Johnson Controls

P2000AE

Security Management System

RMS-XML

Application Programming Interface

Version 4.1 and higher, December, 2008
24-10241-224 Revision –

P2000AE

Security Management System

RMS-XML

Application Programming Interface

Version 4.1 and higher, December, 2008

24-10241-224 Revision –

Johnson Controls
Security Solutions
(805) 522-5555
www.johnsoncontrols.com

Acknowledgment

TABLE OF CONTENTS

P2000AE RMS-XML INTERFACE

This document describes the Application Programming Interface (API) for the P2000AE Remote Messaging Service (RMS) XML Interface. This API details the data and interface requirements for both P2000 applications and third party applications to receive messages from the P2000 RMS-XML Interface. This API does not cover remote servers receiving messages in P2000 Binary format. This API is available for P2000 version 4.1 and higher.

NOTE

- *This document is intended to be used by programmers or other qualified professionals who posses a reasonable level of experience with application program writing.*
- *"P2000AE" is also referred to as "P2000" throughout this manual.*

OVERVIEW

The P2000 RMS-XML is a P2000 interface that allows a remote server or external application to receive real-time messages from the P2000 system. This interface "pushes" messages to computers that are defined as a Remote Server in the P2000 system and that are configured to receive the XML protocol. An external application needs to open an IP socket (at the configured port number) and listen for incoming connections. When the P2000 system has messages to send, it connects to the external computer and sends the data to the port. P2000 messages are sent encoded in XML format using HTTP Post type mechanism.

This interface enables applications to receive access grant and deny messages, hardware status change messages, alarm messages, and audit messages. A message filter can optionally be configured to limit the type of messages transmitted. The RMS-XML interface is an extension of the existing Remote Messaging Service (RMS) Interface that was designed to send P2000 real-time messages to other P2000 systems.

Figure 1: RMS-XML Interface Operation

DETAILS

Communication

The Remote Message Service receives all real-time messages from the RTL Route Service. For each configured remote server, RMS places messages to be sent into a queue for each remote server. If the message does not pass the configured message filter (if any), the message is not queued for that server. If RMS has messages in the queue for a remote server, it will open a TCP/IP socket to the configured remote server computer name or IP address. The message will then be written to the socket and RMS will wait for a valid response. When a valid response is received, the message will be removed from the queue. If a connection cannot be made to the remote server or a valid response is not received, the message remains in the queue and RMS will continue to attempt to send it.

Message Protocol

When a remote server entry is configured in P2000, the operator can select "XML Protocol" or "HTTP Post XML Protocol" ("Binary Protocol" is not covered by this document). If you select the "XML Protocol," the XML document containing the message will be written to the TCP/IP socket as an ASCII string. If you select the "HTTP Post XML Protocol," the XML document will be prefixed by a standard HTTP Post header similar to the following:

```
POST //computername HTTP/1.1<CR>
User-Agent: P2000/4.1.0<CR>
Host: remoteserver:39160<CR>
Server: remotesitename<CR>
Content-Type: text/xml<CR>
Content-Length: 340<CR>
<CR>
```

The XML document will be written to the socket as an ASCII string. A partial sample is shown below:

```
<?xml version="1.0"?><CR>
<P2000Message>
     <MessageBase>
          .
          .
     </MessageBase>
     <MessageDecode>
          .
          .
     </MessageDecode>
     <AlarmDetails>
          .
          .
     </AlarmDetails>
</P2000Message><CR>
```

NOTE

The third element (<AlarmDetails>) varies depending on the P2000 Message Type. For more detailed information, please refer to "Message Details" on page 6.

Expected Response

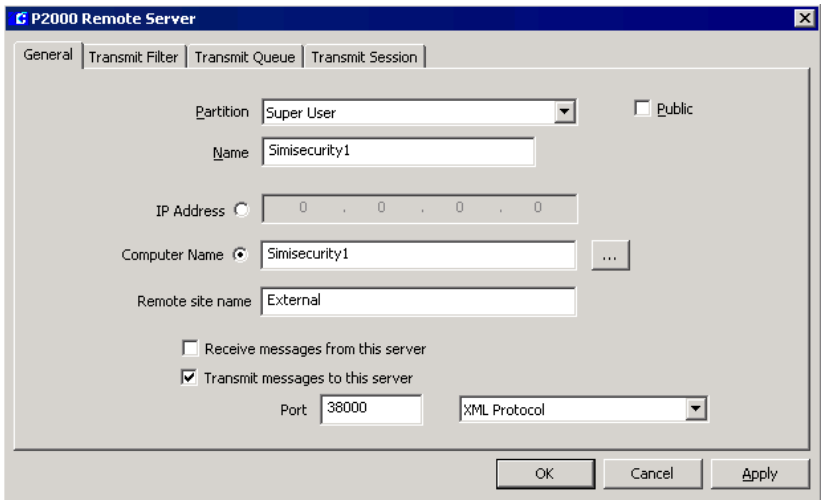
The remote server must respond to every received message by transmitting a valid HTTP response. An example response is shown below:

```
HTTP/1.1 200 OK<CR>
```

The RMS will verify that the response contains the string "200 OK." Any other responses will be considered a transmission failure and the message will remain in the queue to be transmitted again.

Configuration

In order to receive P2000 RMS XML messages, a new remote server entry must be added to the P2000 configuration. This configuration is located in the Remote Server branch of the System Configuration tree. The important configuration items on the General tab are the *Computer Name* (or IP Address), the *Transmit messages to this server* check box, the *Port* number, and the *Protocol*. The options on the Transmit Queue tab control the queue for storing messages to be transmitted. Below is a screen shot of the Remote Server configuration window:



Troubleshooting

The P2000 Remote Messaging Service can be run in "debug" mode to see additional information about messages that are being processed. You must first stop the RMS service using Windows or P2000 Service Control. Then open a command prompt in the P2000 "bin" directory and start the RMS service in debug mode with the following command:

```
RemoteMessageService -d
```

The RMS service will now operate as a console application and will output information to its console window. The RMS service can be stopped when running in debug mode by entering **<Ctrl> C** in its console window.

MESSAGE DATA

All P2000 messages contain at least 3 sections:

Message Base	The Message Base section includes data items that are common to all messages. This section contains all information needed to effectively filter messages.
Message Decode	The Message Decode section includes data items that contain text strings that summarize the message. These data items are the same strings that P2000 uses to populate the list of the Real Time List application.
Message Details	The Message Details section includes the data items that are specific to the message. The XML element name for the message details section varies depending upon message type.

Message Versions

The Message Base and Message Details sections both contain a "MessageVersion" data item. When messages are modified in P2000, the version of that message is changed. These version numbers will enable an external application to change processing based upon the message version if necessary.

MESSAGE REFERENCE

The P2000 RMS-XML interface currently supports three different P2000 message types: Audit Messages, Alarm Messages, and Real Time Data Messages. Real Time Data messages include most all of the messages that come from controllers such as Access Grant and Deny, Output State Change, Input State Change, etc. This interface will be extended in future versions of P2000 to include other message types.

Message Structure

All P2000 messages contain sections indicated in the following table:

Message Type	Sections	Section Node Name
Alarm Message (3)	Message Base	MessageBase
	Message Decode	MessageDecode
	Message Details	AlarmDetails
Audit Message (28675)	Message Base	MessageBase
	Message Decode	MessageDecode
	Message Details	AuditDetails
Real Time Data Message (28673)	Message Base	MessageBase
	Message Decode	MessageDecode
	Message Details	TransactionDetails
Others	Message Base	MessageBase

Message Base

The Message Base section includes data items that are common to all messages. This section contains all information needed to effectively filter messages. The Message Base section contains the following data items:

BaseVersion	integer version number of the Message Base
MessageType	integer message type number (see “Message Types” below)
MessageSubType	integer message sub-type number (message type specific, see below)
SiteName	site generating message
PartitionName	partition that owns message
Public	flag to indicate if message is public
ItemName	item name associated with message
QueryString	query string from message item
Category	alarm category of message (only valid for alarm messages)
Escalation	alarm escalation level of message (only valid for alarm messages)
Priority	alarm priority level of message (only valid for alarm messages)
OperatorName	operator username for message (only valid for alarm and audit messages)

Message Types

The MessageType values in the Message Base section of a message will be one of the following:

Alarm Message	3
Real Time Data Message	28673
Audit Message	28675

Message Decode

The Message Decode section includes data items that contain text strings that summarize the message. These data items are the same strings that P2000 uses to populate the list in the Real Time List application. The Message Decode section contains the following data items:

MessageDateTime	the data and time of the message
MessageTypeText	a text string of the message type
MessageText	a short text string summary of the message
DetailsText	a text string of the important message details

Message Details

The Message Details section includes the data items that are specific to the message.

Audit Message

An Audit Message contains the following data items:

MessageVersion	the version of the Audit message
LocalTimestamp	the local date and time of the audit message
UTCTimestamp	the UTC date and time of the audit message
ItemType	the type of item being changed
Action	the type of action being taken on the item
ItemID	the database ID of the item
ItemGuid	the database Guid of the item
DataChanged	the data that was changed based on this audit

NOTE

Some audit messages may not contain a valid ItemID and/or ItemGuid. In addition, only BLL-based applications support the propagation of the DataChanged element. Legacy applications (e.g. PanelEdit), will not provide any information on this element.

Audit Item Types

The ItemType data item of an audit message indicates what type of item is being changed. The ItemType data member of an audit message contains the same value as the MessageSubType data member of the MessageBase section. The following list details the value for ItemType data items for Audit messages:

Unknown	0	Floor Name Configuration	51
User	1	Cabinet	52
Badge	2	Door Group	53
Badge Layout	3	Door Mask	54
Badge Fields	4	Door Name Configuration	55
Badge Encode	5	Area	56
ID Badge	6	Muster Zone	57
Entity	7	Area Control Layout	58
Panel	8	Connections	59
Terminal	9	CCTV Server	60
Partition	10	CCTV Switch	61
Terminal Group	11	CCTV Tour	62
Access Group	12	CCTV Alarm	63
Holiday	13	CCTV Macro	64
Timezone	14	CCTV System Auxiliary	65
Input Point	15	CCTV Monitor	66
Input Group	16	CCTV Sequence	67
Panel Holiday	17	CCTV Camera	68
Access Template	18	CCTV Preset	69
Alarm Response Text	19	CCTV Pattern	70
Alarm Instruction	20	CCTV Camera Auxiliary	71
Company	21	Enable Code	72
Output Point	22	P900 Flag	73
Output Group	23	P900 Counter	74
Department	24	P900 Trigger Event	75
Panel Timezone	25	P900 Trigger Link	76
Soft Alarms	26	P900 System Parameters	77
Site Parameters	27	Auto-badge Number	78
Workstation	28	Common PIN	79
Map	29	P900 Sequence File	80
Map Icon Set	30	Remote Server	81
User Defined Field	31	Message Filter	82
Event	32	Message Filter Group	83
Panel Card Event	33	Local Site	84
Alarm Filter	34	Service Startup Configuration	85
Message Forwarding	35	Application	86
Permission Group	37	Panel Card Format	87
Panel Relay	38	Reason	88
Report	39	Security Level Range	89
MIS Interface	40	Import File	90
Image Recall Filter	41	Import Consolidation	91
Counter	42	Import Badge Format	92
Action Interlock	43	Audit	94
External IP Address	44	Alarm History	95
Guard Tour Definition	45	Alarm	96
Tour Station Definition	46	Generic Text	97
Loop	47	Muster History	98
Elevator	48	Guard Tour History	99
Floor Mask	49	Transaction History	100
Floor Group	50	Redundancy	101

Audit Actions

The Action data member of an audit message indicates what action the operator is taking on the item. The following list details the value for Action data items for Audit messages:

Execute	0	Redundancy Admin	53
Logon	1	Redundancy Reboot	54
Logoff	2	Redundancy Configuration Export	55
Add	3	Redundancy Configuration Import	56
Edit	4	Download Firmware	57
Delete	5	Verify Firmware	58
Print	6	Apply Firmware	59
Download	7	Erase Database	60
Set	8	Reboot	61
Reset	9	Resync IN	62
Lock	10	Resync OUT	63
Unlock	11	Resync UNDEFINED	64
Timed Override	12	Suppress	65
Lock All	13	Emergency Disable	66
Unlock All	14	Arm	67
Update	15	Forced Arm	68
Write Flash	16	Disarm	69
Start Muster	17	Start Bypass	70
Stop Muster	18	Stop Bypass	71
Demuster	19	Zone Reset	72
Zone Ready	21	Zone Reset Ack	73
Start Muster Drill	22	Activate	74
Print Group	25	Silence	75
Remove Badge	26	Test	76
Expand Zone	27	Resync All	77
Enable Print	28	Reset Entry Time	78
Disable Print	29	Reset Exit Time	79
Save Data	30	Reset All Entry Times	80
Pulse	31	Reset All Exit Times	81
Enable	32	Fast Download Transfer	82
Clear	33	Fast Download Update	83
Disable	34	Fast Download Rebuild	84
Force	35	Fast Download Shrink	85
Calibrate	36	Initial Entity Resync	86
Uncalibrate	37	Update Entity Resync	87
Set in use	38	MCO Status Change	88
Set available	39	Call Station	89
Manual Trigger	40	Terminate Call	90
Store Default	41	Accept Call	91
Security Level	42	Forward Call	92
Logon Invalid	43	Hold	93
Logon Disabled	44	Isolated Station	94
FDA Backup	45	Unisolated Station	95
FDA Violation	46	Start Monitoring	96
FDA Digital Signature	47	Stop Monitoring	97
Redundancy Failover	48	Remoted Station	98
Redundancy Offline	49	Unremoted Station	99
Redundancy Online	50	Changed Value	100
Redundancy Mirror	51	Stop suppressing	101
Redundancy Monitor	52		

Alarm Message

An Alarm Data Message contains the following data items:

MessageVersion	the version of the Alarm message
AlarmGuid	the database Guid of this alarm
AlarmID	the database ID of this alarm
AlarmType	the alarm type (see “Alarm Types” on page 10)
AlarmTypeName	the alarm type name
AlarmTypeID	the database ID of the item for this alarm
AlarmTypeGuid	the database Guid of the item for this alarm
AckRequired	flag to indicate if this alarm requires an ack before it can be completed
ResponseRequired	flag to indicate if this alarm requires a response before it can be completed
InstructionText	the instruction text for this alarm
AlarmState	the state of the alarm (See “Alarm States” on page 11)
AlarmTimestamp	the timestamp of the alarm state
ConditionState	the state of the triggering condition (dependent upon the triggering item)
ConditionSequenceNumber	incremented every time the triggering item changes state
ConditionSequenceGuid	a GUID unique to every condition state change for this alarm
ConditionCompletionState	the state that the triggering item must be in before the alarm can be completed
ConditionTimestamp	the timestamp of the condition state
Popup	flag to indicate if Alarm Monitor should pop to the foreground
Description	the text description of this alarm
AlarmSiteName	the site that generated this alarm
AlarmOptionGuid	the GUID defining the additional alarm options and references of this alarm
AlarmResponseText	the response text for this alarm

In addition, some alarm types add additional data items. The alarm types that add additional data are detailed next.

Alarm Types

The following list details the possible Alarm Type values.

Generic Alarm	1	AV System Alarm	16
Panel Input Point Alarm	2	Intrusion Zone Alarm	17
Area Alarm	3	Access Rights Expired	18
Guard Tour Alarm	4	Alternate Access Granted	19
Muster Running Alarm	5	Asset Tracked	20
Muster Zone Status Alarm	6	Central Access Denied	21
Muster When Disabled Alarm	7	Central Data Unreachable	23
Muster Aborted	8	Central Status Unreachable	24
Loop Tamper Alarm	9	Entity Expired	25
Host Event Generated Alarm	10	Entity Tracked	26
MSEA Alarm	11	Entity Validated	27
AV Motion Alarm	12	Error	28
AV Behavior Alarm	13	Incomplete Group	29
AV Video Loss Alarm	14	Incomplete Group Rule	30
AV Dry Contact Alarm	15	Inconsistent Identifiers	31

Invalid Access Level	32	Invalid Reader	81
Invalid Access Mask	33	Invalid Security Level	82
Invalid Access Profile	34	Local Grant	83
Invalid Access Group	35	Manual Reader	84
Invalid Access Group Timezone	36	Notification Event Dropped	85
Invalid Override Privilege	37	Timed Override	89
Invalid Override Time	38	Panel Down	90
PIN Attempts Exceeded	39	Forced Door Suppressed	91
Invalid Security Mask	40	Controller Event Activate	92
Invalid Smart Card Signature	41	Controller Event Inactive	93
Manual Panel Event	42	Memory Low	94
No Entry	43	Propped Door Suppressed	95
Occupancy Violation	44	Intrusion Area	96
Portal Open Violation	45	Fast Download Started	97
Team Member Validated	46	Fast Download Failed	98
Unaccompanied Asset	47	Fast Download Succeeded	99
Unaccompanied Asset Rule	48	Elevator	100
Unaccompanied Entity	49	Elevator Controller Not Operational	101
Unaccompanied Entity Rule	50	Reader Duress	102
Anti-Loitering Violation	51	Soft AntiPassback Violation	103
Occupancy Limit	52	Soft Occupancy Violation	104
Fault	53	Executive Privilege	105
Anti-Passback Not Operational	54	Intrusion Annunciator Silence	106
Anti-Passback On	55	Firmware Upgrade Failed	107
Output	58	High CPU Usage	108
Biometric Mismatch	59	Anti-Passback Resync	109
Deny Intrusion Area Armed	60	Anti-Passback Reset	110
Door Status	61	Entity Transition In	112
Facility Code Error	62	Entity Transition Out	113
Hardware Module not operational	63	Entity Transition Undefined	114
Hardware Module upgrade failed	64	Entity Entry Time Reset	115
Hardware Module upgrading	65	Entity Exit Time Reset	116
Intrusion Annunciator	66	Entity Configuration Mismatch	117
Intrusion Area Armed	67	ACO not operational	118
Intrusion Zone Armed	71	Interlock State	119
Invalid Card	74	Integration Server	120
Invalid Entity	75	Time Synchronization Problem	121
Invalid Event	76	XMan X-Ray Machine	122
Invalid Event Privilege	77	Device Failure	123
Invalid Entry-Exit	78	Device Down	124
Invalid Issue Level	79	LEC Door Status	125
Invalid PIN Code	80	APM Status	126

Alarm States

The following list details the possible Alarm State values:

Complete	1
Responding	2
Acknowledged	3
Pending	4

Area Alarms

An Area Alarm adds the following data items under the node "/P2000Message/AlarmDetails/AreaDetails":

AreaAlarmVersion	the version of the Area Alarm message
AreaName	the name of the area
AreaAlarmSubtype	the area alarm subtype

AV Behavior Alarms

An AV Behavior Alarm adds the following data items under the node "/P2000Message/AlarmDetails/AVDetails":

AVBehaviorAlarmVersion	the version of the AV Behavior Alarm message
AVChannelID	the AV Channel database ID
AVSiteID	the AV Site database ID

AV Dry Contact Alarms

An AV Dry Contact Alarm adds the following data items under the node "/P2000Message/AlarmDetails/AVDetails":

AVDryContactAlarmVersion	the version of the AV Dry Contact Alarm message
AVChannelID	the AV Channel database ID
AVSiteID	the AV Site database ID

AV Motion Alarms

An AV Motion Alarm adds the following data items under the node "/P2000Message/AlarmDetails/AVDetails":

AVMotionAlarmVersion	the version of the AV Motion Alarm message
AVChannelID	the AV Channel database ID
AVSiteID	the AV Site database ID

AV System Alarms

An AV System Alarm adds the following data items under the node "/P2000Message/AlarmDetails/AVDetails":

AVSystemAlarmVersion	the version of the AV System Alarm message
AVSystemID	the AV System database ID
AVSiteID	the AV Site database ID
AlarmDescription	the text alarm description

AV Video Loss Alarms

An AV Video Loss Alarm adds the following data items under the node "/P2000Message/AlarmDetails/AVDetails":

AVVideoLossAlarmVersion	the version of the AV Video Loss Alarm message
AVChannelID	the AV Channel database ID
AVSiteID	the AV Site database ID

Guard Tour Alarms

A Guard Tour Alarm adds the following data items under the node "/P2000Message/AlarmDetails/GuardTourDetails":

GuardTourAlarmVersion	the version of the Guard Tour Alarm message
TourName	the Guard Tour name
StationName	the Station name
GuardTourAlarmSubtype	the Guard Tour Alarm subtype

Input Point Alarms

An Input Point Alarm adds the following data items under the node "/P2000Message/AlarmDetails/InputDetails":

InputPointAlarmVersion	the version of the Input Point Alarm message
PointStateChange	flag to indicate a point state change
PanelID	the Panel database ID
PanelName	the Panel name
TerminalID	the Terminal database ID
TerminalIndex	the Terminal index
TerminalName	the Terminal name
PointNumber	the Point number
PointName	the Point name
PrevPointState	the previous Point state
PointState	the current Point state
StatusFlag	flag to indicate the Point status

Loop Tamper Alarms

A Loop Tamper Alarm adds the following data items under the node "/P2000Message/AlarmDetails/LoopTamperDetails":

LoopTamperAlarmVersion	the version of the Loop Tamper Alarm message
LoopID	the Loop database ID
LoopNumber	the Loop number
TamperAlarm	flag to indicate if it is a tamper alarm

Muster Alarms

A Muster Alarm adds the following data items under the node "/P2000Message/AlarmDetails/MusterDetails":

MusterAlarmVersion	the version of the Muster Alarm message
ZoneName	the Zone name
HardwareStatus	the status of the hardware causing the alarm

Intrusion Zone Alarms

An Intrusion Alarm adds the following data items under the node "/P2000Message/AlarmDetails/IntrusionZoneDetails":

IntrusionAlarmVersion	the version of the Intrusion Zone Alarm message
IntrusionAlarmSubType	the intrusion alarm sub type

Real Time Data Message

The data items of a Real Time Data message vary depending upon the History Type of the message. Some data items will not contain valid data for all History Types. For example, an Access Grant message will contain panel and terminal data but will not contain point data. A Real Time Data Message may contain the following data items:

MessageVersion	the version of the Real Time Data message
HistoryGroup	the history group (see "History Group Types" on page 16)
HistoryType	the history type (see "History Types" on page 16)
HistorySubType	the history sub type (see "Item Sub Types" on page 20)
LocalTimestamp	the local date and time of the message
PanelID	the Panel database ID (if applicable)
PanelName	the Panel name (if applicable)
TrunkNumber	the trunk number on which the terminal resides (if applicable)
TerminalID	the Terminal database ID (if applicable)
ItemGuid	the database Guid of the Item a message is generated for (if applicable)
TerminalIndex	the Terminal index (if applicable)
TerminalName	the Terminal name (if applicable)
PointID	the Point database ID (if applicable)
PointNumber	the Point number (if applicable)
PointName	the Point name (if applicable)
IdentifierGuid	the database GUID of the identifier (if applicable)
IdentifierNumber	the Identifier number (if applicable)
FacilityCode	the Facility Code of the badge (if applicable)
EventName	the Event name (if applicable)
SecurityLevel	the Security Level (if applicable)
RTLDataGuid	the database Guid of the transaction record in the "xaction" table
SourceMsgGuid	a GUID to group multiple XACTION messages belonging to the same source message received from, for example a controller

RequestID	From P2000 V4.1 onwards it contains the number that is generated by the host when initiating an access request to an ACO object. If no host request, the number is 0.
ItemSubTypeGuid	Sub type of the Item a message is generated for (see “Item Sub Types” on page 20)
ItemStatus	Status of the Item. Unless the ItemSubTypeGuid refers to a *Muster Zone*, the value of -1 indicates that the status has not changed
XmlAdditionalInfo	Xml Document (if applicable)

Badge Data

If the Real Time Data message contains badge data (for messages such as Access Grant), the following data items will be added:

Direction	the direction of the access (0 = undefined, 1 = IN, 2 = OUT)
IdentifierTrace	flag to indicate if this is a badge trace message
IssueLevel	issue level of the badge
ActionInterlockGuid1	the database GUID of the first Action Interlock of the access profile associated with the identifier
ActionInterlockValue1	the floating point value of the first Action Interlock of the access profile associated with the identifier
ActionInterlockGuid2	the database Guid of the second Action Interlock of the access profile associated with the identifier
ActionInterlockValue2	the floating point value of the second Action Interlock of the access profile associated with the identifier

Entity Data

If the Entity Name is filled within the message, the following data items will be added:

EntityGuid	the entity's database GUID that owns the badge
EntityFirstName	the entity’s first name
EntityMiddleName	the entity’s middle name
EntityName	the entity’s name
EntityID	The entity’s ID

Elevator Data

If the Real Time Data message contains badge data (for messages such as Invalid Floor), the following data items will be added:

ElevatorType	the Elevator type (1 = Elevator, 2 = Cabinet)
ElevatorID	the Elevator database ID
ElevatorName	the Elevator name
ElevatorFloor	the Elevator floor number
ElevatorFloorName	the Elevator floor name

Timed Override Data

TimedOverride	the duration of the timed override

History Group Types

P2000 V4.1 introduced the history group type as part of the history message. The history group type contains the filter category for real time list. P2000 V4.1 supports the following History Group types:

Unknown	0
Panel	1
Alarm	2
Access Deny	4
Access Grant	8
Host	16
Guard Tour	32
Elevator	64
Cabinet	128
Area	256
Mustering	512
Audio Video	1024
Intrusion	2048
Trace	4096

Please note that history messages associated with identifier data can belong to two categories: their primary group (i.e. Access Grant, Access Deny, etc.) and the group "Trace." The history group value provided within the message is then the combination of these two history group types.

History Types

The following list details the possible History Type values. Note that many of these History Types are generated by different models of controllers and no one model of controller will generate all of them.

Reader Up	1	Invalid Entry-Exit	36
System Restart	3	Invalid Access Group Timezone	37
Reader Down	5	Invalid PIN Code	38
System Image Success	8	Invalid Issue Level	39
System Image Fail	9	Host Deny (NMAN Rule)	40
Facility Code Error	10	Invalid Security Level	41
System Event Activated	11	Invalid Reader Timezone	42
System Event Deactivated	12	Timed Override Expired	43
Unlock All Doors	15	Invalid Event	44
Lock All Doors	16	Invalid Event Privilege	45
Output Set	17	Biometric Mismatch	46
Output Reset	18	Open Door	47
Reader Locked	19	Denied Intrusion Area Armed	48
Reader Unlocked	20	Major Grant	64
Reader Held Open	21	Host Grant	65
Reader Forced Open	22	Executive Privilege	67
Valid & Unauthorized	23	Local Grant	68
Major Deny	32	Timed Override Enabled	69
Invalid Card	33	Timed Override Disabled	70
Anti-Passback On	34	Timed Override Enabled Host	71
Invalid Reader	35	Timed Override Disabled Host	72

Panel Card Event Activated	73
Panel Card Event Deactivated	74
Soft In-X-It Violation	75
Assisted Access	76
Assisted Access Host	77
Manual Reader	78
Elevator Access Grant	79
Reader Egress	80
Duress Grant	81
Host Duress Grant	82
Alarm Set	96
Alarm Reset	97
Alarm Acknowledge	98
D620 Tamper Alarm Set	99
D620 Tamper Alarm Reset	100
Door Open Alarm	101
Duress	102
PIN Code Retry Alarm	103
Forced Door	104
Card Parity Alarm	105
Prox Card Low Battery Alarm	106
D620 AC Power Set Alarm	107
D620 AC Power Reset Alarm	108
D620 Low Battery Set Alarm	109
D620 Low Battery Reset Alarm	110
Reader Low Battery Set Alarm	111
Reader Low Battery Reset Alarm	112
Reader AC Set Alarm	113
Reader AC Reset Alarm	114
Reader Tamper Set Alarm	115
Reader Tamper Reset Alarm	116
Alarm Open	117
Alarm Short	118
Calibrated	123
Alarm Suppressed	125
APM Tamper Set	128
APM Tamper Clear	129
LEC Open	144
LEC Propped	145
LEC Forced	146
LEC Closed	147
Node Up	224
Fallback	225
Converter Tamper Set Alarm	226
Converter Tamper Reset Alarm	227
Node Down	228
Redundancy Primary System	256
Redundancy Standby System	257
Redundancy Data Link	258
Redundancy IO Link	259
Redundancy HD Primary System	260
Redundancy HD Standby System	261
Redundancy Serial PS Link	264
Host Grant Entry	266
Host Grant Exit	267
Host Duress Grant (Entry)	268
Host Duress Grant (Exit)	269
VCR Tape Low	287
Major Module	288
VCR Reel Lock	289
VCR Cylinder Lock	290
VCR Mechanical Lock	291
Input Module Up	292
Output Module Up	293
Input Module Down	294
Output Module Down	295
All Modules Up	296
All Modules Down	297
CCTV No Response	768
CCTV Incorrect Response	769
CCTV Control Down-Up	770
CCTV Control Up-Down	771
CCTV Normal	772
AV Monitor Set	773
AV Monitor Not Set	774
AV Camera Set	775
AV Camera Not Set	776
CCTV Command Error	777
CCTV Transmission Error	778
Input Point Pending Alarm	784
Input Point Acknowledged Alarm	785
Input Point Responded Alarm	786
Input Point Pending Secure	787
Input Point Acknowledged Secure	788
Input Point Responded Secure	789
Input Point Pending Open	790
Input Point Acknowledged Open	791
Input Point Responded Open	792
Input Point Pending Short	793
Input Point Acknowledged Short	794
Input Point Responded Short	795
Redundancy Crash	1024
Redundancy Restore	1025
Redundancy Power Up	1026
Redundancy Shutdown	1027
Redundancy Started	1028
Redundancy Network Failure	1029
Redundancy Network Restore	1030
Redundancy Serial Failure	1031
Redundancy Serial Restore	1032
Redundancy Wall Power UPS	1033
Redundancy Periodic Check	1034
Redundancy Modem Check	1035
Intrusion Annunciator Silence	1280
Intrusion Annunciator Error	1281
Intrusion Annunciator Unknown	1282
Intrusion Annunciator Active	1283
Intrusion Annunciator Inactive	1284
Intrusion Area Armed	1296
Intrusion Area Disarmed	1297
Intrusion Area Mixed	1298
Intrusion Area Arming	1300
Intrusion Area Disarming	1301
Intrusion Area Error	1302
Intrusion Area Unknown	1303
Intrusion Area Fault	1304
Intrusion Keypad Error	1312
Intrusion Keypad Unknown	1313

Intrusion Zone Alarm	1328
Intrusion Zone Bypass	1329
Intrusion Zone Acknowledge	1332
Intrusion Zone Error	1333
Intrusion Zone Unknown	1334
Intrusion Zone Normal	1335
Intrusion Zone Alarm Trouble	1337
Intrusion Zone Alarm Tamper	1338
Intrusion Zone Alarm Open	1339
Intrusion Zone Alarm Short	1340
Intrusion Zone Armed	1341
Intrusion Zone Disarmed	1342
Intrusion Zone Fault	1343
Intrusion Zone Arming	1344
Intrusion Zone Disarming	1345
Intrusion Zone Unbypassed	1346
Intrusion Zone Tamper	1347
Intrusion Zone Open	1348
Intrusion Zone Sealed	1349
Intrusion Area Zones Bypassed	1350
Intrusion Area Zones Unbypassed	1351
Intrusion Area Zones Sealed	1352
Intrusion Area Zones Unsealed	1353
Device Connected	1354
Device Disconnected	1355
Device Invalid Vendor Address	1356
Device Valid Vendor Address	1357
Device Port Opened	1358
Device Port Closed	1359
Device Mains Failure	1360
Device Mains Normal	1361
Device Battery Low	1362
Device Battery Normal	1363
Device Battery Test	1364
Device Battery Test Done	1365
Device Battery Test Failure	1366
Device Battery Test Success	1367
Device Battery Missing	1368
Device Battery Inplace	1369
Invalid Entity	1536
Memory Low	2023
Memory Normal	2024
ACO Error	4096
Central Data Request	4097
Central Status Request	4098
Manual Panel Event	4099
Asset Tracked	4101
Entity Tracked	4102
Entity/Asset Validated	4103
Team Member Validated	4104
Alternate Access Granted	4105
No Entry	4107
PIN Attempts Exceeded	4111
Invalid Access Group	4113
Invalid Access Mask	4115
Invalid Access Level	4116
Invalid Security Mask	4117
Occupancy Violation	4121
Invalid Override Time	4122
Invalid Override Privilege	4123
Central Data Unreachable	4124
Central Status Unreachable	4125
Central Access Denied	4126
Access Rights Expired	4127
Entity Expired	4128
Unaccompanied Asset Rule	4129
Unaccompanied Entity Rule	4130
Incomplete Group Rule	4131
Portal Open Violation	4132
Unaccompanied Asset	4133
Unaccompanied Entity	4134
Incomplete Group	4135
Invalid Access Profile	4137
Inconsistent Identifiers	4138
Invalid Smart Card Signature	4140
ACO operational	4141
ACO Fault	4142
ACO Unknown	4143
DSO Fault	4353
Door Locked and Open	4354
Door Locked and Closed	4355
Door Unlocked and Open	4356
Door Unlocked and Closed	4357
Door Status Unknown	4358
Suppress propped door on	4359
Suppress propped door off	4360
Suppress forced door on	4361
Suppress forced door off	4362
Fast Download Started	4384
Fast Download Succeeded	4385
Fast Download Failed	4386
Supervised Input Unknown	4608
Output Unknown	4688
Notification Events Dropped	4704
Controller Event Activated	4720
Controller Event Deactivated	4721
Controller Event Error	4722
Node Up Duplicate	20481
Reader Status Unknown	20482
Input Status Unknown	20483
Output Status Unknown	20484
Node Disconnected	20485
Node Misconfigured	20486
Panel Reboot from Flash	20487
Input Point Set	20576
Input Point Reset	20577
Input Point Open	20597
Input Point Short	20598
Input Point Suppressed	20599
Input Point Unknown	20600
Event Triggered	24577
Event Triggered Manually	24578
Duress Alarm	28673
Start	28674
Running	28675
Station Early	28676
Station Late	28677
Out of Order	28678

Stopped	28679	T&A Break Start	41101
Restarted	28680	T&A Break End	41102
Aborted	28681	T&A Lunch Start	41103
Completed	28682	T&A Lunch End	41104
Late Time	28683	Work Schedule Grace Period Start	41105
Terminated	28684	Work Schedule Grace Period End	41106
Area Reader Exit	32769	Anti-Passback Entry Time Reset	41476
Area Reader Entry	32770	Anti-Passback Exit Time Reset	41477
Area Input Exit	32771	MCO State 0	41728
Area Input Entry	32772	MCO State 1	41729
Area Manual Exit	32773	MCO State 2	41730
Area Manual Entry	32774	MCO State 3	41731
AV Motion	36865	MCO State 4	41732
AV Behavior	36866	MCO State 5	41733
AV Video Loss	36867	MCO State 6	41734
AV Dry Contact	36868	MCO State 7	41735
AV System	36869	MCO State 8	41736
Occupancy Within Limits	40976	MCO State 9	41737
Occupancy At Low Limit	40977	MCO State 10	41738
Occupancy At High Limit	40978	MCO State 11	41739
Occupancy Below Limit	40979	MCO State 12	41740
Occupancy Above High Limit	40980	MCO State 13	41741
Fault	40981	MCO State 14	41742
Fault - Invalid Configuration	40982	MCO State 15	41743
Out of Memory Fault	40983	MCO State 16	41744
General Fault	40984	MCO State 17	41745
Occupancy Fault	40985	MCO State 18	41746
ACO Door Sequence Fault	40986	MCO State 19	41747
ACO Primary Reader Fault	40987	MCO State 20	41748
ACO Secondary Reader Fault	40988	MCO State 21	41749
Anti-Passback Operational	40992	MCO State 22	41750
Anti-Passback not Operational	40993	MCO State 23	41751
Anti-Passback Peers Offline	40994	MCO State 24	41752
Anti-Passback-Star Center Offline	40995	MCO State 25	41753
Anti-Passback Fault	40996	MCO State 26	41754
Hardware Module Operational	41008	MCO State 27	41755
Hardware Module not Operational	41009	MCO State 28	41756
Hardware Module Upgrading	41010	MCO State 29	41757
Hardware Module Upgrade Failed	41011	MCO State 30	41758
Hardware Module Fault	41012	MCO State 31	41759
Anti-Loitering Violation	41040	MCO State Unknown	41760
Unprocessed Event	41041	Interlock False	41984
Security Level Changed	41066	Interlock True	41985
Elevator Controller Operational	41072	Interlock Fault	41986
Elevator Controller Not Operational	41073	Interlock Unknown	41987
Elevator Controller Fault	41074	Intrusion Up	45057
Soft AntiPassback Violation	41075	Intrusion Down	45058
Soft Occupancy Violation	41076	Integration Up	45072
CPU Usage too high	41088	Integration Down	45073
Firmware Upgrade Failed	41091	Time Sync Problem	45074
Anti-Passback IN	41092	Integration Heart Beat Received	45075
Anti-Passback OUT	41093	Device Up	46352
Anti-Passback Undefined	41094	Device Down	46353
Anti-Passback Resync Request	41095	Logged On	46368
Anti-Passback Reset	41096	Logged Off	46369
Work Schedule Start	41097	Not Installed	46370
Work Schedule End	41098	Not Ready	46371
T&A Shift Start	41099	Ready	46372
T&A Shift End	41100	Busy	46373

Hold	46374	Released	50009
Offline	46416	Interviewed	50010
Idle	46417	Released After Interview	50011
Call Request	46418	Retained After Interview	50012
Call on Hold	46419	Invalid	50032
Incoming Call	46420	Not Connected	50033
Connect Station	46421	Ready	50034
Call Terminated	46422	Busy	50035
Isolated	46423	Created	50036
Fault	46424	Configured	50037
Tamper	46425	Fatal Error	50038
Unisolated	46426	Not Ready	50039
Remoted	46427	Scan Status Invalid	50048
Unremoted	46428	Scan Done	50049
Monitor Started	46429	Scan Rejected	50050
Monitor Stopped	46430	Scan Aborted	50051
Fault Recovered	46431	Scan Do	50052
Tamper Recovered	46432	Scan Dummy	50053
Entry (Random Search)	50000	Scan Timeout	50054
Entry (Manual Search)	50001	Scan Done (Forced)	50055
Entry (Free Pass)	50002	Scan Operator Override	50056
Exit (Random Search)	50003	Scan Error	50057
Exit (Manual Search)	50004	Scan Search	50058
Exit (Free Pass)	50005	Scan Search Forced	50059
Entry (Guilty)	50006	Scan Dummy Forced	50060
Exit (Guilty)	50007	Scan Manual Rec	50061
Free Pass	50008		

Item Sub Types

Following are Item Sub Types defined in the enumeration with ID of 200513. P2000 utilizes GUIDs associated with item sub types in Real Time Data messages. The Value column lists enumeration values associated with the item type.

Item Sub Type Name	Item Sub Type Guid	Value
Unknown	00000000-0000-0000-0000-000000000000	N/A
CK722 Panel	DD16345F-7B10-4FC1-ADBC-AB22D9E72B07	100
Legacy Panel	21C05043-E489-4121-98DE-BC7DD114EBCC	101
Legacy Input Terminal	3EFE1894-7CFC-4DCB-A98C-1CD03752DC19	200
Legacy Output Terminal	602CB784-585F-48B9-B60A-50671D88B0DA	201
Legacy Reader Terminal	A9A13094-E53B-4D54-9942-8649FC32A7C2	202
Legacy Input Point	73C04F1B-ECD7-4BA2-9AEB-E2AD72749E28	300
Legacy Soft Input Point	42072CB3-DDDC-4C7F-B92F-56D8B23EED0C	301
CK722 Input Point	0BFBE143-791B-44CF-AFC4-FFBC392D68B6	302
Legacy Output Point	BD6A6EF3-F1F6-4090-A7BA-9FAE58C1678A	400
CK722 Output Point	770D5C08-D5DE-4762-BF7F-AEB72AB3CEBE	401
ACO Terminal	FE8AF097-019B-43D5-974E-23DB54740DE8	500
DSO Terminal	70091B98-CEED-4005-B33F-3578658DA5FE	600
Anti-Loitering	EA5D3313-DEE8-42A9-89D8-F2824172FE98	700
Anti-Passback	CB4609A2-25E6-4893-A086-408AE5D37B06	800
P2000 Area	A7219FF8-0E9B-4740-BC70-2435A431D5ED	900
T&A Terminal	EF4E5381-18AD-4D0F-AE78-41E04BBB35C5	1000

Item Sub Type Name	Item Sub Type Guid	Value
MLT T&A Terminal	FF9A6800-DA7E-4CCE-BA3A-F83E5927D76D	1001
S300 Hardware Module	8541C067-7395-4A40-8EB5-618726F22D5A	1100
CK720 Elevator	A0ACA367-FFB1-40E8-9DFA-DBA812FD3D70	1200
CK722 Elevator	F88880FC-13BB-43C8-A419-6605DC7BC65F	1201
Guard Tour	37FB232A-0DAE-497C-ACF8-953460A65064	1300
Muster Zone	4612A19A-5190-4118-86F3-010952AD646B	1400
Intercom Station	D90DED9E-A247-4672-89D6-1DD0EC10FF65	1500
Jacques Intercom Master Station	14DC0322-3347-49C3-B20E-136CFD7F7D75	1501
Jacques Intercom Slave Station	A5DB3129-94D6-43AE-90DD-C1FF511D9B5F	1502
Occupancy	73175B01-8AA3-44F9-A547-A61FC1AED953	1600
Notification Object	84FC4FDB-09A7-48D4-9264-69802EF226FA	1700
P2000 Counter	1EC1AA0D-14D3-4800-AB51-7860D4092F37	1800
P2000 Event	17D4BBCE-451C-4853-A62A-35B98D3E1304	1900
Intrusion Annunciator (CK722)	579AEB05-5EEE-4B67-A4ED-E5BCFA7DEF08	2000
Intrusion Annunciator (Aritech)	CC2FB086-27E9-49A8-ACE5-5A677BE81ACA	2001
Intrusion Area (CK722)	F5C99AF3-6CAB-44C7-AA85-B55FD240B81D	2100
Intrusion Area (Aritech)	F7476E07-6696-4B28-A067-663E7563EBDB	2101
Intrusion Keypad Display (CK722)	CF555659-F6A8-4962-B7A8-52EB9411F39E	2200
Intrusion Zone (CK722)	3A0FBC1F-51E2-4A51-AB4C-84132B32BA94	2300
Intrusion Zone (Aritech)	DA9BD8DA-F01B-4DF1-A492-2E254D44BE82	2301
Intrusion Device (Aritech)	DB99A772-5E42-464C-B8E4-4EEBC636A950	2400
AV Switch	69D56648-734C-4167-95B1-DEC969EC5E24	2500
AV Camera	EAE1BAB6-61AE-427B-A1DF-D86B91144AB0	2600
AV Dry Contact	065BC58F-DD38-42E7-8518-BBA8EB83134D	2700
AV Monitor	3C32E459-9237-4A76-9F9D-9B0CE8F13BB2	2800
P2000 Map	213DD6DD-C82B-4F0E-9C4F-79334128E308	2900
Loop Tamper	6FCA22BD-A89B-42F9-81B2-25B671511B50	3000
Multiple Command Object	7ECD5DCB-4A2B-4D80-A6BB-9A7DDB04E18C	3200
BACNet Interlock	55CCE864-D029-4F5D-9D98-4FC3D09D1C16	3300
DSO Terminal Group	589D8EC8-E409-4627-A4FB-ECF449C0A049	3400
ACO Terminal Group	C24970B6-94FB-4EEA-BE10-9CCF5A55439D	3401
Legacy Terminal Group	CDAF633C-F773-43F1-820F-22489674B8A9	3402
Legacy Output Group	205B29E6-7586-4B42-9E9B-358B7D7D6EFE	3501
Legacy Input Group	F8C2319F-F9F0-414A-B3BE-728872A03E91	3601
RAMS Integration Server	D5F1BB00-9859-42D0-8AC7-F7564B159770	3700
XMan Integration Server	F0D0DD29-9182-4ED4-BC1E-5982DA750323	3701
Jacques Intercom Integration	A6214266-B251-409F-8B89-3309C6FBF676	3702
ACS Interface Integration	DE4C4BCE-3296-43AE-8472-F16F90BD7B71	3703
Voorspoed Stop Search	E82556FF-BAC6-428B-A79E-B7A41276ED6E	3800
XMan Operator Station	68771A4D-CDDB-4D30-BCF4-4E66A031CB01	3900
XMan Viewer Station	CAC72489-FB59-47A3-93A8-36A428CE09E6	3901
XMan XRAY Machine	9D65A3B6-E1DB-42CC-BE71-3EB78A56325F	4000
Jacques Intercom Server	B9A2A577-8868-4359-928D-A3A2DFE4FAF0	4100
S300 Trunk	3D5589C8-DF2A-459F-B925-F18EE62A7799	4200
Intrusion Server (Aritech)	954BDCF4-880B-49AB-8A7C-B188438CA700	4300
XMan Holding Room	24008B78-6137-4139-825E-EADAA96D2F54	4401
CK720 Cabinet	D1B6D060-4D32-411E-8082-C861C5334591	4500

Item Sub Type Name	Item Sub Type Guid	Value
Company	5DD4B9C9-5626-4015-9B71-0493E09D8E2B	4600
Department	C72DF7AA-7457-4A24-8143-2E2EEF95B240	4700
Division	E6680386-D93C-4751-8EFA-70B757231E3A	4800
Team	7A02B2B2-D934-4A6A-9DCC-E78B50C73181	4900
Lane Equipment Cabinet	58178A05-8298-4EBA-9358-8478260A8DE0	5000
Automatic Payment Machine	2C31534C-399E-4CC4-A225-59E1E7752F63	5001
P2000 Root Element	205F091A-883F-4318-B08B-97E27D83CA55	6000

To retrieve the list of supported Item Sub Types, the following database query can be used.

```
Use P2000EntityConfig
select enumvalue.Name, enumValue.Guid, enumValue.Value from enumvalue
        inner join EnumSet on enumvalue.enumsetguid = EnumSet.guid
where enumset.id = 200513
order by value
```

Item Status

Item Status values depend on the item sub type. The following table lists status set used for each of the item sub types. The sections that follow list the applicable status value for each status set.

Item Sub Type Name	Status Set
Unknown	None
CK722 Panel	Panel
Legacy Panel	Panel
Aritech Panel	Panel
Input Terminal	Input Terminal
Output Terminal	Output Terminal
Reader Terminal	Input Terminal
Legacy Input Point	Input Point
Legacy Soft Input Point	Input Point
CK722 Input Point	Input Point
CK722 Panel Input Point	Input Point
CK722 Soft Input Point	Input Point
Legacy Output Point	Output Point
CK722 Output Point	Output Point
CK722 Panel Output Point	Output Point
ACO Terminal	Reader
DSO Terminal	Reader
Anti-Loitering	Anti-Loitering
Anti-Passback	Anti-Passback
P2000 Area	Area
TA Terminal	Panel
S300 Hardware Module	Input Terminal

Item Sub Type Name	Status Set
CK720 Elevator	Elevator
CK722 Elevator	Elevator
Guard Tour	N/A
Occupancy	N/A
Notification Object	N/A
Intrusion Annunciator CK722	Intrusion Annunciator
Intrusion Annunciator Aritech	Intrusion Annunciator
Intrusion Area CK722	Intrusion Area
Intrusion Area Aritech	Intrusion Area
Intrusion Keypad CK722	N/A
Intrusion Keypad Aritech	N/A
Intrusion Zone CK722	Intrusion Zone
Intrusion Zone Aritech	Intrusion Zone
Intrusion Device Aritech	Panel
AV Switch	N/A
AV Camera	Camera
AV Dry Contact	AV Dry Contact
AV Monitor	N/A
P2000 Map	Map
Loop Tamper	Loop Tamper
Camera	Camera
P2000 Event	Event
P2000 Counter	Counter

Panel

The following table lists the possible values for the “Panel” status set.

Status Name	Value
Up	0
Down	1
Unknown	2
Misconfigured	7

Input Terminal

The following table lists the possible values for the “Input Terminal” status set.

Status Name	Value
Up	0
Down	1
Unknown	2
Mixed	3

Output Terminal

The following table lists the possible values for the “Output Terminal” status set.

Status Name	Value
Up	0
Down	1
Unknown	2

Input Point States

The following table lists the possible values for the “Input Point” status set.

Status Name	Value
Secure / Reset	0
Set	1
Short	2
Open	3
Suppressed	4
Unknown	5

Output Point States

The following table lists the possible values for the “Output Point” status set.

Status Name	Value
Reset	0
Set	1
Unknown	2

Reader Terminal States

The following table lists the possible values for the “Reader” status set.

Status Name	Value
Locked	0
Down	1
Unknown	2
Held Open	3
Forced Open	4
Unlocked	5
Disabled	6
Override	7
Unlocked & Open	8
Unlocked & Closed	9
Locked & Open	10
Locked and Closed	11

Intrusion Annunciator States

The following table lists the possible values for the “Intrusion Annunciator” status set.

Status Name	Value
Inactive	300
Active	301
Unknown	302

Intrusion Area States

The following table lists the possible values for the “Intrusion Area” status set.

Status Name	Value
Disarming	200
Disarmed	201
Arming	202
Armed	203
Mixed	204
Fault	205
Unknown	206
Disarmed - No Bypass Sealed	207
Disarmed - No Bypass Unsealed	208
Disarmed - Bypass Sealed	209
Disarmed - Bypass Unsealed	210
Armed - No Bypass Sealed	211
Armed - No Bypass Unsealed	212
Armed - Bypass Sealed	213
Armed - Bypass Unsealed	214
Alarmed - No Bypass Sealed	215
Alarmed - No Bypass Unsealed	216
Alarmed - Bypass Sealed	217
Alarmed - Bypass Unsealed	218
Alarmed Armed - No Bypass Sealed	219
Alarmed Armed - No Bypass Unsealed	220
Alarmed Armed - Bypass Sealed	221
Alarmed Armed - Bypass Unsealed	222

Intrusion Zone States

The following table lists the possible values for the “Intrusion Zone” status set.

Status Name	Value
Arming	100
Armed	101
Bypassed	102
Disarming	103
Disarmed	104

Status Name	Value
Fault	105
Unknown	106
Normal	107
Open	108
Open Bypassed	109
Tamper	110
Tamper Open	111
Tamper Bypassed	112
Tamper Bypassed Open	113
Alarm	114
Alarmed Open	115

Intrusion Panel

The following table lists the possible values for the “Intrusion Device” status set.

Status Name	Value
Normal	800
Fault	801
Down	802
Unknown	803

AV Dry Contact

The following table lists the possible values for the “AV Dry Contact” status set.

Status Name	Value
Secure	0
Alarm	1
Unknown	2

Map

The following table lists the possible values for the “Map” status set.

Status Name	Value
Normal	0
Alarm	1
Unknown	2

Camera

The following table lists the possible values for the “Camera” status set.

Status Name	Value
Event	0
Unknown	1

Counter

The following table lists the possible values for the “Counter” status set.

Status Name	Value
Negative	0
Zero	1
Positive	2
Unknown	3

Interlock

The following table lists the possible values for the “Interlock” status set.

Status Name	Value
True	0
False	1
Fault	2
Unknown	3

Event

The following table lists the possible values for the “Event” status set.

Status Name	Value
Event	0
Event Unknown	1

Muster

The following table lists the possible values for the “Muster” status set.

Status Name	Value
Disabled	0
Inoperable	1
Degraded	2
Ready	3
Running	4
Stopped	5
Aborted	6
Unknown	7

Loop Tamper

The following table lists the possible values for the “Loop Tamper” status set.

Status Name	Value
Set	0
Secure	1
Unknown	2

MCO

The following table lists the possible values for the “MCO” status set.

Status Name	Value
MCO State 0	0
MCO State 1	1
MCO State 2	2
MCO State 3	3
MCO State 4	4
MCO State 5	5
MCO State 6	6
MCO State 7	7
MCO State 8	8
MCO State 9	9
MCO State 10	10
MCO State 11	11
MCO State 12	12
MCO State 13	13
MCO State 14	14
MCO State 15	15
MCO State 16	16
MCO State 17	17
MCO State 18	18
MCO State 19	19
MCO State 20	20
MCO State 21	21
MCO State 22	22
MCO State 23	23
MCO State 24	24
MCO State 25	25
MCO State 26	26
MCO State 27	27
MCO State 28	28
MCO State 29	29
MCO State 30	30
MCO State 31	31
MCO Unknown	32

Example Query

To retrieve the status values supported for each Item Sub Type, the following database query can be used.

```
Use P2000EntityConfig
select Ev2.Name, Ev2.Value
        as Value from EnumSet as ES
        inner join EnumValue as EV on ES.guid = EV.enumsetguid
                                        and ES.ID = 200513
                                        and EV.Value = 500
        inner join EnumValueEnumValue as EVEV on EV.guid = EVEV.enumvalueguidparent
        inner join EnumValue Ev2 on Ev2.Guid = EVEV.enumvalueguidchild
        inner join EnumSet Es2 on Es2.Guid = Ev2.EnumSetGuid
                                        and Es2.Id = 200088
                                        and EV2.Value < 10000
union
select Ev2.Name, (EV2.value % 100)
        as Value from EnumSet as ES
        inner join EnumValue as EV on ES.guid = EV.enumsetguid
                                        and ES.ID = 200513
                                        and EV.Value = 500
        inner join EnumValueEnumValue as EVEV on EV.guid = EVEV.enumvalueguidparent
        inner join EnumValue Ev2 on Ev2.Guid = EVEV.enumvalueguidchild
        inner join EnumSet Es2 on Es2.Guid = Ev2.EnumSetGuid
                                        and Es2.Id = 200088
                                        and EV2.Value >= 10000
order by EV.value, ES.name, EV2.value
```

Please note that the number **500** in the above example needs to be replaced with the Item Sub Type value from the previous table.

SAMPLE MESSAGES

Sample Audit Message

The following is an audit message generated by an operator editing a badge:

```
<?xml version="1.0"?>
<P2000Message>
    <MessageBase>
        <BaseVersion>300</BaseVersion>
        <MessageType>28675</MessageType>
        <MessageSubType>86</MessageSubType>
        <SiteName>P2000Site</SiteName>
        <PartitionName>Super User</PartitionName>
        <Public>0</Public>
        <ItemName>Real Time List</ItemName>
        <QueryString />
        <Category />
        <Escalation>0</Escalation>
        <Priority>0</Priority>
        <OperatorName>Cardkey</OperatorName>
    </MessageBase>
    <MessageDecode>
        <MessageDateTime>5/25/2006 4:01:53 PM</MessageDateTime>
        <MessageTypeText>Audit</MessageTypeText>
        <MessageText>Execute Application</MessageText>
        <DetailsText>Real Time List</DetailsText>
    </MessageDecode>
    <AuditDetails>
        <MessageVersion>200</MessageVersion>
        <LocalTimestamp>2006-5-25T16:1:53</LocalTimestamp>
        <UTCTimestamp>2006-5-25T23:1:53</UTCTimestamp>
        <ItemType>86</ItemType>
        <Action>0</Action>
        <ItemID>0</ItemID>
        <ItemGuid />
    </AuditDetails>
</P2000Message>
```

Sample Alarm Message

The following is an input alarm message generated by an input point going into the set state:

```
<?xml version="1.0"?>
<P2000Message>
    <MessageBase>
        <BaseVersion>300</BaseVersion>
        <MessageType>3</MessageType>
        <MessageSubType>2</MessageSubType>
        <SiteName>P2000Site</SiteName>
        <PartitionName>Super User</PartitionName>
        <Public>0</Public>
```

```
            <ItemName>mn t3 i2</ItemName>
            <QueryString />
            <Category>P2000</Category>
            <Escalation>0</Escalation>
            <Priority>0</Priority>
            <OperatorName />
        </MessageBase>
        <MessageDecode>
            <MessageDateTime>5/30/2006 9:38:51 AM</MessageDateTime>
            <MessageTypeText>Alarm</MessageTypeText>
            <MessageText>Pending, Alarm</MessageText>
            <DetailsText>mn t3 i2, mn T3, cneusempc1</DetailsText>
        </MessageDecode>
        <AlarmDetails>
            <MessageVersion>300</MessageVersion>
            <AlarmGuid>A8406731-955D-403B-9F05-D1A25EF878BD</AlarmGuid>
            <AlarmID>1</AlarmID>
            <AlarmType>2</AlarmType>
            <AlarmTypeName>Input Point</AlarmTypeName>
            <AlarmTypeID>7</AlarmTypeID>
            <AlarmTypeGuid>2E70D7B3-5DF7-4E20-B8B9-E14E2E51237D</AlarmTypeGuid>
            <AckRequired>0</AckRequired>
            <ResponseRequired>0</ResponseRequired>
            <InstructionText />
            <AlarmState>4</AlarmState>
            <AlarmTimestamp>2006-5-30T9:38:51</AlarmTimestamp>
            <ConditionState>1</ConditionState>
            <ConditionSequenceNumber>4</ConditionSequenceNumber>
            <ConditionSequenceGuid>7ADE2F11-F806-4188-8C06-83CBE1969615</ConditionSequenceGuid>
            <ConditionCompletionState>0</ConditionCompletionState>
            <ConditionTimestamp>2006-5-30T9:38:51</ConditionTimestamp>
            <Popup>1</Popup>
            <Description>mn t3 i2, mn T3, cneusempc1</Description>
            <AlarmSiteName>P2000Site</AlarmSiteName>
            <AlarmOptionGuid>6FDAEE0F-EB6F-4604-AB3E-B8B5600DD478</AlarmOptionGuid>
            <InputDetails>
                <InputPointAlarmVersion>200</InputPointAlarmVersion>
                <PointStateChange>1</PointStateChange>
                <PanelID>2</PanelID>
                <PanelName>cneusempc1</PanelName>
                <TerminalID>2</TerminalID>
                <TerminalIndex>2</TerminalIndex>
                <TerminalName>mn T3</TerminalName>
                <PointNumber>2</PointNumber>
                <PointName>mn t3 i2</PointName>
                <PrevPointState>4</PrevPointState>
                <PointState>1</PointState>
                <StatusFlag>4</StatusFlag>
            </InputDetails>
        </AlarmDetails>
    </P2000Message>
```

Sample Access Grant Message

The following is a real time data arm message generated by an access grant at a reader:

```
<?xml version="1.0"?>
<P2000Message>
    <MessageBase>
        <BaseVersion>300</BaseVersion>
        <MessageType>28673</MessageType>
        <MessageSubType>68</MessageSubType>
        <SiteName>P2000Site</SiteName>
        <PartitionName>Super User</PartitionName>
        <Public>0</Public>
        <ItemName>mn T1</ItemName>
        <QueryString />
        <Category />
        <Escalation>0</Escalation>
        <Priority>0</Priority>
        <OperatorName />
    </MessageBase>
    <MessageDecode>
        <MessageDateTime>5/30/2006 10:57:01 AM</MessageDateTime>
        <MessageTypeText>Access Grant</MessageTypeText>
        <MessageText>Access Granted Local</MessageText>
        <DetailsText>mn T1, 102, Michael Neuser</DetailsText>
    </MessageDecode>
    <TransactionDetails>
        <MessageVersion>200</MessageVersion>
        <HistoryGroup>8</HistoryGroup>
        <HistoryType>68</HistoryType>
        <HistorySubType>-1</HistorySubType>
        <LocalTimestamp>2006-5-30T10:57:1</LocalTimestamp>
        <PanelID>2</PanelID>
        <PanelName>cneusempc1</PanelName>
        <TrunkNumber>0</TrunkNumber>
        <TerminalID>1</TerminalID>
        <TerminalIndex>0</TerminalIndex>
        <TerminalName>mn T1</TerminalName>
        <ItemGuid>C3FA66C3-8C8A-48EB-B4A4-33CDACB6239A</ItemGuid>
        <PointID>0</PointID>
        <PointNumber>0</PointNumber>
        <PointName />
        <IdentifierGuid>D7E10DCD-3A76-4D5A-A9A3-BA581A181143</IdentifierGuid>
        <IdentifierNumber>102</IdentifierNumber>
        <FacilityCode>0</FacilityCode
        <Direction>0</Direction>
        <IdentifierTrace>0</IdentifierTrace>
        <IssueLevel>0</IssueLevel>
        <EntityGuid>A411AA6E-FFD3-47FC-B134-C92AAB8877B1</EntityGuid>
        <EntityFirstName>Michael</EntityFirstName>
        <EntityMiddleName />
        <EntityName>Neuser</EntityName>
        <ActionInterlockGuid1 />
        <ActionInterlockValue1>0</ActionInterlockValue1>
        <ActionInterlockGuid2 />
        <ActionInterlockValue2>0</ActionInterlockValue2>
```

```
        <EventName />
        <SecurityLevel>0</SecurityLevel>
        <RTLDataGuid>D7757D31-AD98-4DF9-8CB1-90D6A07263A6</RTLDataGuid>
        <SourceMsgGuid />
    </TransactionDetails>
</P2000Message>
```

Sample Input Point State Change Message

The following is a real time data arm message generated by an input point going into the set (alarm) state:

```
<?xml version="1.0"?>
<P2000Message>
    <MessageBase>
        <BaseVersion>300</BaseVersion>
        <MessageType>28673</MessageType>
        <MessageSubType>20576</MessageSubType>
        <SiteName>P2000Site</SiteName>
        <PartitionName>Super User</PartitionName>
        <Public>0</Public>
        <ItemName>mn t3 i2</ItemName>
        <QueryString />
        <Category />
        <Escalation>0</Escalation>
        <Priority>0</Priority>
        <OperatorName />
    </MessageBase>
    <MessageDecode>
        <MessageDateTime>5/30/2006 9:30:51 AM</MessageDateTime>
        <MessageTypeText>Input Point State Change</MessageTypeText>
        <MessageText>Alarm</MessageText>
        <DetailsText>mn t3 i2</DetailsText>
    </MessageDecode>
    <TransactionDetails>
        <MessageVersion>200</MessageVersion>
        <HistoryGroup>1</HistoryGroup>
        <HistoryType>20576</HistoryType>
        <HistorySubType>-1</HistorySubType>
        <LocalTimestamp>2006-5-30T9:38:51</LocalTimestamp>
        <PanelID>2</PanelID>
        <PanelName>cneusempc1</PanelName>
        <TrunkNumber>0</TrunkNumber>
        <TerminalID>2</TerminalID>
        <TerminalIndex>2</TerminalIndex>
        <TerminalName>mn T3</TerminalName>
        <ItemGuid />
        <PointID>7</PointID>
        <PointNumber>2</PointNumber>
        <PointName>mn t3 i2</PointName>
        <IdentifierGuid />
        <IdentifierNumber />
        <FacilityCode>0</FacilityCode>
        <EventName></EventName>
```

```
        <SecurityLevel>0</SecurityLevel>
        <RTLDataGuid>B71DD021-6E9D-4FF2-BF77-B08B654AF11E</RTLDataGuid>
        <SourceMsgGuid />
    </TransactionDetails>
</P2000Message>
```

Sample Output Point State Change Message

The following is a real time data arm message generated by an output point going into the set state:

```
<?xml version="1.0"?>
<P2000Message>
    <MessageBase>
        <BaseVersion>300</BaseVersion>
        <MessageType>28673</MessageType>
        <MessageSubType>17</MessageSubType>
        <SiteName>P2000Site</SiteName>
        <PartitionName>Super User</PartitionName>
        <Public>0</Public>
        <ItemName>mn t1 o1</ItemName>
        <QueryString />
        <Category />
        <Escalation>0</Escalation>
        <Priority>0</Priority>
        <OperatorName />
    </MessageBase>
    <MessageDecode>
        <MessageDateTime>5/30/2006 10:57:00 AM</MessageDateTime>
        <MessageTypeText>Panel</MessageTypeText>
        <MessageText>Output Set</MessageText>
        <DetailsText>cneusempc1, mn T1, mn t1 o1</DetailsText>
    </MessageDecode>
    <TransactionDetails>
        <MessageVersion>200</MessageVersion>
        <HistoryGroup>1</HistoryGroup>
        <HistoryType>17</HistoryType>
        <HistorySubType>-1</HistorySubType>
        <LocalTimestamp>2006-5-30T10:57:0</LocalTimestamp>
        <PanelID>2</PanelID>
        <PanelName>cneusempc1</PanelName>
        <TrunkNumber>0</TrunkNumber>
        <TerminalID>1</TerminalID>
        <TerminalIndex>0</TerminalIndex>
        <TerminalName>mn T1</TerminalName>
        <ItemGuid>C3FA66C3-8C8A-48EB-B4A4-33CDACB6239A</ItemGuid>
        <PointID>1</PointID>
        <PointNumber>1</PointNumber>
        <PointName>mn t1 o1</PointName>
        <IdentifierGuid />
        <IdentifierNumber />
        <FacilityCode>0</FacilityCode>
        <EventName></EventName>
        <SecurityLevel>0</SecurityLevel>
        <RTLDataGuid>983D8CFD-51AF-4939-98B3-4CEADE8EAB0C</RTLDataGuid>
```

```
            <SourceMsgGuid />
        </TransactionDetails>
    </P2000Message>
```