Intrusion Management Installation and User Guide

9.12.0v1

SECURITY MANAGEMENT SYSTEM

9600-0401

AMAG Technology Limited cannot be held liable for technical and editorial omissions or errors made herein; nor for incidental or consequential damages resulting from the furnishing, performance or use of this material.

Intrusion Management Installation and User Guide
(9600-0401)

Issue 9.12.0v1 – 9th April 2025
Applies to version 9.12.0 or later of the Symmetry software, until superseded by a later issue of the manual.

Contents

About this Guide

This guide explains the following:

- How to integrate third-party intrusion systems with Symmetry. **Note:** Features specific to M2150 intrusion are covered in the *M2150/M4000 Intrusion Guide*.
- Concepts of how the interfaces operate.
- How to install, configure and administer the interfaces.

This guide is intended to be of use to:

- Sales and management personnel.
- Installation and product support personnel.
- Users of the software.

This document is supported by context-sensitive online help available from the Symmetry software.

Note: See page 3 for a description of terminology used by Symmetry.

Chapter 1: Introduction

Overview of the Intrusion Management

The Symmetry Intrusion Management module enables alarm intrusion systems to be integrated with the Symmetry software. The interfaces provide the following features:

- **Intrusion system alarm monitoring** – Symmetry can monitor alarm and event transactions generated by supported intrusion systems. The transactions received are blended seamlessly into Symmetry, becoming part of the standard alarm reporting system available to Symmetry users. The interfaces run automatically in the background to ensure that users are automatically advised of any changes in the security status of protected areas.

- **Automatic Configuration upload** – Depending on the intrusion system used (see Table 1), Symmetry is able to upload details of the panels, zones, zone groups, areas and outputs configured in the intrusion system. This ensures that Symmetry correctly represents the current configuration of the intrusion system in the Command Center and elsewhere.

- **Full Intrusion Management interface** – Selected intrusion systems (see Table 1) are supported by the Full Intrusion Management Interface. This interface enables you to:

  c) Send commands from Symmetry to the intrusion system to perform actions such as to:

    – Arm or disarm areas or zone groups (zone groups apply only to CU30 and ThorGuard).

    – Enable, disable or bypass zones.

    – Silence an alarm.

    – Switch outputs on or off.

  b) View the current status of zones, areas, outputs, etc. in the Command Center, Intrusion Status Toolbar and graphics.

  a) Use a dedicated Intrusion Status toolbar (Figure 1) to view the current status of intrusion alarms, areas, zones and outputs. The toolbar gives an immediate heads-up view of information such as the number of alarms, areas armed, areas disarmed, zone alarms, zone faults, zones disabled and zones bypassed.

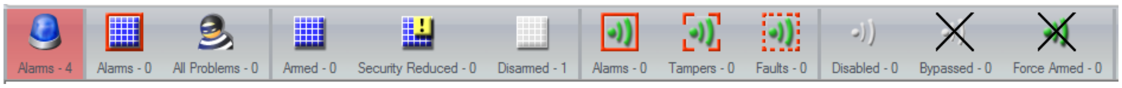


Figure 1 Intrusion Status Toolbar

- **Downloadable serial messages** – Selected intrusion systems (see Table 1) allow Symmetry to download commands containing user-definable messages. The commands can be sent as manual, scheduled or trigger commands. The messages are definable in a text format and could be used to perform actions such as to arm areas, disarm areas or display messages at keypads. The commands are sent to the intrusion system via the same serial or network link used to transfer transactions from the intrusion system to Symmetry.

- **Flexible communication options** – Communication between the intrusion system and Symmetry uses either a serial or network connection, depending on the requirements of the intrusion system used (see Table 1).

- **Intrusion user creation and maintenance** – Symmetry can be used to create and maintain intrusion users for Bosch B9512G, ThorGuard and DMP intrusion systems (see Table 1). This is achieved by assigning card holders access rights to the appropriate intrusion panels in the Card Holders screen. Symmetry downloads the user details such as the user code to the panels, which allows each user to set, unset and perform other tasks in the same way as if the user had been created at the panel itself. Symmetry can upload user data from the panels to enable valid data to be assigned in the card holder access rights. A manual download can be carried out using the "Maintenance/Download/Intrusion Users" screen in Symmetry.

- **M2150 Intrusion reader control of third-party intrusion areas** – Arming/disarming readers connected to a Symmetry M2150 intrusion node can be used to arm or disarm a selected area in Bosch B9512G, Vanderbilt (Vanderbilt Industries), DMP XR500N\XR550, DSC 4030 (SN4442) and HISEC intrusion systems. **Note:** M2150 control of third-party areas is described on page 31. Other features of M2150 intrusion are covered in the *M2150/M4000 Intrusion Guide*.

Supported Intrusion Systems	Configuration Upload	Comms Method	Full Intrusion Management	Download Serial Messages	Intrusion User Creation	Notes
DMP (Digital Monitoring Products) XR500N\XR550 Command Processor™	Yes	Network	Yes	No	Yes	
DMP XR200 Command Processor	No	Network or serial	No	Yes	No	
DSC® (Digital Security Controls) PC4020	No	Serial	No	Yes	No	
DSC PC4030 SRI	No	Serial	No	No	No	
DSC PC4030 via SN4442	Yes	Serial	Yes	No	No	Support is provided for multiple panels connected to the same DSC intrusion system.
HISEC ThorGuard	Yes	Serial	Yes	No	Yes	The interface uses the HISEC GPI COM module (special firmware variants required).
HISEC CU30	Yes	Serial	Yes	No	No	
Galaxy Dimension (GD-48, GD-96, GD-264 or GD-520)	Yes	Network or serial	No	No	No	
Bosch B9512G Intrusion Panel	Yes	Network	Yes	No	Yes	The panel requires firmware version 3.06.012 or later.
Vanderbilt SPC Series	Yes	Network	Yes	No	No	Encryption supported (AES 128).

Table 1: Supported Intrusion Systems and Features

Summary of Key Features

Key features of the software are as follows:

- **Integrated solution for security management** – Diverse systems can be integrated into a single security management package. The Symmetry Intrusion Management module interfaces to popular intrusion systems.
- **Integrated alarm monitoring** – Alarms from intrusion systems can be monitored using the same user interface used for monitoring access control and other Security Management functions.

- **Automatic upload** – Depending on the make/model of intrusion system, Symmetry can automatically upload the panels, zones, zone groups, areas and users configured.
- **Full Intrusion Management** – Enables Symmetry to monitor the status of the intrusion system in real time, and send commands to perform actions such as to arm/disarm areas or enable/disable zones.
- **Dedicated intrusion Status toolbar** – For systems supported by Full Intrusion Management, this gives a heads-up view of the current status of the intrusion system.
- **Symmetry M2150 integration** – For systems supported by Full Intrusion Management, this enables M2150 intrusion readers to arm or disarm a selected area in a third-party intrusion system.
- **Downloadable serial messages** – Depending on the make/model of intrusion system, Symmetry can control the operation of the intrusion system through user-definable message strings. The messages can be sent as manual, scheduled or trigger commands from Symmetry.
- **Integrated reporting** – Transactions from intrusion systems can be viewed in exactly the same way as other Symmetry messages.
- **Integrated intrusion user creation and maintenance** – Card holders in Symmetry can be intrusion users to perform tasks such as setting or unsetting the system at intrusion keypads, etc.
- **Monitoring of connected panels** – Symmetry displays when panels go online and offline.

Terminology

The following terms are used by Symmetry:

- **Output** – An electrical connection on a panel that may, for example, by used to control external equipment or alarm signaling devices. Vanderbilt systems use the term "mapping gate".
- **Panel** – The controller unit of an intrusion system.
- **Zone** – A single input to the alarm panel for an alarm detector. Note that in some cases, detectors may be wired in series, but connect to the panel using a single input; this is still known as a single "zone". Hisec documentation uses the term "input" to mean a Symmetry "zone".
- **Zone Group** – This term is used only for CU30 and ThorGuard panels, and refers to a group of Symmetry "zones", i.e. a group of detectors. The grouping is defined by the panel software. Hisec documentation uses the term "zone" to mean a Symmetry "zone group".
- **Area** – For CU30 and ThorGuard panels, this refers to a group of Symmetry "zone groups". Symmetry and the Hisec documentation have the same meaning for "area". For other panel types, a Symmetry "area" is a group of Symmetry "zones", i.e. a group of detectors.

Software Installation and Licensing

No additional Symmetry software needs to be installed for the intrusion panel interfaces. The interfaces can be enabled by adding an appropriate "Intrusion Panels" license in the "Maintenance/Licensing/System Licenses" screen at a Symmetry client.

Chapter 2: Configuring the Intrusion Hardware

This section describes the settings you need to configure in the intrusion hardware. Only the settings necessary to enable the interface are described.

Note: The following information is provided for guidance only. For further information, please refer to the manufacturer's documentation.

DMP XR200 Systems

At the DMP panel, enter engineer mode by shorting jumper J16 for two seconds and entering the password of 6653. Set:

COMMUNICATION / COMM TYPE to HST.

COMMUNICATION / CHECKIN to 1.

COMMUNICATION / ACCOUNT NO to specify an account number for the system.

Leave other settings at their default values.

You need to configure the panel's IP address and other settings. Refer to one of the following publications:

- If you are using the iCOM™ PAD for communications over the Ethernet network, please refer to the instructions supplied with the panel.
- If you are using an MSS1 PAD, please refer to a pre-issue 9.0 version of the *NIC Module Configuration Guide*.

For a serial connection between a Symmetry client PC and a DMP panel, use the DMP Model 394 PROG cable (supplied when you purchase the 462 IO module).

DMP XR500N\XR550 Systems

Note: The panel must have firmware version 114 or later.

Zone Configuration

The Symmetry Enhanced Intrusion Interface uses only those DMP messages that have an **Alarm** or **Trouble** status. Before using the interface, set **Report to Transmit** for **Disarmed Open**, **Disarmed Short**, **Armed Open** and **Armed Short** (as applicable) to **Alarm** or **Trouble**.

Communications Setup

Enter engineer mode by shorting jumper J16 for two seconds, enter the passcode of 6653 at the keypad, press the COMMAND button and set the following (leave other settings at their default values).

IMPORTANT: To save the changes, scroll through the top-level menus until ‘STOP’ is displayed, then press any of the unmarked keys in the top row of the keypad.

COMMUNICATION / COMM TYPE to NET

COMMUNICATION / RMT IP ADDRESS to the IP address of your Symmetry client.

COMMUNICATION / ALARM PORT to a unique port number (e.g. 2001, 2002 or 2003 - no two panels on the same DMP LAN chain can have the same port number).

COMMUNICATION / CHECKIN to 1.

COMMUNICATION / ACCOUNT NO to specify an account number for the system.

COMMUNICATION / XMIT DELAY: set this to 0 to disable any delay.

NETWORK OPTIONS / DHCP to NO.

NETWORK OPTIONS / LOCAL IP ADDRESS to the IP address you want the panel to assume (see your Network Administrator).

NETWORK OPTIONS / GATEWAY ADDRESS to the IP address of the gateway if the panel and Symmetry PC are on different networks.

NETWORK OPTIONS / SUBNET MASK to match the subnet mask of the Symmetry PC (e.g. 255.255.0.0).

NETWORK OPTIONS / PROGRAMMING PORT to a unique port number (e.g. 3001). This is the port used for commands.

REMOTE OPTIONS / RMT Key: this password may be left blank; if a string value is entered, the identical value must be configured in the password field of the Symmetry software ("Install/Intrusion/Intrusion/System Configuration" screen).

REMOTE OPTIONS / DISARM to YES (enables areas to be disarmed remotely).

DSC PC4020 Systems

At any enrolled keypad:

1. Enter installer mode.

2. Enroll the DSC 4401 serial I/O module. You may need to secure then open the tamper zone on the module to enroll the module.

3. Use the datalink communications setting (not printer or dvac). Datalink mode defaults to 4800 baud.

4. Connect one end of the supplied DSC PC-Link serial cable to the Symmetry PC, and the other end to the Datalink port of the 4401 serial I/O module. This is the smaller telephone-type RJ11 port (do not connect to the larger network-type RJ45 port).

DSC PC4030 Systems

Note: In the [Intrusion] section of multimax.ini, set PanelLanguage to 0 for a Norwegian panel, or 1 for a Swedish panel. This ensures that the correct characters are used in area and zone names.

At any enrolled keypad:

1. Enter installer mode.

2. Choose No if prompted to Initiate a PC-Link.

3. If you are using a PC4030SRI, enroll a DSC 4400 serial I/O module. If you are using a PC4030 with an SN4442, enroll a SN4442 Alarm Presentation Interface. You may need to secure then open the tamper zone on the module to enroll the module.

4. Connect one end of the supplied DSC PC-Link serial cable to the Symmetry PC, and the other end to:
   - The "con1" port of the 4400 serial I/O module, if you are using a PC4030SRI. This is the smaller telephone-type RJ11 port (do not connect to the larger network-type RJ45 port).
   - The “Con 16” port of the SN4442, if you are using a PC4030 with an SN4442.

HISEC Systems

Connect the Symmetry client PC to the HISEC GPI COM module (special firmware variant required). Connections to the module from a 9-pin serial connector are:

Pin 2: Tx   Pin 3: Rx   Pin 5: 0V

The Symmetry client PC does not need an ID on the HISEC network.

Vanderbilt SPC-Series Systems

The following procedure describes how to configure a Vanderbilt panel for the integration with Symmetry.

Note: For further information about the panel options, please refer to the *SPC Pro Configuration Manual* or other Vanderbilt documentation.

Step 1 – Check Network Settings

At a keypad connected to the panel:

1. Log in as an engineer.
2. Check the following options:

   COMMUNICATION/ETHERNET PORT/IP ADDRESS – Ensure that a fixed IP address is specified. You will need to enter this in the Symmetry "Install/Intrusion/Intrusion/System Configuration" screen.

   COMMUNICATION/ETHERNET PORT/IP NETMASK – Check that the Symmetry client that is going to be used to communicate with the panel is on the same subnet as the panel.

   COMMUNICATION/ETHERNET PORT/DHCP – Set to **DISABLED**.

3. Restore all alerts and log out.

Step 2 – Install SPC Pro

Install the Vanderbilt SPC Pro software if it is not already installed. This can be installed on any PC on the network.

Step 3 – Check Firmware

Using the SPC Pro:

1. Click **General** in the side bar.
2. Click **Status**.
3. Check that **Firmware Version** is 3.4.1 or later. If it is not, update the firmware as described in the *SPC Pro Configuration Manual*.

Step 4 – Configure EDP Receiver in SPC Pro

Using the SPC Pro:

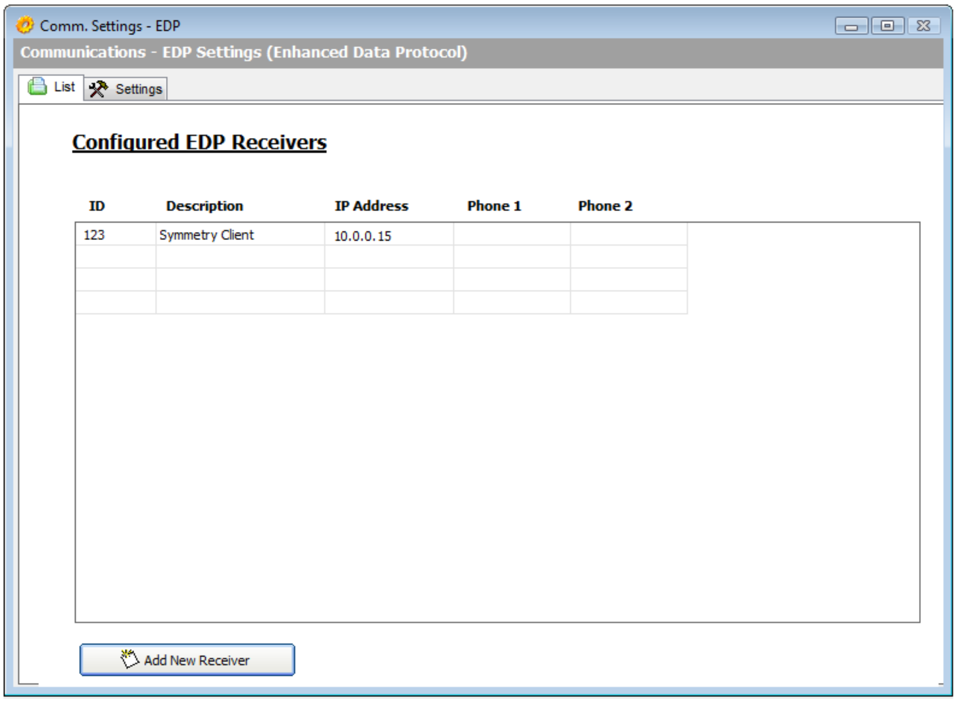
1. Click **Communications** in the side bar.
2. Click **EDP Settings**.
3. Click **Add New Receiver** and set the following:

   Description - Any name (e.g. "Symmetry Client").

Receiver ID - A unique ID for this EDP receiver (e.g. "123"). You will need to enter this in the Symmetry "Install/Intrusion/Intrusion/System Configuration" screen.

Receiver IP Address - The IP address of the Symmetry client PC that is to manage communications to the Vanderbilt panel.

4. Click **OK**. The receiver is listed:



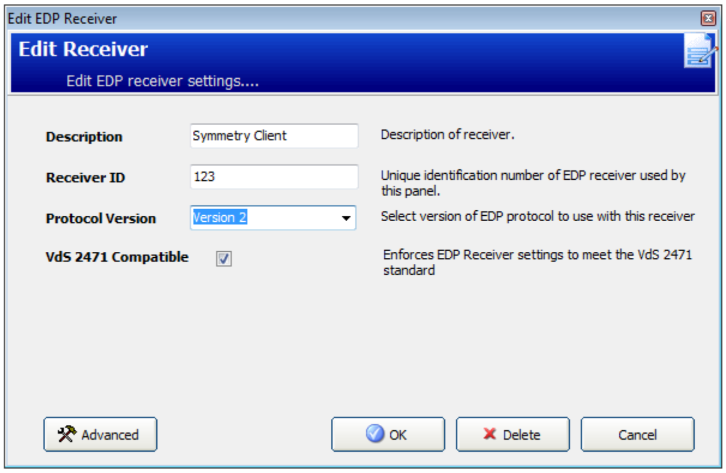
Comm. Settings - EDP

Communications - EDP Settings (Enhanced Data Protocol)

Configured EDP Receivers

ID	Description	IP Address	Phone 1	Phone 2
123	Symmetry Client	10.0.0.15		

5. Double-click the receiver and set **Protocol Version** to **Version 2**:



Edit EDP Receiver

Edit Receiver

Edit EDP receiver settings....

Description	Symmetry Client	Description of receiver.
Receiver ID	123	Unique identification number of EDP receiver used by this panel.
Protocol Version	Version 2	Select version of EDP protocol to use with this receiver
VdS 2471 Compatible	☑	Enforces EDP Receiver settings to meet the VdS 2471 standard

6. Click the **Advanced** button and set the following:

Commands Enable – Select this option.

Encryption Enabled – Select if communications encryption is required.

Encryption Key – If **Encryption Enabled** is selected, specify an encryption key.

Network Enable – Select this option.

Network Protocol – Select **TCP/IP**.

Receiver Address – This should already be set to the IP address of the Symmetry client PC that is to manage communications to the Vanderbilt panel.

Receiver Port – Enter any available port number on the Symmetry client that can be used for two-way communication with the panel (e.g. 50000). You will need to enter this in the Symmetry "Install/Intrusion/Intrusion/System Configuration" screen.

Always Connected – Select this option.

Panel Master – Select this option.

Generate Network Fault – Select this option.

Primary Receiver – Select this option.

Requeue Events – Select this option.

Event Filter – Click the **Filter** button and make sure all events and areas are selected.

7. Click **OK**, three times to finish editing the receiver.

8. Click the **Settings** tab and set the following:

   Enable – Select this option.

   EDP Panel ID – Enter a unique ID for the panel (e.g. "1"). You will need to enter this in the Symmetry "Install/Intrusion/Intrusion/System Configuration" screen.

   Event Logging Options – Make sure all checkboxes are selected.

Step 5 – Configure Panel Settings in SPC Pro

Using SPC Pro:

1. Click **Panel Settings** in the side bar.

2. Click **System Settings**.

3. If more than one area is being used, click the Options tab and set the **Areas** checkbox.

4. Click the Timers tab and set **Dialler Delay** to 0 seconds.

Step 6 – Download Settings to Panel

Using SPC Pro:

1. If the tooltip for the Engineer Mode button in the Config Mode Toolbar shows **Select Full Engineer Mode**, click it to enter full engineer mode.

2. In the Config Mode Toolbar, click **Send Config File to Panel**. This sends the changes to the panel.

Galaxy Systems

Before configuring a Galaxy panel, ensure that a battery is connected to the panel and that the tamper switch is closed. Configure the panel as described in the following steps.

Network-Connected Galaxy Panel

Configure the panel as follows if the panel communicates with the Symmetry software over a network connection.

Step 1 – Enable Engineer Mode

Enable engineer mode as follows:

1. Type "12345" (the manager code) at the keypad and press <ent>.
2. Warning or fault messages may be displayed. Press <ent> to continue.
3. "10=SETTING" is displayed. Press <ent>.
4. Type "48" (ENG ACCESS) and press <ent>. "1=System Access" is displayed.
5. Press <ent>. "1=Engineer" is displayed.
6. Press <ent>. "0=Disabled" or "1=Enabled" is displayed.
7. If "0=Disabled" is displayed, press "1" to display "1=Enabled" and press <ent>.
8. Exit manager mode by pressing <esc> several times until the date and time are displayed.

Step 2 – Enter Engineer Mode

Select the engineer mode "Settings" option as follows:

1. Type "112233" and press <ent>.
2. Warning or fault messages may be displayed. Press <ent> to continue.
3. "10=SETTING" is displayed. Press <ent>.

Step 3 – Set TCP Communications Protocol

Set TCP communications protocol, as follows:

1. Type:

   "56" (COMMUNICATION) <ent>
   "4" (ETHERNET) <ent>
   "02" (ALARM REPORT) <ent>
   "8" (PROTOCOL) <ent>

2. Select "TCP" (using <A>), then press <ent>.
3. Keep pressing <esc> until "56=COMMUNICATION" is displayed.

Step 4 – Specify the IP Address and Port Number of the Symmetry Client

Set the IP address and port number of the Symmetry client PC as follows:

1. Type:

   "56" (COMMUNICATION) <ent>

   "4" (ETHERNET) <ent>

   "02" (ALARM REPORT) <ent>

   "2" (PRIMARY IP) <ent>

   "1" (IP ADDRESS) <ent>. The current IP address is displayed.

2. Press <B> to delete the current IP address, type the IP address of the Symmetry client PC and press <ent>.

3. Press <A> until "2=PORT NO" is displayed, then press <ent>. The existing port number is displayed.

4. Check and, if necessary, change the port number to 10002, then press <ent>.

5. Keep pressing <esc> until "56=COMMUNICATION" is displayed.

Step 5 – Set the Account Number

Set the account number, as follows:

1. Type:

   "56" (COMMUNICATION) <ent>

   "4" (ETHERNET) <ent>

   "02" (ALARM REPORT) <ent>

   "4" (ACCOUNT NO) <ent>

2. Press <B> to delete the current account number, type the panel account number (e.g. "54321") and press <ent>.

3. Keep pressing <esc> until "56=COMMUNICATION" is displayed.

Step 6 – Set the SIA Communications Protocol

Set SIA communications protocol as follows:

1. Type:

   "56" (COMMUNICATION) <ent>

   "4" (ETHERNET) <ent>

   "02" (ALARM REPORT) <ent>

   "1" (FORMAT) <ent>

2. Select "SIA" (using <A>), then press <ent>.

3. Select level "4" (using <A>), press <ent>, then press <ent> again when you see "TRIGGER EVENTS".

4. Using the <A> and <B> keys, step through the triggers. The triggers control the events that are transmitted to the Symmetry software. If the trigger is set to On, any events that are controlled by the trigger are transmitted.

   To modify a trigger status, press <ent>, press <ent> when you see "STATUS", press "1" (On) or "0" (Off), then <ent>. The **Zone Restoral** trigger must be set to On, otherwise the user will not be able to clear alarms in the Symmetry software.

5. Keep pressing <esc> until "56=COMMUNICATION" is displayed.

Step 7 – Leave Engineer Mode

Leave Engineer Mode, as follows:

1. Press <esc> until "ENGINEER MODE" is displayed.

2. Type "112233" and press <esc>. "CHECKING FOR TAMPERS" is displayed.

3. Wait for "NO MODULES ADDED" to be displayed, then press <esc>. After a few moments, the default (date and time) screen is displayed.

RS232-Connected Galaxy Panel

Configure the panel as follows if the panel connects to the Symmetry software over an RS232 serial connection.

Step 1 – Enable Engineer Mode

Enable engineer mode s follows:

1. Type "12345" (the manager code) at the keypad and press <ent>.

2. Warning or fault messages may be displayed. Press <ent> to continue.

3. "10=SETTING" is displayed. Press <ent>.

4. Type "48" (ENG ACCESS) and press <ent>. "1=System Access" is displayed.

5. Press <ent>. "1=Engineer" is displayed.

6. Press <ent>. "0=Disabled" or "1=Enabled" is displayed.

7. If "0=Disabled" is displayed, press "1" to display "1=Enabled" and press <ent>.

8. Exit manager mode by pressing <esc> several times until the date and time are displayed.

Step 2 – Enter Engineer Mode

Select the engineer mode "Settings" option as follows:

1. Type "112233" and press <ent>.

2. Warning or fault messages may be displayed. Press <ent> to continue.

3. "10=SETTING" is displayed. Press <ent>.

Step 3 – Configure the RS232 Settings

Set the panel for RS232 communications as follows:

1. Type:

   "56" (COMMUNICATION) <ent>

   "6" (INT RS232 1) <ent>

2. Type "1" (MODE) <ent>, then:

   Select "DIRECT" (using <A>), then press <ent>.

3. Type "2" (FORMAT) <ent>, then

   a) Select "SIA" (using <A>), then press <ent>.

   b) Select level "3" (using <A>), press <ent>, then press <ent> again when you see "TRIGGER EVENTS".

   c) Using the <A> and <B> keys, step through the triggers. The triggers control the events that are transmitted to the Symmetry software. If the trigger is set to On, any events that are controlled by the trigger are transmitted.

   To modify a trigger status, press <ent>, press <ent> when you see "STATUS", press "1" (On) or "0" (Off), then <ent>. The **Zone Restoral** trigger must be set to On, otherwise the user will not be able to clear alarms in the Symmetry software.

   d) Press <esc> until "FORMAT" is displayed.

4. Type "3" (ACCOUNT NO) <ent>, then

   Enter an account number, then press <ent>.

5. Type "4" (COMMS SET-UP) <ent>, then

   Select "BAUD RATE" (using <A>), then press <ent>.

   Select "9600" (using <A>), then press <ent>.

   Select "DATA BITS", then press <ent>.

   Select "8 DATA BITS", then press <ent>.

   Select "STOP BITS", then press <ent>.

   Select "1 STOP BIT", then press <ent>.

   Select "PARITY", then press <ent>.

   Select "NO PARITY", then press <ent>.

6. Keep pressing <esc> until "56=COMMUNICATION" is displayed.

Step 4 – Leave Engineer Mode

Leave Engineer Mode, as follows:

1. Press <esc> until "ENGINEER MODE" is displayed.

2. Type "112233" and press <esc>. "CHECKING FOR TAMPERS" is displayed.

3. Wait for "NO MODULES ADDED" to be displayed, then press <esc>. After a few moments, the default (date and time) screen is displayed.

Step 5 – Connect the Serial Cable

Connect the RS232 port on the panel to the Symmetry client PC using a serial cable wired as follows:

PC	Galaxy Panel
CTS (pin 8)	RTS
RTS (pin 7)	CTS
GND (pin 5)	GND (important)
Tx (pin 3)	Rx
Rx (pin 2)	Tx

Bosch B9512G Intrusion Panel

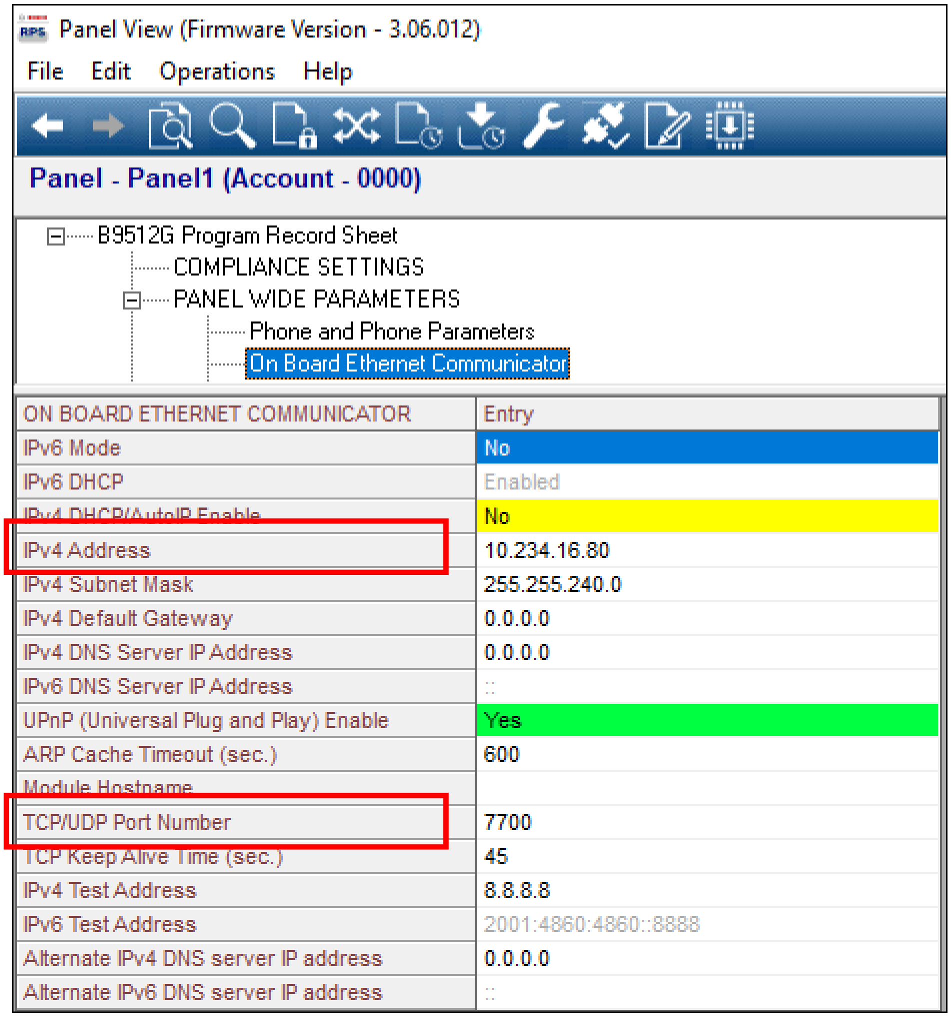
Configure the following using the Bosch RPS (Remote Programming Software), which is available from the Bosch web site. Please refer to the Bosch RPS documentation for further information.

Note: After changing any settings, you must use the Send/Rcv button to send the changes to the panel before connecting to Symmetry.

On Board Ethernet Communicator Page

In the panel's Program Record Sheet, open the **"PANEL WIDE PARAMETERS, On Board Ethernet Communicator"** page, and configure the following:

- **IPv4 Address −** Assign the panel an IP address.
- **TCP/UDP Port Number −** This is the port used for communication with Symmetry (default 7700).


RPS
Panel View (Firmware Version - 3.06.012)
File
Edit
Operations
Help
Panel - Panel1 (Account - 0000)
B9512G Program Record Sheet
COMPLIANCE SETTINGS
PANEL WIDE PARAMETERS
Phone and Phone Parameters
On Board Ethernet Communicator

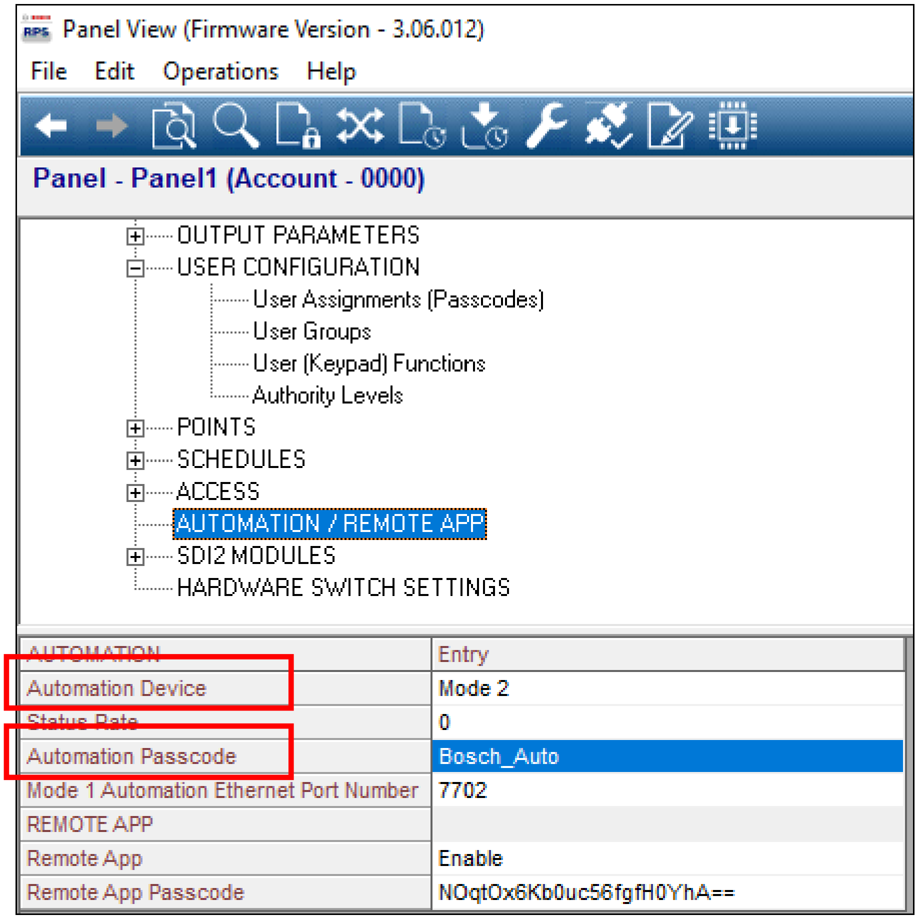
ON BOARD ETHERNET COMMUNICATOR	Entry
IPv6 Mode	No
IPv6 DHCP	Enabled
IPv4 DHCP/AutoIP Enable	No
IPv4 Address	10.234.16.80
IPv4 Subnet Mask	255.255.240.0
IPv4 Default Gateway	0.0.0.0
IPv4 DNS Server IP Address	0.0.0.0
IPv6 DNS Server IP Address	::
UPnP (Universal Plug and Play) Enable	Yes
ARP Cache Timeout (sec.)	600
Module Hostname	
TCP/UDP Port Number	7700
TCP Keep Alive Time (sec.)	45
IPv4 Test Address	8.8.8.8
IPv6 Test Address	2001:4860:4860::8888
Alternate IPv4 DNS server IP address	0.0.0.0
Alternate IPv6 DNS server IP address	::

Automation / Remote App Page

In the panel's Program Record Sheet, open the **"AUTOMATION / REMOTE APP"** page, and configure the following:

- **Automation Device** − Set to **Mode 2**.

- **Automation Passcode** − Specify a passcode of your choice that Symmetry must use to communicate with the panel.

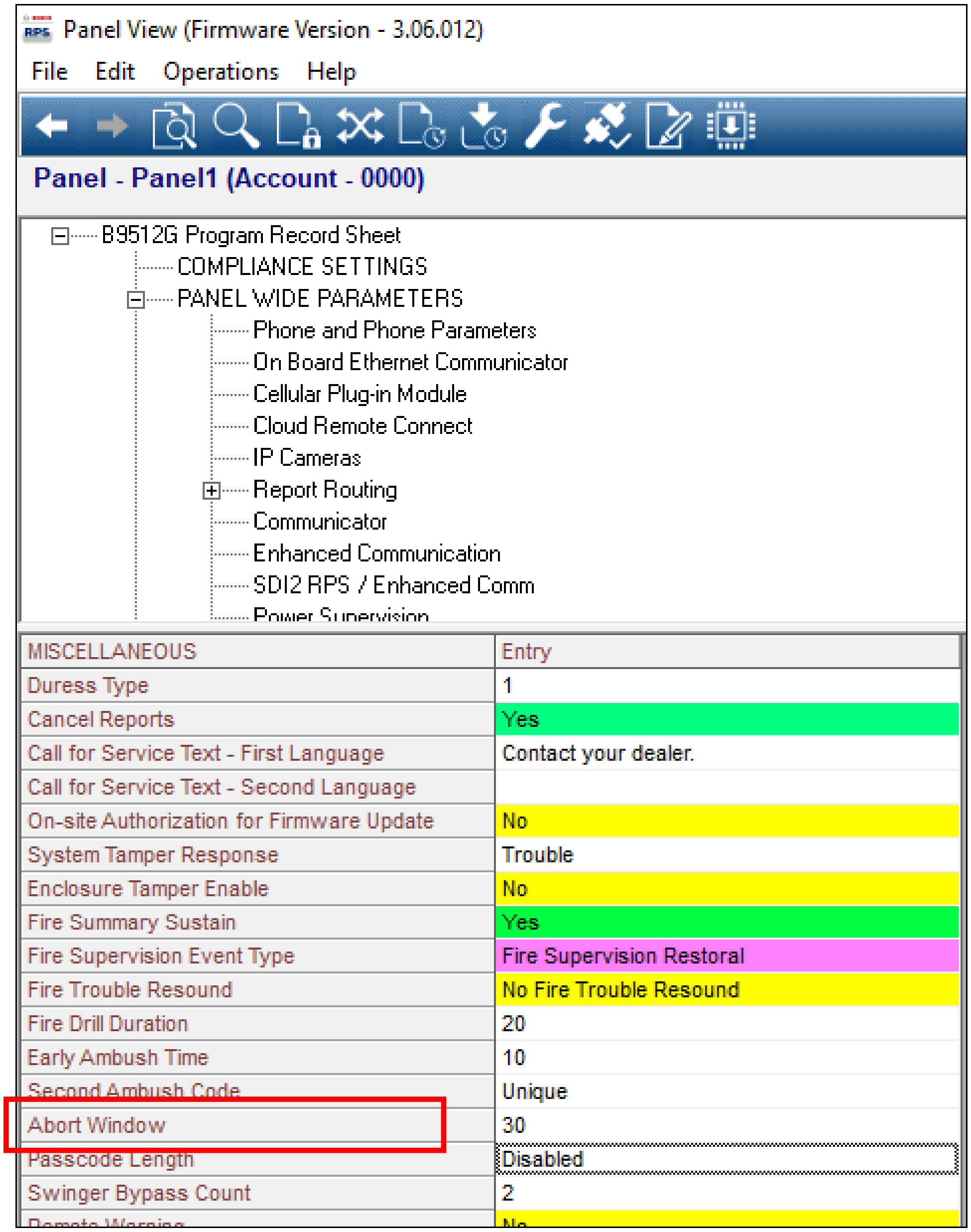


AUTOMATION	Entry
Automation Device	Mode 2
Status Rate	0
Automation Passcode	Bosch_Auto
Mode 1 Automation Ethernet Port Number	7702
REMOTE APP	
Remote App	Enable
Remote App Passcode	NOqtOx6Kb0uc56fgfH0YhA==

Miscellaneous Page

In the panel's Program Record Sheet, open the **"PANEL WIDE PARAMETERS, Miscellaneous"** page, and configure the following:

- **Passcode Length –** Specify the required length of passcodes (equivalent to Symmetry IDS codes). If you select **Disabled**, passcodes (IDS codes) can be any length. If, for example, you specify a length of 4, all IDS codes must be four digits long.



Panel - Panel1 (Account - 0000)

- B9512G Program Record Sheet
  - COMPLIANCE SETTINGS
  - PANEL WIDE PARAMETERS
    - Phone and Phone Parameters
    - On Board Ethernet Communicator
    - Cellular Plug-in Module
    - Cloud Remote Connect
    - IP Cameras
    - Report Routing
    - Communicator
    - Enhanced Communication
    - SDI2 RPS / Enhanced Comm
    - Power Supervision

MISCELLANEOUS	Entry
Duress Type	1
Cancel Reports	Yes
Call for Service Text - First Language	Contact your dealer.
Call for Service Text - Second Language	
On-site Authorization for Firmware Update	No
System Tamper Response	Trouble
Enclosure Tamper Enable	No
Fire Summary Sustain	Yes
Fire Supervision Event Type	Fire Supervision Restoral
Fire Trouble Resound	No Fire Trouble Resound
Fire Drill Duration	20
Early Ambush Time	10
Second Ambush Code	Unique
Abort Window	30
Passcode Length	Disabled
Swinger Bypass Count	2
Remote Warning	No

Chapter 3: Configuring Symmetry

This chapter explains how to configure Intrusion Management in the Symmetry software.

Initial Tasks for All Intrusion Panels

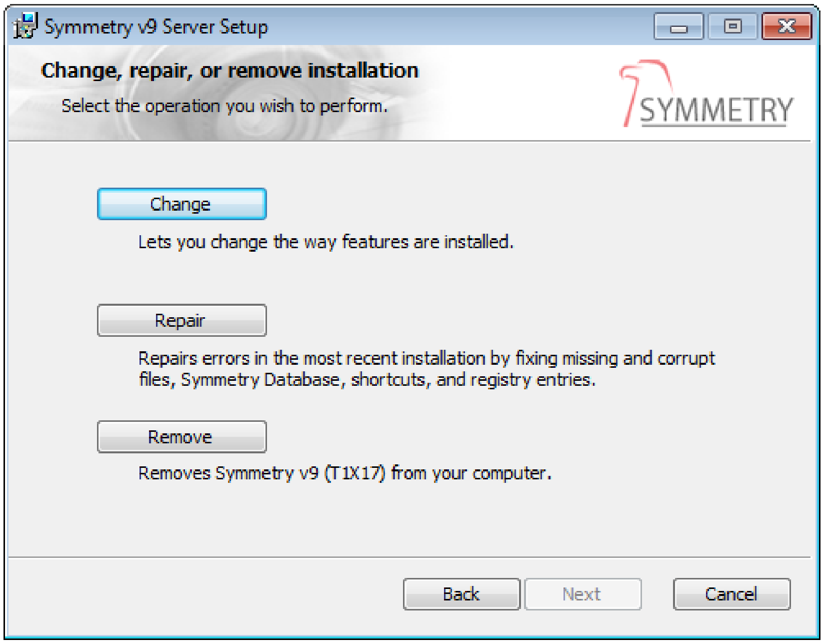
This section describes configuration tasks you need to carry out when using any type of supported intrusion panel.

Step 1 – Install the Device Integration

If the device integration was not selected during the installation of Symmetry:

1. Re-run the Symmetry installation software.

2. Follow the prompts. When you see the following, click **Change**:



Symmetry v9 Server Setup

Change, repair, or remove installation

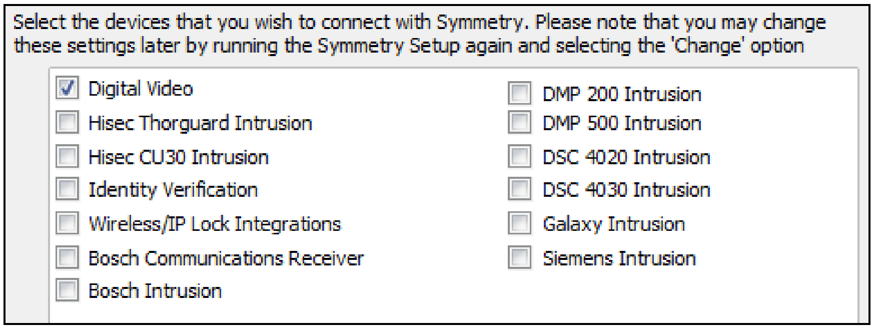
Select the operation you wish to perform.

Lets you change the way features are installed.

Repairs errors in the most recent installation by fixing missing and corrupt files, Symmetry Database, shortcuts, and registry entries.

Removes Symmetry v9 (T1X17) from your computer.

3. Follow the prompts. When you see the Select Device Integrations page, select the integration you require:

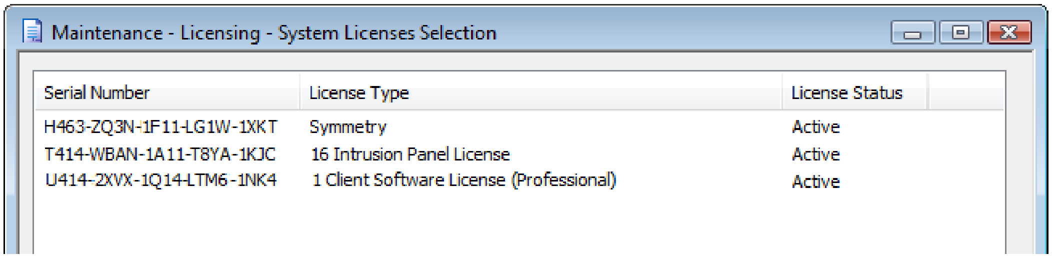


Select the devices that you wish to connect with Symmetry. Please note that you may change these settings later by running the Symmetry Setup again and selecting the 'Change' option

- ☑ Digital Video
- □ Hisec Thorguard Intrusion
- □ Hisec CU30 Intrusion
- □ Identity Verification
- □ Wireless/IP Lock Integrations
- □ Bosch Communications Receiver
- □ Bosch Intrusion
- □ DMP 200 Intrusion
- □ DMP 500 Intrusion
- □ DSC 4020 Intrusion
- □ DSC 4030 Intrusion
- □ Galaxy Intrusion
- □ Siemens Intrusion

4. Click **Next** and follow the prompts.

Step 2 – Install License



Maintenance - Licensing - System Licenses Selection

Serial Number	License Type	License Status
H463-ZQ3N-1F11-LG1W-1XKT	Symmetry	Active
T414-WBAN-1A11-T8YA-1KJC	16 Intrusion Panel License	Active
U414-2XVX-1Q14-LTM6-1NK4	1 Client Software License (Professional)	Active

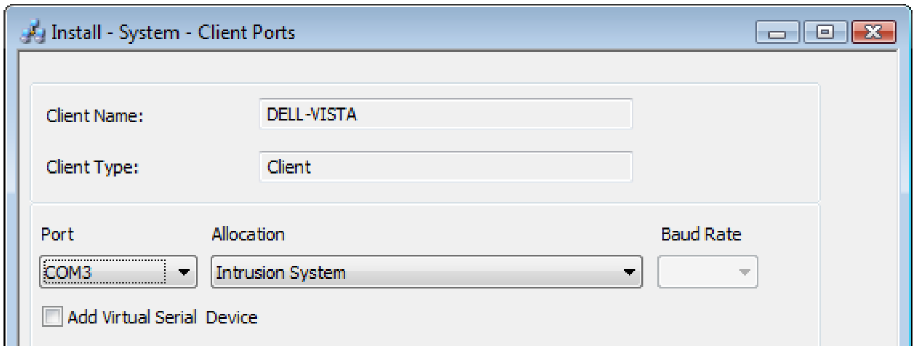
The interface can be enabled by adding the "Intrusion Panel License" in the "Maintenance/Licensing/ System Licenses" screen at a Symmetry client. Please refer to the Online Help for further information.

Step 3 – Define the Client Port

Note: This step is not required for a Bosch B9512G or Vanderbilt panel, since a client port and LAN chain can be created automatically when defining the panel in the "Install/Intrusion/Intrusion/System Configuration" screen (Step 5).

For all but a Bosch B9512G or Vanderbilt panel, use the "Install/System/Client Ports" screen to specify the client port that will be used to communicate with the intrusion system. Choose a **COM** port to set up a serial link to a single intrusion system, or **IPNet** to set up a network link to one or more intrusion systems.

In the **Allocation** drop-down list, choose **Intrusion System** for a COM port, or **Intrusion System LAN Chain** for a network link. Please refer to Table 1 on page 2 for details of whether serial or network communications is supported for the type of intrusion system you are using.



Install - System - Client Ports

Client Name: DELL-VISTA

Client Type: Client

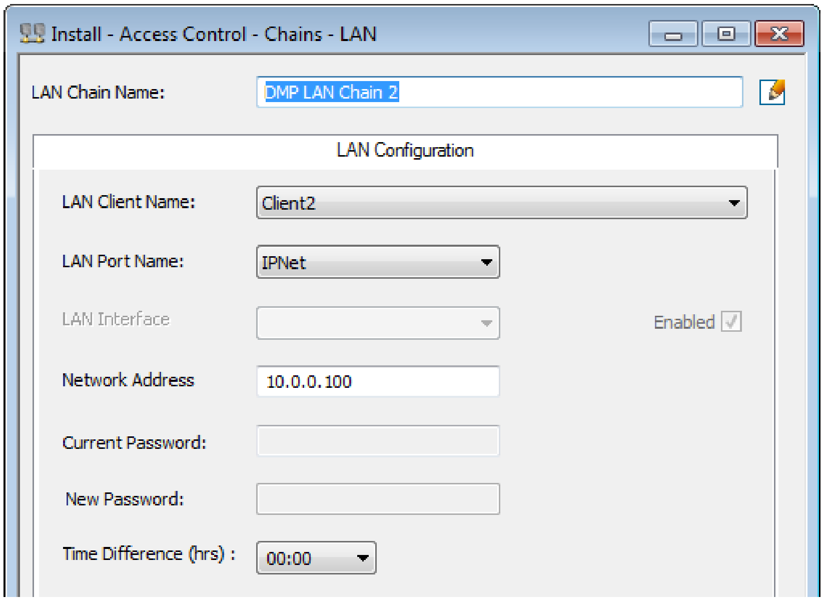
Port	Allocation	Baud Rate
COM3	Intrusion System	

□ Add Virtual Serial Device

Step 4 – Define LAN Chains

Note: This step is not required for a Bosch B9512G or Vanderbilt panel.

If you set up an **IPNet** network port in step 3, use the "Install/Access Control/Chains/LAN" screen to create a new LAN chain definition for each intrusion system that is being used:



Install - Access Control - Chains - LAN

LAN Chain Name: DMP LAN Chain 2

LAN Configuration

LAN Client Name: Client2

LAN Port Name: IPNet

LAN Interface:

Enabled ☑

Network Address 10.0.0.100

Current Password:

New Password:

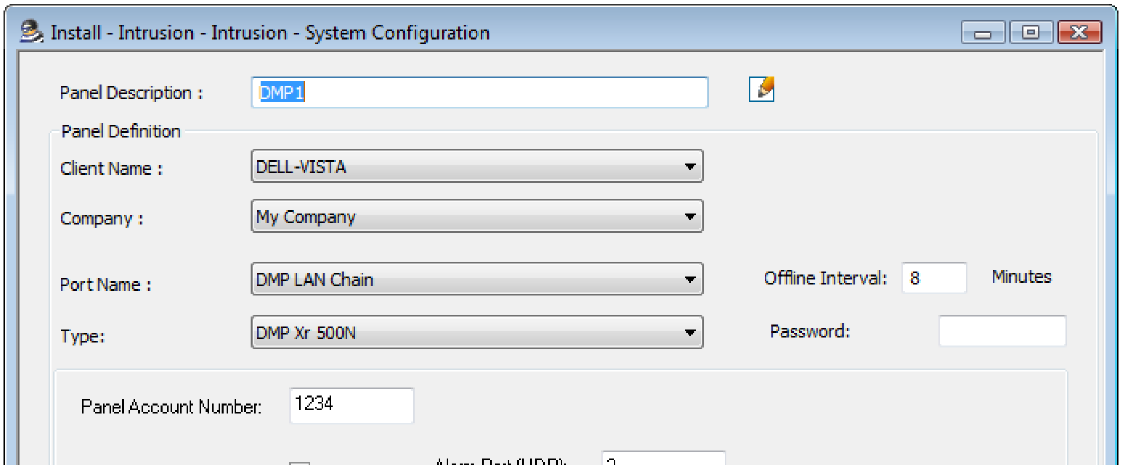
Time Difference (hrs) : 00:00

By default, the date and time of an intrusion alarm is the date and time when the alarm is received by the Symmetry software. If the intrusion system is in another time zone, the time can be adjusted automatically by specifying the time difference in **Time Difference**.

Enter the IP address or network (DNS) name of the intrusion system in **Network Address**.

Step 5 – Define each Intrusion System Used

Create a new record in the "Install/Intrusion/Intrusion/System Configuration" screen for each intrusion system that is being used.



Install - Intrusion - Intrusion - System Configuration

Panel Description : DMP1

Panel Definition

Client Name : DELL-VISTA

Company : My Company

Port Name : DMP LAN Chain

Offline Interval: 8 Minutes

Type: DMP Xr 500N

Password:

Panel Account Number: 1234

Note the following:

Client Name – Choose the Symmetry client PC that is going to be used to communicate with the panel.

Port Name – If you set up a client port in Step 1, select the COM port or LAN chain. Otherwise, for a Bosch B9512G or Vanderbilt panel, choose **Create a new port**.

Type – Choose the type of panel.

Additional options are provided, depending on the type of intrusion system. Please refer to the *Symmetry Online Help* for further details.

Note: For a Bosch B9512G panel, when you click **OK**, all areas, zones, outputs and users are uploaded to the Symmetry database (except users with a Bosch Authority Level of zero). A **Resync** button is provided for the Bosch panel − you must use this button if you make any changes at the panel to keep Symmetry synchronized.

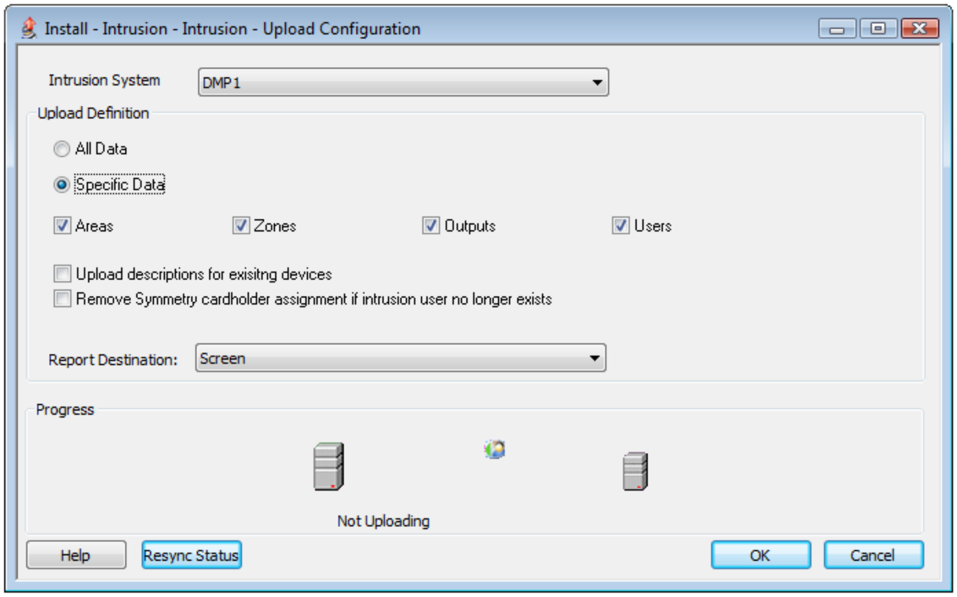
Additional Tasks for Bosch B9512G, Vanderbilt, DMP XR500N\XR550, DSC 4030 (SN4442), HISEC and Galaxy Panels

This section describes the remaining tasks to configure the Symmetry software for the above intrusion panels. If you are using a different make or model of panel, please turn to page 26.

Step 1 – Upload the Panel Configuration

Note: Do not carry out this step for a Bosch B9512G panel, as all areas, zones, outputs and users are automatically uploaded from the panel when you define the panel in the "Install/Intrusion/ Intrusion/System Configuration" screen.

For panels other that a Bosch B9512G, open the "Install/Intrusion/Intrusion/Upload Configuration" screen and select the intrusion system to upload to Symmetry.



Install - Intrusion - Intrusion - Upload Configuration

Intrusion System: DMP1

Upload Definition

○ All Data

● Specific Data

☑ Areas ☑ Zones ☑ Outputs ☑ Users

☐ Upload descriptions for exisitng devices

☐ Remove Symmetry cardholder assignment if intrusion user no longer exists

Report Destination: Screen

Progress

Not Uploading

The Symmetry software checks for changes each time you perform an upload. In this way, Symmetry keeps in step with changes at the panel.

Although you can choose to upload specific data, it is recommended that you use the default **All Data** setting and click **OK** to upload all data. Details of the panels, areas, zone groups, zones, outputs and users (as appropriate) are uploaded to the Symmetry database. Zone groups are applicable to ThorGuard and CU30 systems only.

Note: To improve performance for ThorGuard systems, set RoundTripMessageEnabled to 1 in multimax.ini if you are using ThorGuard GPIs with a firmware level of v0102.006 or above. For further information, please refer to the *Symmetry Software Installation Manual*.

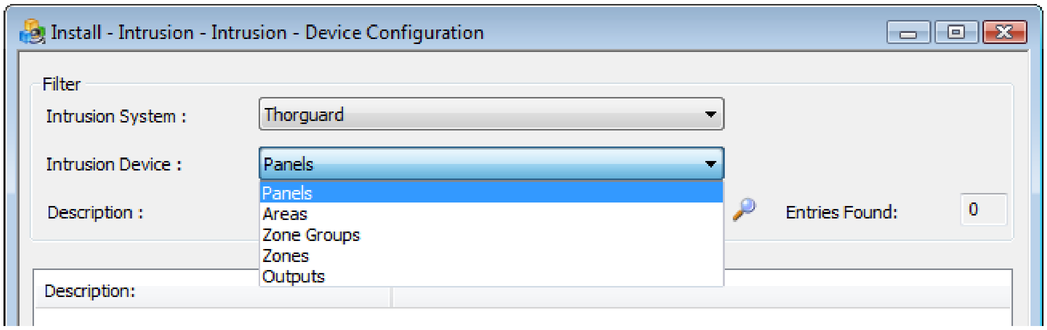
Step 2 (Optional) – Set up Intrusion "Devices"

You can use the "Install/Intrusion/Intrusion/Device Configuration" screen to:

- Rename panels, areas, zone groups, zones and outputs (as appropriate) uploaded from the intrusion system. The new names are used only within the Symmetry software and do not affect the names stored at the intrusion system.

  Note: For areas, you can use the **Permissions** button to specify the user roles that are allowed to arm or disarm the area from Symmetry.

- Associate a graphic created in the "Setup/Graphics/Add" screen with an area or zone group. If an area or zone group icon is added to a graphic, double-clicking the icon in the "Home/Monitoring/Graphics" screen displays the associated graphic. More than one area or zone group can be associated with the same graphic.



Install - Intrusion - Intrusion - Device Configuration

Filter

Intrusion System : Thorguard

Intrusion Device : Panels

Description :

Entries Found: 0

Description:

To carry out any of the above changes:

1. Select the intrusion system from the **Intrusion System** menu.

2. Select **Panels**, **Areas**, **Zone Groups**, **Zones** or **Outputs** (as applicable) from the **Intrusion Device** menu. Some of these options may not be available, depending on the type of intrusion system.

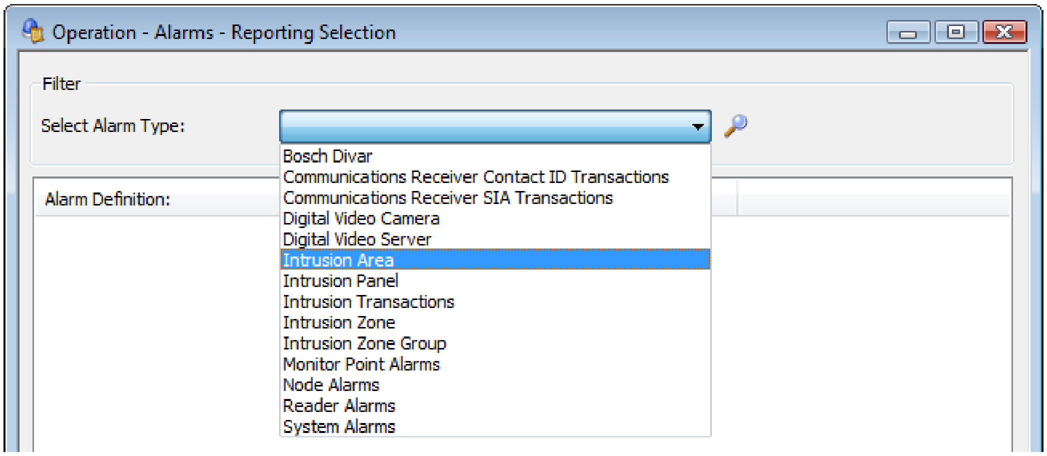
3. Click **Find**.

4. Double-click the panel, area, zone or output you want to configure, and make the required changes in the screen displayed.

Step 3 – Set Up Symmetry Alarm Reporting

You can use the "Operation/Alarms/Reporting" and/or "Operation/Alarms/Definitions" screen to define the attributes of each intrusion alarm/event message, such as the priority, sound and whether to report the message as an alarm or event. If you are using the "Operation/Alarms/Reporting" screen:

1. Choose **Intrusion Area**, **Intrusion Panel**, **Intrusion Zone** or **Intrusion Zone Group** from the **Select Alarm Type** menu, as shown next.



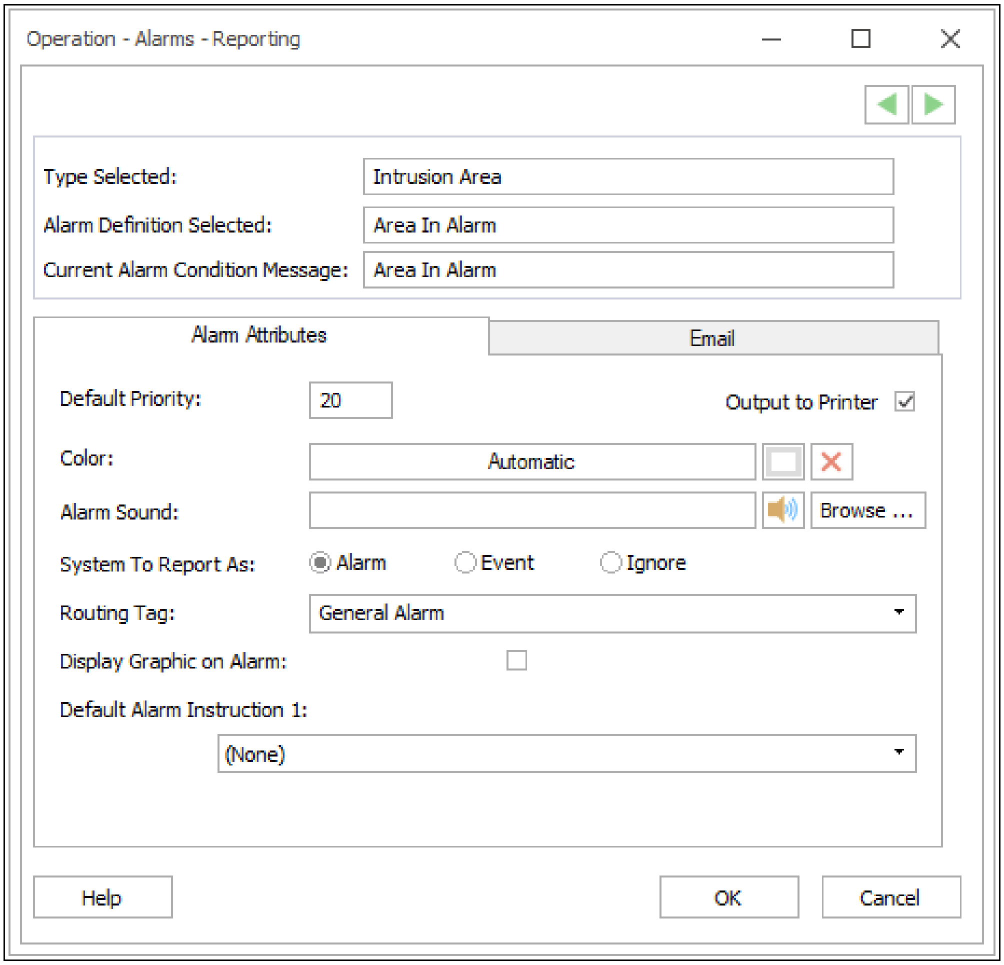
Note: the **Intrusion Transactions** option is not used for the panel you are configuring. It is used for other panel types (see page 26).

2. Click **Find**.

3. Double-click the alarm/event message.

   Note: Many of the alarm/event messages apply only to one type of intrusion system.

4. Make the necessary changes in the screen shown next, then save changes.



Operation - Alarms - Reporting

Type Selected: Intrusion Area

Alarm Definition Selected: Area In Alarm

Current Alarm Condition Message: Area In Alarm

Default Priority: 20

Output to Printer ☑

Color: Automatic

Alarm Sound:

System To Report As: ● Alarm ○ Event ○ Ignore

Routing Tag: General Alarm

Display Graphic on Alarm: □

Default Alarm Instruction 1: (None)

Step 4 – Configuring Graphics

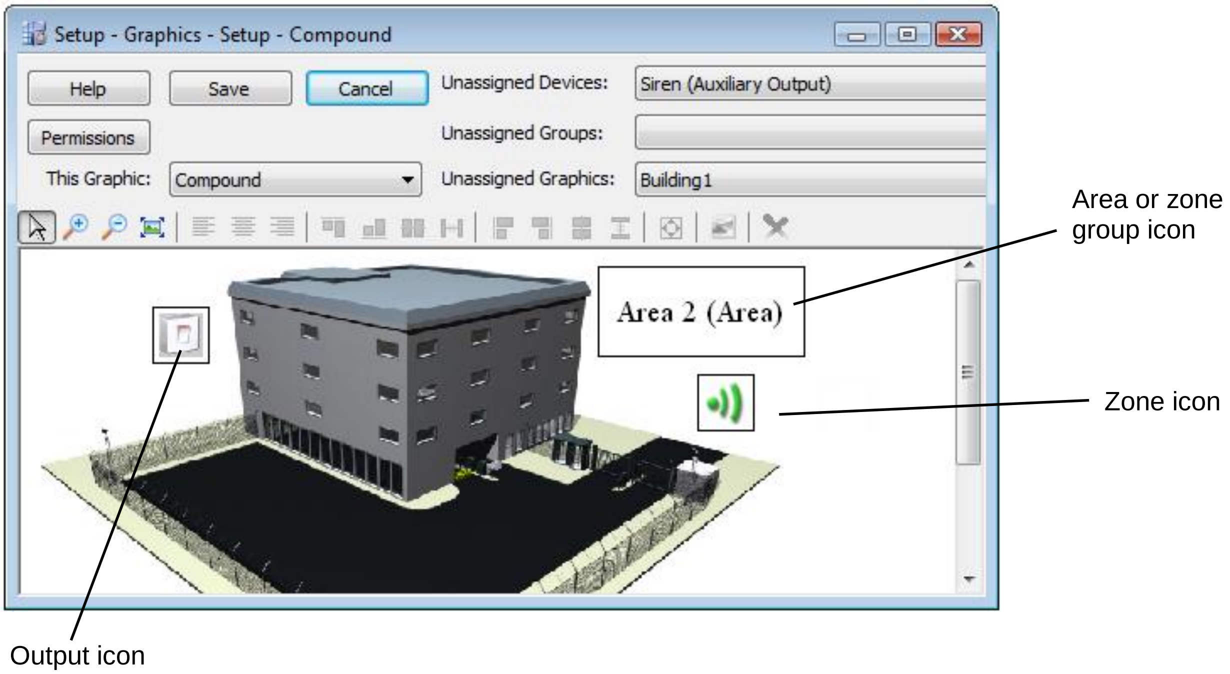
Using the "Setup/Graphics/Setup" screen, you can add icons for intrusion panels, areas, zone groups, zones and outputs to a graphic (depending on the intrusion system). Adding these icons to a graphic enables the "Home/Monitoring/Graphics" screen to be used to view the status of areas, zones, etc. and to send commands to the intrusion system. For example, depending on the intrusion system, users can:

- Arm or disarm areas or zone groups.
- Delay, change or cancel auto-arming of an area (depending on the intrusion system).
- Enable or bypass zones.
- Activate or deactivate outputs.
- Display an associated graphic.
- View whether areas are armed or disarmed, and the status of zones.

Please refer to page 34 for further information about available commands status information in graphics.

Note: With the exception of displaying an associated graphic, the Symmetry software is not able to carry out the above for Galaxy systems.

To add an item to a graphic, select it in the **Unassigned Devices** menu, then drag and drop the icon onto the graphic. The following shows an example.



Setup - Graphics - Setup - Compound

Unassigned Devices: Siren (Auxiliary Output)

Unassigned Groups:

This Graphic: Compound

Unassigned Graphics: Building1

Step 5 – Configuring Permissions

In addition to the standard permissions available with Symmetry, the permissions described next can be set up for Bosch 9512G, Vanderbilt, DMP XR500N\XR550, DSC 4030 (SN4442), HISEC and Galaxy intrusion systems.

"Maintenance/User & Preferences/System Preferences" screen:

- **Mandatory Intrusion Comments** – Selecting this option makes it mandatory to enter the "Action Taken" when sending a command to disarm an area, bypass a zone or disable a zone from the Command Center or Graphics screen, providing the **Enable Comments on Graphic** system preference is also selected.

- **Enable Comments on Graphic –** Selecting this option causes the "Action Taken" prompt to be displayed when sending a command to disarm an area, bypass a zone or disable a zone from the Graphics screen.

"Maintenance/User & Preferences/Roles" screen:

- The **Send Commands** permission can be configured under the Home/Monitoring/Command Center/Intrusion Systems branch to allow/disallow a user role from sending commands in the Command Center.

- The **Allow Zone Bypass when Arming** permission can be configured under the Home/Monitoring/Command Center/Intrusion Systems branch to allow/disallow a user role from bypassing intrusion zones that are in an active state using the Bypass Active Zones setting when arming. This setting does not affect the ability to bypass zones individually.

"Maintenance/User & Preferences/Command Roles" screen:

- For Vanderbilt intrusion systems, you can set permissions for user roles to use Disable Zone and Bypass Zone commands from, for example, the Command Center.

"Install/Intrusion/Intrusion/Device Configuration" screen:

- The **Permissions** button can be used to allow/disallow a user role from setting/unsetting an area.

Additional Tasks for DMP XR200, DSC 4020 and DSC 4030 (SRI) Panels

This section continues from page 21, and describes the remaining Symmetry configuration tasks for the above intrusion systems.

Step 1 – Map Panel Transactions to Symmetry Alarm Messages

Map transaction messages generated by the intrusion system to new Symmetry alarm/event messages as follows:

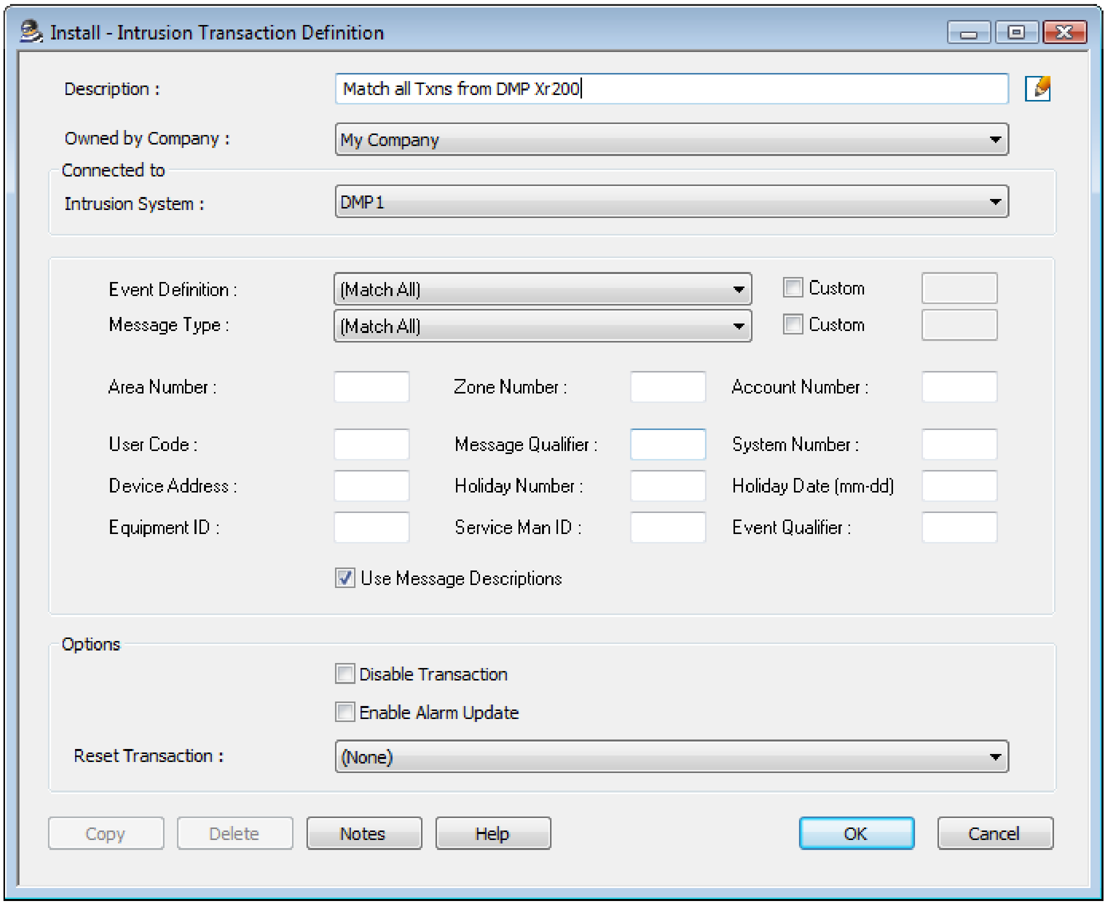
1. In the "Install/Intrusion/Intrusion/Device Configuration" screen, select the intrusion system in the **Intrusion System** menu.

2. Select **Transactions** in the **Intrusion Device** menu.

3. Click **New**.

4. In the Definition screen (shown next), specify the conditions that are to generate the Symmetry alarm/event, then save the details.

   The options displayed on the screen depend on the type of intrusion system. Please refer to the *Symmetry Online Help* for details.



Install - Intrusion Transaction Definition

Description : Match all Txns from DMP Xr200

Owned by Company : My Company

Connected to

Intrusion System : DMP1

Event Definition : (Match All) □ Custom

Message Type : (Match All) □ Custom

Area Number :

Zone Number :

Account Number :

User Code :

Message Qualifier :

System Number :

Device Address :

Holiday Number :

Holiday Date (mm-dd)

Equipment ID :

Service Man ID :

Event Qualifier :

☑ Use Message Descriptions

Options

□ Disable Transaction

□ Enable Alarm Update

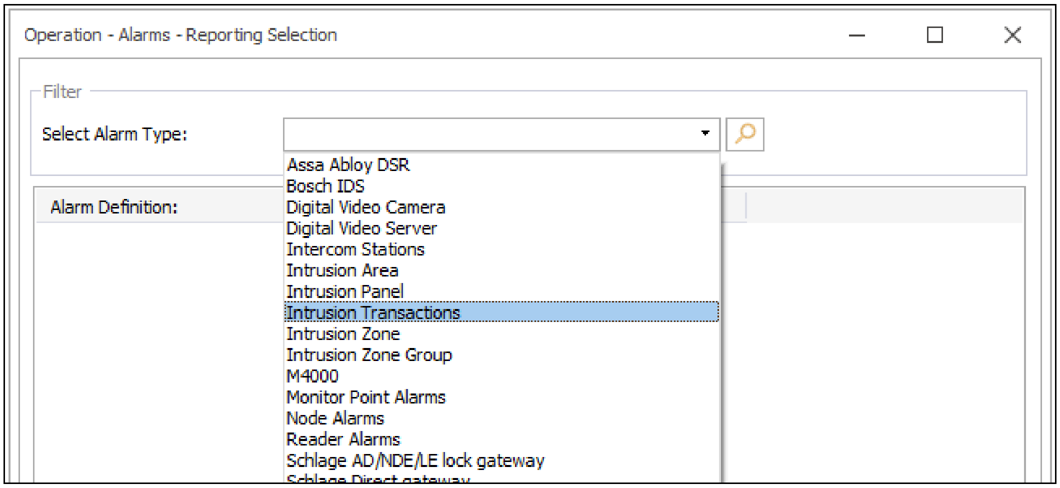
Reset Transaction : (None)

By default, all messages set up in this step are alarms. If required, you can change the messages to be events, as described next.

Step 2 – Set Up Symmetry Alarm Reporting

Use the "Operation/Alarms/Reporting" and/or "Operation/Alarms/Definitions" screen to define the attributes of each intrusion alarm/event message, such as the priority, sound and whether to report the message as an alarm or event. If you are using the "Operation/Alarms/Reporting" screen:

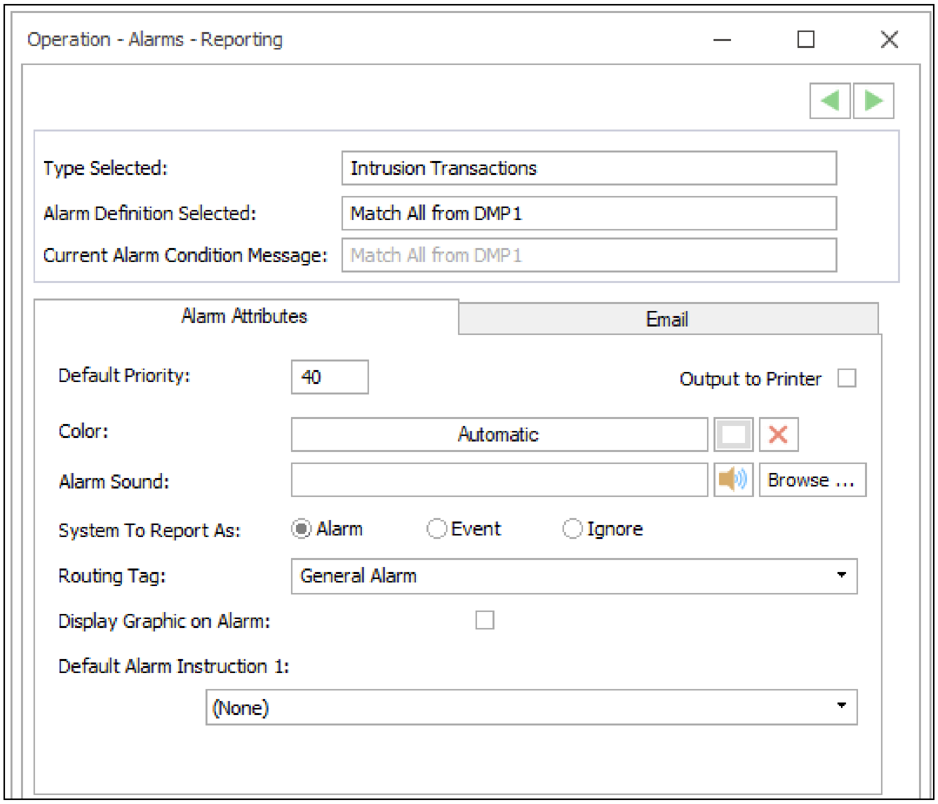
1. Choose **Intrusion Transactions** from the **Select Alarm Type** menu:



2. Click **Find**.

3. Double-click the alarm/event message you want to configure.

4. Choose the required settings in the following screen, then save changes.



Type Selected: Intrusion Transactions

Alarm Definition Selected: Match All from DMP1

Current Alarm Condition Message: Match All from DMP1

Default Priority: 40

Output to Printer □

Color: Automatic

Alarm Sound:

System To Report As: ● Alarm ○ Event ○ Ignore

Routing Tag: General Alarm

Display Graphic on Alarm: □

Default Alarm Instruction 1:

(None)

Step 3 – Configure Downloadable Serial Messages

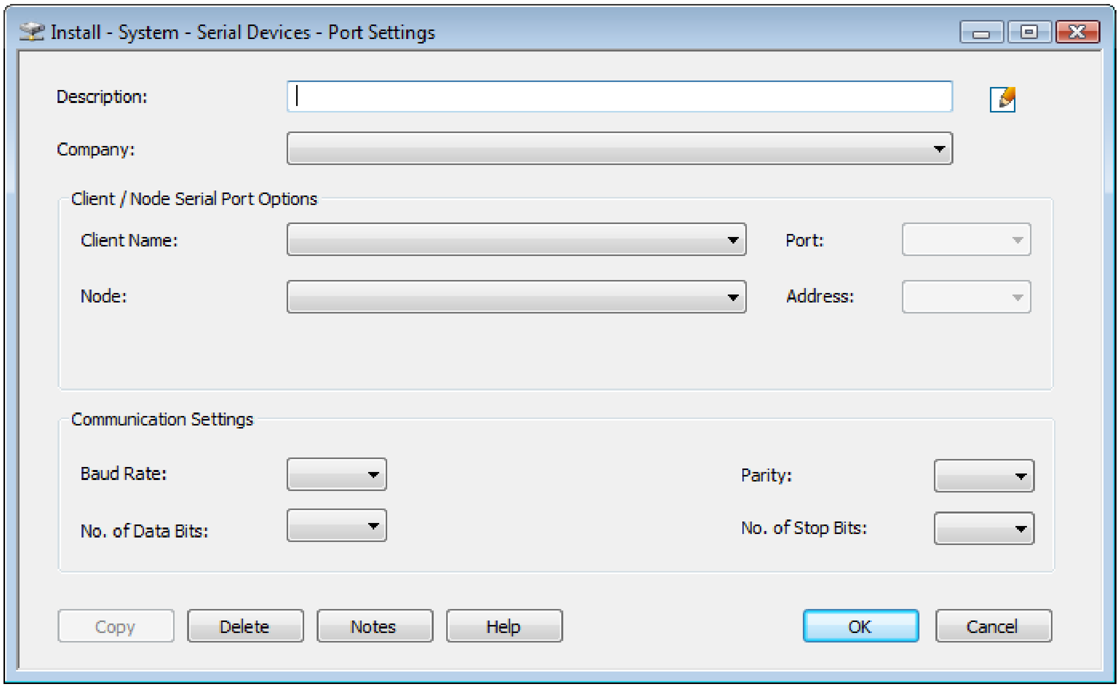
Some intrusion systems (see Table 1 on page 2) allow the Symmetry software to download commands containing user-definable messages. The messages are definable in a text format and could, for example, be used to arm and disarm areas or display messages at keypads. A message can be sent to a panel using Symmetry commands, such as manual, scheduled and trigger commands.

To use this feature:

1. Select **Add Virtual Serial Device** in the "Install/System/Client Ports" screen (page 19).

2. Make sure the panel has been defined in the "Install/Intrusion/System Configuration" screen.

3. Open the "Install/System/Serial Devices/Port Settings" screen, and click **New** to display the following screen, as shown next.



Note: You need to use this screen even if the Symmetry client connects to the intrusion system through a network.

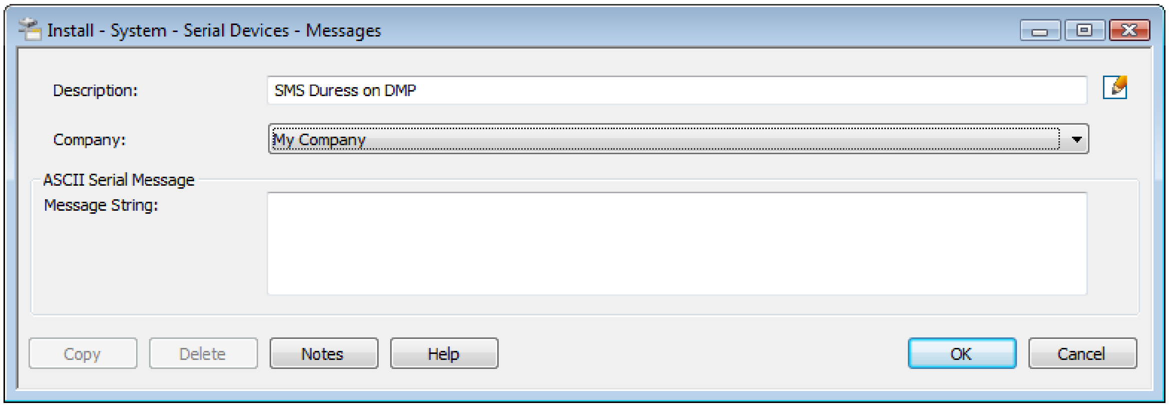
4. Enter a name in the **Description** field that will help to identify the intrusion system. This name is displayed in screens such as "Home/Monitoring/Command Center", "Operation/Commands/Scheduled" and "Operation/Commands/Trigger" when choosing the intrusion system that is to receive a selected message.

   Specify the **Client Name** and **Port**. If you select **IPNet** in the **Port** menu, a **LAN** menu appears for you to choose a LAN chain. The LAN chain you choose (as defined in Step 3 on page 20) identifies the intrusion system that will receive messages.

   Selecting **Provide Protocol** avoids the need to provide termination characters and other data in the message string (as described next) and is the recommended choice. When **Provide Protocol** is not selected, a raw format message can be sent.

   Complete the remaining settings and save changes.

5. Use the Install/System/Serial Devices/Messages screen to define each message:



Description: SMS Duress on DMP

Company: My Company

Message String:

Please refer to the distributor of the intrusion system for details of the message strings to use. The string depends on whether **Provide Protocol** is selected in the Serial Device Port Settings screen.

Note: The time at the intrusion system can be updated with the PC's time by setting **Provide Protocol** and sending the message string =Clock (case is important). This command can be applied to all types of intrusion system for testing purposes. For DMP systems, the PC's clock must be set to a 12-hour format for this message to be recognized.

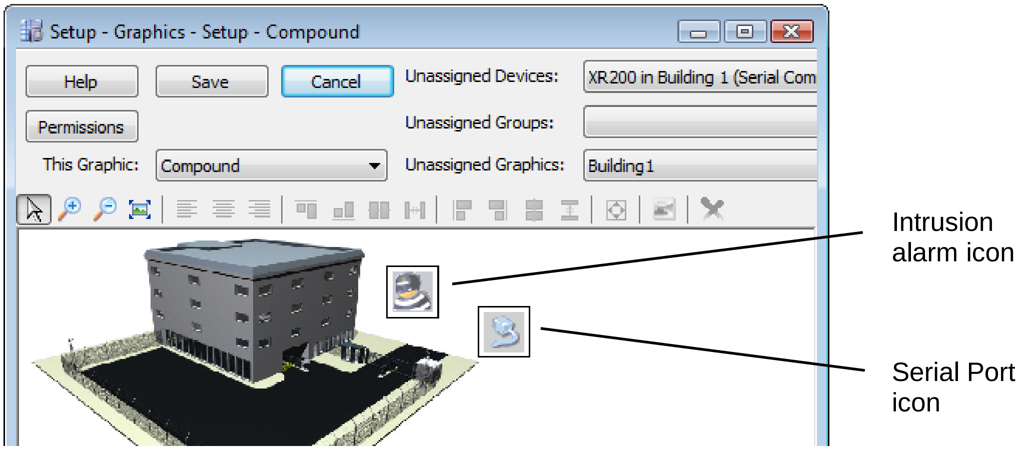
6. You can now use Symmetry commands to send a message to the intrusion system.

Step 4 – Configuring Graphics

The "Setup/Graphics/Setup" screen enables you to add icons for:

- The Symmetry alarm messages set up in Step 5 (page 26). This allows users to view intrusion alarms in the "Home/Monitoring/Graphics" screen.
- Any port set up for serial messages in the "Install/System/Serial Devices/Port Settings" screen (page 29). Users can right-click on the icon in the "Home/Monitoring/Graphics" screen and choose a command to send to the intrusion system.

To add an icon to a graphic, select the required item in the **Unassigned Devices** menu, then drag and drop the icon onto the graphic.



Unassigned Devices: XR200 in Building 1 (Serial Com

Unassigned Groups:

This Graphic: Compound

Unassigned Graphics: Building1

M2150 Reader Control of Third-Party Intrusion Areas

Arming/disarming readers connected to a Symmetry M2150 intrusion node can be used to arm or disarm a selected area in a Bosch B9512G, Vanderbilt, DMP XR500N\XR550, DSC 4030 (SN4442) or HISEC (CU30 or ThorGuard) intrusion system.

This features is of use when Symmetry hardware is used to control access in a building that already has one of these third-party intrusion systems installed.

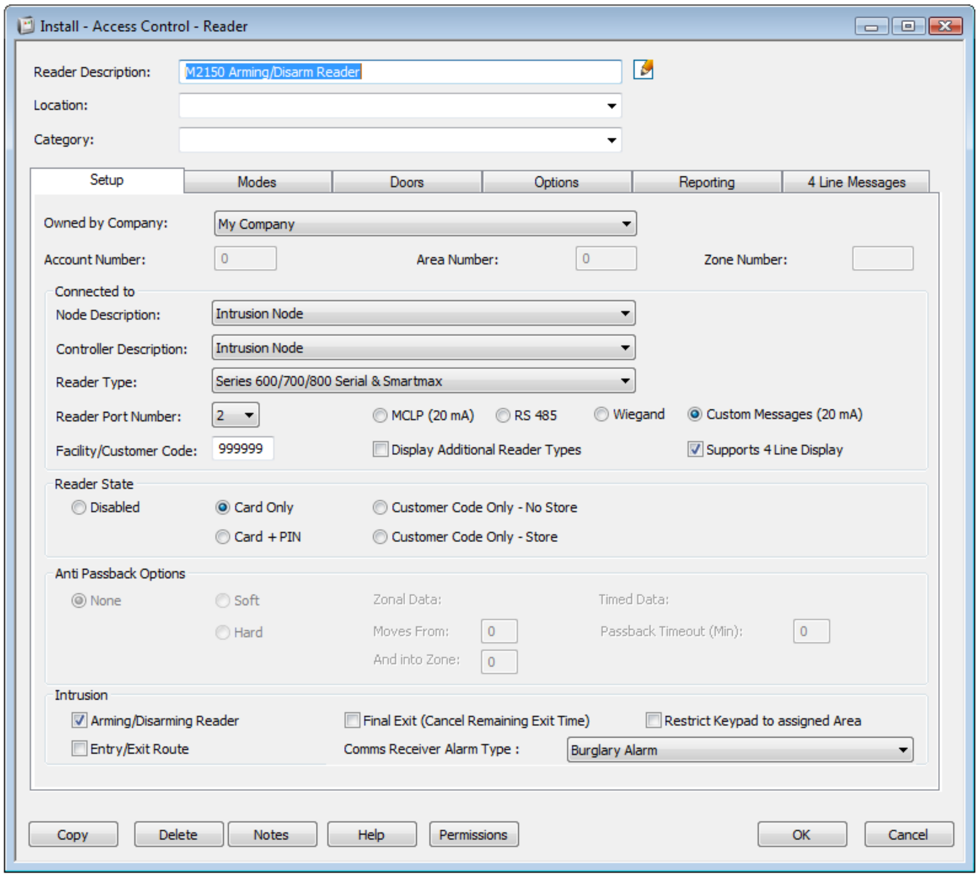
Note: Other features of M2150 intrusion are covered in the *M2150/M4000 Intrusion Guide*.

To use this feature:

1. Define the M2150 arming/disarming reader(s) in the "Install/Access Control/Reader" screen. As shown in the following picture, select:

   - The appropriate **Reader Type**.
   - **Custom Messages (20mA)**.
   - **Arming/Disarming Reader**.
   - **Supports 4 Line Display** if the reader is a Javelin S884.

   Note: Do not select **Entry/Exit Route** or **Final Exit**. These options are not permitted when an M2150 reader is used to arm/disarm a third-party intrusion system. If you select one or both of these options, an error message is displayed when you assign the reader to an intrusion area.



Install - Access Control - Reader

Reader Description: M2150 Arming/Disarm Reader
Location:
Category:

Owned by Company: My Company
Account Number: 0
Area Number: 0
Zone Number:

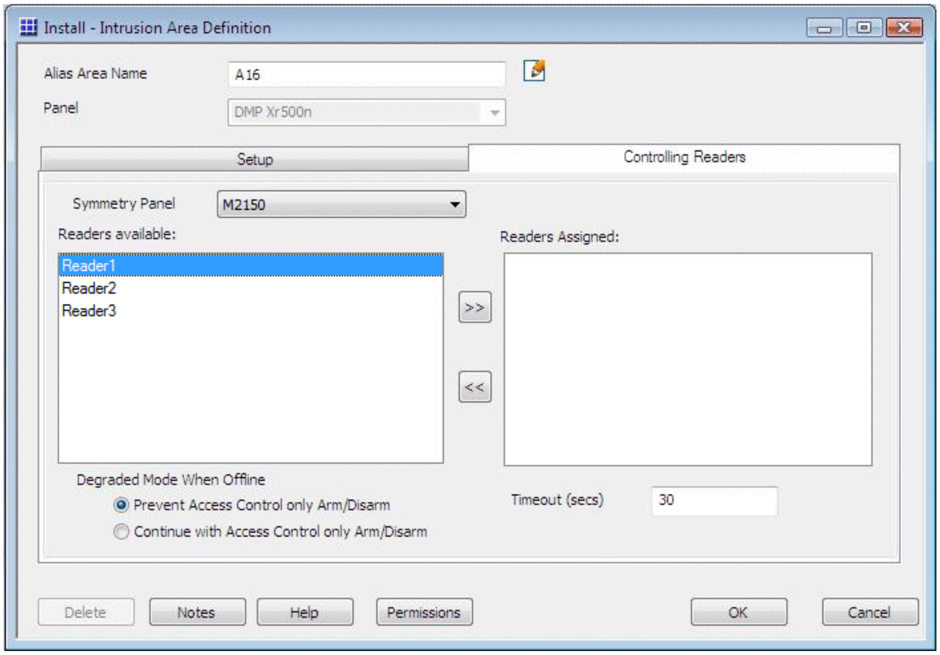
Connected to
Node Description: Intrusion Node
Controller Description: Intrusion Node
Reader Type: Series 600/700/800 Serial & Smartmax
Reader Port Number: 2
○ MCLP (20 mA) ○ RS 485 ○ Wiegand ● Custom Messages (20 mA)
Facility/Customer Code: 999999
□ Display Additional Reader Types
☑ Supports 4 Line Display

Reader State
○ Disabled ● Card Only ○ Customer Code Only - No Store
○ Card + PIN ○ Customer Code Only - Store

Anti Passback Options
● None ○ Soft ○ Hard
Zonal Data:
Moves From: 0
And into Zone: 0
Timed Data:
Passback Timeout (Min): 0

Intrusion
☑ Arming/Disarming Reader
□ Entry/Exit Route
□ Final Exit (Cancel Remaining Exit Time)
□ Restrict Keypad to assigned Area
Comms Receiver Alarm Type : Burglary Alarm

2. In the "Install/Intrusion/Intrusion/Device Configuration" screen, open the third-party intrusion area that is to be armed or disarmed using the M2150 intrusion reader. In the Controlling Readers tab, choose the M2150 node from the **Symmetry Panel** menu, as shown next.



Alias Area Name: A16

Panel: DMP Xr500n

Symmetry Panel: M2150

Readers available:
Reader1
Reader2
Reader3

Readers Assigned:

Degraded Mode When Offline
● Prevent Access Control only Arm/Disarm
○ Continue with Access Control only Arm/Disarm

Timeout (secs): 30

With only the node selected (and no readers moved to the **Readers Assigned** area), any arming/disarming reader connected to the node can be used to arm or disarm the area. For this function to work, a card holder requires only the area to be in their access rights.

4. Decide whether or not to move readers into the **Readers Assigned** box. If you move a reader into the **Readers Assigned** box, a valid access-control transaction at the reader will disarm the area and open the door. For this to function, the reader and area must be in the card holder access rights.

   A reader can be assigned to only one area.

5. The additional settings are optional. Please refer to the *Online Help* if you need information about them.

Chapter 4: Using Intrusion Management

This chapter describes how to use the features of Intrusion Management in the Symmetry software.

Bosch B9512G, Vanderbilt, DMP XR500N\XR550, DSC 4030 (SN4442) and HISEC Panels

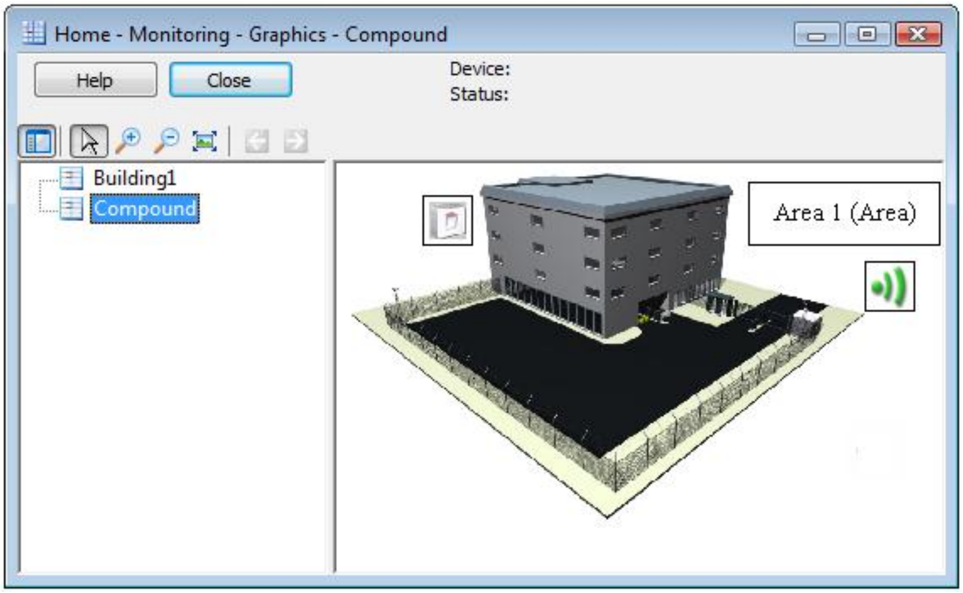
Viewing Intrusion Alarms

Alarms are displayed in the same way as other alarms in screens such as "Home/Monitoring/Alarms", "Home/Monitoring/Graphics", "Home/Video & Audio/Virtual Matrix", "Reports/History/Activity" and "Reports/History/Predefined Reports/Activity".

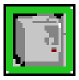
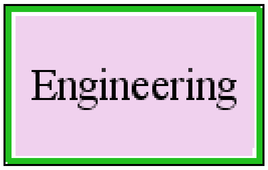
Note:

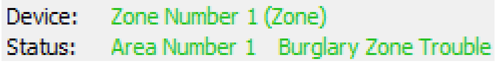
- Acknowledging an alarm silences the alarm at the panel.
- Clearing an alarm removes the alarm message from the alarm list at the panel.
- You may not be able to clear an alarm if the area is still armed.
- If **Clear Alarm if Cleared on Intrusion Panel** is selected in the "Maintenance/User & Preferences/System Preferences" screen, clearing an alarm at a panel automatically clears the alarm in the Symmetry software.

Viewing Graphics



The "Home/Monitoring/Graphics" screen can display the icons shown next, as configured in the "Setup/Graphics/Setup" screen (page 24).

Icon Type	Icon Graphic and Right-Click Commands	Displayed Status Information
Panel	 Panel Commands (see online help for standard commands): **Arm Area** (Bosch B9512G) – Arms all areas. **Disarm Area** (Bosch B9512G) – Disrms all areas. **Restore Alarms** (Vanderbilt) – Restores (resets) all alerts at the panel. **Reset Sensors** (Bosch B9512G) – Resets all alerts at the panel. **Set Clock** – Sets the date and time at the panel to be the same as at the PC. **Set Service Mode** (CU30 and ThorGuard) – Enables an installer to log into the panel from a keypad. **Silence Alarm** (Bosch B9512G, Vanderbilt, CU30 and ThorGuard) – Silences alarm sounds. **Unset Service Mode** (CU30 and ThorGuard) – Unsets service mode.	Device: AC's CU30 Status: Panel Normal The status indicates **Panel Normal**, **Panel Fault** or **Offline**. The border is red when there is an unacknowledged alarm (click **Acknowledge** to acknowledge an alarm). The border is green if an alarm has been acknowledged but not cleared.
Area	 	Device: Engineering Status: Area Disarmed , Area Normal The status area near the top of the screen shows whether the area is, for example, normal, in alarm, armed or disarmed (please refer to the *Online Help*).

	Area Commands (see online help for standard commands): **Arm Area** – Arms the area. **Disarm Area** – Disarms the area. **Cancel Auto Arm** (DMP) – Cancels auto arming until the next day. **Delay Autoarm** (CU30, ThorGuard and DSC) – Delays automatic arming of the area. The delay period is specified at the intrusion system. **Reset Sensors** (Bosch B9512G) – Resets all alerts in the area. **Silence Alarm** (Bosch B9512G and DSC) – Silences an alarm caused by a zone in the area. Double-clicking the icon displays an associated map, if configured (page 22). **Part Arm A/B** (Vanderbilt) – Places the panel into "Partset A" or "Partset B" mode.	The border is red when there is an unacknowledged alarm. The border is green if an alarm has been acknowledged but not cleared. The status of the area is also indicated by the color of the background. **Note:** The background and border colors are configured in the "Install/Intrusion/ Intrusion/Status Color Configuration" screen. Please refer to this screen for the color meanings, as the colors used vary between intrusion systems. The border may also be set up to flash, depending on the state. **Note:** The Symmetry software uses only those DMP messages with an Alarm or Trouble status (see page 5).
Output (Bosch B9512G , Vanderbilt, DSC, DMP and ThorGuard)	Output Commands (see online help for standard commands): **Output On** – Switches output on. **Output Off** – Switches output off.	 Device: OUTPUT NAME 3 Status: No Status Information The status of an output is **Output On**, **Output Off** or **Offline**. Note: For Vanderbilt panels, Symmetry cannot determine the status of an output unless the change of status has been activated from Symmetry.
Zone	Zone Commands (see online help for standard commands): **Bypass** – Prevents the zone from generating alarms. The bypass is cancelled when the area is next disarmed. The zone must have bypassing/isolation allowed at the panel. **Disable** (Vanderbilt, DSC and ThorGuard) – Disables the zone until re-enabled. **Enable** – This cancels the effect of **Disable**. For all but Vanderbilt panels, it also cancels the effect of **Bypass**. **Un-Bypass** (Vanderbilt) – Cancels **Bypass**. **Silence Alarm** (DMP) – Silences an alarm caused by the zone. Double-clicking a zone icon that has an uncleared alarm in the "Home/Monitoring/Alarms" screen enables you to acknowledge and clear the alarm.	 Device: Zone Number 1 (Zone) Status: Area Number 1 Burglary Zone Trouble The status area near the top of the screen displays the current status of the zone. The status of the zone is also indicated by the icon: **Enabled**. The zone is enabled (not bypassed or disabled). **Disabled** (Vanderbilt, DSC and ThorGuard).The icon is grayed out. **Bypassed**. The icon is grayed out, with a large cross. **Force Armed**. The border also provides the zone status. **Note:** The following shows the default border colors; the colors can be changed in the "Install/Intrusion/Intrusion/Status Color Configuration" screen. The border may also be set up to flash, depending on the state.

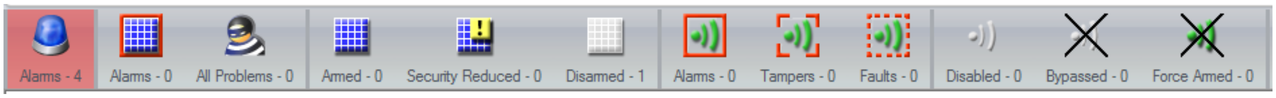
		□ Normal state (icon not selected). 🟥 A red border indicates that the zone has an unacknowledged alarm.
		🟩 A green border (when the icon is not selected) indicates that an alarm has been acknowledged but not cleared. 🟦 A blue border (not available for Bosch B9512G, Vanderbilt, CU30 and ThorGuard) indicates that an alarm has been acknowledged but the device has not been reset. ⬚ A dashed (rather than solid) border indicates that the zone has a fault or tamper condition. The color depends on the acknowledged/cleared status (as above). ⌜⌟ Corners highlighted indicates a tamper condition (for DSC, CU30 and ThorGuard). The color depends on the acknowledged/ cleared status (as above).
Zone Group (ThorGuard and CU30)	 Zone Group Commands (see online help for standard commands): **Arm Zone Group** – Arms the zone group. **Disarm Zone Group** – Disarms the zone group. Double-clicking the icon displays an associated map, if configured (page 22). The border of the icon is red when there is an unacknowledged alarm in the "Home/Monitoring/Alarms" screen.	The status information is similar to that displayed for an area (see above). Please refer to the *Online Help* for details.

Table 2: Icons in the View/Graphics Screen

Using the Intrusion Status Toolbar

The Intrusion Status toolbar, as shown below, provides status information about areas, zones and outputs. From left to right, the toolbar provides the information shown in Table 3.

Note: The intrusion Status toolbar can be displayed by selecting **Show Toolbar** in the "Maintenance/User & Preferences/Accounts" screen.



Icon	Meaning
0	**Acknowledge Alarms** – Total number of unacknowledged alarms (from any source). The background is red when there is at least one unacknowledged alarm.
0	**Area Alarms** – Total number of areas that are currently in an alarm. An area alarm may occur only if the area is armed.
0	**All Problems** – Total number of alarm, tamper, fault, panel offline, zone group with problem and area with problem conditions.
1	**Areas Armed** – Total number of areas that are currently armed.
0	**Areas Security Reduced** – This is applicable only for Bosch B9512G, DSC, ThorGuard and CU30 systems. It indicates the number of armed areas with security reduced (e.g. because areas are partially armed).
9	**Areas Disarmed** – Total number of areas that are currently disarmed.
1	**Zone Alarms** – Total number of zones that are currently in an alarm condition.
0	**Zone Tampers** – This is applicable for Vanderbilt, DSC, CU30 and ThorGuard systems and indicates the number of zones with an open-circuit zone tamper condition. For CU30 and ThorGuard systems, a zone tamper condition is temporary and changes to a zone alarm.
0	**Zone Faults** – Total number of zones that are currently in a fault or tamper condition. For DSC systems, a fault occurs when the zone is short circuit.
0	**Zones Disabled** – Total number of zones that are currently disabled. This applies to Vanderbilt, DSC and ThorGuard systems.
1	**Zones Bypassed** – Total number of zones that are currently bypassed.
0	**Zones Force Armed** – Total number of zones that have been force armed by the intrusion system (not applicable to Bosch B9512G systems). A force-armed zone is one that was in a triggered condition while the area was in the process of being armed. The zone was automatically armed after a specified period of time, or when the zone returned to its normal state (depending on type of intrusion system).

Table 3: Icons in the Intrusion Status Toolbar

Clicking the **Acknowledge Alarms** button displays the "Home/Monitoring/Alarms" screen. Clicking any other button opens the "Home/Monitoring/Command Center" screen, with only the relevant objects displayed according to the button clicked (see the next section).

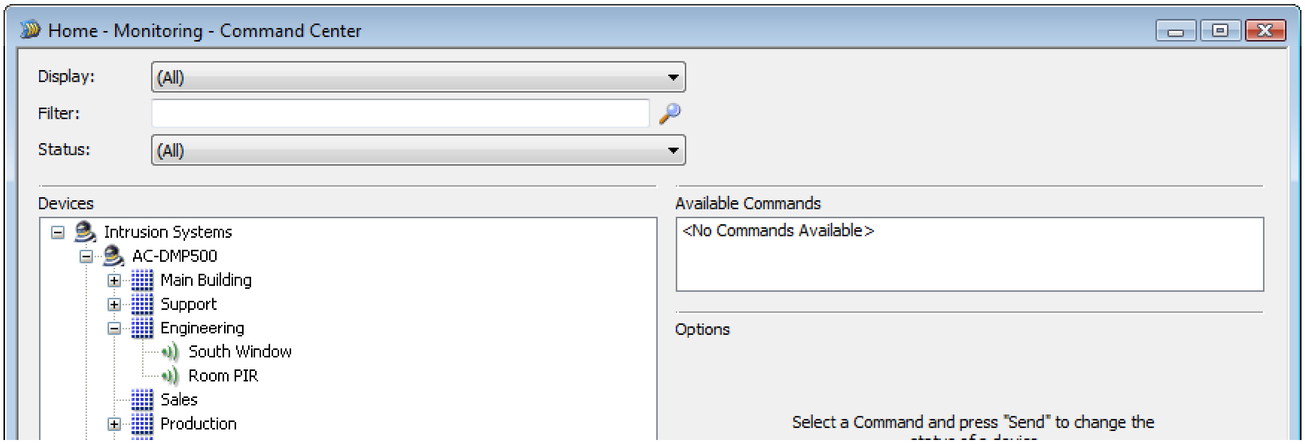
Using the Command Center

The "Home/Monitoring/Command Center" screen enables you to send commands to intrusion systems, and to view their current status. The intrusion panels, areas, zone groups, zones and outputs are listed in a tree view.

You can display the Command Center from several locations in the user interface. For example, by:

- Clicking any button in the Intrusion Status toolbar, except **Acknowledge Alarms**. In this case, the Command Center filters the intrusion areas, zones, etc. according to the button clicked. For example, clicking the **Disarmed** button causes the Command Center to display only those areas that are have a disarmed status.

- Selecting **Command Center** from "Home/Monitoring". This enables you to view all intrusion systems and their areas, zones, outputs, etc. The following shows an example of the Command Center.



Home - Monitoring - Command Center

Display: (All)

Filter:

Status: (All)

Devices

- Intrusion Systems
  - AC-DMP500
    - Main Building
    - Support
    - Engineering
      - South Window
      - Room PIR
    - Sales
    - Production

Available Commands

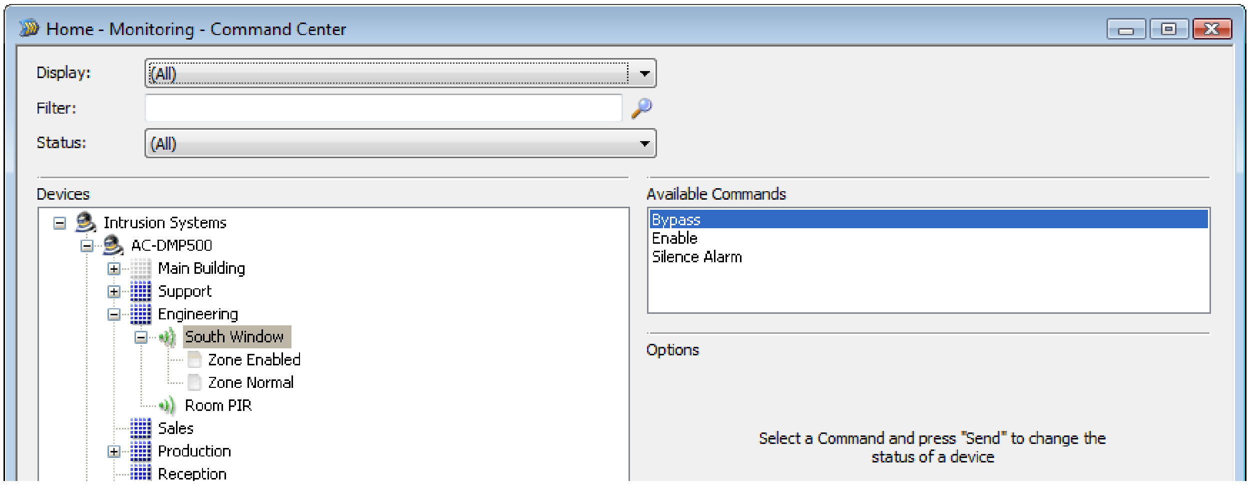
<No Commands Available>

Options

Select a Command and press "Send" to change the

Sending Commands and Viewing Status

To send a command from the Command Centre, select an area, zone group, zone or output in the tree view, choose the command and click **Send**. The list of available commands is displayed on the right-hand side of the screen. Please refer to page 34 for command details.



Home - Monitoring - Command Center

Display: (All)

Filter:

Status: (All)

Devices

- Intrusion Systems
  - AC-DMP500
    - Main Building
    - Support
    - Engineering
      - South Window
        - Zone Enabled
        - Zone Normal
      - Room PIR
    - Sales
    - Production
    - Reception

Available Commands

Bypass
Enable
Silence Alarm

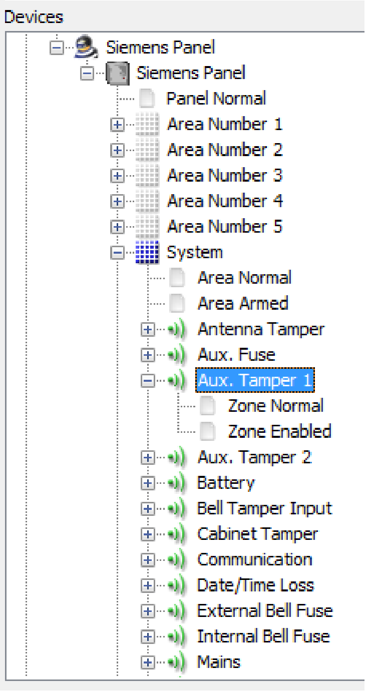
Options

Select a Command and press "Send" to change the status of a device

To view the status of intrusion devices, expand the required panel, area, zone group or zone in the tree view. In the previous example, the South Window zone is in the normal (non-alarm) state and is enabled.

Vanderbilt Panels – "System" Status Information

For Vanderbilt panels, an area named "System" is automatically included for each panel. This contains zones that allow you to determine the current status of the tampers, battery, fuses, power supply, modems, X-Bus and other items. You may need this information to determine which system alerts are active and which need to be cleared before areas can be armed. The following shows an example.



Using Intrusion Commands

You can action or configure intrusion commands using any of the following screens in the Symmetry software:

"Home/Monitoring/Command Centre" (manual commands; described in the previous section)

"Home/Monitoring/Graphics" (commands from graphics; see page 34)

"Operation/Commands/Trigger" (trigger commands)

"Operation/Commands/Scheduled" (scheduled commands)

"Operation/Commands/Predefined" (predefined commands)

"Operation/Alarms/Commands" (alarm commands)

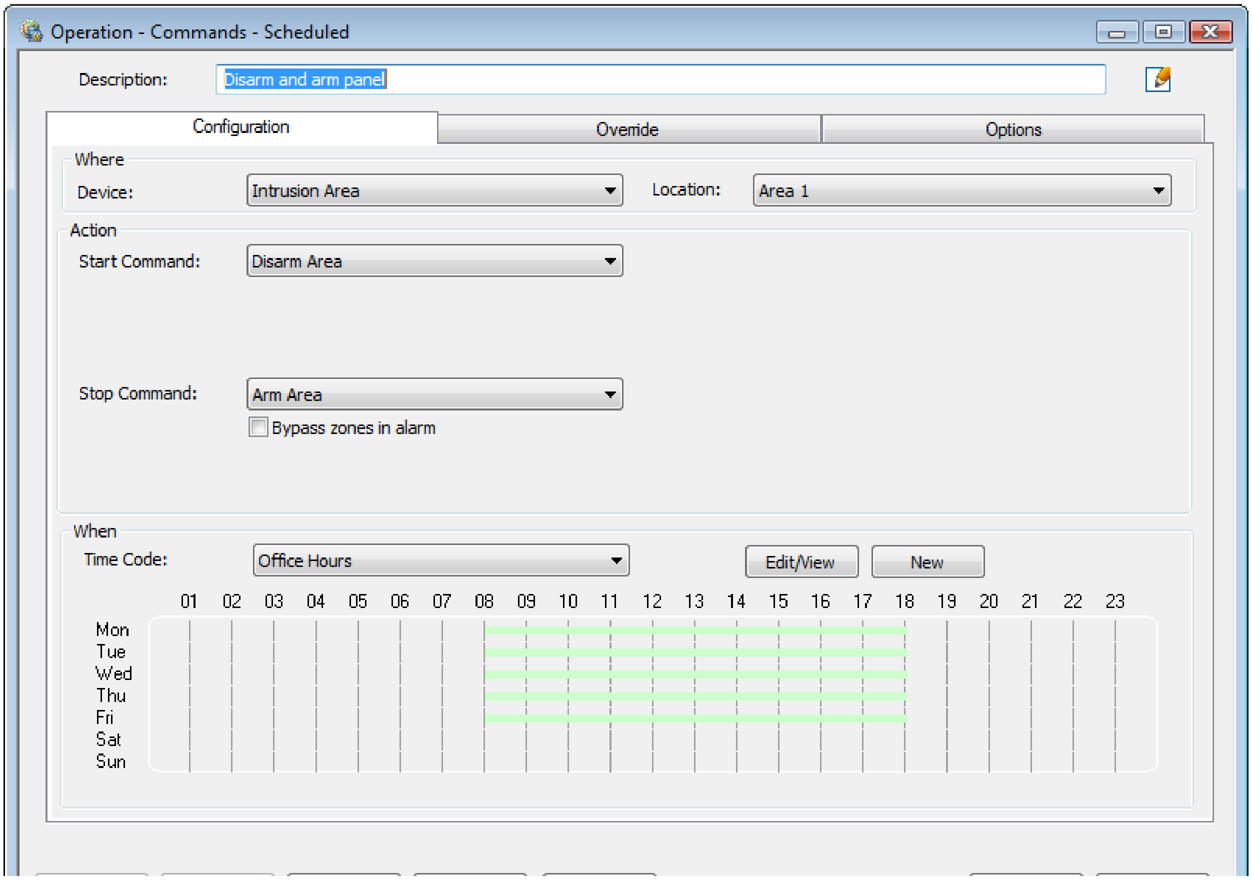
"Setup/Configuration/Threat Levels" (threat level commands)

You may, for example, want to send a command to arm an area or bypass a zone. When defining the command, select a device type of **Intrusion Area**, **Intrusion Output**, **Intrusion Panel**, I**ntrusion Zone** or **Intrusion Zone Group** as appropriate (intrusion zone groups are applicable only to CU30 and ThorGuard panels). The following sections provide examples.

Note: When setting up a trigger or alarm command, you can choose to action the command by an alarm/event from an intrusion area, panel, zone or zone group.

Scheduled Commands

The following is an example of a scheduled command set up to disarm and arm an area automatically at specified times.



Operation - Commands - Scheduled

Description: Disarm and arm panel

Where

Device: Intrusion Area

Location: Area 1

Action

Start Command: Disarm Area

Stop Command: Arm Area

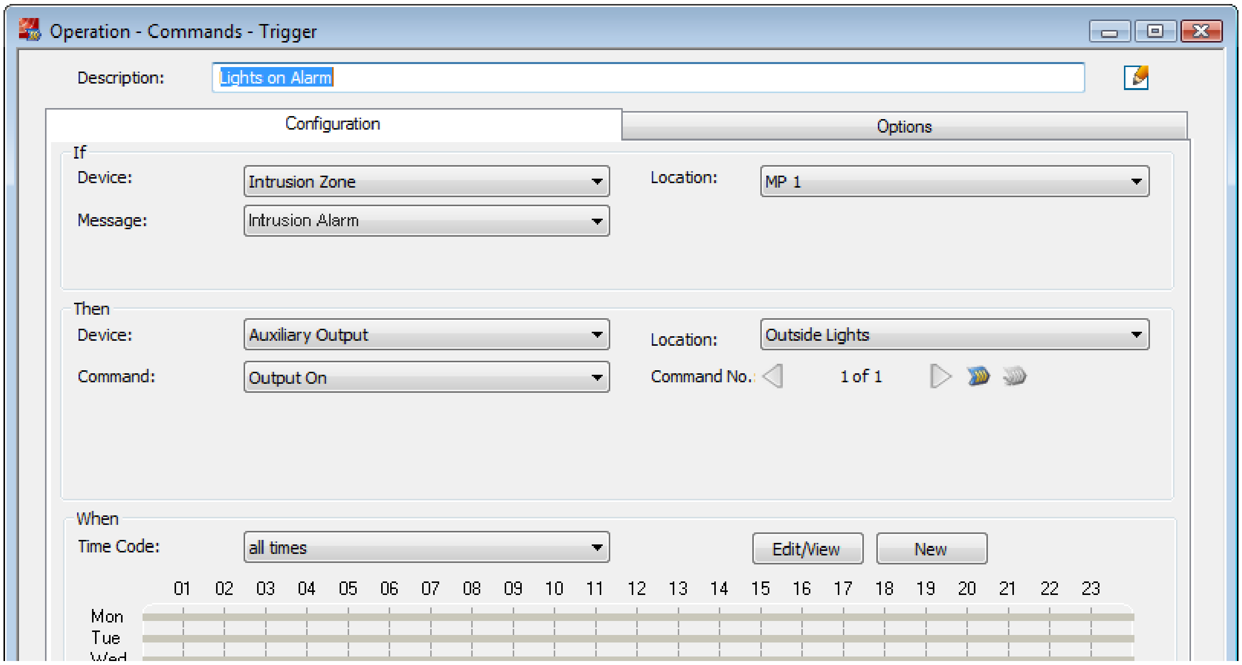
□ Bypass zones in alarm

When

Time Code: Office Hours

Trigger Commands

In the following example, a command is set up to switch on the Outside Lights. The command is triggered by an "Intrusion Alarm" from the zone named "MP 1".



Operation - Commands - Trigger

Description: Lights on Alarm

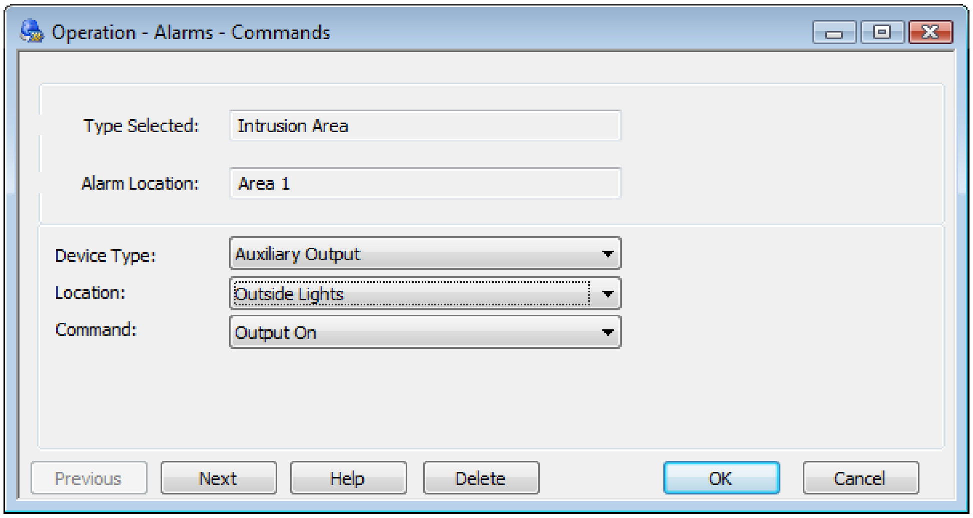
If
Device: Intrusion Zone
Message: Intrusion Alarm
Location: MP 1

Then
Device: Auxiliary Output
Command: Output On
Location: Outside Lights
Command No.: 1 of 1

When
Time Code: all times

Alarm Commands

In the following example, an alarm command has been set up for the intrusion area named "Area 1". If an alarm occurs in the area, the command enables an operator to click the **Command** button when acknowledging an alarm to switch on the Outside Lights.



Operation - Alarms - Commands

Type Selected: Intrusion Area
Alarm Location: Area 1
Device Type: Auxiliary Output
Location: Outside Lights
Command: Output On

Creating Intrusion System User Access Rights

You can assign access rights to card holders to enable them to become intrusion users. An intrusion user is a user who is able to set, unset and perform other tasks at keypads, etc. attached to the intrusion system, in the same way as if the user had been created at the intrusion panel itself.

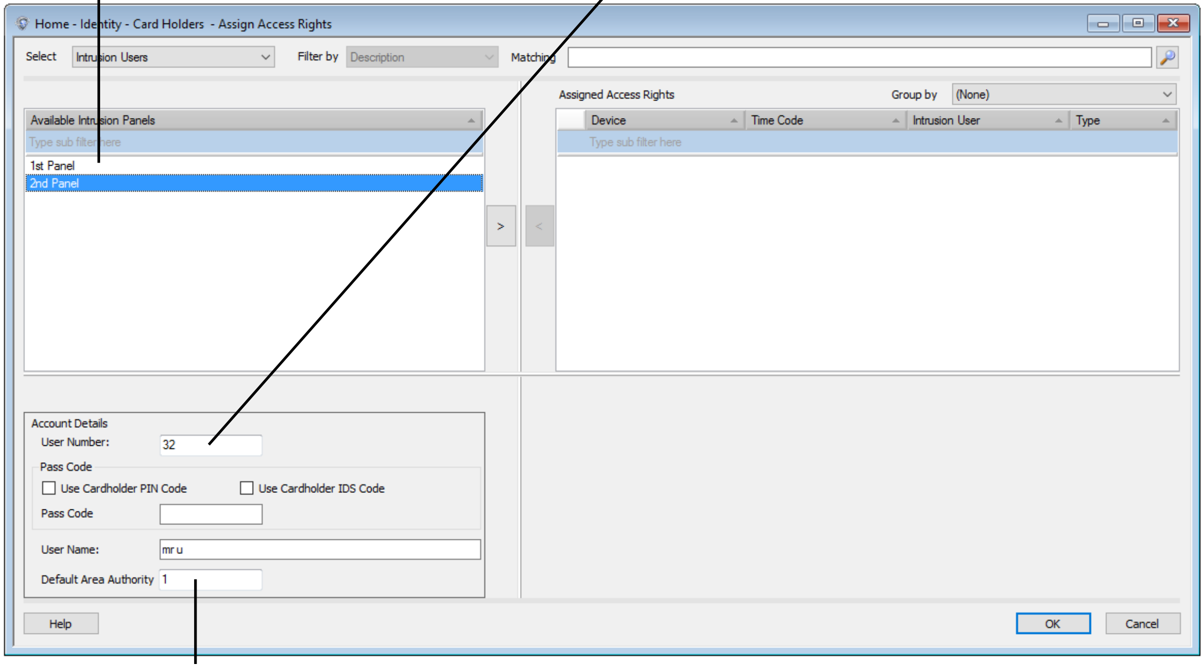
Before you assign the access rights, you need to upload user data from the intrusion panels using the "Install/Intrusion/Intrusion/Upload Configuration" screen (or the "Install/Intrusion/Intrusion/System Configuration" screen for Bosch B9512G panels). This enables Symmetry to know user data, such as the user numbers (users) already defined at the panels.

To enable a card holder to become an intrusion user, select **Intrusion System Users** in the Access Rights tab of the "Home/Identity/Card Holders" screen, click **Assign** and set up the required access rights as shown below. The data is automatically downloaded to the intrusion panels. A manual download can be carried out using the "Maintenance/Download/Intrusion Users" screen.

Permissions to be able to set up and edit intrusion system access rights (intrusion users) can be defined in the "Maintenance/User & Preferences/Roles" screen.

Select the panels you want to give the card holder access to, then click **>**.

The **User Number** is the next available unused user number at the panels. You can use this number, or specify another. If you specify an existing user number, you will be prompted whether to overwrite the existing user details at the panel(s).



Select: Intrusion Users

Group by: (None)

User Number: 32

☐ Use Cardholder PIN Code ☐ Use Cardholder IDS Code

Pass Code:

User Name: mr u

Default Area Authority: 1

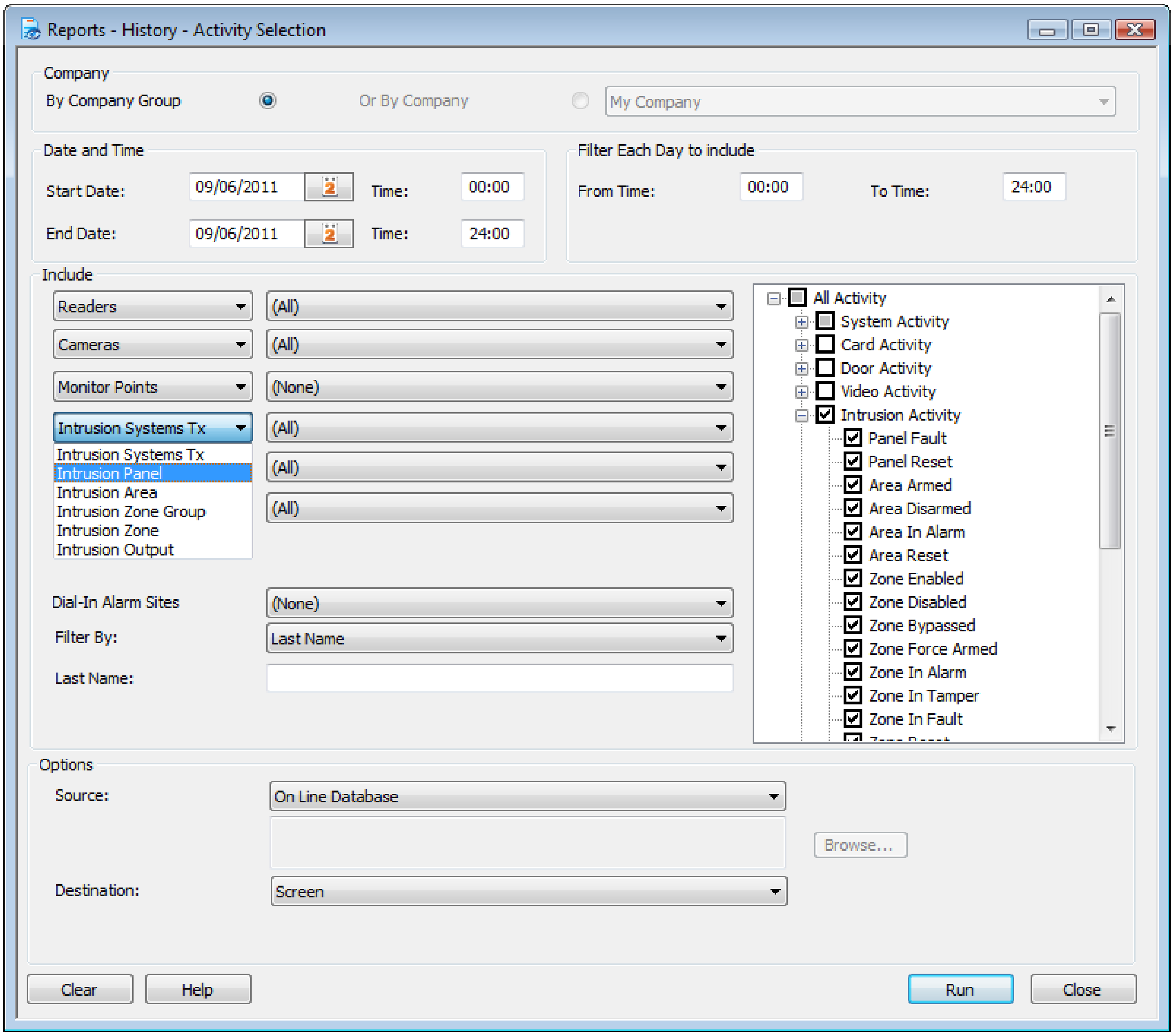
The options in this area depend on the panel you are using. Specify the **Pass Code** (or **User Code**), **User Name** and **Profile** (or **Default Area Authority**). For further information, please refer to the *Online Help*.

Note: The **Remove Users from Intrusion Panels** system preference controls what happens to user details at panels if the card holder is deleted from Symmetry, or if the access rights are removed. For further information, please refer to the *Online Help* in the "Maintenance/User & Preferences/System Preferences" screen.

Producing History Reports

History reports of intrusion alarms and events can be produced from the "Reports/History/Activity" screen by selecting **Intrusion Panel**, **Intrusion Area**, **Intrusion Zone Group**, **Intrusion Zone** or **Intrusion Output**, as indicated in the following picture. You can select **All** to include all panels, areas, zone groups, zones or outputs in the report, as applicable. Alternatively, you can choose to report on a specific item.

Select the intrusion alarms/events you want to include in the report using the checkboxes on the right-hand side of the screen.



Reports - History - Activity Selection

Company

By Company Group ● Or By Company ○ My Company

Date and Time

Start Date: 09/06/2011 Time: 00:00

End Date: 09/06/2011 Time: 24:00

Filter Each Day to include

From Time: 00:00 To Time: 24:00

Include

Readers	(All)
Cameras	(All)
Monitor Points	(None)
Intrusion Systems Tx	(All)
	(All)
	(All)

Intrusion Systems Tx
Intrusion Panel
Intrusion Area
Intrusion Zone Group
Intrusion Zone
Intrusion Output

Dial-In Alarm Sites: (None)

Filter By: Last Name

Last Name:

- □ All Activity
  - □ System Activity
  - □ Card Activity
  - □ Door Activity
  - □ Video Activity
  - ☑ Intrusion Activity
    - ☑ Panel Fault
    - ☑ Panel Reset
    - ☑ Area Armed
    - ☑ Area Disarmed
    - ☑ Area In Alarm
    - ☑ Area Reset
    - ☑ Zone Enabled
    - ☑ Zone Disabled
    - ☑ Zone Bypassed
    - ☑ Zone Force Armed
    - ☑ Zone In Alarm
    - ☑ Zone In Tamper
    - ☑ Zone In Fault
    - ☑ Zone Reset

Options

Source: On Line Database

Destination: Screen

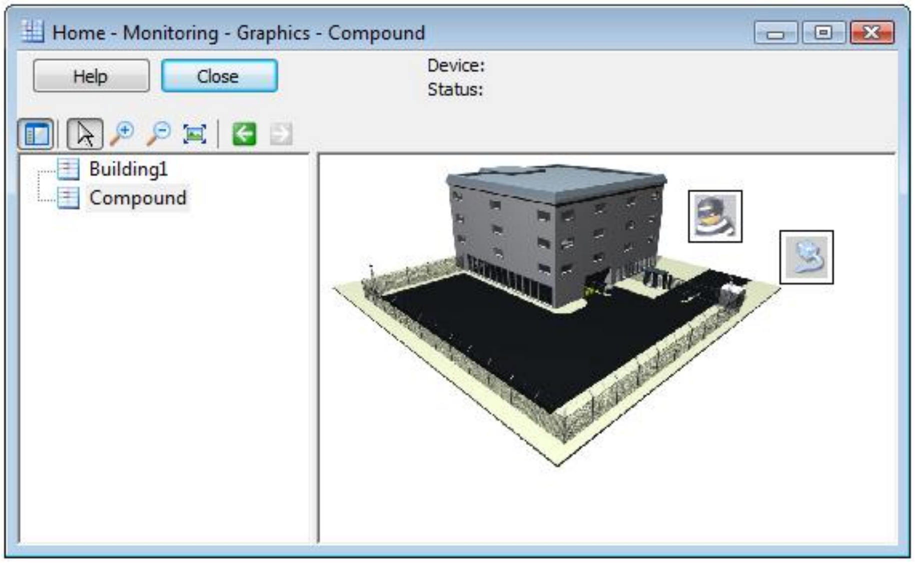
DMP XR200, DSC 4020 and DSC 4030 (SRI) Panels

Viewing Intrusion Alarms

Intrusion transaction alarms are displayed in the same way as other alarms in the following screens:

"Home/Monitoring/Alarms"
"Home/Monitoring/Graphics"
"Home/Video & Audio/Virtual Matrix"
"Reports/History/Activity"
"Reports/History/Predefined Reports/Activity"

Viewing Graphics



The "Home/Monitoring/Graphics" screen can display the icons shown in the following table, depending on how a graphic has been configured in the "Setup/Graphics/Setup" screen (page 30).

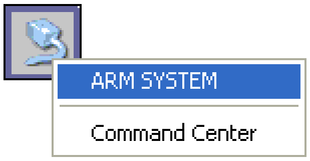
Icon Type	Icon Graphic and Right-Click Options	Purpose
Intrusion Transaction		Enables intrusion alarms to be indicated, as set up in the "Install/Intrusion/Intrusion/Device Configuration" screen (page 26).
Port (for Serial Messages)		Enables you to download serial messages (commands) to the intrusion system, if configured (page 29).

Table 4: Icons in the "Home/Monitoring/Graphics" Screen

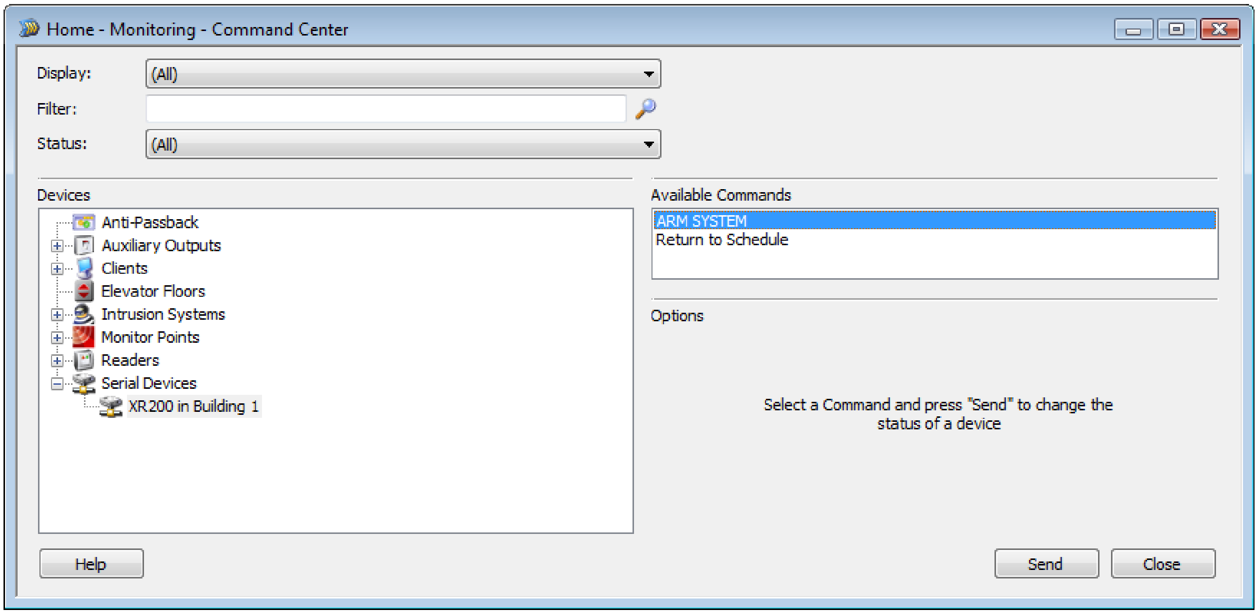
Using Commands to Send a Serial Message

If serial messages (commands) have been set up in the Install/Serial Device/Messages screen (page 30), you can use any of the following screens in the Symmetry software to send a selected command to the intrusion system:

"Home/Monitoring/Command Centre"
"Home/Monitoring/Graphics" (see page 44)
"Operation/Commands/Trigger" (trigger commands)
"Operation/Commands/Scheduled" (scheduled commands)
"Operation/Alarms/Commands" (alarm commands)
"Operation/Commands/Predefined" (predefined commands)
"Setup/Configuration/Threat Levels" (threat level commands)

When defining the command, select a device type of **Serial Device(s)**. The following sections provide examples.

Commands from the Command Center



Home - Monitoring - Command Center

Display: (All)

Filter:

Status: (All)

Available Commands: ARM SYSTEM, Return to Schedule

Select a Command and press "Send" to change the status of a device

To send a serial message from the Command Centre:

1. Select **Serial Devices** from the Display menu.

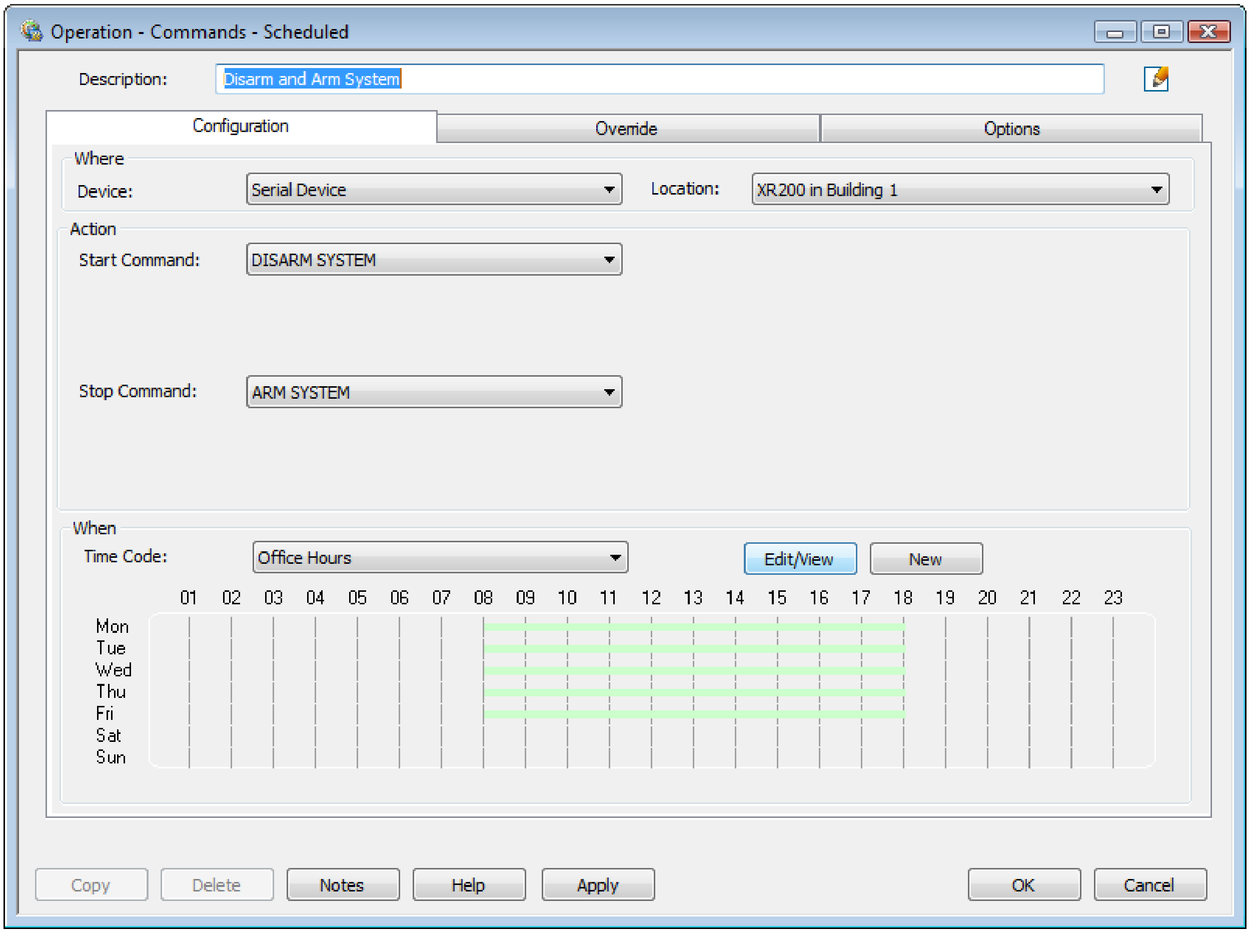
2. Select the serial device from the tree view.

3. Select the command from the right-hand side of the screen.

4. Click **Send**.

Scheduled Commands

The following is an example of a scheduled command set up to disarm and arm an area automatically at specified times.



Description: Disarm and Arm System

Where

Device: Serial Device

Location: XR200 in Building 1

Action

Start Command: DISARM SYSTEM

Stop Command: ARM SYSTEM

When

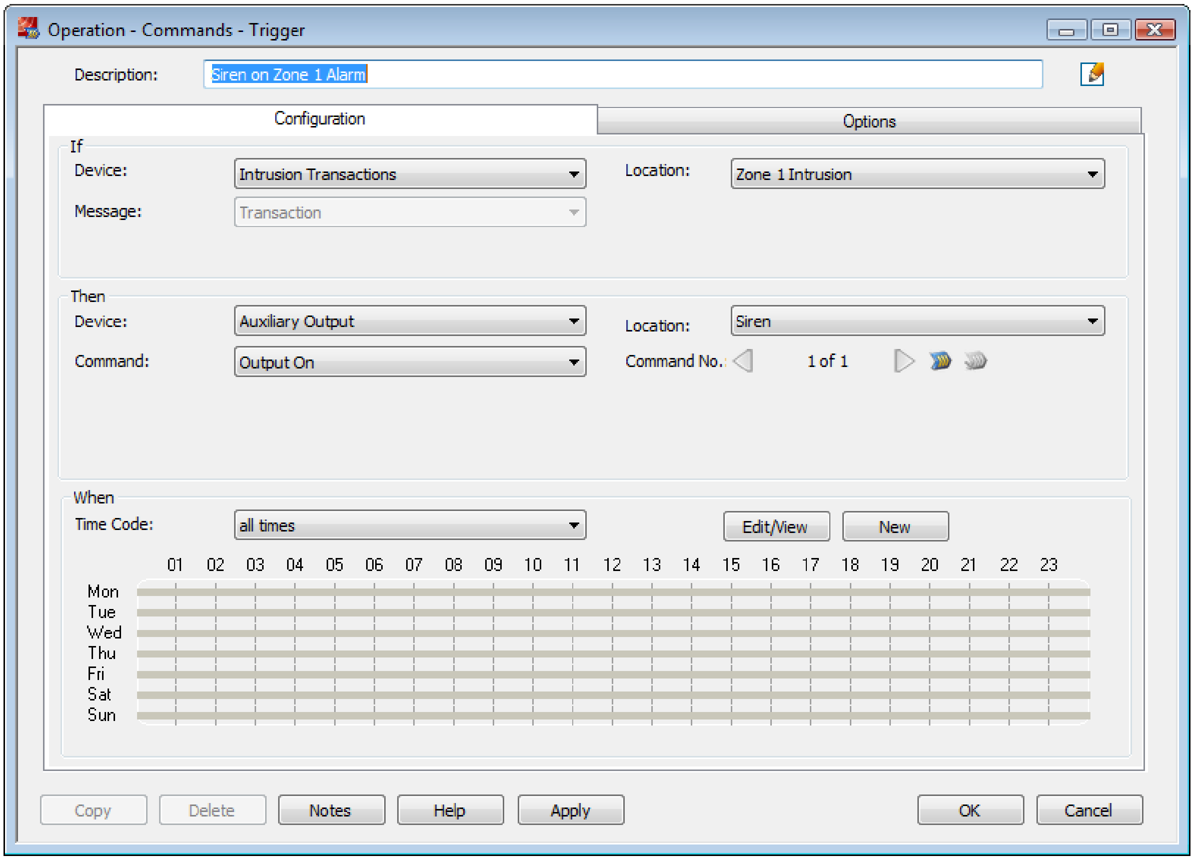
Time Code: Office Hours

Using Intrusion Transactions to Start Commands

Intrusion transactions set up in the "Install/Intrusion/Intrusion/Device Configuration" screen (page 26) can be used to start trigger and alarm commands. When defining the command, select a device/alarm type of **Intrusion Transactions**. The following provide examples.

Trigger Commands

The following example shows a trigger command that switches on a siren when an intrusion system sends a "Zone 1 Intrusion" transaction.



Operation - Commands - Trigger

Description: Siren on Zone 1 Alarm

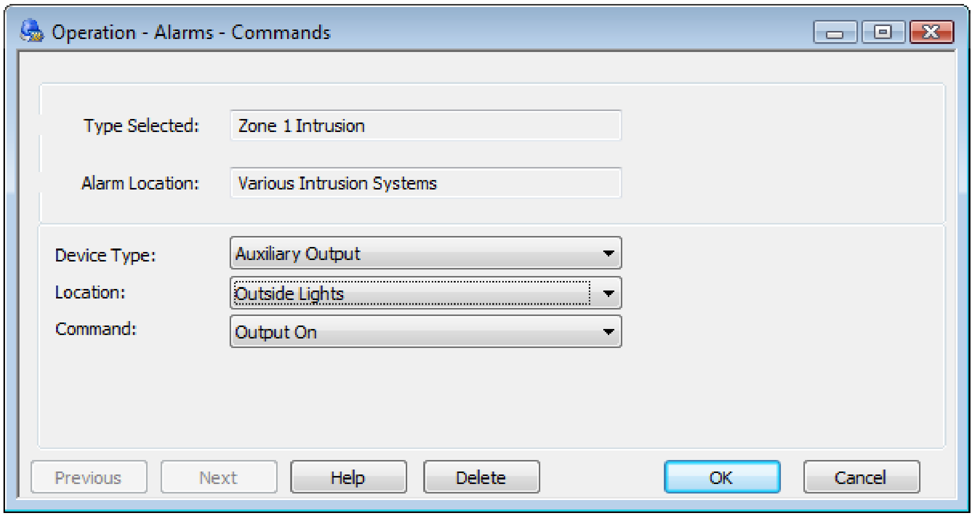
If
Device: Intrusion Transactions
Message: Transaction
Location: Zone 1 Intrusion

Then
Device: Auxiliary Output
Command: Output On
Location: Siren
Command No.: 1 of 1

When
Time Code: all times

Alarm Commands

In the following example, a command to switch on the Outside Lights has been set up for the alarm named "Full Alarm - Production". If the alarm occurs, an operator can click the **Command** button in the Acknowledge Alarms screen to switch on the Outside Lights.



Operation - Alarms - Commands

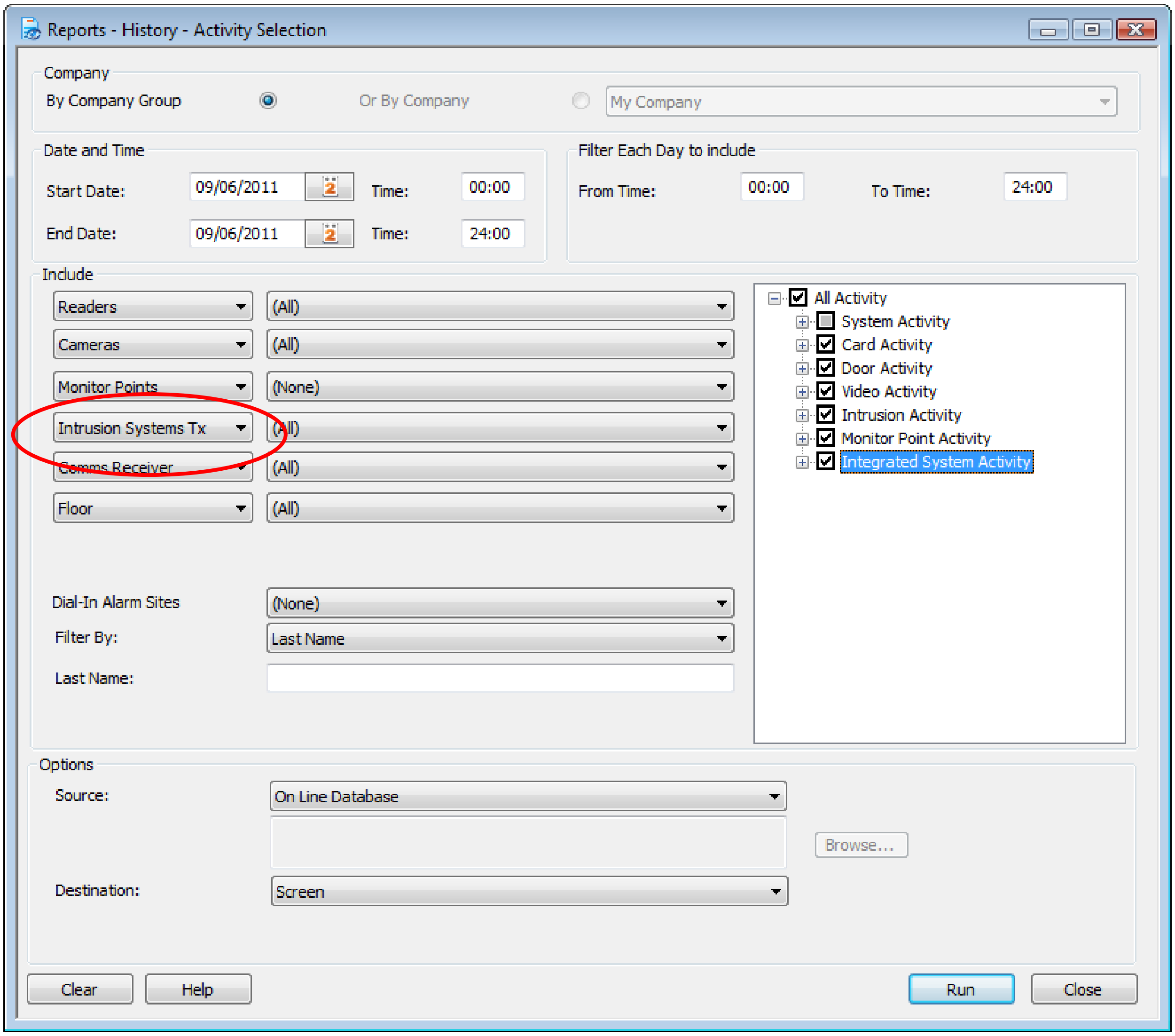
Type Selected: Zone 1 Intrusion
Alarm Location: Various Intrusion Systems

Device Type: Auxiliary Output
Location: Outside Lights
Command: Output On

Producing History Reports

History reports of intrusion alarms and events can be produced from the "Reports/History/Activity" screen by selecting **Intrusion Systems Tx**, as indicated in the following picture.

Note: The other intrusion options in the menu (**Intrusion Panel**, **Intrusion Area**, **Intrusion Zone Group**, **Intrusion Zone** and **Intrusion Output**), and the **Intrusion Activity** checkboxes on the right-hand side of the screen are not applicable to the panel you are configuring.



Reports - History - Activity Selection

Company

By Company Group ● Or By Company ○ My Company

Date and Time

Start Date: 09/06/2011 Time: 00:00

End Date: 09/06/2011 Time: 24:00

Filter Each Day to include

From Time: 00:00 To Time: 24:00

Include

Readers (All)

Cameras (All)

Monitor Points (None)

Intrusion Systems Tx (All)

Comms Receiver (All)

Floor (All)

Dial-In Alarm Sites (None)

Filter By: Last Name

Last Name:

- ☑ All Activity
  - □ System Activity
  - ☑ Card Activity
  - ☑ Door Activity
  - ☑ Video Activity
  - ☑ Intrusion Activity
  - ☑ Monitor Point Activity
  - ☑ Integrated System Activity

Options

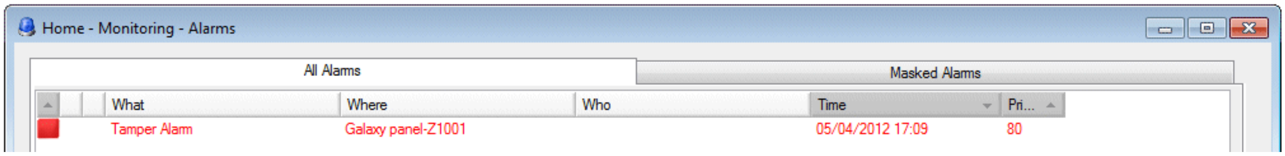
Source: On Line Database

Destination: Screen

Galaxy Dimension Panels

Viewing Intrusion Alarms

Alarms are displayed in the same way as other alarms, such as in the "Home/Monitoring/Alarms", screen:



	What	Where	Who	Time	Pri...
🟥	Tamper Alarm	Galaxy panel-Z1001		05/04/2012 17:09	80

Note: Mains fail alarms are reported only if a reset has not been received within one hour of the alarm being generated.

The following table specifies the alarms and events that can be reported by the Symmetry software for Galaxy intrusion systems.

Message	Symmetry Reporting (Alarm or Event)
A.C. Power Failure	**Alarms**
RF Interference	
RF Battery trouble	
Comms Failure	
Line Trouble	
System Battery trouble	
Area Failed to Arm	
Zone Alarm	
Fire Alarm	
Holdup Alarm	
Panic Alarm	
Medical Alarm	
Tamper Alarm	
Zone Fault	
RF Interference Restored	**Events**
RF Battery Restored	
System Battery restored	
Time/Date Changed	
Local Programming Begin	
Local Programming End	
Listen in End	
Line Restore	

Automatic test	Events (continued)
Power Up	
Auto arming	
Auto arm delay	
Area Armed	
Area Late to Arm	
Recent Arming	
Late to Disarm	
Area Disarmed	
Area Disarmed early	
Area Reset	
Walk Test Started	
Walk Test Ended	
Zone Reset	
Zone Bypassed	
Zone Unbypassed	
Fire Alarm Reset	
Holdup Alarm Reset	
Panic Alarm Reset	
Medical Alarm Reset	
Tamper Reset	
Confirmed Alarm	
Relay Closed	
Relay Opened	
Programming Denied	
Programming Success	
Engineer test	

Viewing Graphics

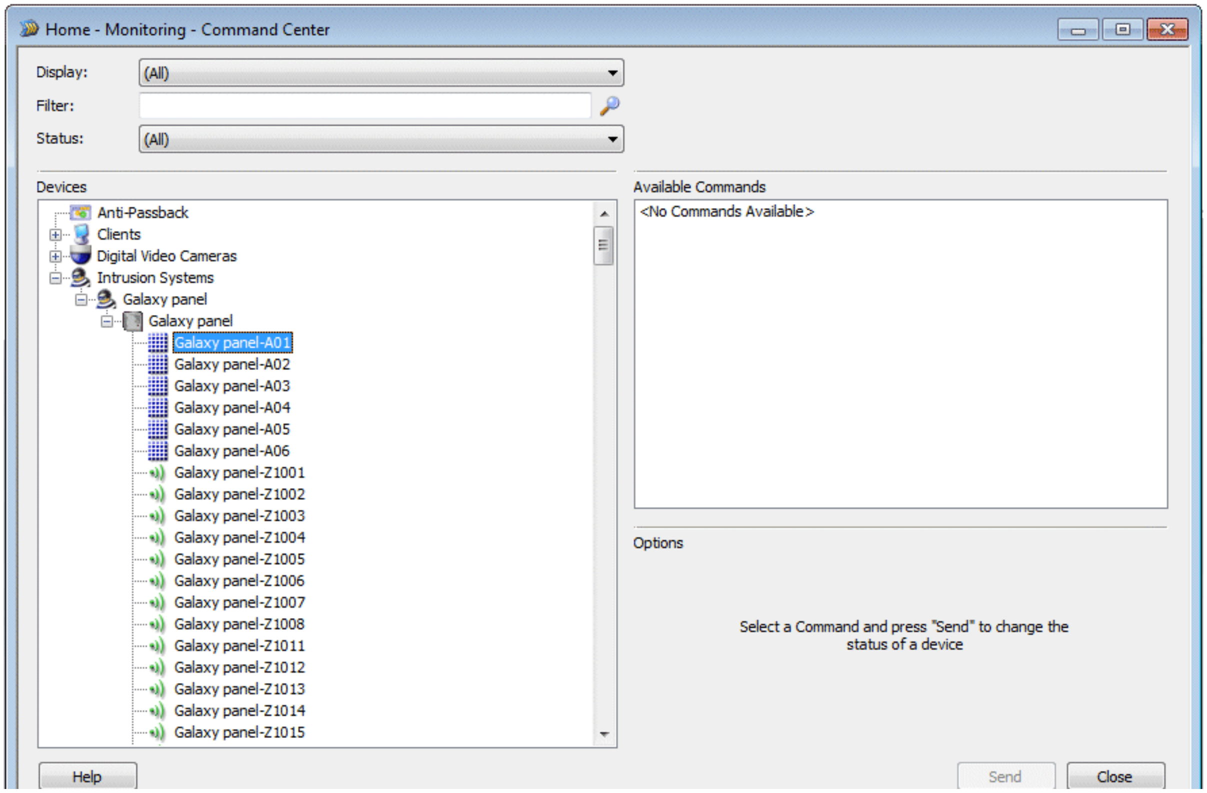
The "Home/Monitoring/Graphics" screen can display the alarm state of a Galaxy panel, area or zone. The border of the panel, area or zone icon indicates the current alarm status:

- Red (alarm is unacknowledged).
- Blue (alarm is acknowledged, but the device needs to be reset).
- Green (alarm is acknowledged but is not cleared).

Note: For Galaxy panels, the icons cannot indicate other status information.

Using the Command Center

You can use the "Home/Monitoring/Command Center" screen to display the areas and zones of a Galaxy panel in a tree view:



Home - Monitoring - Command Center

Display: (All)

Filter:

Status: (All)

Available Commands

<No Commands Available>

Select a Command and press "Send" to change the status of a device

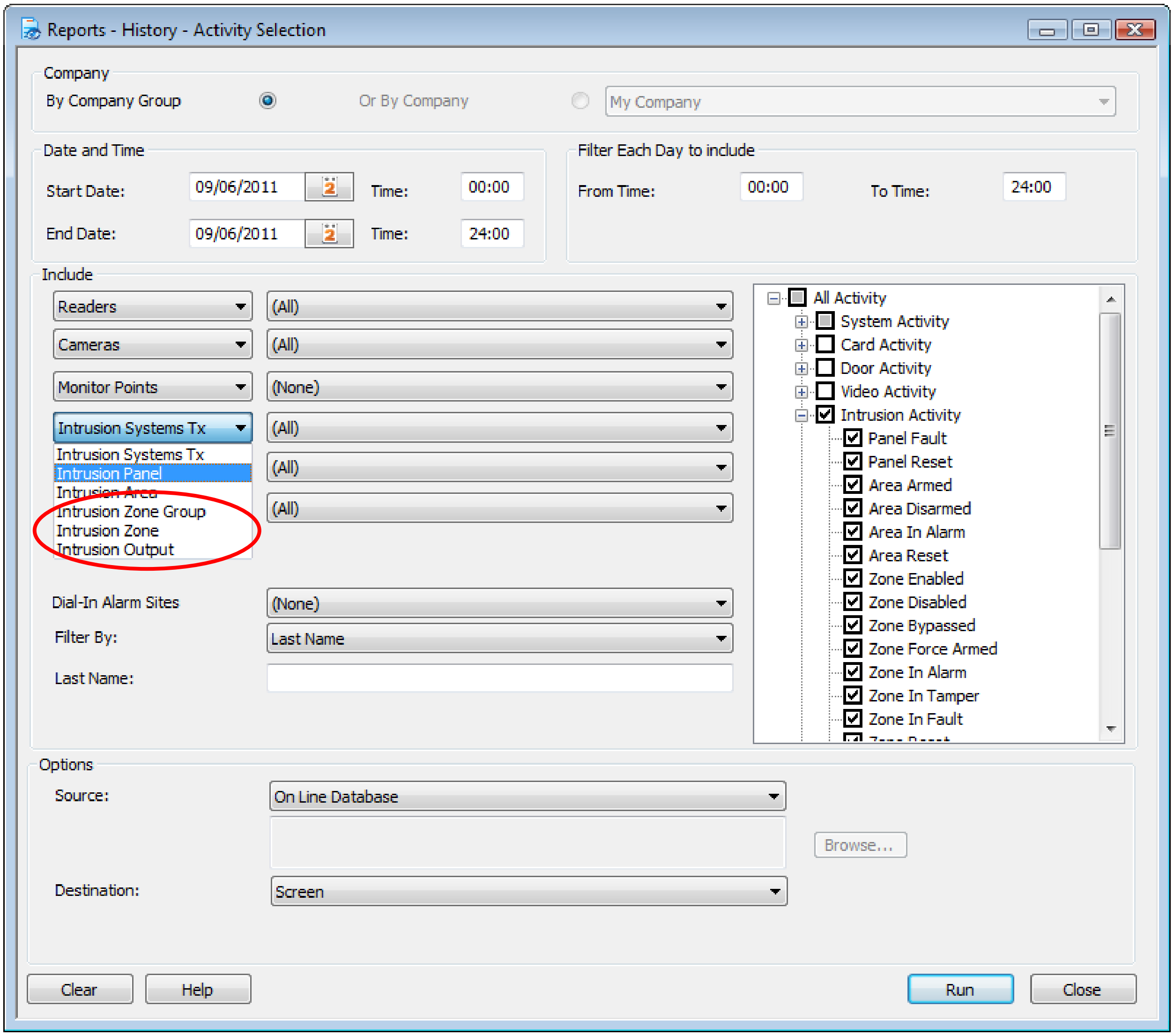
The area and zone names include the area/zone address.

The Symmetry software does not support sending of commands to Galaxy panels.

Producing History Reports

History reports of intrusion alarms and events can be produced from the "Reports/History/Activity" screen by selecting **Intrusion Panel**, **Intrusion Area**, or **Intrusion Zone**, as indicated in the following picture. You can select **All** to include all panels, areas or zones in the report, as applicable. Alternatively, you can choose to report on a specific item.

Select the intrusion alarms/events you want to include in the report using the checkboxes on the right-hand side of the screen.



Reports - History - Activity Selection

Company

By Company Group ● Or By Company ○ My Company

Date and Time

Start Date: 09/06/2011 Time: 00:00

End Date: 09/06/2011 Time: 24:00

Filter Each Day to include

From Time: 00:00 To Time: 24:00

Include

Readers	(All)
Cameras	(All)
Monitor Points	(None)
Intrusion Systems Tx	(All)
	(All)
	(All)

Intrusion Systems Tx
Intrusion Panel
Intrusion Area
Intrusion Zone Group
Intrusion Zone
Intrusion Output

Dial-In Alarm Sites: (None)

Filter By: Last Name

Last Name:

- □ All Activity
  - □ System Activity
  - □ Card Activity
  - □ Door Activity
  - □ Video Activity
  - ☑ Intrusion Activity
    - ☑ Panel Fault
    - ☑ Panel Reset
    - ☑ Area Armed
    - ☑ Area Disarmed
    - ☑ Area In Alarm
    - ☑ Area Reset
    - ☑ Zone Enabled
    - ☑ Zone Disabled
    - ☑ Zone Bypassed
    - ☑ Zone Force Armed
    - ☑ Zone In Alarm
    - ☑ Zone In Tamper
    - ☑ Zone In Fault

Options

Source: On Line Database

Destination: Screen