texecom-milestone

User Manual

UM0098_1

Unit 10 Concept Park
Innovation Close
Poole
Dorset
BH12 4QT

t: +44 (0) 1202 723535
w: www.tdsi.co.uk
e: sales@tdsi.co.uk
e: support@tdsi.co.uk

Foreword

Time and Data Systems International Ltd operate a policy of continuous improvement and reserves the right to change specifications, colours or prices of any of its products without prior notice.

Guarantee

For terms of guarantee, please contact your supplier.

Trademarks

Microsoft and Windows are registered trademarks of Microsoft Corporation.
All other brands and product names are trademarks or registered trademarks of their respective owners.

Document Control

Issue	Date Issued	Change Summary	Issued by
1	30th August 2016	Initial release	GFH

Contents

1 Introduction

The Texecom to Milestone Service provides a method for monitoring Texecom Elite panels for any changes and then sending these messages to the Milestone XProtect® Video Management System.

All Texecom events are transmitted, whether these be zone status changes or tamper / alarm events.

The integration uses the Generic Events functionality within the XProtect VMS. This manual does not describe how to create generic events or alarms. Reference should be made to the relevant VMS manual for this.

2 Installation

3 Configuration

Before the system can be used the Texecom panel and Milestone system has to be configured. This is achieved through the IntruderConfig tool.

To run this select TDSi->IntruderMilestone->Intruder Config from the menu. This will then start the configuration tool allowing you to specify the details for the panels and the XProtect Server.

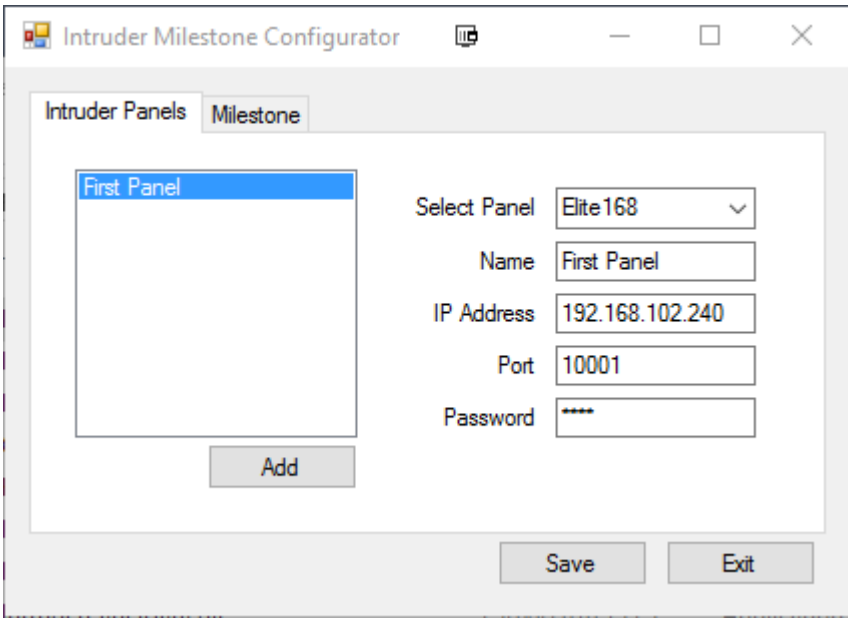

Figure 1 - Intruder Configuration

3.1 Add Intruder Panel

To add a new panel, click the Add button. This will add a new panel to the list on the left. The default name will be Panel X where X will be an incremental number.

Select this panel by clicking on it which will then display the details on the right. The following details are required:

Element	Description
Select Panel	Select the panel type from the drop down box
Name	This can be any name and should relate to the location of the panel
IP Address	Specify the IP address of the panel
Port	The port used by the panel, the default is 10001
Password	Enter the UDL password of the panel

When you have entered your details click the save button.

3.2 Milestone Details

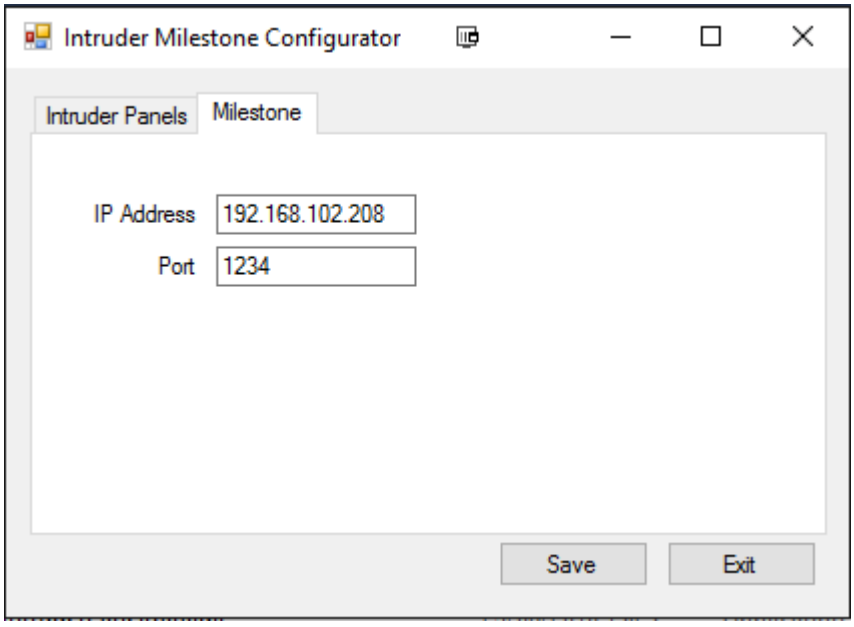

Figure 2 - Milestone Configuration

For the Milestone system you need to enter the IP address and port for the Milestone server. The port is defined within the XProtect Management Application (see Figure 4)

3.2.1 Milestone Generic Events Port

To check the port number used by the XProtect Server you need to login to the XProtect Management Application. Click on the Events and Outputs tab as shown below.

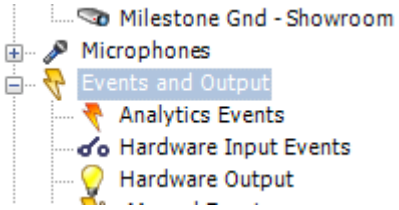

Figure 3 - XProtect Event Settings

The port number will then be shown under the Alert and Generic Event Port. This is the value that you need to use in the configuration tool.

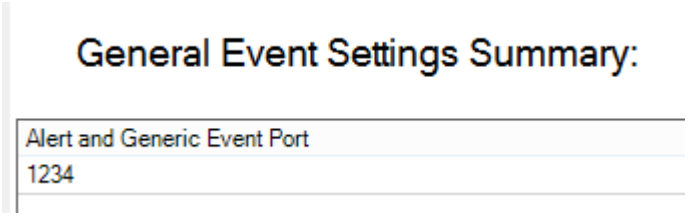

Figure 4 - XProtect Generic Event Port

4 Start / Stop Service

The service is a standard Windows® service and can be started either from the services page or using the StartStop tool. To run this, go to your menu and select TDSi->IntruderMilestone->StartStop Tool

5 Test Utility

Included with the service is a simple test utility. This monitors a local network connection and displays messages from the intruder panel. In order to use this you need to set the address of the Milestone server as 127.0.0.1.

Then from the menu select TDSi->IntruderMilestone->Console Test Server

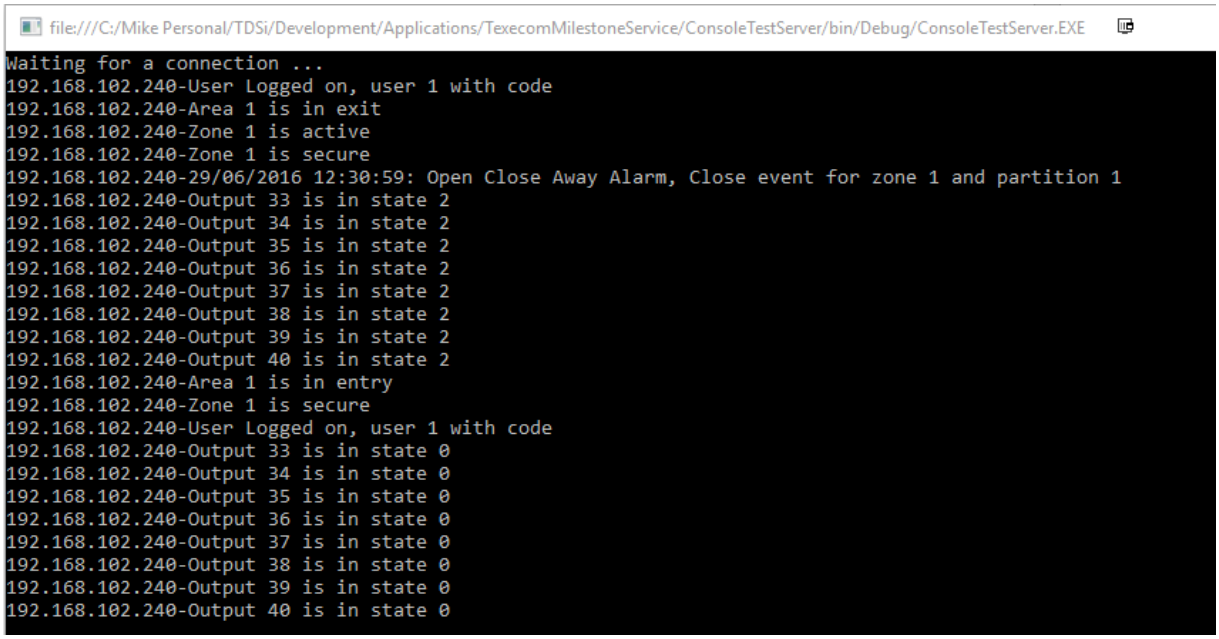

Figure 5 - Example Intruder Messages

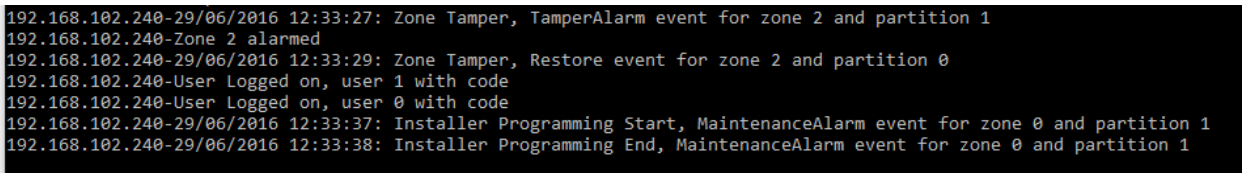

Figure 6 - Example Tamper Alarm Message

6 Messages

Messages are transmitted in ASCII text format. There are 5 types of events that can be transmitted.

6.1 Zone Events

Zone events provide details on a state change of a zone, for example from secure to tamper. The format of the message sent is:

[IP Address]-[Message]

These are the messages that can be transmitted:

- Zone X is secure
- Zone X is active
- Zone x is tampered
- Zone X is short
- Zone X is in fault
- Zone X failed test
- Zone X alarmed
- Zone X is manual bypassed
- Zone X is auto bypassed
- Zone X is masked

Where X is the zone number from the panel.

For example, the Event message expression below matches the string above for Zone X secure

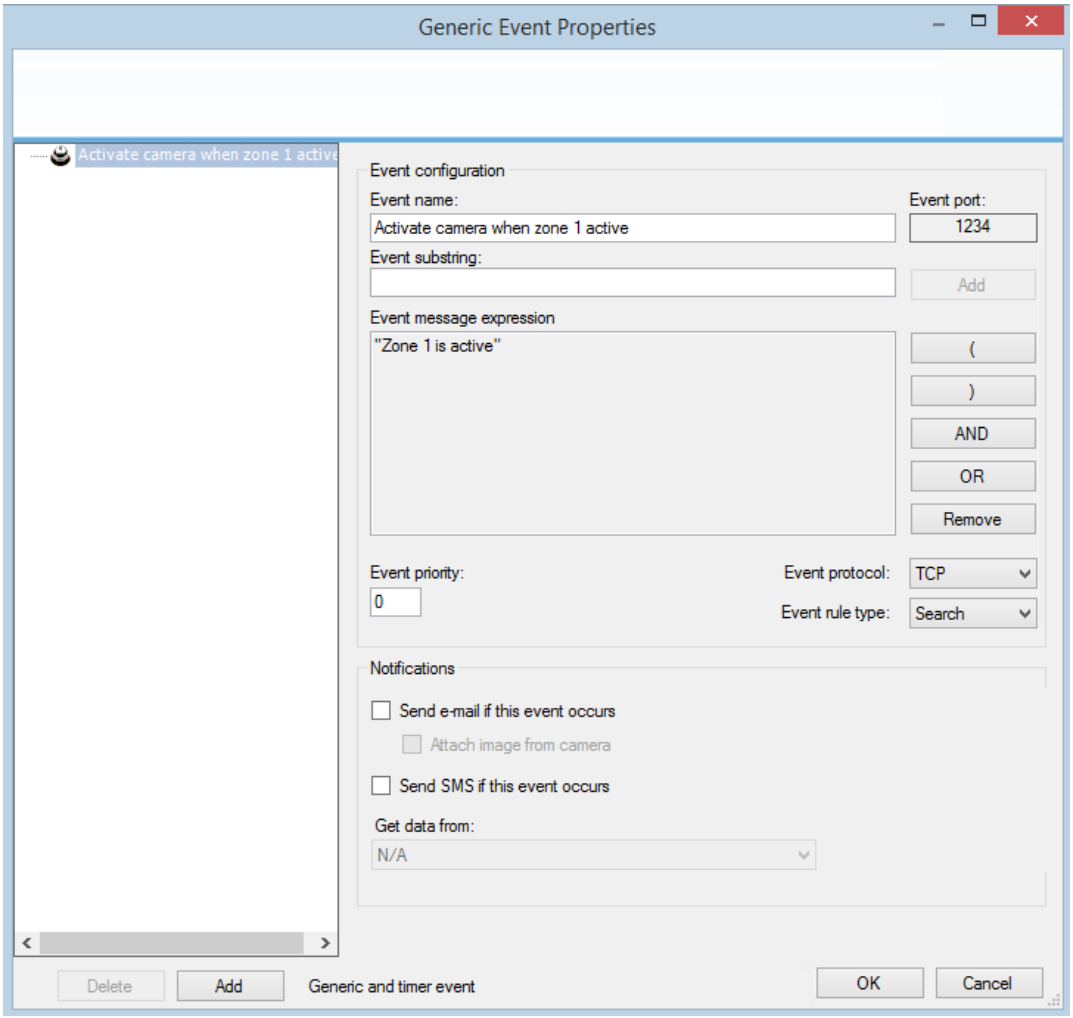

Figure 7 - Example XProtect Generic Event

6.2 Area Events

Area events provide details on the state change of an area, for example disarmed to armed. The format of the message sent is:

[IP Address]-[Message]
These are the messages that can be transmitted:

- Area X is disarmed
- Area X is in exit
- Area X is in entry
- Area X is armed
- Area X is part armed
- Area X is in alarm

Where X is the zone number from the panel.

Note: The Area ID in Texecom will be converted to a numeric value in Milestone. For example Texecom Area A will be displayed as Area 1 in the Milestone Event message expression window. The maximum area value will be dependent on panel type.

6.3 Output Events

Output events report a change of state of an output. The format of the message is:

Output X is in state Y

Where X is the output type and Y is the output state.

The output type is one of the following:

Output Type Value	Output
0 (0x00)	Panel Outputs
1 (0x01)	Digi Outputs
2 (0x02)	Digi Channel low 8 (outputs 1 – 8)
3 (0x03)	Digi Channel high 8 (outputs 9 – 16)
4 (0x04)	Redcare outputs
5 (0x05)	Custom outputs 1
6 (0x06)	Custom outputs 2
7 (0x07)	Custom outputs 3
8 (0x08)	Custom outputs 4
9 (0x09)	X-10 outputs
16 (0x10)	Network 1, keypads (all 8 keypads)
17 (0x11)	Network 1, expander 1 outputs
18 (0x12)	Network 1, expander 2 outputs
…	…
32 (0x20)	Network 2 keypads (all 8 keypads)
33 (0x21)	Network 2, expander 1 outputs
…	…
48 (0x30)	Network 3, keypads (all 8 keypads)
49 (0x31)	Network 3, expander 1 outputs
…	…

The state is the decimal value that relates to the binary value of the outputs, for example a state value of 2 for the panel outputs means output 2.

6.4 User Events

User events are reported for any user activity on the keypad. The format of the message sent is:

[IP Address]-[Message]

The format of these messages is:

- User Logged on, user X with code
- User Logged on, user X with tag

Where X is the user within the intruder panel. By default User 0 is the Engineer and User 1 is the Master.

6.5 Log Events

Log events are reported for any log entry written in the intruder panel. The format of the message sent is:

[IP Address]-[Message]

The format of *Message* is:

[*DateTime*]: [*Event Type*], [*Event Group*] event for zone X and partition Y

Where Event Type and Event Group are defined below. X is the Zone number and Y is the partition detail.

6.5.1 Event Type

Where Event Type is one of the following:

Entry/Exit 1	Exit Started	Expander Tamper	AC Cleared Down
Entry/Exit 2	Exit Error Arming Failed	Keypad Tamper	Monitored Alarm
Guard	Entry Started	Expander Trouble	Expander Low Voltage
Guard Access	Part Arm Suite	Remote Keypad Trouble	Supervision Fault
24hr Audible	Armed With Line Fault	Fire Zone Tamper	PA From Remote Fob
24hr Silent	Open Close Away Alarm	Zone Tamper	RF Device Battery Low
PA Audible	Part Armed	Keypad Lockout	Site Data Changed
PA Silent	Auto Open Close	Code Tamper Alarm	Radio Jamming
Fire	Auto Arm Deferred	Soak Test Alarm	Test Call Passed
Medical	Open After Alarm	Manual Test Transmission	Test Call Failed
24hr Gas	Remote Open Close	Automatic Test Transmission	Zone Fault
Auxiliary	Quick Arm	User Walk Test Start End	Zone Masked
Tamper	Recent Closing	NVM Defaults Loaded	Faults Overridden
Exit Terminator	Reset After Alarm	First Knock	SUAC Failed
Momentary Key	Auxiliary 12V Fuse Fail	Door Open Alarm	PSU Battery Fail
Latched Key	AC Fail	Part Arm 1	PSU Low Output Fail
Security	Low Battery	Part Arm 2	PSU Tamper
Omit Key	System Power Up	Part Arm 3	PSU Tamper Restore
Custom	Bell Fuse Failure	Auto Arming Started	Door Access
Confirmed PA Alarm	Telephone Line Fault	Confirmed Alarm	Comm Remote Command
Confirmed PA Silent	Fail To Communicate	Prox Tag	User Added
Keypad Medical	Download Start	Access Code Changed Deleted	User Deleted
Keypad Fire	Download End	Arm Failed	Confirmed PA
Keypad PA Audible	Log Capacity Alert	Log Cleared	User Acknowledge
Keypad Audible Silent	Date Changed	ID Loop Shorted	PSU Fail
Duress	Time Changed	Communication Port	Charger Fault
Alarm Active	Installer Programming Start	TAG System Exit	Confirmed Intruder
Bell Active	Installer Programming End	TAG System Exit Battery Low	GSM Lost
ReArm	Panel Box Tamper	TAG System Entry	Corrupt Event
Verified Cross Zone Alarm	Bell Tamper	TAG System Entry Battery Low	
User Code	Auxiliary Tamper	Microphone Activated	

6.5.2 Event Group

Event Group is one of:

NotReported	Ended
PriorityAlarm	Fault
PriorityAlarmRestore	Omitted
Alarm	Reinstated
Restore	Stopped
Open	Start
Close	Deleted
Bypassed	Active
Unbypassed	NotUsed
MaintenanceAlarm	Changed
MaintenanceRestore	LowBattery
TamperAlarm	Radio
TamperRestore	Deactivated
TestStart	Added
TestEnd	BadAction
Disarmed	PaTimerReset
Armed	PaZoneLockout
Tested	GroupTypeCommsDelayed
Started	GroupTypeCommunicated

Page intentionally left blank

ACCESS EVERYWHERE

Because everyone deserves peace of mind

TDSi UK
Unit 10 Concept Park, Innovation Close, Poole, Dorset BH12 4QT United Kingdom
t: +44 (0)1202 723535 f: +44 (0)1202 724975 e: sales@tdsi.co.uk

TDSi France
Immeuble ATRIA, 2 rue du Centre, 93160 NOISY LE GRAND France
t: +33 (0)1 58 84 20 90 f: +33 (0)1 58 84 20 91 e: tdsif@wanadoo.fr

bsia british security industry association

Beacon company