Site Information" tab contains a section titled "Network Operations Control Centre" with two input fields: "IP Address or Phone Number" containing "192.168.0.111" and "IP Port" containing "3001". At the bottom of the window, there is a checkbox labeled "Only upload changed settings" which is checked, and three buttons: "OK", "Apply", and "Cancel".

Figure 139 - Device Properties – Site Information

C.9. Peripherals

The sitePORTAL Lite has two serial ports that can be used to connect third-party hardware to the sitePORTAL Lite. Peripheral 2 is only available when the primary communication channel to the sitePORTAL Lite is either Ethernet or a PSTN modem, thereby freeing the second serial port.

Third-party software can then connect to the device by having the sitePORTAL Lite into pass-through mode. Then siteVIEW APEX will open a virtual serial port that the third-party software can communicate with. siteVIEW APEX will then pass on any data it receives from the virtual port on to the sitePORTAL Lite, which will pass the data on to the peripheral device. Data from the peripheral device is passed on to the third-party application in the same way.

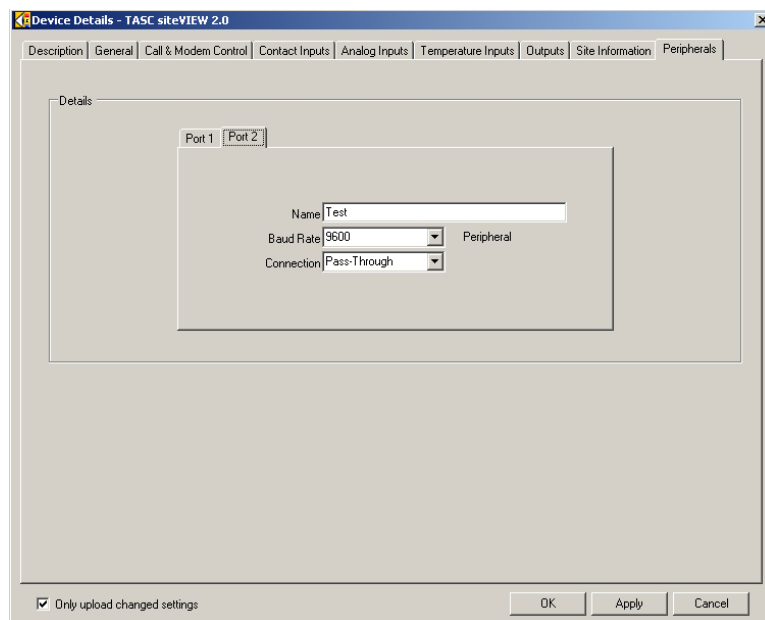


Figure 140 - Device Properties – Peripherals

Set the name of the connected peripheral device and the baud rate it expects to communicate at. Then select “Edit->Passthrough” from the main menu in siteVIEW APEX to start peripheral pass-through.

C.10. Peripheral Pass-through in siteVIEW

Once a device is setup for peripheral pass-through, connect to that device. Once connected right click on the device’s network tree node and select “Pass-through” and then the peripheral that you would like to connect to.

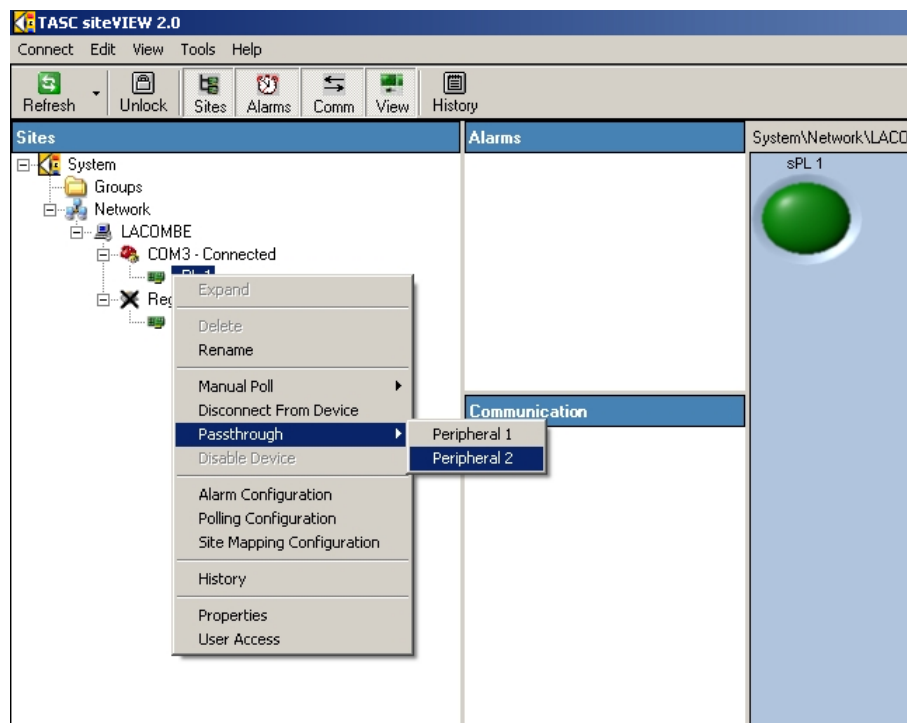


Figure 141 – Starting Peripheral Pass-through

Once the peripheral connection has begun, siteVIEW APEX will launch a program that will create a virtual COM port and facilitate a connection to the peripheral device and any application that connects to the virtual port. Once the connection is established, use the peripheral device's configuration software to connect to the virtual COM port.

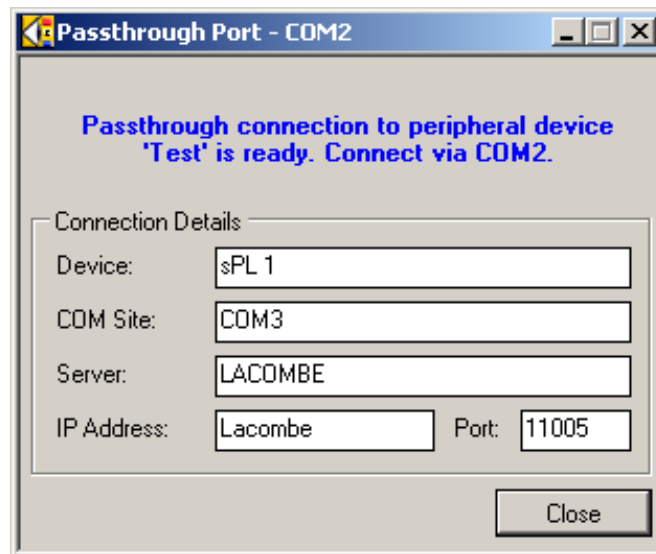


Figure 142 – Peripheral Pass-through Connection Waiting

In the figure above, siteVIEW APEX selected COM2 as the virtual port because it was the first port available. Once a program then connects to COM2, the pass-through port window then hides itself. If the program then releases the COM port, the pass-through port window then becomes visible again. Closing the pass-through port window releases the pass-through connection and siteVIEW APEX closes the connection to the device. If the pass-through connection sits connected for too long without passing any data to or from the device, then eventually the device will disconnect after the peripheral inactivity timeout has expired and the pass-through port window will be closed.

APPENDIX D. TASC SITERSM CONFIGURATION

The TASC siteRSM is a hardware device that can be used in conjunction with siteVIEW. The device has its own firmware configuration that can be changed either using the siteCOMMANDER Configuration Utility (SCCU) or by using siteVIEW.

Some highlights of the siteRSM features include:

- Monitoring of 8 built in contact inputs, plus support for adding TASC Contact Input expansion boards.
- Monitoring of 8 built in analog inputs, plus support for adding TASC Analog Input expansion boards.
- Monitoring and control of 8 built in digital outputs.
- Support for adding and monitoring TASC Temperature Sensors.
- Connectivity via RS232 or Ethernet.
- Low power mode.

This section discusses how to change the siteRSM device settings.

Refer to the siteRSM User Manual (050-015-0052) for detailed instructions and examples of use of the siteRSM.

D.1. Description

The description tab contains the name and description of the device, which is used in siteVIEW.

The screenshot shows the 'Device Details - TASC siteVIEW 2.0' window with the 'Description' tab selected. The window has a tabbed interface with 'Description', 'General', 'Communication', 'Contact Inputs', 'Analog Inputs', 'Temperature Inputs', and 'Outputs'. The 'Device Description' section contains three fields: 'Name' with the value 'siteRSM 1', 'Description' (empty), and 'Network Path' with the value 'System\Network\Server1\Prince George\siteRSM 1'. At the bottom, there is a checkbox labeled 'Only upload changed settings' which is checked, and three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 143 - Device Details - Description

D.2. General

The general tab contains read-only information about the device such as the device type, the device's internal firmware version, extra device options available, analog and contact input expansion boards attached to the device and the number of temperature sensors that are attached to the device.

The screenshot shows the 'Device Details - TASC siteVIEW 2.0' window with the 'General' tab selected. The window has a tabbed interface with 'Description', 'General', 'Communication', 'Contact Inputs', 'Analog Inputs', 'Temperature Inputs', and 'Outputs'. The 'Device Details' section contains several fields: 'Type' with the value 'siteRSM', 'Firmware Version' with the value '4.7.1.0', 'Extra Options' with the value 'DUAL_RS232', and '# Temperature Sensors Present' with the value '1'. At the bottom, there is a checkbox labeled 'Only upload changed settings' which is checked, and three buttons: 'OK', 'Apply', and 'Cancel'.

Figure 144 - Device Details - General

D.3. Communication Settings

Making changes to the communication form after the first communication has been established causes the communication configuration to be altered.

The device COM port specifies the COM port the device is to use as its primary COM port.

The module type of the device operates like a siteCOMMANDER in slave no mapping mode, which is used for remote devices in both siteVIEW APEX and non-siteVIEW APEX applications.

The COM port packet retry count decides how many times the device should send a message before giving up. The packet retry timeout determines how long to wait for a response after sending a packet. The inter-byte timeout determines how long the com port should wait between incoming bytes before timing out.

Serial port 2 can only be changed when siteVIEW APEX is in a local connection with the device. This is to ensure that siteVIEW APEX does not lose connectivity with the device it is configuring. To configure serial port 2 siteVIEW APEX must connect to the device locally.

See Recommended Communication Timing Parameters, Table 2 – Recommended Communication Timing Parameters, on page 61, for recommended timing parameters.

Device Details - TASC siteVIEW 2.0

Description | General | **Communication** | Contact Inputs | Analog Inputs | Temperature Inputs | Outputs

Device Addressing

Device COM Port: SerialPort2

Module Type: SlaveNoMapping

Address: 1

Serial Port 1 | **Serial Port 2**

Port Configuration

Baud Rate: 9600

Protocol: BinMP

Inter-Byte Timeout (msec): 300

Packet Retry

Count: 5

Timeout (msec): 500

☒ Only upload changed settings

OK Apply Cancel

Figure 145 - Device Details – Communication

D.4. Contact Inputs

The siteRSM comes with 8 built in contact inputs, but can be expanded with a maximum of 4 TASC digital expansion boards, each with 8 contact inputs, allowing a maximum of 40 contact inputs.

If *Enable Event* is selected for a contact input, the device will notify siteVIEW APEX whenever the input is turned on or off. The off state specifies if the input is normally in the open state or if it is normally closed. The state that is specified as normal then becomes the off state of the device.

By selecting a local output, an input can be set such that when the input is turned on, an output is turned on and when the input is turned off that same output is then turned off.

The hold time specifies the amount of time the input must stay on before the output will be turned on or off. The local output specifies the output to be turned on and off. The output delay indicates how long the device should wait before turning on the local output.

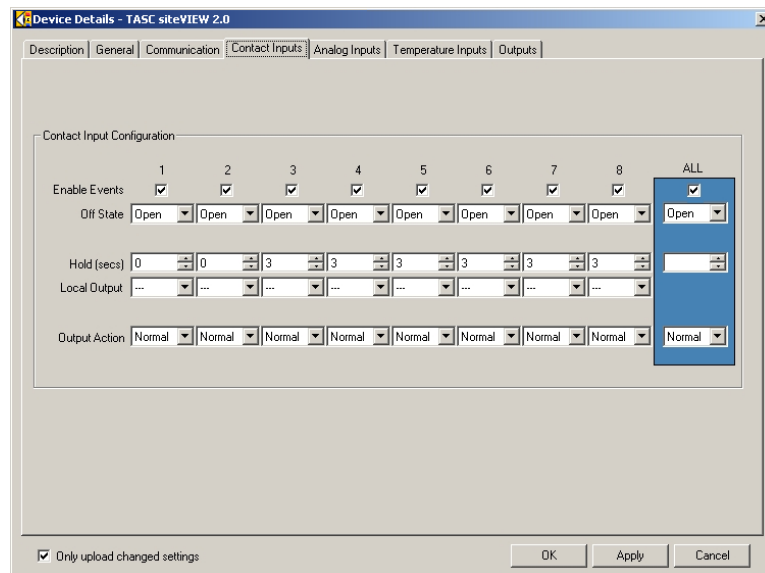


Figure 146 - Device Properties – Contact Inputs

The output action can be normal, set or reset. If the output action is normal, then the output turns on when the input is turned on and the output turns off when the input is turned off. If the output action is set, then the output is turned on when the input is turned on, but the output is unaffected when the input is turned off. Reset causes the output to be turned off when the input is turned on, but is unaffected when the input is turned off.

D.5. Analog Inputs

The siteRSM comes with 8 built in analog inputs, but can be expanded with a maximum of 2 TASC Analog Expansion boards, each with 8 analog inputs, allowing a maximum of 24 analog inputs.

If enable event is selected for an analog input, the device will notify siteVIEW APEX whenever the input crosses either the low or high threshold voltage.

The range indicates the analog input type that is connected to the device. If this value is not set correctly, siteVIEW APEX may report invalid analog input information.

Various sensors are available that attach to the analog input. If a sensor is connected to an analog input use the sensor drop down list to specify which sensor is present.



Selecting the TASC sensor will provide configure the sensor for use within siteVIEW. (Since most TASC sensors provide 5V input, they will not be visible unless the range selected is 0-5V.) Once the sensor is selected, the units will change automatically depending on the range and sensor that are selected.

The offset value allows an analog's value to be adjusted by the specified amount.

The analog formula and Hi & Low adjusted values allow an analog input to be formatted using an equation (For more information see Extra Device Configuration on page 78). Formulas may also be used with TASC sensors.

The input qualifier causes the analog threshold changes to be ignored if the input qualifier is off. In other words, when an analog input crosses a threshold, the value will only be reported to siteVIEW APEX if the assigned input qualifier is on.



Inputs 1 through 8 should be used if the analog has a hold time of 1 second (default hold time). Inputs greater than 8 should be used as qualifiers only if the analog hold time is greater than 2 seconds.

By selecting a local output, an analog input is set such that when the input voltage goes above the high threshold, an output is turned on and when the input voltage goes below the low threshold that same output is then turned off.

The hold time specifies the amount of time the analog input must stay above or below the threshold before the output will be turned on or off. The local output specifies the output to be turned on and off. The output delay indicates how long the device should wait before turning on the local output. The output action offers several conditions for when the local output will turn on or off based on the analog voltage.

The siteRSM module cannot accept voltages on its inputs that are negative with respect to ground. Application of negative voltages to the digital and analog inputs will damage the module.

The module provides fixed input ranges of 0-5 VDC and 0-25 VDC depending on jumper settings. Four user ranges of X2, X4, X10 and X20 can also be programmed based on a 5.12 VDC internal reference.

Device Details - TASC siteVIEW Enterprise 2.0

Description | General | Communication | Contact Inputs | Analog Inputs | Temperature Inputs | Outputs

Analog Input Configuration

	1	2	3	4	5	6	7	8	ALL
Enable Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Range	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V	0-25.0V
Sensor									
Offset	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	
Input Qualifier	---	---	---	---	---	---	---	---	
Units	Volts	Volts	Volts	Volts	Volts	Volts	Volts	Volts	Volts
Formula	-none-	-none-	-none-	-none-	-none-	-none-	-none-	-none-	-none-
High Threshold Set Points									
Threshold	12.0	12.0	12.0	12.0	12.0	12.0	12.0	12.0	12.0
Adjusted	12.0	12.0	12.0	12.0	12.0	12.0	12.0	12.0	12.0
Local Output	---	---	---	---	---	---	---	---	---
Low Threshold Set Points									
Threshold	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
Adjusted	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0	5.0
Local Output	---	---	---	---	---	---	---	---	---
Hold (secs)	1	1	1	1	1	1	1	1	1

☒ Only upload changed settings

OK Apply Cancel

Figure 147 - Device Properties – Analog Inputs

D.6. Temperature Inputs

If *Enable Event* is selected for a temperature input, the device will notify siteVIEW APEX whenever the input crosses either the low or high threshold temperature.

The device may have zero to eight temperature sensors present. The present indicator lets the user know which sensor is available for configuration.

The temperature units field specifies which temperature scale to use for calculating values related to the temperature input.

Figure 148 - Device Properties – Temperature Inputs

The input qualifier causes the temperature threshold changes to be ignored if the input qualifier is off. In other words, when a temperature input crosses a threshold, the value will only be reported to siteVIEW APEX if the assigned input qualifier is on.



Inputs 1 through 8 should be used if the analog has a hold time of 1 second (default hold time). Inputs greater than 8 should be used as qualifiers only if the analog hold time is greater than 2 seconds.

The hold time specifies the amount of time the temperature input must stay above or below the threshold before the event is reported to siteVIEW.

By selecting a local output, a temperature input is set such that when the input temperature goes above the high threshold, an output is turned on and when the input temperature goes below the low threshold, an output is then turned off.

D.7. Outputs

The off state specifies if the output is normally in the open state or if it is normally closed. The state that is specified as normal then becomes the off state of the device.

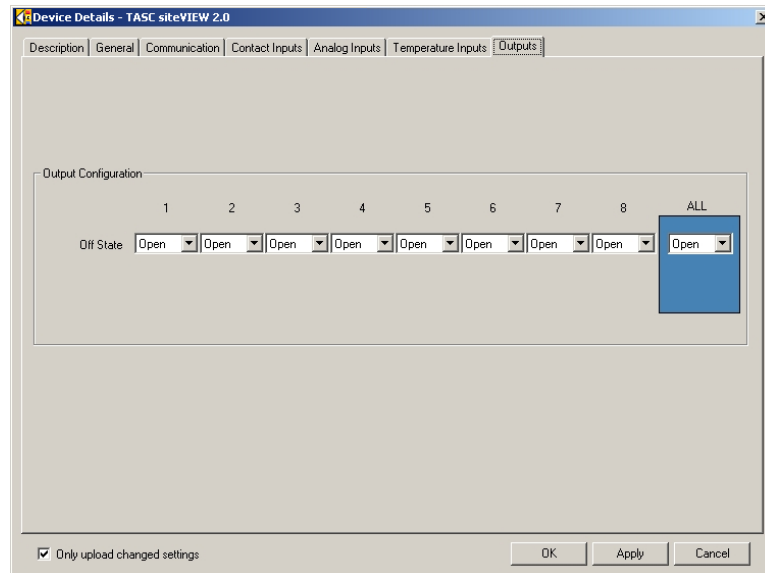


Figure 149 - Device Properties – Outputs

APPENDIX E. SUMMIT CONFIGURATION

The Summit is a hardware platform that can be used in conjunction with siteVIEW Apex. Summit uses the Crest web administration tool for configuration.

Some highlights of the Summit features include:

- Monitoring of 48 built in contact inputs.
- Monitoring of 32 built in analog inputs.
- Monitoring and control of 16 built in digital outputs.
- Monitoring and control of 8 built in analog outputs.
- Monitoring and control of 8 serial ports (configurable as RS-232/485/422)
- Ability to manage ping devices (e.g., for Kenwood Trunking system control)
- Ability to send events via SNMP, SMTP

Refer to the Summit User manual (050-015-0112) for detailed configuration instructions.

E.1.Description

The description tab contains the name and description of the device, which is used in siteVIEW Apex.

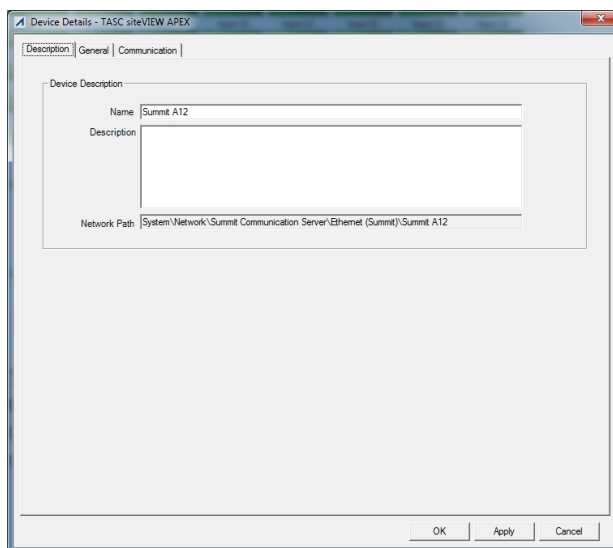


Figure 150 - Device Details - Description

E.2.General

The general tab contains read-only information about the device such as the device type, the device's internal firmware version, extra device options available, analog and contact input expansion boards attached to the device and the number of temperature sensors that are attached to the device.

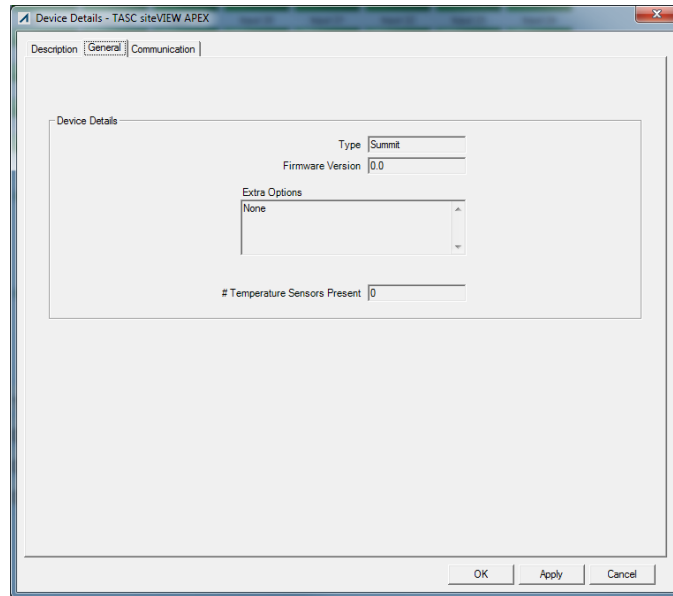


Figure 151 - Device Details - General

E.3.Communication Settings

Making changes to the communication form after the first communication has been established causes the communication configuration to be altered.

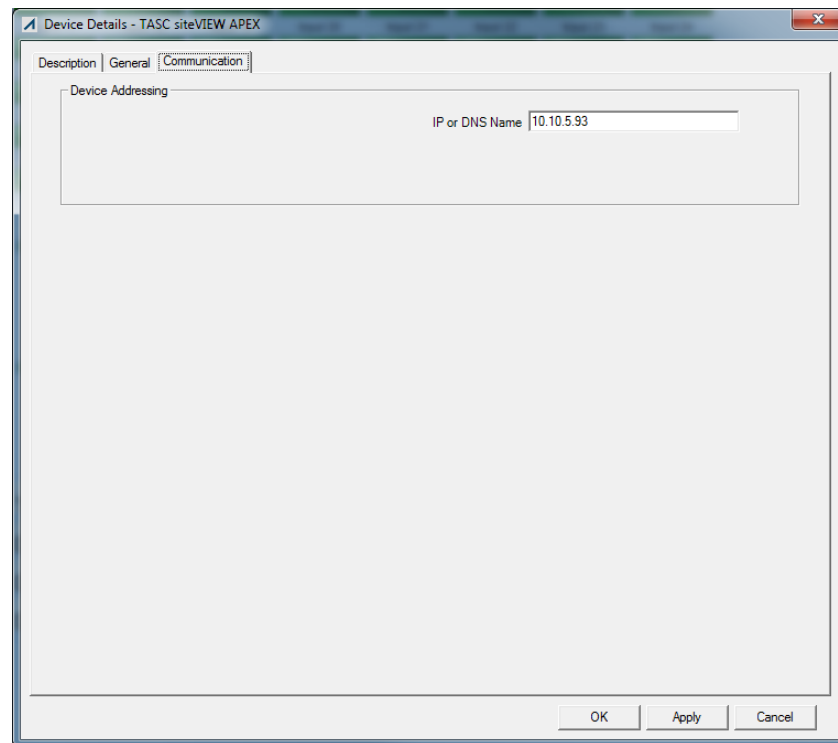


Figure 152 - Device Details - Communication

APPENDIX F. PING DEVICE CONFIGURATION

Ping devices work in a similar manner as the widely used [Ping networking utility](#) which is used to test the reachability of a host on an Internet Protocol (IP) network.

siteVIEW APEX Ping devices can be used to determine whether an IP device is available or “up and running”.

F.1.Adding Ping Devices

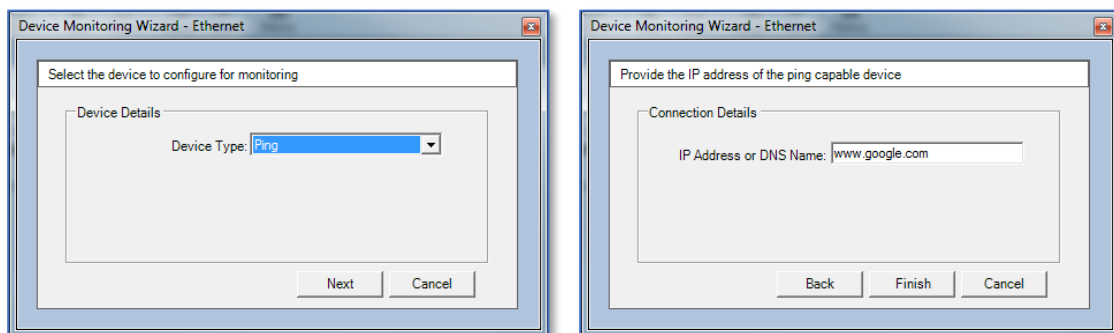
Before adding Ping device, an Ethernet communication port must be added. Ping devices cannot be added to Serial communication ports.

To add a Ping device, use the Edit – Add Device function or right-click on the Ethernet communication port and select Add Device. The resulting Device Monitoring Wizard is used to define the Ping device’s properties:

For the Device Details section, select Ping as the Device Type, then select Next

For the Device Identification section, enter a user-friendly name describing the Ping device in the Name field. Optionally, add additional long-form information within the Description field, then select Next.

For the Connection Details, enter an IP (IPv4) address or a DNS name for the device. siteVIEW APEX will automatically resolve a DNS name to the IPv4 address of the device. Then press Finish to add the Ping device. Currently, siteVIEW APEX does not support IPv6 addressing.



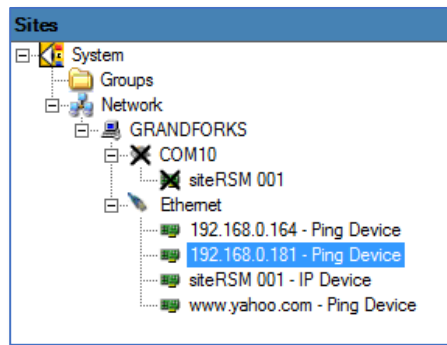


Figure 153 - Ping Device - Add Device

F.2. Using Ping Devices

Ping devices can only be polled using a siteVIEW APEX DeviceStatus command. The DeviceStatus command is interpreted by the siteVIEW APEX TASC Communication Server as request to send ping message.

siteVIEW APEX Ping devices are “stateless” devices and therefore are never “offline”. Ping devices either respond to a Device Status command, which indicates that the device is available, or they do not respond, which indicates that the device is unavailable. Unavailability can be alarmed using siteVIEW’s “Non-Responsive” alarm trigger.

F.2.1. Understanding Ping Transactions

Each DeviceStatus poll initiates a ping message transaction. The ping transaction sends a single ICMP packet to the Ping device (host) and listens for a response.

If a response is received, the TASC Communication Server will signal that the DeviceStatus command has completed successfully. The Ping device will also show that it is ready for another transaction.

If the device does not respond after 500ms, the TASC Communication Server will try again three times (every ~3 seconds). If after the initial attempt and the three retries, the device still hasn’t responded, the TASC Communication Server will signal that the device has timed out and is not responding. This “No Response” event can be used with the siteVIEW APEX alarm system to indicate that the device is not available on the network. On the Sites network tree, the Ping device will also show an “X”, indicating a failed transaction, but will be ready for another transaction.

F.2.2. Generating Ping Transactions

The DeviceStatus command can be sent in two ways:

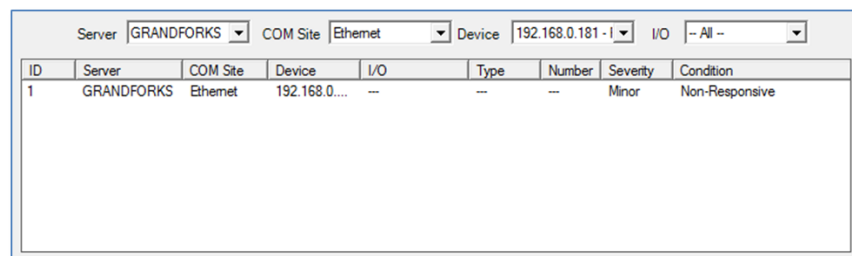
- By pressing the Refresh button which sends out an immediate DeviceStatus command. This method is useful to quickly verify the device's availability as required.
 - If the Ethernet communication port is selected in the Sites network tree when the Refresh button is pressed, all Ping devices underneath the Ethernet communication port will be sent a DeviceStatus command.
 - If a specific Ping device is selected in the Sites network tree when the Refresh button is pressed, only the selected Ping device will be sent a DeviceStatus command.
- The most typical use for Ping devices is to set up a DeviceStatus poll using siteVIEW's Polling Configuration utility. In this way, DeviceStatus commands can be sent to a Ping device(s) periodically and if the device doesn't respond, a siteVIEW APEX alarm can be triggered.

Though the Polling Configuration utility allows for non-DeviceStatus commands to be sent to Ping devices, non-DeviceStatus commands are ignored by the siteVIEW APEX TASC Communication Server.

F.2.3. Monitoring Ping Devices Transactions

The combination of a repetitive Device Status poll and a Non-Responsive alarm will provide functional monitoring of the device – allowing notifications if the device becomes unavailable.

Within the Alarm Configuration utility, select the Ping device, but for I/O select "None" – this creates a Non-Responsive alarm for the device.



ID	Server	COM Site	Device	I/O	Type	Number	Severity	Condition
1	GRANDFORKS	Ethernet	192.168.0....	--	--	--	Minor	Non-Responsive

Figure 154 - Ping Device - Non-Responsive Alarms

F.2.4. Reviewing Ping Device Transactions

siteVIEW APEX logs all activity with Ping devices.

- siteVIEW APEX History – To view historical communication and alarm information associated with a Ping device, select the History button to initiate a Log View session. The Communication link shows all communication transactions, filterable by device type and other criteria. The Alarm link shows all alarm occurrences, filterable by device type and other criteria.
- Device Communication Log – each device keeps a detailed log of transaction communication. This detailed text file is found in the CommSvc folder and is called TransmitReceive<device name>.log. The <device name> is the IP or DNS name of the device – for example: TransmitReceive192.168.0.100.log. To differentiate between TASC IP devices, remember that Ping devices do not reference a port number.

APPENDIX G. SNMP AGENT DEVICE CONFIGURATION

siteVIEW APEX can be used to monitor values from SNMP Agents using incoming SNMP traps to update, and optionally alarm, on OID values associated with the device.

G.1. Managing SNMP Communication

The siteVIEW APEX SNMP Communication Server manages the SNMP communications between SNMP Agents and the siteVIEW APEX system.

The siteVIEW APEX SNMP Communication Server will auto-connect to Data Manager and begin listening for incoming SNMP messages.

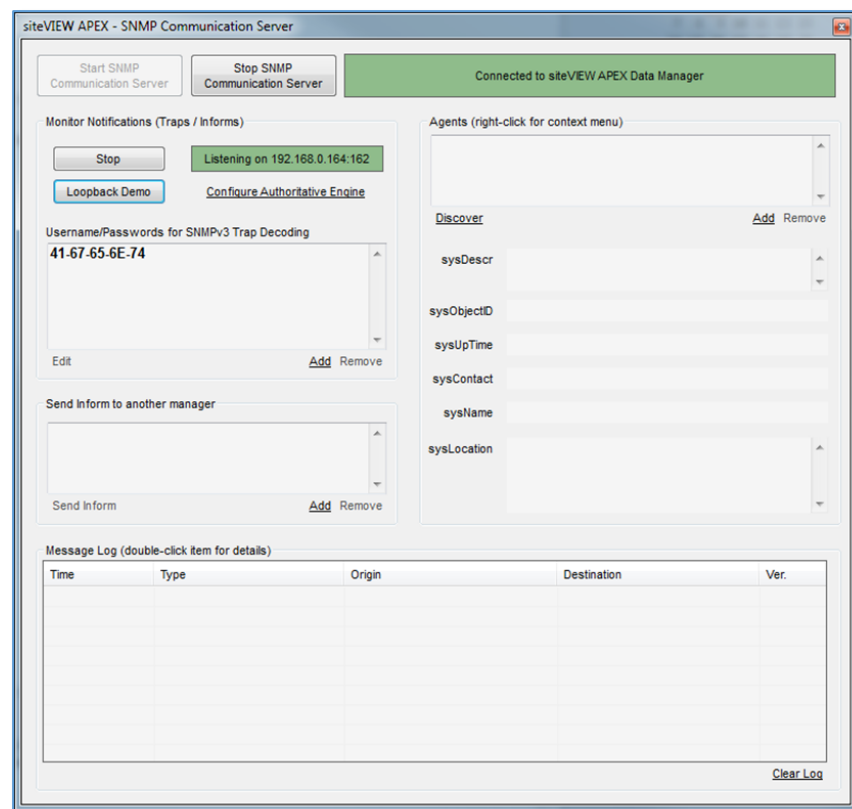


Figure 155 - siteVIEW APEX - SNMP Communication Server

G.1.1. Monitoring SNMP Traps

By default, the SNMP Communication Server will start listening for SNMP messages on the default local IP address and port 162.

To select another port, press the “Stop” button and then press “Start” again to select another address and port.

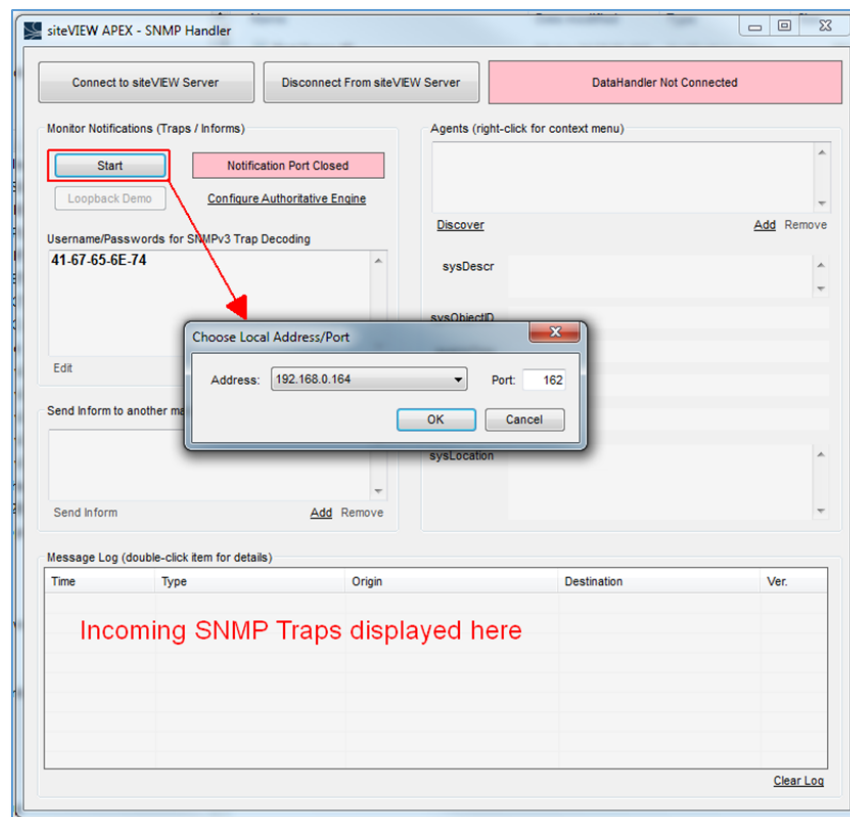


Figure 156 - siteVIEW APEX - SNMP Communication Server - Listen Settings

Incoming SNMP traps will be displayed in the Message Log area.

The screenshot shows the 'Message Log' area with a table of incoming traps. The table has the following columns: Time, Type, Origin, Destination, and Ver. The data is as follows:

Time	Type	Origin	Destination	Ver.
11:38:21.5419885	Trap1Message (Received)	192.168.0.164:64244	192.168.0.164:162	One
11:38:22.0759885	Trap1Message (Received)	192.168.0.164:64245	192.168.0.164:162	One
11:38:22.7109885	Trap1Message (Received)	192.168.0.164:64247	192.168.0.164:162	One
11:38:23.1129885	Trap1Message (Received)	192.168.0.164:64248	192.168.0.164:162	One

Figure 157 - siteVIEW APEX - SNMP Communication Server - Incoming Traps

Detailed information on the trap can be viewed by double-clicking on the trap within the Message Log.

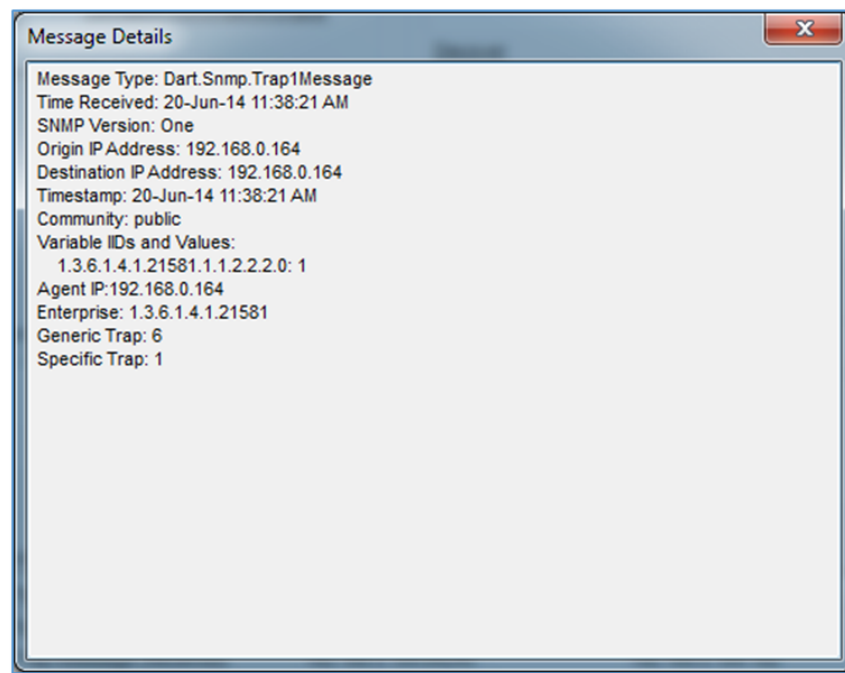


Figure 158 - siteVIEW APEX - SNMP Communication Server - Detailed Trap Information

G.1.2. Connecting the SNMP Communication Server to siteVIEW APEX

By default, the siteVIEW Communication Server will connect to the siteVIEW Data Server on start up. Once connected, all SNMP messaging will be forwarded as received to siteVIEW APEX for analysis and operation.

Use the “Stop SNMP Communication Server” button to disconnect from the siteVIEW APEX infrastructure. If the Data Manager is at a different location, edit the `SNMPCommServer.exe.config` file, located in the SNMP Communication Server directory, to adjust the ServerIP and ServerPort values to match the location of the Data Manager. Once the changes have been saved, press the Start SNMP Communication Server button to connect to the Data Manager.

```

1  <?xml version="1.0" encoding="utf-8"?>
2  <configuration>
3  <startup>
4    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
5  </startup>
6  <appSettings>
7    <!-- User application and configured property settings go here.-->
8    <!-- Example: <add key="settingName" value="settingValue"/> -->
9    <add key="ServerIP" value="127.0.0.1" />
10   <add key="ServerPort" value="11003" />
11   <add key="SnmpHandlerLogging" value="true" />
12   <add key="PassthroughSupported" value="True" />
13   <add key="EthernetSupported" value="True" />
14 </appSettings>
15 </configuration>

```

Figure 159 – siteVIEW APEX - SNMP Communication Server - Configuration File Settings



If the *SNMP Communication Server* is running on the same machine as the *Data Manager*, the recommended IP Address is localhost (127.0.0.1).

G.1.3. Minimizing the SNMP Communication Server

The close icon, at the top right, minimizes the siteVIEW Communication Server and it will continue to run in the background.

G.1.4. Log Files for the SNMP Communication Server

A log file for each device entered in siteVIEW, based on the IP Address of the device, is created and updated by the SNMP Communication Server. These files are located in the `C:\<Program Files>\TASC\siteVIEW APEX\SNMPCommServer` directory.

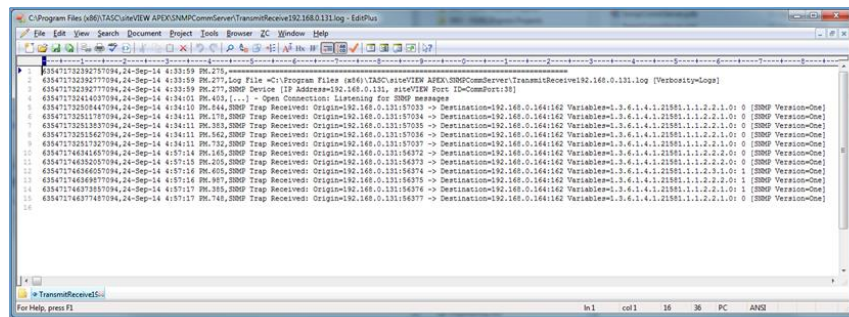


Figure 160 - siteVIEW APEX - SNMP Communication Server - Log Files

G.2. Managing SNMP Agent Devices

G.2.1. Defining SNMP Agent Devices

Predefined SNMP Agent Devices

siteVIEW APEX provides a set of pre-defined SNMP Agent devices within the `C:\<Program Files>\TASC\siteVIEW APEX\APEXDataManager\SnmpDevices` directory. Each file in this directory represents an SNMP Agent model. Contents of the file detail the list of OIDs that siteVIEW APEX can use as input values.

Devices in this directory are shown automatically within the drop-down list in the Add Device wizard.

Define a New SNMP Agent Device

The siteVIEW APEX MIB Translator utility can be used to create a SNMP Agent model file by reading zero or more MIB files which define the SNMP Agent and then extracting the vital Integer OIDs that are to be used within siteVIEW APEX to monitor the device.

siteVIEW APEX MIB Translator

Starting the siteVIEW APEX MIB Translator Tool

The siteVIEW APEX MIB Translator converts SNMP MIB file data to a siteVIEW SNMP device (stored in XML format). To start the siteVIEW APEX MIB Translator, launch the siteVIEWMIBTranslator.exe executable.

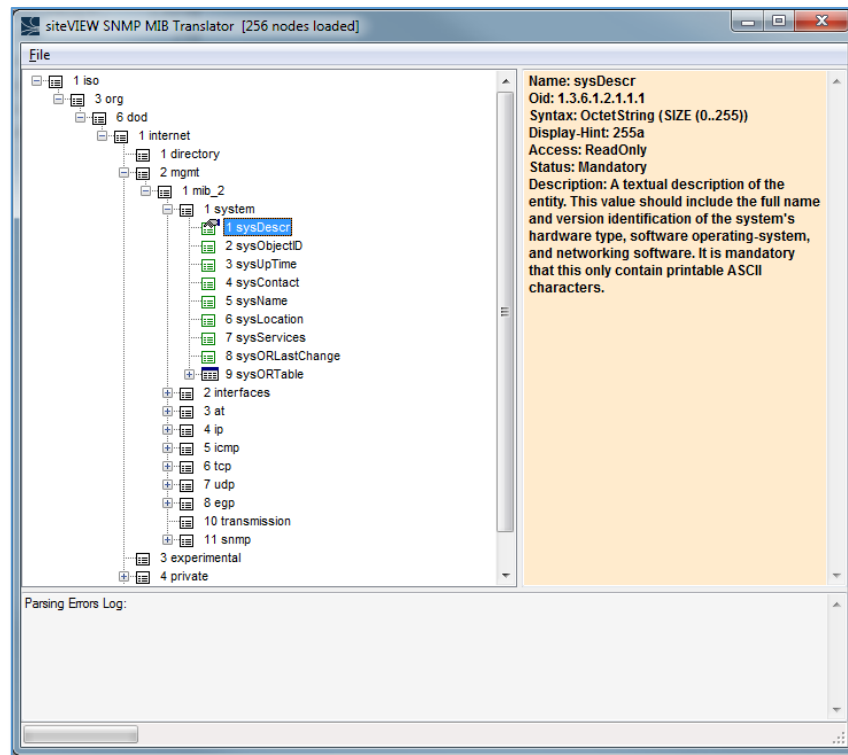


Figure 161 – siteVIEW APEX MIB Translator Utility

Using the siteVIEW MIB File Translator Tool

To use the siteVIEW APEX MIB File Translator, use the following steps:

- Load MIB files that define the device
- Generate a siteVIEW APEX SNMP device file (XML format)
- Use the siteVIEW APEX SNMP device file within siteVIEW APEX

Load MIB Files

Select the “File – Load MIBs” option to import all the MIB files that represent the sensor or device to be translated.

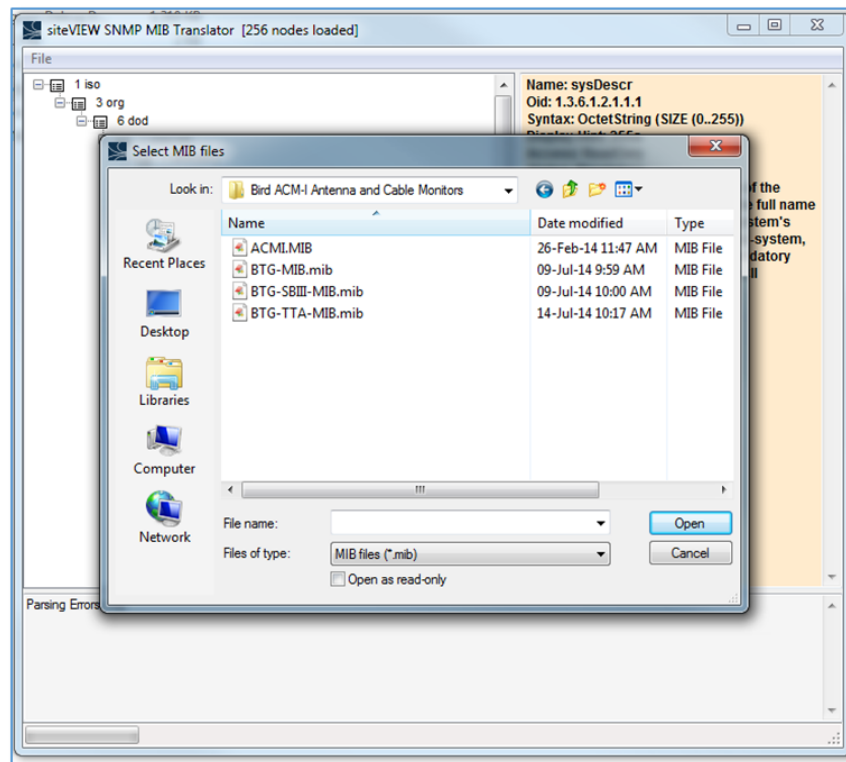


Figure 162 – siteVIEW APEX MIB Translator Utility – Load MIBs

Use the network tree to verify the import includes the SNMP Object IDs (OIDs) to be included as part of the translation. Also, confirm that there are no Parsing Errors in the log area.

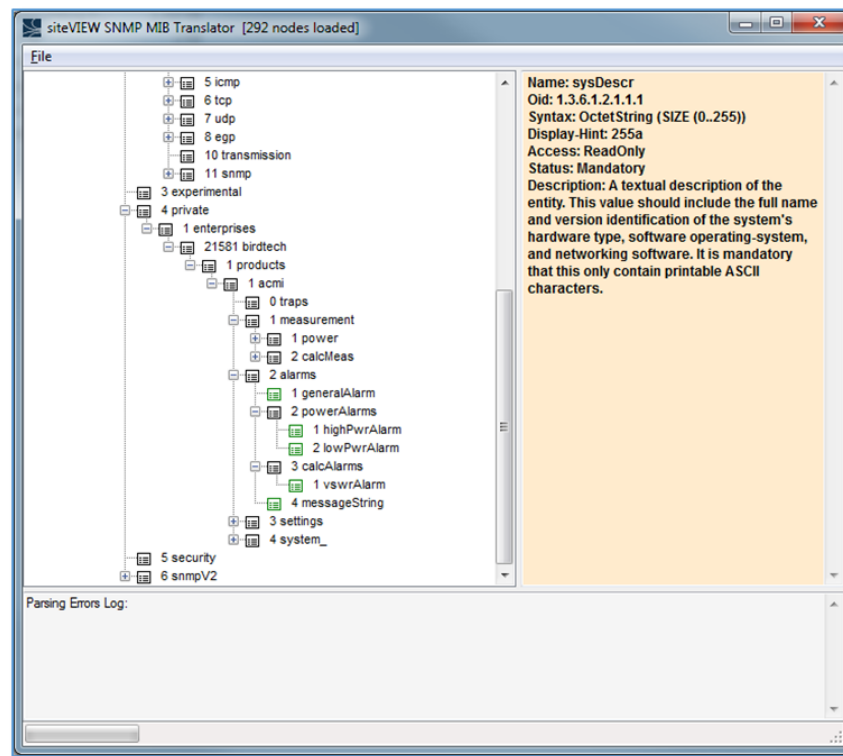


Figure 163 - siteVIEW APEX MIB Translator Utility- Confirm OIDs

Generate a siteVIEW Device File

Select the “File – Generate siteVIEW XML file” option to export the SNMP OIDs into a siteVIEW SNMP device (XML) file. Once selected, the “MIB Translator Option” dialog will open and allow you to enter:

- Device Name – A user-friendly name representative of the device, shown in siteVIEW’s device selection list
- Filtering Options – The following options are available:
 - Filter by the origin of the OID in a module – used to filter out SNMP and RFC module OIDs
 - Filter by OID type – used to include specific OID types, specifically Integer or Table Columns
 - Use the “Check/Select All OIDs”/“Uncheck All” to bulk select/deselect OIDs
 - Use the “Enabled” column in the grid to select or deselect specific OIDs

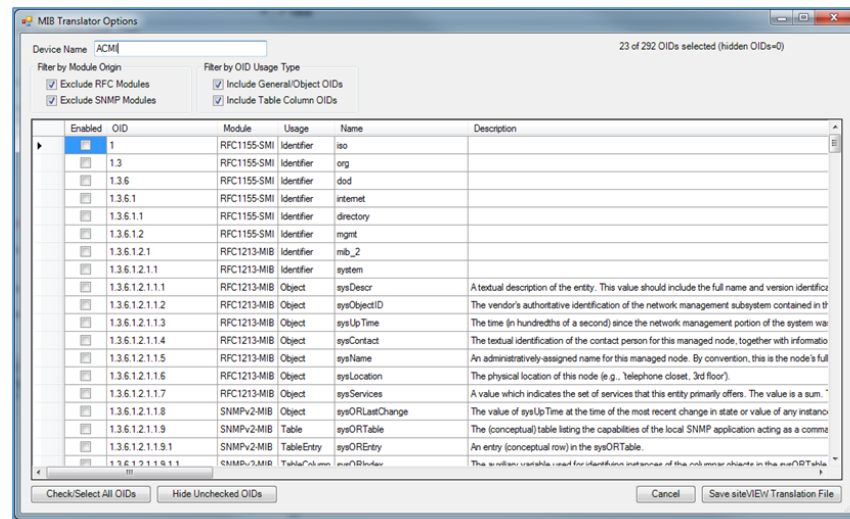


Figure 164 - siteVIEW APEX MIB Translator Utility - MIB Translator Options

Upon selecting “Save siteVIEW Translation File” on the MIB Translator Options dialog, you will be prompted for a location to save the siteVIEW XML device file. For siteVIEW to be able to use this SNMP device, save the file to the `C:\<Program Files>\TASC\siteVIEW APEX\APEXDataManager\SnmpDevices` directory.

Use siteVIEW SNMP Device file(s) within siteVIEW APEX

The siteVIEW Data Handler must be restarted to read new files located with the SnmpDevices directory. Once restarted, siteVIEW will provide the SNMP device as an option within the siteVIEW client.

G.2.2. Adding SNMP Agent Devices

Before adding a SNMP Agent device, an Ethernet communication port must be added to a SNMP Communication Server.

To add a SNMP Agent device, use the Edit – Add Device function or right-click on the Ethernet communication port and select Add Device. The resulting Device Monitoring Wizard is used to define the SNMP Agent's device properties:

- For the Device Details section, select SNMP Agent as the Device Type and select the SNMP Agent from the drop-down list, then select Next
- For the Device Identification section, enter a user-friendly name describing the SNMP Agent device in the Name field. Optionally, add additional long-form information within the Description field, then select Next.
- For the Connection Details, enter an IP (IPv4) address or a DNS name for the device. siteVIEW APEX will automatically resolve a DNS name to the IPv4 address of the device. Then press Finish to add the SNMP Agent. Currently, siteVIEW APEX does not support IPv6 addressing.

G.2.3. Monitoring SNMP Agent Devices

Monitoring in siteVIEW APEX Client

The siteVIEW APEX Client will show incoming SNMP trap messages in the Communication view area and OID updates in the Panel View area for the selected device.

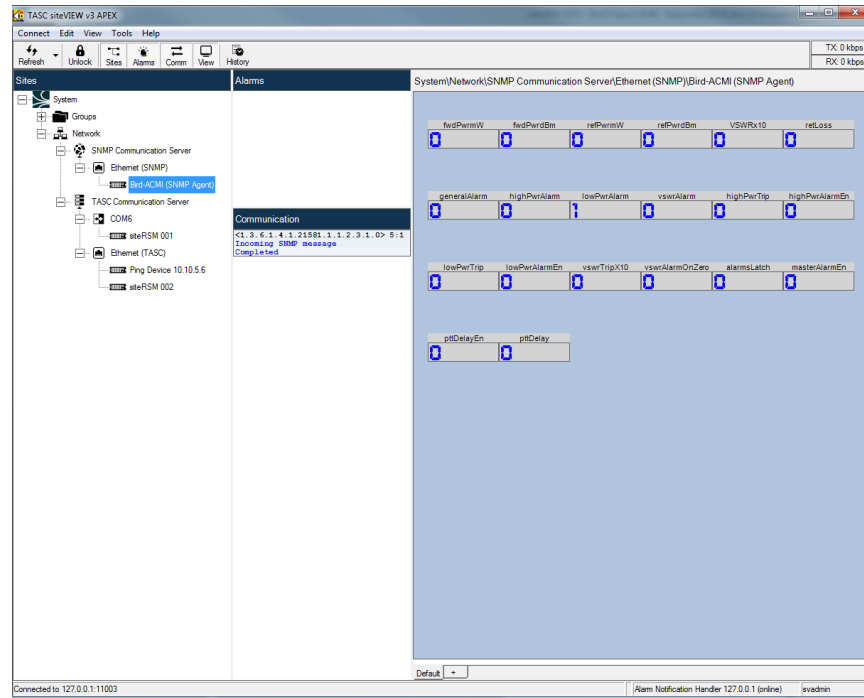


Figure 165 - siteVIEW APEX – Monitoring SNMP Agent Devices in siteVIEW APEX Client

Configuring Alarms

Use siteVIEW's Alarm Configuration dialog, accessible via the Edit menu option or context-sensitive right-click access, to add or modify an alarm condition for a SNMP OID.

Once an alarm has been defined, an alarm notification will be annunciated upon a condition match.

Monitoring Historical Activity

To view historical activity, use the History button to start the siteVIEW Log Viewer application. Select the “I/O” option under the siteVIEW Logs menu to view a historical record of SNMP OID changes.

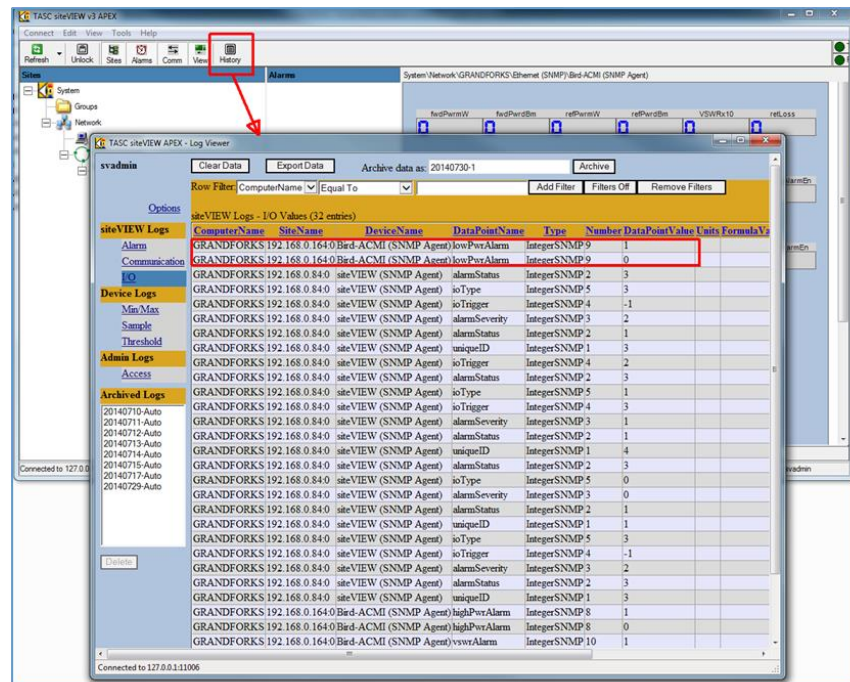


Figure 166 - siteVIEW APEX – Monitoring SNMP Agent Devices in siteVIEW APEX History

APPENDIX H. SITEVIEW TO DEVICE COMMUNICATIONS

H.1. siteVIEW APEX to siteRSM Communication Management

F.1.1. Overview

There are three methods of communicating with a siteRSM device:

- Serial Device – using a computer COM port
- Lantronix CPR Port – using a Lantronix's COM Port Redirector (CPR) technology
- Ethernet Port – using IP-based communication

During normal operations TASC serial, CPR-based serial and Ethernet devices, work identically. Each device processes transactions in order received. If multiple commands are sent – for example, as the result of a Refresh operation – these commands are queued and transacted sequentially.

F.1.2. Selecting TASC Serial, CPR Serial and Ethernet Devices

Since there are several ways to connect siteVIEW APEX to a siteRSM, here are some guidelines to build a robust monitoring network:

- Use the siteRSM's "primary" transmission port as the main connection
 - Only one port on the siteRSM can be configured to send threshold events - by default, the IP port on the siteRSM is defined as the primary port. Use the primary port as the main connection because it can respond to refresh and poll requests, and send threshold events in real-time.
 - While the siteRSM's serial port may be configured as the primary transmission port, generally, it is purposed for local configuration via the SCCU software. In the case where the serial port is configured as the primary port, use a siteVIEW APEX serial device to monitor the siteRSM.
- Use only one siteVIEW APEX device per siteRSM connection
 - It is not possible to connect to a siteRSM IP port using multiple active siteVIEW APEX devices simultaneously since the siteRSM's IP

port accepts only one connection at a time. Use either an IP device or a CPR serial device connection – not both.



For existing siteVIEW APEX networks, it is possible to migrate from CPR devices to IP devices. In this case, it is important to remove, or at minimum, disable, the CPR device when adding the IP device for the siteRSM.

- A Ping device can be added to a siteRSM connection to monitor availability
 - A Ping device may be added to a siteRSM, even if an IP device or CPR device previously exists. A Ping device works independently to a IP device or CPR device to monitor the availability of the siteRSM.
- A Ping devices can be added to non-siteRSM connections
 - A Ping device may be added to monitor non-siteRSM devices within a network. For example, it may be useful to monitor the availability of a critical device(s) within the network.

F.1.3. Differences between TASC Serial, CPR Serial and IP Devices

However, during failed communications and communication interruption recovery, there are subtle differences related to the differences between the underlying physical communication methods:

	Serial Port	CPR Port	Ethernet Port
Connection interrupted failures – for example, if a cable is unplugged	If the cable is disconnected, current and all queued transactions will be attempted, but will fail (with retries) as timed out (no response).	Initial transactions will fail due to time out (with retries). When the connection is confirmed as failed (as determined by the CPR Manager's TCP Keep Alive settings), the transaction being processed will fail with a communication error. All subsequent queued transactions remain queued.	Initial transactions will fail due to time out (with retries). In 30 seconds, when the connection is confirmed as failed, the transaction being processed will fail with a communication error. All subsequent queued transactions remain queued.
Recovery from connection interruptions	If the cable is reconnected, all subsequent commands will be transacted normally.	siteVIEW APEX continuously checks the connection and upon recovery, all queued events are processed.	siteVIEW APEX continuously checks the connection and upon recovery, all queued events are processed.

It is important to note that during connection interruptions, all events from the TASC device may be lost, therefore the connection should be validated frequently.



To ensure that serial, CPR serial and IP devices are connected, use a repetitive Device Status poll (every x minutes) in combination with a Non-Responsive alarm. Using this mechanism will allow notification of any connection failures and limit any loss of events being sent from the device.

F.1.4. Communication Alarms

Steps can be used to ensure administrative awareness of communication problems. siteVIEW APEX can be configured to report non-responsive connections using the built-in notification system. (The non-responsive alarm functionality is also available via the SNMP notification option.)



Use the non-responsive alarms to receive notifications of failed connections to quickly localize and make any required repairs to the communication infrastructure used by siteVIEW APEX to communicate with siteRSM devices.

To add a non-responsive communication alarm:

- Bring up the Alarm Configuration dialog
- Select the Server, COM Site and Device to monitor. Importantly, leave the I/O option as “- None –”. The “- None –” option is used to signal the Device communication health
- Optionally, set any Notifications to be used for the alarm (Sound, Text to Speech, Email or SNMP)
- Press the “Update” button to save and activate the alarm.

Alarm Configuration

Alarm Properties

Server: GRANDFORKS COM Site: COM10 Device: siteRSM 001 I/O: - None -

Severity: Minor ☒ Enabled

Non-Responsive Device Alarm

Details: This alarm is used to alert on failed connections associated with COM Port 10

Notification ☐ Do not send notifications when alarm is being cleared

New Update Delete

Server: GRANDFORKS COM Site: COM10 Device: siteRSM 001 I/O: - All -

ID	Server	COM Site	Device	I/O	Type	Number	Severity	Condition
20	GRANDFORKS	COM10	siteRSM 001	Input 08	Input	8	Minor	is on
22	GRANDFORKS	COM10	siteRSM 001	--	--	--	Minor	Non-Responsive

Close

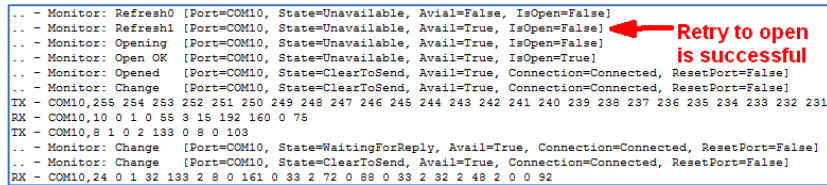
Figure 167 – Communication Alarms – Non-Responsive Alarms

F.1.5. Communication Logging System

siteVIEW APEX provides a communication logging sub-system:

- TransmitReceiveCOMxxx log files - The TransmitReceiveCOMxxx (where xxx is the port number) log file system, which is enabled by default, provides detailed information related to the health and status of the COM port.

This file is located in the `C:\<Program Files>\TASC\siteVIEW APEX\TASCommServer` directory



```

.. - Monitor: Refresh0 [Port=COM10, State=Unavailable, Avail=False, IsOpen=False]
.. - Monitor: Refresh1 [Port=COM10, State=Unavailable, Avail=True, IsOpen=False]
.. - Monitor: Opening [Port=COM10, State=Unavailable, Avail=True, IsOpen=False]
.. - Monitor: Open OK [Port=COM10, State=Unavailable, Avail=True, IsOpen=True]
.. - Monitor: Opened [Port=COM10, State=ClearToSend, Avail=True, Connection=Connected, ResetPort=False]
.. - Monitor: Change [Port=COM10, State=ClearToSend, Avail=True, Connection=Connected, ResetPort=False]
TX - COM10,255 254 253 252 251 250 249 248 247 246 245 244 243 242 241 240 239 238 237 236 235 234 233 232 231
RX - COM10,10 0 1 0 55 3 15 192 160 0 75
TX - COM10,8 1 0 2 133 0 8 0 103
.. - Monitor: Change [Port=COM10, State=WaitingForReply, Avail=True, Connection=Connected, ResetPort=False]
.. - Monitor: Change [Port=COM10, State=ClearToSend, Avail=True, Connection=Connected, ResetPort=False]
RX - COM10,24 0 1 32 133 2 8 0 161 0 33 2 72 0 88 0 33 2 32 2 48 2 0 0 92

```

Figure 168 – Communication Logging System – Transmit Receive Log Files

- CommunicationService log file – siteVIEW APEX a new, though optional, log file called the CommunicationService.log. This log file provides high-level operational information for the siteVIEW APEX TASC Communication Server software module, including:
 - Message requests and responses from siteVIEW APEX (Data Manager)
 - Overall health of all underlying communication ports

By default, the CommunicationService.log file is disabled. To enable the CommunicationService.log file:

- Navigate to the `C:\<Program Files>\TASC\siteVIEW APEX\TASCommServer` directory
- Use a text editor to edit the `CommunicationService.exe.config` configuration file
- Add the following line before the `</appSettings>` line:

```
<add key="CommunicationServiceLogging" value="True" />
```

- Save the file

- Use the TASC Communication Server Utility to restart the CommunicationService
- This file is located in the `C:\<Program Files>\TASC\siteVIEW APEX\TASCommServer` directory













```













4:35:56 PM.174,Disconnected from Data Handler Server
2:00:01 PM.643,=====
2:00:01 PM.645,Log File=C:\SVEZRoot\Enterprise2\Enterprise2\appSoftware\Bin\CommunicationService\CommunicationService.log [Verbosity=Logs]
2:00:01 PM.645,Connecting to Data Handler Server at 127.0.0.1:11003
2:00:02 PM.896,Connected to Data Handler Server
2:00:03 PM.60,CommSvc->Server [---]: Msg=Update.ClientIdentification
2:00:03 PM.386,Server->CommSvc [---]: Msg=Update.ClientIdentification for Service(2)
2:00:03 PM.391,CommSvc->Server [---]: Msg=Retrieve.SystemSettings
2:00:03 PM.391,CommSvc->Server [---]: Msg=Retrieve.RedundantServerConfig
2:00:03 PM.391,CommSvc->Server [---]: Msg=Retrieve.CommPortConfig
2:00:03 PM.803,Server->CommSvc [---]: Msg=Update.SystemSettings [Server=GRANDFORKS Version=1.0.4813.20928]
2:00:04 PM.16,Server->CommSvc [---]: Msg=Update.CommPortConfig [Port=COM10 (COM10) ID1=2 Type=Serial]
2:00:04 PM.184,CommSvc->Server [---]: Msg=Update.ConnectionState for CommPort (2)
2:00:05 PM.201,Server->CommSvc [---]: Msg=Update.CommPortConfig [Port=COM6 (COM6) ID1=3 Type=Serial]
2:00:05 PM.206,CommSvc->Server [---]: Msg=Update.CommPortStatus for CommPort (2) is Connected
2:00:13 PM.29,Server->CommSvc [001]: Msg=Update.CommPortTransaction Cmd=Retrieve.DeviceStatus using PortID=2 [Status=Queued]
2:00:13 PM.29,Server->CommSvc [002]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllAnalogInputs using PortID=2 [Status=Queued]
2:00:13 PM.30,Server->CommSvc [003]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllContactInputs using PortID=2 [Status=Queued]
2:00:13 PM.30,Server->CommSvc [004]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllOutputs using PortID=2 [Status=Queued]
2:00:13 PM.30,Server->CommSvc [005]: Msg=Update.CommPortTransaction Cmd=Retrieve.AllTemperatureInputs using PortID=2 [Status=Queued]
2:00:13 PM.30,CommSvc->Server [---]: Msg=Update.TransactionStatus
2:00:13 PM.171,CommSvc->Server [001]: Msg=Update.TransactionStatus
2:00:16 PM.785,CommSvc->Server [001]: Msg=Update.TransactionStatus
2:00:17 PM.45,CommSvc->Server [001]: Msg=Update.CommPortTransaction Cmd=Status.DeviceStatus using PortID=2
2:00:17 PM.60,CommSvc->Server [002]: Msg=Update.TransactionStatus
2:00:17 PM.293,CommSvc->Server [002]: Msg=Update.CommPortTransaction Cmd=Status.AllAnalogInputs using PortID=2

```

Figure 169 – Communication Logging System – TASC Communication Server Log File

F.1.6. Communication State Icons

State Image	Description of State
	TASC Communication Server online
	TASC Communication Server disabled
	TASC Communication Server offline <i>Check to see if TASC Communication Server is running or connected to siteVIEW APEX Data Manager</i>
	SNMP Communication Server online
	SNMP Communication Server disabled
	SNMP Communication Server offline <i>Check to see if SNMP Communication Server is running or connected to siteVIEW APEX Data Manager</i>
	Communication (Serial) Port enabled and available
	Communication (Serial) Port disabled
	Communication (Serial) Port disabled or unavailable <i>If port is disabled, it must be enabled to communicate. Check to see if cable unplugged or, in the case of a CPR port, whether the IP Address is available</i>
	Device enabled and available
	Device disabled or unavailable <i>If device is disabled, it must be enabled to communicate. If previous communication to device was lost (e.g., no response), or other communication error - check to see if device is operational or if there is a connection (e.g., cabling) issue</i>
	Modem connected

State Image	Description of State
	Modem disconnected or unavailable <i>Check modem status.</i>
	Modem pool available
	Modem pool unavailable
	Alarm is active
	siteVIEW APEX Network <i>Top most node on siteVIEW APEX network. All TASC Communication Servers nodes and children will be connected here.</i>
	Group Folder <i>Group folder allows organization of devices</i>
	siteVIEW APEX system <i>Top most node within a siteVIEW APEX system – includes groupings and network.</i>
	Shortcut to an enabled and available Device <i>A shortcut to a device within a group folder</i>
	Shortcut to a disabled or unavailable Device <i>If device is disabled, it must be enabled to communicate. If previous communication to device was lost (e.g., no response), or other communication error - check to see if device is operational or if there is a connection (e.g., cabling) issue</i>
	Ethernet Port enabled and available
	Ethernet Port disabled or unavailable <i>If port is disabled, it must be enabled to communicate. Check to see if cable unplugged or, in the case of a CPR port, whether the IP Address is available</i>
	Device Updates Waiting <i>siteVIEW APEX has sensed a difference between the siteVIEW APEX representation of the device and the actual device contents.</i>

State Image	Description of State
	<i>siteVIEW APEX recommends a status and/or configuration refresh to ensure that the siteVIEW APEX device representation is synchronized with the actual device.</i>

H.2. siteVIEW APEX Communication via Lantronix CPR Ports

F.2.1. Lantronix CPR Overview

siteVIEW APEX utilizes Lantronix technology to implement an IP connection to the siteRSM. siteVIEW APEX and related components can be configured to ensure robust communications.

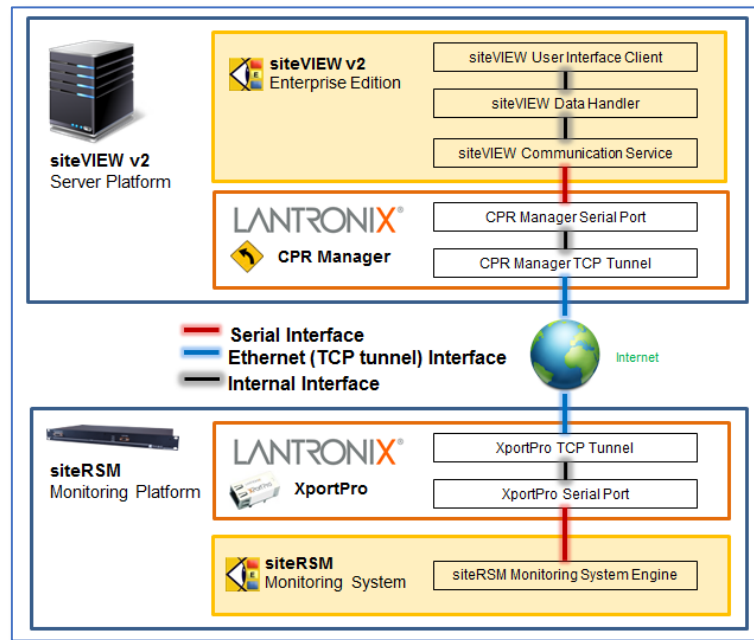


Figure 170 – siteVIEW APEX to siteRSM Connections

siteVIEW APEX can automatically recognize failed IP connections on Lantronix Com Port Redirector (CPR) managed ports for siteRSM devices. Specifically, failures are recognized at any attempt to request information (write) from a damaged IP connection. Failed connections are immediately closed and marked as unavailable.

This siteVIEW APEX manages all of these IP communication failure modes:

- (Temporary) Ethernet disconnections – this represents the most prevalent failure type and includes unplugged networking cables, router/switch malfunctions and ISP network adjustments.
- siteRSM power cycles – restarting the siteRSM will disrupt communications. This failure is prevalent during deployment.
- Loss of Windows network adapter – includes any disruptions to the siteVIEW APEX host's underlying IP infrastructure. For example, entry/exit from sleep mode or changes to the Window's network system setup.

Auto-recovery is implemented by using siteVIEW's polling mechanism to constantly recheck the port for a restored connection.



TASC Systems recommends using an indefinite Device Status poll on each CPR serial-to-IP port. This poll acts as a “ping” mechanism and serves two purposes:

- Allows siteVIEW APEX to recognize (and close) failed connections
- For failed ports, the Device Status poll is a recurring check for a restored connection

The Device Status poll should be set to request Device Status information every minute, indefinitely.

A Device Status poll is recommended as it represents the smallest message exchange between siteVIEW APEX and the siteRSM over connection and, hence, has no material influence on the system's communication overhead. Furthermore, no I/O information is exchanged thereby ensuring that all alarming and site mapping is influenced.

Using a check every minute, the smallest time granularity for a siteVIEW APEX poll, ensures that a failed connection is recognized in no more than a minute. Furthermore, a connection is re-established in no more than a minute after it has been restored.

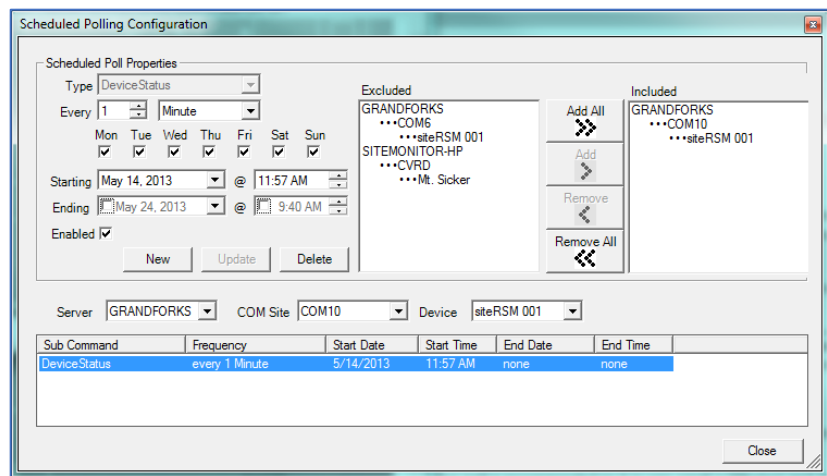


Figure 171 – Connection Management – Device Status Poll

F.2.2. siteRSM Tunnel Settings

The siteRSM's IP Interface is implemented using an embedded Lantronix XPort Pro (or XPort) adapter. Though the Lantronix Xport Pro (or XPort) is pre-configured at the factory, reducing the TCP Keep Alive time to 10,000msec is recommended to more quickly dismantle bad connections.



TASC Systems recommends setting the Lantronix XPort Pro's Tunnel setting for the TCP Keep Alive parameter to 10,000 msec. This ensures that any broken or failed connection is dismantled in no more than ~10 seconds of failure.

To change the setting:

- Use a web browser to access the IP address of the siteRSM
- Login to the siteRSM using user=admin and password=PASS
- Select the Tunnel option (on the left-hand menu list)
- Select Accept Mode option (on the top menu list)
- Change the TCP Keep Alive value to 10000 msec
- Press the "Submit" button to accept and save the change

The screenshot shows the XPort Pro web interface. On the left is a vertical menu with options: Status, CLI, CPM, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Modbus, Network, PPP, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System, Terminal, TFTP, Tunnel (highlighted), VIP, and XML. The main content area is titled 'Tunnel 1' and contains tabs for Statistics, Serial Settings, Packing Mode, Accept Mode (selected), Connect Mode, and Disconnect Mode. Below the tabs, the 'Tunnel 1 - Accept Mode' section is displayed. A red box highlights the following settings: Mode: Always, Local Port: 10001, Protocol: TCP, and TCP Keep Alive: 10000 milliseconds. Other settings include Flush Serial: Enabled, Block Serial: Disabled, Block Network: Disabled, Password: <None>, Email on Connect: <None>, Email on Disconnect: <None>, and CP Output: Group. A 'Logout' link is in the top right corner. The footer contains the copyright notice: Copyright © Lantronix, Inc. 2007-2010. All rights reserved.

Figure 172 – siteRSM Tunnel Settings – XPort Pro



TASC Systems recommends setting the Lantronix XPort's Tunnel setting for the TCP Keep Alive parameter to 10,000 msec. This ensures that any broken or failed connection is dismantled in no more than ~10 seconds of failure.

To change the setting:

- Use a web browser to access the IP address of the siteRSM
- Login to the siteRSM using user=admin and password=<empty>
- Select the Server option (on the left-hand menu list)
- Change the TCP Keep Alive value to 10 seconds
- Press the “OK” button to accept and save the change

The screenshot displays the 'Server Settings' page in the TASC siteVIEW APEX web interface. On the left, a vertical menu lists various configuration options, with 'Server' currently selected and highlighted. The main content area is titled 'Server Settings' and contains two sections: 'Server Configuration' and 'Advanced'. In the 'Advanced' section, the 'TCP Keepalive (secs)' field is set to '10' and is highlighted with a red rectangular box. Other visible fields include 'Telnet Password', 'Retype Password', 'ARP Cache Timeout (secs)' (set to NaN), 'Monitor Mode @ Bootup' (set to Enable), 'CPU Performance Mode' (set to Regular), 'HTTP Server Port' (set to NaN), 'Config Server Port' (set to NaN), and 'MTU Size' (set to NaN). An 'OK' button is located at the bottom right of the configuration area.

Figure 173 – siteRSM Tunnel Settings - XPort

F.2.3. Lantronix CPR Settings

The siteVIEW APEX IP infrastructure is implemented using the Lantronix CPR Manager software, which provides IP connections for serial ports used within siteVIEW. Amended settings are recommended to more quickly dismantle bad connections.



TASC Systems recommends setting the CPR Manager port setting for the TCP Keep Alive parameter to 10,000 msec. This ensures that any broken or failed connection is dismantled in no more than ~10 seconds of failure.

TASC Systems recommends disabling the CPR Manager port setting for Timeout Reconnect. This ensures that failed port is closed until fully restored by siteVIEW.

To change the setting:

- Run the Lantronix CPR Manager software
- Select the COM port to modify
- On the Settings tab, ensure TCP Keep Alive is enabled (checked), set the KeepAlive Time to 10000 msec and KeepAlive Interval to 1000 msec
- On the Settings tab, disable (uncheck) the Timeout Reconnection option.
- Press the “Save” button on the top ribbon menu to accept and save the changes

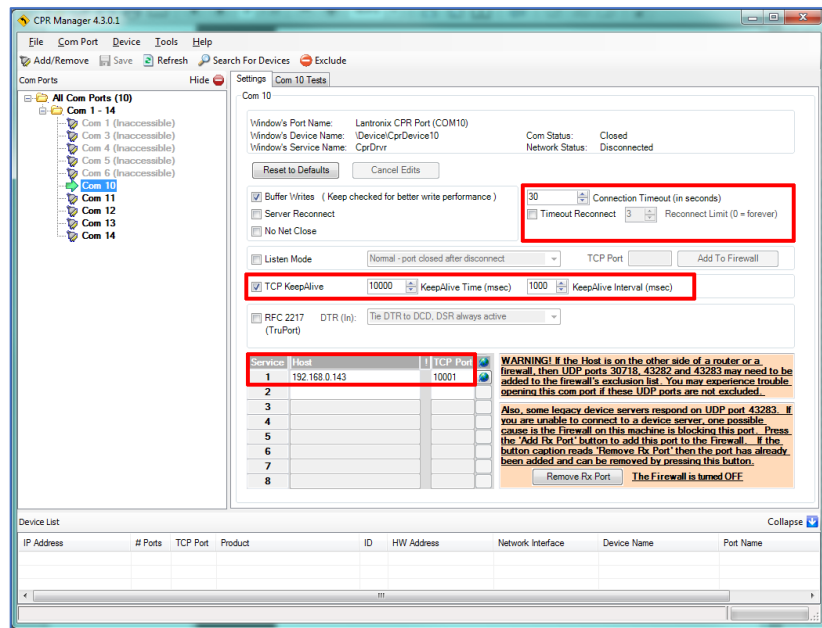


Figure 174 – siteRSM Tunnel Settings

H.3. siteVIEW APEX Communication via Ethernet Ports

F.3.1. Adding Ethernet Devices

To connect to a TASC device via IP, an Ethernet communication port must be added.

Once an Ethernet port has been added, use the Edit – Add Device function or right-click on the Ethernet communication port and select Add Device. The resulting Device Monitoring Wizard is used to define the TASC IP device's properties:

- For the Device Details section, select the type of TASC device and address then select Next
- For the Device Identification section, enter a user-friendly name describing the TASC device in the Name field. Optionally, add additional long-form information within the Description field, then select Next.
- For the Connection Details, enter an IP (IPv4) address or a DNS name for the device. siteVIEW APEX will automatically resolve a DNS name to the IPv4 address of the device. Specify the port number, typically for siteRSM

devices this will be 10001. Specify the Packet Timeout (time between retries), then press Finish to add the device.

IPv6 interfaces are not supported.

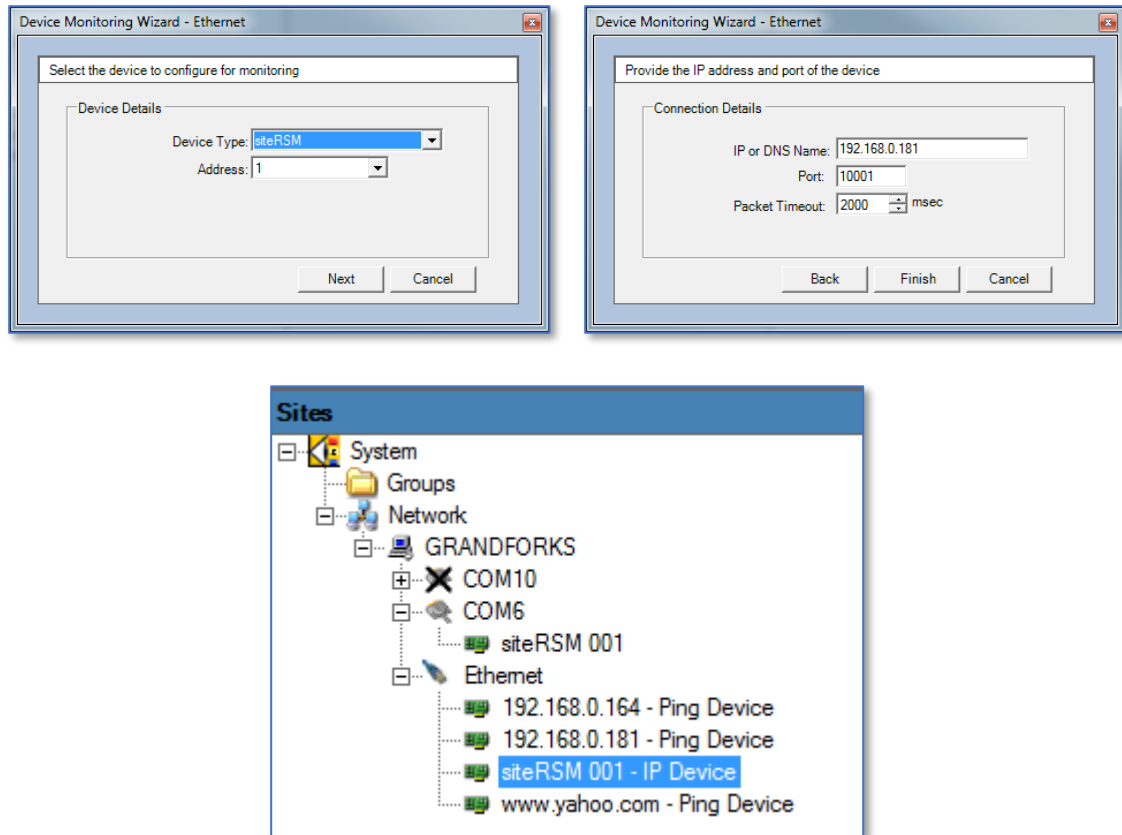


Figure 175 - Ethernet Port Communication - Add Device

F.3.2. Using Ethernet Devices

TASC IP devices operate almost the same as conventional serial or CPR devices, with the only difference being the underlying physical communication interface.

F.3.2.1. Understanding Ethernet Device Transactions

For TASC devices, siteVIEW APEX supports a set of TASC protocol commands. These commands allow siteVIEW APEX to request either status or configuration information from the device. The siteVIEW APEX TASC Communication Server sends each command as a transaction to the device.

If a response to a transaction is received, siteVIEW APEX will interpret and process the results automatically.

If the device does not respond within the Interbyte timeout specified, the TASC Communication Server will try again as per the number of Retries configured for the device. If after the initial attempt and the three retries, the device still hasn't responded, the TASC Communication Server will signal that the device has timed out and is not responding. This "No Response" event can be used with the siteVIEW APEX alarm system to indicate that the device is not available on the network. On the Sites network tree, the device will also show an "X", indicating a failed transaction.

F.3.2.2. Generating IP Device Transactions

siteVIEW APEX communicates with IP devices, as with serial or CPR device, in the following three ways:

- Through manual refresh button presses. Each refresh button press consists of multiple commands, which are processed sequentially as individual transactions. There are three types of refreshes:
 - Status refresh: commands to request the current status of the device and associated I/O.
 - Configuration refresh: commands to request the current configuration of the device.
 - Full: commands to request both status and configuration of the device.
- Through scheduled polled commands. Use the siteVIEW APEX Polling Configuration editor to set up one or more commands to send to the device.
- Through events received from the device based on digital input change of state, analog input threshold crossings or temperature threshold crossings.

F.3.2.3. Monitoring TASC Ethernet Device Transactions

The combination of a repetitive Device Status poll and a Non-Responsive alarm will provide functional monitoring of the device – allowing notifications if the device becomes unavailable.

Within the Alarm Configuration utility, select the IP device, but for I/O select "None" – this creates a Non-Responsive alarm for the device.

Server	GRANDFORKS	COM Site	Ethernet	Device	192.168.0.181 - I	I/O	-- All --	
ID	Server	COM Site	Device	I/O	Type	Number	Severity	Condition
1	GRANDFORKS	Ethernet	192.168.0....	--	--	--	Minor	Non-Responsive

Figure 176 - Ethernet Port Communication - Monitoring Port Health

F.3.2.4. Reviewing Ethernet Device Transactions

siteVIEW APEX logs all activity with IP devices.

siteVIEW APEX History – To view historical communication and alarm information associated with a IP device, select the History button to initiate a Log View session. The Communication link shows all communication transactions, filterable by device type and other criteria. The Alarm link shows all alarm occurrences, filterable by device type and other criteria.

Device Communication Log – each device keeps a detailed log of transaction communication. This detailed text file is found in the CommSvc folder and is called TransmitReceive<device name>.log. The <device name> is the IP or DNS name of the device, followed by an underscore and then followed by the port number – for example: TransmitReceive192.168.0.200_10001.log. To differentiate between TASC Ping devices, remember that Ping devices do not reference a port number.

H.4. Migrating TASC Serial or CPR Serial Devices to Ethernet Devices

To take advantage of a direct IP connection, it may be desirable to convert existing TASC serial or CRP serial devices to an IP device. While the process of adding an IP device will automatically upload fundamental information directly from the siteRSM, including basic I/O configuration, siteVIEW-specific information, which is stored in the siteVIEW APEX database, must be also considered to fully convert the device to IP. siteVIEW APEX-specific database information includes panel designs, formulas, alarms, poll schedules and mapping.

H.4.1. Adjusting siteRSM IP Settings

Check to see if the siteRSM requires Adjusting

Older siteRSMs must be prepared for siteVIEW APEX IP connections. To identify if the siteRSM's configuration must be prepared for siteVIEW APEX IP connections, using an Internet browser, navigate to the IP address of the siteRSM (user=admin, password=<nothing/empty>).

If you are unable to login (Error=401 Authorization Failed), then no configuration changes are required, the siteRSM is ready for use with siteVIEW.

However, if you see a screen like the one below, indicating the siteRSM's IP interface is using an XPort Device Server, then additional steps must be taken to prepare the siteRSM for operation with siteVIEW's IP interface.



Figure 177 - Migrating to Ethernet - siteRSM Config Logon Screen

Adjust Serial Packing Settings

For siteRSMs that require adjustments, use a Telnet session to adjust the Serial Packing Control, so that siteVIEW APEX messages will be sent as one packet, not multiple. To do this:

1. Run the Lantronix Device Installer software and then allow the Device Installer software to locate the siteRSM's adapter (IP address)
2. Select the siteRSM adapter and then select the Telnet Configuration tab and press Connect

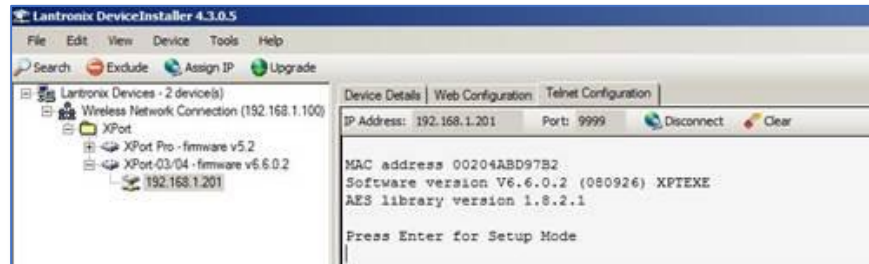


Figure 178 - Migrating to Ethernet - Telnet Config

3. Press Enter to enter the configuration menu, then select the “1 – Channel 1” option.

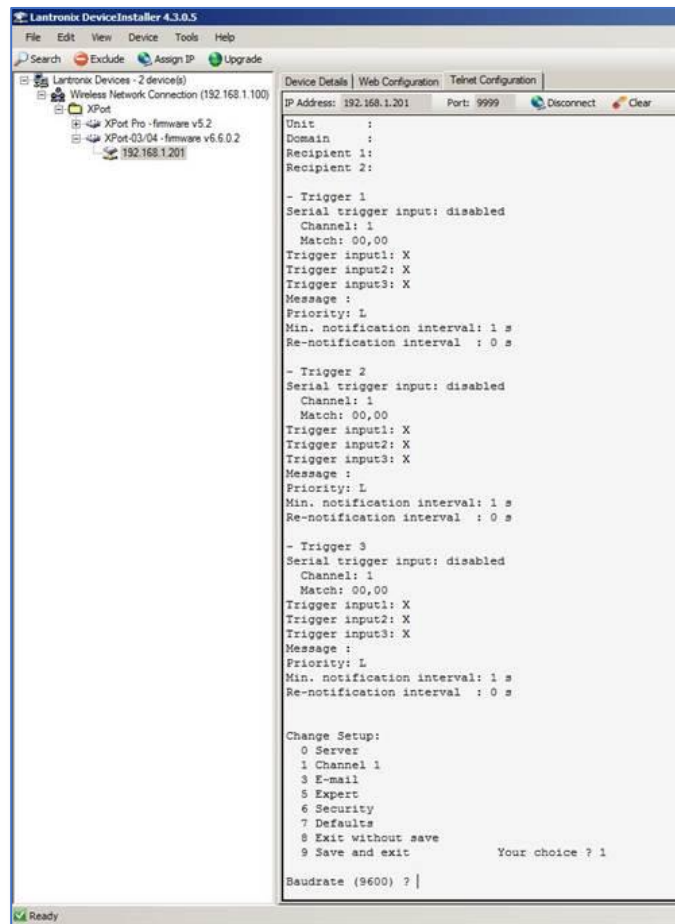


Figure 179 - Migrating to Ethernet - Select Channel

4. Press Enter (no change) until you get to FlushMode. The default is 77, which means that Packing is disabled. Enter f7 and Enter, to enable Packing. The default for Pack Cntrl is 00, which means 12ms Packing Interval. Enter 01 and Enter, which means 52ms Packing Interval. Press Enter (no change) for the rest of the settings, until you return to the menu.

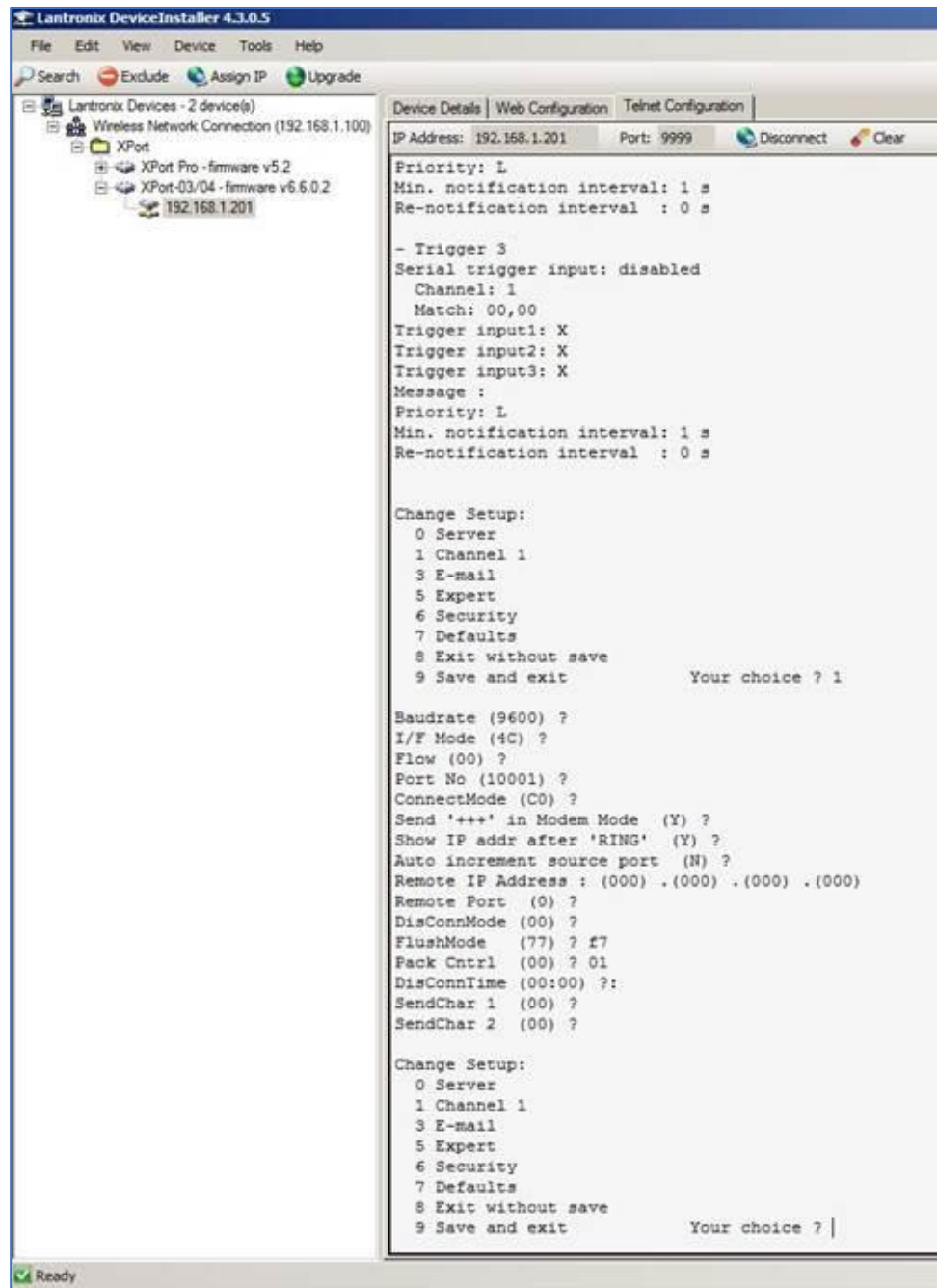


Figure 180 - Migrating to Ethernet - Flush Mode

5. Press 9 and Enter to Save and exit.

```

Change Setup:
 0 Server
 1 Channel 1
 3 E-mail
 5 Expert
 6 Security
 7 Defaults
 8 Exit without save
 9 Save and exit          Your choice ? 1

Baudrate (9600) ?
I/F Mode (4C) ?
Flow (00) ?
Port No (10001) ?
ConnectMode (C0) ?
Send '+++ ' in Modem Mode (Y) ?
Show IP addr after 'RING' (Y) ?
Auto increment source port (N) ?
Remote IP Address : (000) . (000) . (000) . (000)
Remote Port (0) ?
DisConnMode (00) ?
FlushMode (77) ? f7
Pack Cntrl (00) ? 01
DisConnTime (00:00) ? :
SendChar 1 (00) ?
SendChar 2 (00) ?

Change Setup:
 0 Server
 1 Channel 1
 3 E-mail
 5 Expert
 6 Security
 7 Defaults
 8 Exit without save
 9 Save and exit          Your choice ? 9

Parameters stored ...
|

```

Figure 181 - Migrating to Ethernet - Save Config



While the Device Installer offers a web interface option to adjust these settings, TASC recommends using the Telnet interface, as cached settings may result in unexpected behavior using the web interface.

H.4.2. Creating the IP Device

The following steps are recommended to convert an existing TASC Serial or CPR Serial device to an IP device:

1. Ensure that the CPR Serial device is disabled. Since the IP connection on a siteRSM allows one connection at a time, disabling the CPR Serial will ensure that the IP device is given precedence to the connection.
2. Create an Ethernet communication port. This port represents the Ethernet adapter for siteVIEW's TASC Communication Server and will serve as the connection to all IP devices.

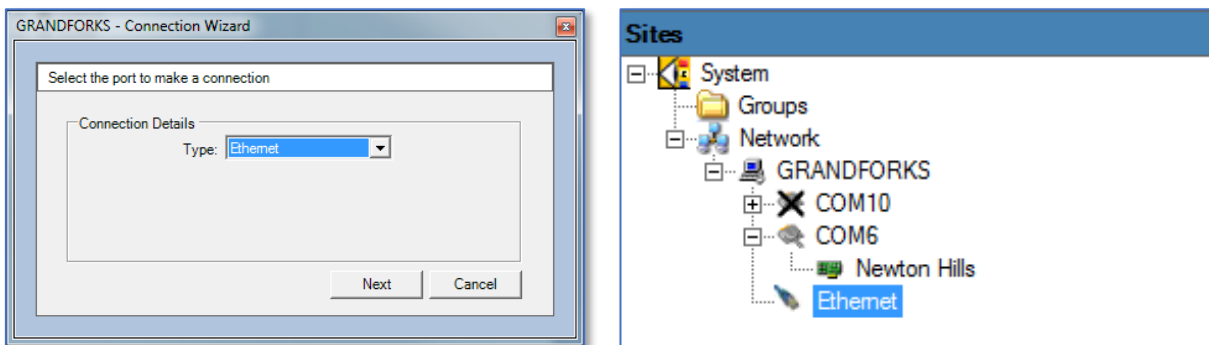


Figure 182 - Migrating to Ethernet - Create Ethernet Port

3. Create a siteRSM device under the Ethernet communication port. Use the IP address for the siteRSM – if you previously had a CPR serial port, use the IP address which was used within the CPR Manager software for the CPR serial port. The port address by default is 10001. Packet Timeout is the amount of time to wait before retrying a communication message – the default is 2000msec (2 seconds).

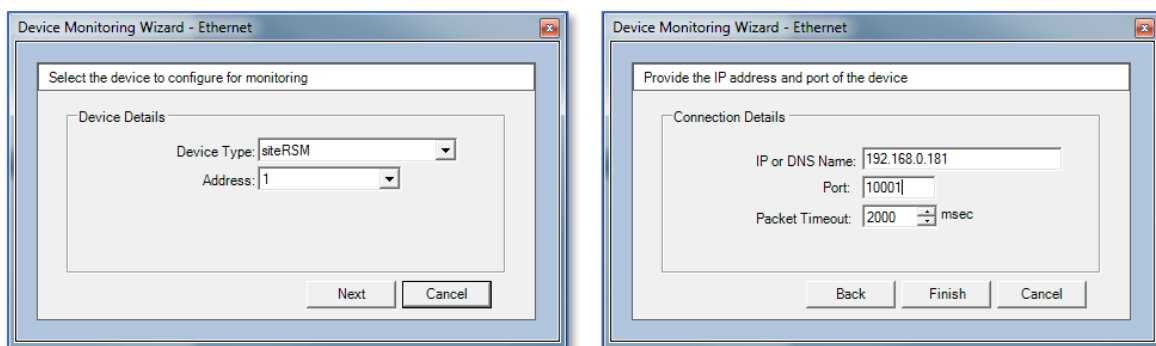


Figure 183 - Migrating to Ethernet - Add Device

As part of the creation process, siteVIEW APEX will automatically interrogate the siteRSM and upload all information related to the device's hardware configuration and current status – this includes:

- Amount of digital inputs, digital outputs, analog inputs and temperature inputs, and which points are enabled/disabled.
- Current I/O configuration including:
 - Digital inputs – off state, hold times, local outputs and output action
 - Analog inputs – ranges, sensor types, offsets, qualifiers, thresholds, local outputs and hold times
 - Temperature inputs – units, qualifiers, thresholds, local outputs and hold times
 - Outputs – off states

H.4.3. Migrating siteVIEW-specific Data

Panel Information

1. Export the panel design from the existing CPR serial (or TASC serial) device. The panel design includes the background image and I/O control user interface settings. To export, right-click anywhere on the Panel View screen for the CPR serial (or TASC serial) device and select “Export Panel”, then select a location to store the resulting .PNL file.

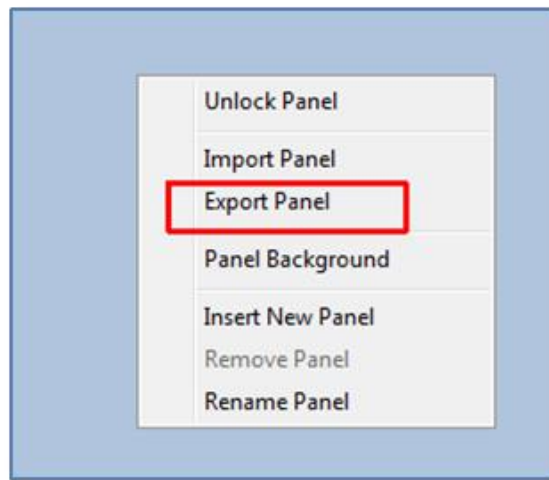


Figure 184 - Migrating to Ethernet - Export Panel

2. Import the panel design to the new IP device. To import, right-click anywhere on the Panel View screen for the IP device and select “Import Panel”, then select the previously saved .PNL file. During the import process, an Importing Options dialog will be presented. To ensure that the panel mimics the information previously assigned, enable both the “Import names of panel control items” (which ensures any names previously attached to your panel are

imported) and “Delete extra panel controls that are not in the import file” (which will delete any controls that were not in the previous panel).

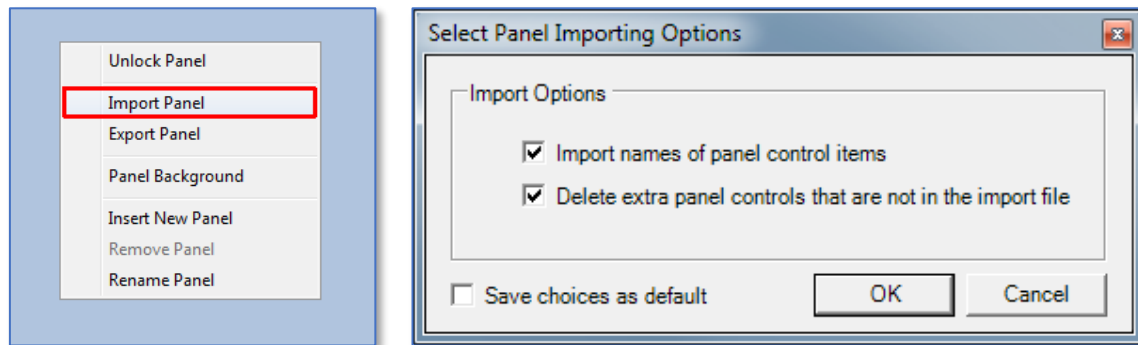


Figure 185 - Migrating to Ethernet - Import Panel

Update Formulas

3. If the previous TASC serial or CPR serial device used formulas, adjust the properties of the analog inputs to use the formula. Open up the Device Properties and select the Analog Inputs tab, and then use the Formula drop down list to select the appropriate formula.

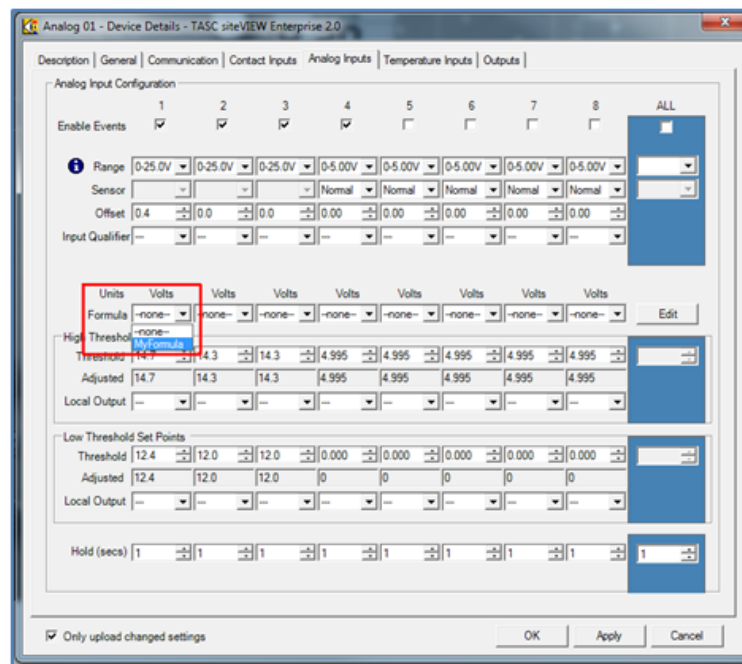


Figure 186 - Migrating to Ethernet - Update Formulas

Create Alarms

4. Create the alarms for the IP device using the Alarm Configuration form. At this time, alarms cannot be modified or exported/imported for a new device - it is necessary to re-create the alarms.

Adjust Scheduled Polls

5. Adjust the scheduled polls for the IP device using the Schedule Polling Configuration form. Select the polls that you would like to add the IP device to and then use the “Add” button to include the IP device to the list of devices support for the selected poll.

Sub Command	Frequency	Start Date	Start Time	End Date	End Time
DeviceStatus	every 1 Minute	16-May-14	2:38 PM	none	none
DeviceStatus	every 1 Minute	20-May-14	4:41 PM	none	none
DeviceStatus	every 1 Hour	06-Jun-14	10:35 AM	none	none

Figure 187 - Migrating to Ethernet - Adjust Scheduled Polls

Create Site Mappings

6. Create the site mappings for the IP device using the Site Mappings Configuration form. At this time, site mappings cannot be modified or exported/imported for a new device - it is necessary to re-create the site mappings

H.4.4. Testing and Finalizing Migration

1. Confirm operation of the IP device. Use the IP device during normal operations to verify that the device is operating properly before deleting the previous CPR serial or TASC serial devices.
2. Delete the CPR serial or TASC serial devices. Once the migrated IP device has been validated, delete the obsolete CPR serial or TASC serial device. This is an optional step and can be carried out at any time as long as the device remains disabled.

APPENDIX I. SITEVIEW APEX PANEL DESIGN

I.1. Panel Design Guidelines

siteVIEW APEX panel is the container for the siteVIEW APEX view window. The panel image is the background image used to define the context for the user.

I.1.1. Panel Image Size

Maximum panel background sizes for a siteVIEW APEX Client are determined by resolutions provided by your system's graphics card. (It is useful to remember that the resolution is determined by the graphics card and then matched to the monitor.)

You must account for ~150 pixels used vertically (menus, status) and ~410 pixels (typical) used vertically (network tree, communication and alarm windows). That is, use the given screen resolution, subtract the pixels used by the siteVIEW APEX software to arrive at the allowable panel background size.

Below are popular screen resolutions for Windows platforms (shown in rough order of popularity as of end of year 2012) and the associated siteVIEW APEX background panel size:

Screen Resolution	Recommended siteVIEW APEX Background Panel Image Size	Comments
1920 x 1080, 1920 x 1200	1400-1500 x 930	16:9, recent desktops, *Recommended, popular* , 1920 x 1200 (used by 24" widescreen LCD monitors)
1366 x 768	950 x 615	16:9, laptops *Popular* but limited vertical depth, (Minimum resolution required to support all the features of Windows 8)
1280 x 720	870 x 570	16:9, recent laptops/desktops *Popular* but limited vertical depth
1680 x 1050, 1600 x 900	1190 x 750	16:9, recent desktops/laptops 1680 x 1050 (used by 20"/22" widescreen LCD monitors)
1280 x 1024	870 x 870	4:3, older resolution, declining in popularity

Sources:

- http://www.w3schools.com/browsers/browsers_resolution_higher.asp (mentioned popular and/or growing in popularity resolutions).
- <http://msdn.microsoft.com/en-us/library/windows/apps/hh780612.aspx> (for Windows 8 resolutions)
- <http://windows.microsoft.com/en-CA/windows7/Getting-the-best-display-on-your-monitor>

It may be beneficial to create a wider canvas than the panel's background image to allow storage of hidden controls. In this way, when the screen is unlocked the unused controls are accessible via a simple scroll.

Due to their popularity, it may be desirable to design the panel a widescreen (16:9) format. Wider formats are recommended because users can control the hiding or modifying the pixels allocated to the network tree and/or the Communication/Alarm regions.

I.1.2. Panel Image Layout

The following guidelines are recommended for creation of siteVIEW APEX panels:

- A grouping element (e.g., lined perimeter, box) should be used to enclose all siteVIEW APEX controls. Sub-grouping elements should be used to group controls of similar functionality – for example, all environmental controls may be placed together.
- All critical (i.e., alarming) controls should be placed near the top and/or grouped together
- All controls should be accompanied by either an icon or label to clearly indicate functionality.
- A title, associated logo or both should be placed at the top of the screen to indicate the domain of the panel. For example, if the panel is for a particular site, the site's name could be the title or if the panel is designed for a particular customer, the customer's logo could be displayed at the top. Breadcrumb navigation may be used as part of the titling.
- The recommended format for panel backgrounds is either PNG or JPG.
- If siteVIEW APEX will be deployed on a touchscreen, layout sizing must take into account human ergonomics to ensure proper selection of siteVIEW APEX controls.

I.1.3. Panel Sub-Groups

Typical panel sub-group elements include:

- Transmit/Receive information (e.g., forward power, transmit voltage/current)
- Equipment related information (e.g., signals from the radio/repeater)
- Environmental information (e.g., door sensor, temperature, fuel, battery levels)

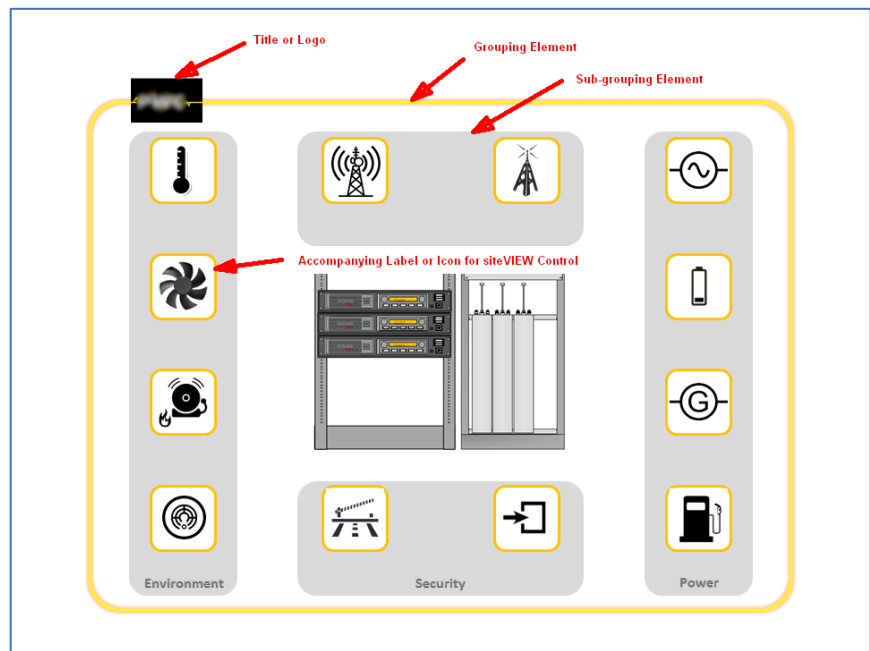


Figure 188 – Sample Panel Layout

I.1.4.HMI Standards

The following HMI standards may be considered as part of the panel design process. They provide guidance on color schemes, layout and other ergonomic factors.

- ISA (Instrument Society of America) 101 Human-Machine Interface:
 - Official Standard: <http://www.isa.org/MSTemplate.cfm?MicrositeID=1142&CommitteeID=6899>
 - 3rd Party Overview: http://www.yca-yokogawa-usersgroup.com/uploads/3/1/8/5/3185440/mesatutorial_-_isa101_hmiworkshop.pdf
- A Human Factors Approach to Supervisory Control Interface Improvement: http://cdn.intechopen.com/pdfs/4695/InTech-A_human_factors_approach_to_supervisory_control_interface_improvement.pdf

I.1.5. Panel Image Design Tools

While there are many tools that can be used to design background panel images, the following considerations may be useful in the selection of a design tool:

- Ability to concretely define in pixels canvas size, grouping elements and sub-grouping elements
- Ability to control location of titling, logos and/or icons by pixel
- Ability to generate PNG or JPG files

Suitable products, shown in order of recommendation are listed:

- Adobe Photoshop (or Illustrator) or equivalent, for example, Paint.NET, Gimp
- Microsoft PowerPoint

I.2. Panel Icons

Icons are embedded within a Panel Image to provide semantic context for individual I/O points, devices or network nodes.

I.2.1. Icon Usage

- siteVIEW APEX panels should utilize standard icon sets, which conform to industry standard or de facto meaning. siteVIEW APEX ships with a sample set of icons located in the \PanelIcons folder.
- The recommended format for icons is either PNG or JPG.
- If siteVIEW APEX will be deployed on a touchscreen, icon sizing must take into account human ergonomics to ensure proper selection of siteVIEW APEX controls.

I.2.2. Icon Design Tools

While there are many tools that can be used to design icon images, the following considerations may be useful in the selection of a design tool:

- Ability to concretely define size, resolution, colors in pixels
- Ability to generate PNG or JPG files

Suitable products, shown in order of recommendation are listed:

- Adobe Photoshop (or Illustrator) or equivalent, for example, Paint.NET, Gimp
- Microsoft PowerPoint

I.3. siteVIEW APEX Control Guidelines

siteVIEW APEX controls are elements that represent I/O points. Controls are provided for contact inputs, contact outputs, analog inputs and temperature sensors.

siteVIEW APEX utilizes a subset of the National Instrument Measurement Studio control set: <http://www.ni.com/mstudio/gallery/start.htm> – four basic control types are supported: Boolean, Knob, Slide and Display. Each type has multiple styles and properties.

siteVIEW APEX loads a default set of controls and associated properties, upon first accessing a TASC device.

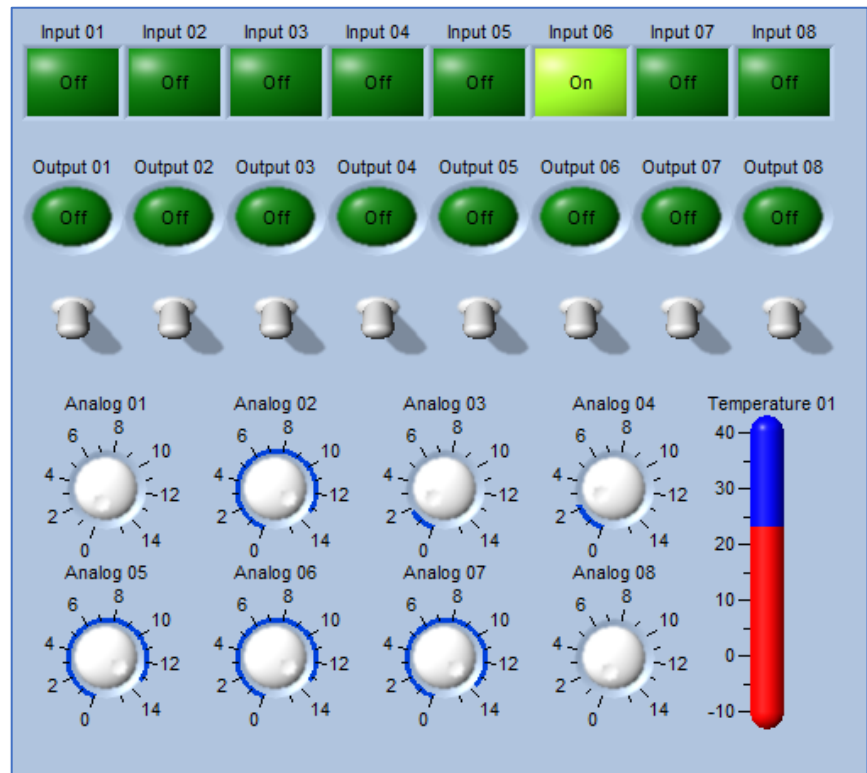


Figure 189 – Default siteVIEW APEX Controls

I.3.1. siteVIEW APEX Control Usage

- If siteVIEW APEX will be deployed on a touchscreen, sizing must take into account human ergonomics to ensure proper selection of siteVIEW APEX controls

I.3.2. Contact Input Controls

- Recommended type is Boolean
- Recommended style is LED. Do not use Toggle, Slide, Rocker or Button styles as they may indicate controllable characteristics
- Recommended color scheme:
 - For OFF status, use non-active color like grey
 - For ON status, use active color like green

I.3.3. Contact Outputs Controls

- Recommended type is Boolean
- Recommended styles are Toggle, Slide, Rocker or Button styles as they indicate controllable characteristics. Do not use LED styles.
- Recommended color scheme:
 - For OFF status, use non-active color like grey
 - For ON status, use active color like green

I.3.4. Analog Input Controls

- Recommended type is Knob, Slide or Display. Do not use Boolean.

I.3.5. Temperature Controls

- Recommended type is Knob, Slide or Display. Do not use Boolean.

I.4. Standard siteVIEW APEX Icon Sets

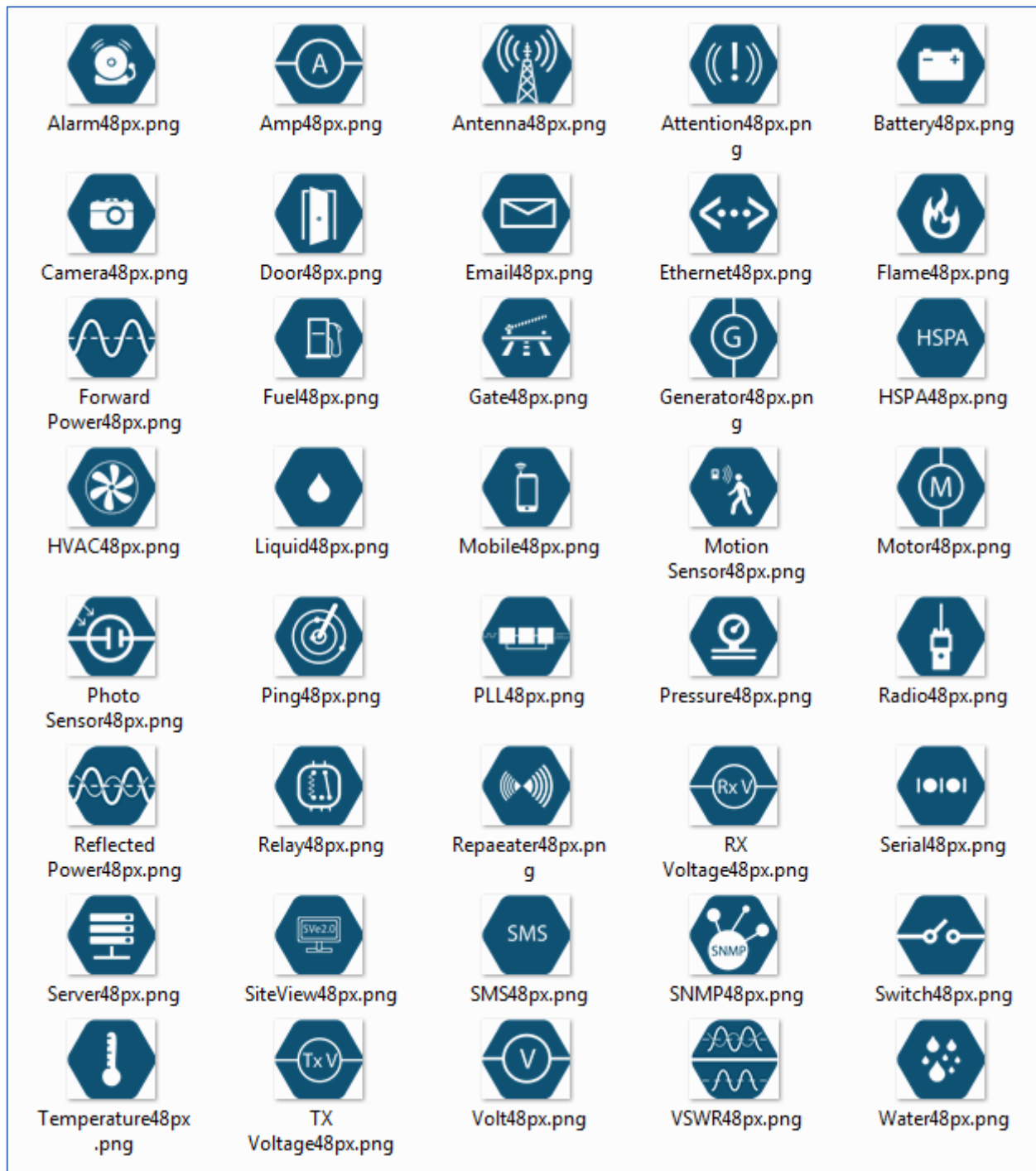


Figure 190 – Standard siteVIEW APEX Icon Set

APPENDIX J. SITEVIEW APEX ADMINISTRATION

J.1. siteVIEW APEX Deployment

As an enterprise solution, a siteVIEW APEX deployment involves multiple steps or phases. The following task guideline is provided to properly plan and implement a siteVIEW APEX deployment:

J.1.1. Device Planning

- Sensor planning – determine what is to be monitored and what sensors will be used to provide the monitoring capability.
- I/O assignment – based on the points to be monitored, use the device configuration software (e.g., SCCU) to define and enable the I/O layout map, including qualifiers, hold times and threshold ranges.
- Backhaul communications – determine the method in which the device will communicate events to siteVIEW.

J.1.2. System Communication/Network Design

- Determine the layout architecture of the various siteVIEW APEX components.
 - Location and redundancy of the siteVIEW APEX Data Manager.
 - To determine number and location of siteVIEW APEX TASC Communication Servers, consider communication load balancing for the number of managed devices.
 - Location of siteVIEW APEX Alarm Notification system by considering notification mechanisms to be used.
 - Location and number of siteVIEW APEX Clients required.
- Install the various siteVIEW APEX components.
- Determine siteVIEW APEX interfaces to other IT systems including SMTP servers, SNMP managers and backup systems.

J.1.3. siteVIEW APEX Client (User Interface) Design

- Implement panel design for each device including:

- Image design and import for background panel.
- Naming, location, type and theme selection for each I/O control.

J.1.4.siteVIEW APEX I/O Properties Refinement

- Select supported sensor settings (e.g., TASC differential sensors, TASC BPS sensors).
- Validate qualifiers, hold times, threshold and local output settings for each I/O point to ensure real-world congruency, and, if required, validate formula settings and offsets.
- Determine and configure site-mapping requirements.

J.1.5.siteVIEW APEX User Account Management

- Define user accounts and rights.
- Define groups and user access rights.

J.1.6.siteVIEW APEX Notification and Alarming Definition

- Use Global Notification Settings to define mechanisms to be used for notification.
- Use Alarm Settings to define alarms, configure the related notification methods and users to be notified.

J.1.7.siteVIEW APEX Communication Optimization

- Determine and configure polling strategy.
- Review system communications and mitigate communication retries by adjusting packet timeouts.
- Review communications load to determine if thresholds need to be adjusted or if devices should be balanced amongst TASC Communication Server servers.

J.1.8.Operational Preparedness

- Review logging infrastructure and resultant files.
 - For cases where the frequency of I/O and alarm history is high, further refine qualifiers, hold times and threshold to decrease the I/O and alarm events.

- If there is sufficient data, exporting to Excel or other analysis tool may provide insight into system tuning or trends.
- Using device configuration software (e.g., SCCU), create backups of the device's system.
- Export siteVIEW APEX panels for reuse and/or recovery. *(Panel export files maybe preferential for managing and tracking user interface changes where the rest of the system siteVIEW APEX configuration is static.)*
- Determine and configure system database scheduled archiving strategy. Define backup and recovery strategy, including off-site backups.
- Confirm operational readiness:
 - Confirm integration with other IT components.
 - Power stability (e.g., UPS).
 - Network stability and redundancy.
 - Consider managing all shutdowns, including shutting of operating system updates.
 - Create Windows restore points or system ghost copies in case of catastrophic failure.
- User and administrative training.