Intrusion Detection QuickStart

Hardware Installation and Setup

1. Install the control/communicator panel and connecting devices.
2. Set the jumpers and wire the devices.
3. Connect the Serial Interface Module for configuration and operation.
4. Configure the device. If you are using Bosch hardware, then Bosch Remote Programming Software (RPS) is needed to configure the panel.

Software Configuration

Implementation of Galaxy products and some Bosch products requires the configuration using their respective keypads as well as the configuration of OnGuard components using OnGuard software. Refer to the manufacturer manuals when configuring the panel with the keypad.

Implementation of some Bosch products requires the configuration of the Bosch components using Bosch software as well as the configuration of OnGuard components using OnGuard software. Refer to the Bosch manuals when working with Bosch software.

System Administration application - device procedures

1. Configure panel user groups.
2. Add intrusion panels.
3. Configure intrusion detection zones.
4. Configure intrusion detection onboard relays.
5. Configure intrusion detection offboard relays.
6. Configure intrusion detection doors.
7. Configure intrusion detection areas.

System Administration application - procedures to monitor alarms

1. Set up operator permissions.
2. Add intrusion devices to monitor zones.
3. Customize intrusion alarms.
4. Create instructions to display with intrusion alarms.*
5. Create pre-configured acknowledgment notes.*
6. Create intrusion detection maps.*


Operator Checklist

Monitor Intrusion Detection Devices/Alarms

Refer to the following checklist when preparing to monitor detection devices/alarms.

1. Select events to monitor (filter events).
2. Select column configuration.
3. Filter the hardware view.
4. Verify the status of areas, zones and devices.

Respond To Intrusion Detection Alarms

Refer to the following checklist when responding to intrusion detection alarms.

1. Display alarm details.
2. View live video associated with an alarm.*
3. View or listen to stored instructions for a specific alarm.*
4. Display an intrusion detection map.
5. Acknowledge an intrusion alarm.
6. Execute intrusion detection commands.
7. Send an e-mail and/or page.*
8. Print an intrusion detection report.*
9. Trace an intrusion detection device.*
10. Delete an alarm.*

Note: Procedures for * items are located in the Alarm Monitoring User Guide.
Table of Contents

Intrusion Detection QuickStart ................................................................. 3
Hardware Installation and Setup ............................................................. 3
Software Configuration ........................................................................... 3
Operator Checklist .................................................................................. 4

Introduction ............................................................................................ 9

Chapter 1: Intrusion Detection Overview .............................................. 11
Functions .................................................................................................. 11
Lenel Intrusion Detection Solutions ......................................................... 11
  Next Generation Panel (NGP) ............................................................... 11
  Guardall PX/QX/RX Panels ................................................................. 12
Types of Third-Party Intrusion Detection Panels .................................... 12
Conventions Used in this Documentation .............................................. 13

Chapter 2: Intrusion Detection Hardware .............................................. 17
Bosch DS7400Xi/DS7400XiV4 ................................................................. 17
  Serial Interface Module ....................................................................... 17
  Configure the DS7412 ....................................................................... 20
Bosch G Series Control Panels .............................................................. 21
  Configure the Control Panel ............................................................ 21
  G Series Panel Firmware ................................................................... 26
Downstream Devices .............................................................................. 27
Chapter 4: License and Permissions ....................................... 59

Licenses for Intrusion Detection ............................................................... 59
User Permissions for Alarm Monitoring ............................................................. 59
Set Permissions for Intrusion Detection ............................................................ 60

Operator Procedures .......................................................... 61

Chapter 5: Alarm Monitoring Operator Procedures ..................... 63

Intrusion Detection in Alarm Monitoring .......................................................... 63

Monitor Intrusion Detection Devices/Alarms .......................................................... 63
Respond to Intrusion Detection Alarms ............................................................... 63

Monitor Intrusion Detection Devices/Alarms Procedures ......................... 64

Select Events to Monitor (filter events) ............................................................... 64
Select Column Configuration .............................................................................. 64
Filter the Hardware View .................................................................................. 66
Verify the Status of Areas, Zones and Devices ....................................................... 66

Respond To Intrusion Detection Alarm Procedures ....................... 67

Display Alarm Details ...................................................................................... 67
Display an intrusion detection Map ........................................................................ 67
Acknowledge an Intrusion Alarm .......................................................................... 68

Intrusion Detection Command Procedures .................................................. 68

Execute Panel Commands ................................................................................. 69
Execute Zone Commands ..................................................................................... 69
Execute Area Commands ..................................................................................... 69
Onboard/Offboard Relay Commands ................................................................. 70
Execute Door Commands ..................................................................................... 71
Appendices ........................................................................................................73

Appendix A: Intrusion Detection Device Statuses  ...............75

Alarm Panel Statuses ..........................................................................................75
Zone Statuses ........................................................................................................76
Onboard and Offboard Relay Statuses .................................................................77
Door Statuses ........................................................................................................77

Appendix B: Alarm Definitions .................................................................79
Introduction
Chapter 1: Intrusion Detection Overview

OnGuard is configurable to provide intrusion detection support. Lenel provides its own intrusion detection solutions, and OnGuard also integrates with third-party intrusion panels.

OnGuard is designed to interface with intrusion controllers and to request the controllers to perform supported actions (such as bypass/unbypass zone, activate/deactivate an output and arm/disarm an area).

Functions

Intrusion detection devices perform the following functions:

• Monitor intrusion detection alarms and device status in Alarm Monitoring
• Control intrusion detection devices and send commands (e.g. arm/disarm area, control doors)
• Link intrusion alarms to Global I/O and digital video
• Report event transactions from controllers
• Support the execution of actions (for example, bypass/unbypass zone)

Lenel Intrusion Detection Solutions

Next Generation Panel (NGP)

Refer to the following documents for more information about integrating NGP with OnGuard:

• NGP Hardware Installation Guide
• System Administration User Guide
• NGP Keypad Installation Guide
• NGP Keypad Programming Reference Guide
• NGP Keypad User Guide
• Alarm Monitoring User Guide
• ID CredentialCenter User Guide
Guardall PX/QX/RX Panels

Refer to the following documents for more information about integrating the Guardall PX/QX/RX intrusion panels with OnGuard:

- System Administration User Guide

Note: The remainder of this guide provides information on integrating third-party intrusion detection panels with OnGuard.

Types of Third-Party Intrusion Detection Panels

The following third-party intrusion panels are compatible with OnGuard:

Note: If using a Bosch D9412GV3, D9412GV2, D9412G, or D9412 control panel, select “Bosch D9412G” from the Intrusion detection panel type drop-down on the System Administration > Intrusion Detection Configuration > Intrusion Panels form. Likewise, if using a Bosch D7412GV3, D7412GV2, D7412G, or D7412 control panel, select “Bosch D7412G” from the Intrusion detection panel type drop-down.

- Bosch D7412GV3/D7412GV2/D7412G/D7412
- Bosch D9412GV3/D9412GV2/D9412G/D9412
- Bosch DS7400Xi Version 3+ (formerly Detection Systems)
- Bosch DS7400Xi Version 4+ (formerly Detection Systems)
- Galaxy 128
- Galaxy 18
- Galaxy 3-144
- Galaxy 3-48
- Galaxy 3-520
- Galaxy 500
- Galaxy 504
- Galaxy 512
- Galaxy 60
- Galaxy 8
- Galaxy Dimension GD48
- Galaxy Dimension GD520
Conventions Used in this Documentation

Where a term is defined, the word is represented in *italics*.

- Field names, menus, and menu choices are shown in **bold**.
- Keyboard keys are represented in angle brackets. For example: `<Tab>`, `<Ctrl>`.

Keyboard key combinations are written in two ways:

- `<Ctrl>` + `<Z>` means hold down the first key, then press the second
- `<Alt>`, `<C>` means press the first key, then press the second

Window buttons on the screen are represented in square brackets. For example: `[OK]`, `[Cancel]`.

Throughout the documentation, flowcharts are used to illustrate processes. Each shape and line used has a distinct purpose:

<table>
<thead>
<tr>
<th>Shape or line</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Start or end of a process" /></td>
<td>Indicates the start or end of a process</td>
</tr>
<tr>
<td><img src="image" alt="Process" /></td>
<td>Indicates a process</td>
</tr>
<tr>
<td><img src="image" alt="Optional" /></td>
<td>A dotted line indicates that whatever specified within that shape is optional</td>
</tr>
<tr>
<td><img src="image" alt="Decision" /></td>
<td>Indicates that a decision is made</td>
</tr>
<tr>
<td><img src="image" alt="Feedback received" /></td>
<td>Feedback is received</td>
</tr>
</tbody>
</table>
Hardware Installation
Chapter 2: Intrusion Detection Hardware

OnGuard is integrated for intrusion detection with panels from Bosch and Galaxy.

Overview of basic communications

Follow the instructions for setting up an intrusion detection system below.

**Bosch DS7400Xi/DS7400XiV4**

The Bosch (formerly Detection Systems) DS7400Xi/DS7400XiV4 is an addressable control panel. For serial connections, the DS7412 RS-232 Serial Interface Module is used in conjunction with the control/communicator. In order to establish communication with this panel over a direct connection or LAN connection, a NULL modem cable is required.

The Intrusion Detection panel can also be configured over a LAN connection. For more information, refer to the section, OEM Devices Supported Over IP in the OEM Device Configuration Guide.

**Serial Interface Module**

The DS7412 provides the means for connecting to a serial device (such as a printer to print history events as they occur or at a later time using a keypad command). The interface also allows for direct connection to a computer for programming.
2: Intrusion Detection Hardware

DS7412 Serial Interface Module

1. Disconnect the power to the control panel by unplugging the transformer and removing the red battery lead.
   Before handling the circuit board, touch the control panel cabinet or another source of ground to discharge any static electricity that may be in your body. Failing to do so could damage the circuit board.

2. Mount the DS7412 in the control panel enclosure using the supplied clips and screws.

3. Install the program plugs and connect the wiring as shown.

   **Wiring the DS7412**

4. Re-apply power and set the panel time and date using a master PIN.

*Jumpers*

There are three jumpers on the circuit board that must be configured.

*Diagnostic LEDs*

Jumper P2 controls the diagnostic LEDs, which can be used as a troubleshooting aid. To enable the LEDs, place P2 on both pins.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPT Tx</td>
<td>Option bus transmit date to control panel</td>
</tr>
<tr>
<td>OPT Rx</td>
<td>Option bus receive data from control panel</td>
</tr>
<tr>
<td>SER Rx</td>
<td>RS-232 receive data from printer</td>
</tr>
<tr>
<td>SER Tx</td>
<td>RS-232 transmit data to printer</td>
</tr>
</tbody>
</table>

The DS7412 draws more current in this mode so P2 should not be in place under normal circumstances.
**RS-232 Cable Ground**

Some printers may cause a ground fault condition on the control panel. If this occurs, remove P3. This will disconnect the printer cable ground from the cabinet ground.

Some desktop computers can cause a ground fault even if P3 is removed. If connecting the DS7412 to a desktop PC and a ground fault occurs, use the connection only temporarily and disconnect for normal control operation.

**Option Bus Address**

Add jumper P4 if there is another device at options bus address 14. When a jumper is installed on both pins, the option bus corresponds to address 13. When the jumper is placed on only the bottom pin, it is option bus address 14.

**DB9 Socket Layout**

The DB9 socket layout is as follows:

<table>
<thead>
<tr>
<th>DS7412 9-pin connector</th>
<th>DCE 9-pin</th>
<th>DTE 9-pin</th>
<th>DCE 25-pin</th>
<th>DTE 25-pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 DCD (not used)</td>
<td>1 DCD</td>
<td>1 DCD (6)</td>
<td>8 DCD</td>
<td>8 DCD (6)</td>
</tr>
<tr>
<td>2 RxD</td>
<td>2 RxD</td>
<td>3 TxD</td>
<td>3 RxD</td>
<td>2 TxD</td>
</tr>
<tr>
<td>3 TxD</td>
<td>3 TxD</td>
<td>2 RxD</td>
<td>2 TxD</td>
<td>3 RxD</td>
</tr>
<tr>
<td>4 DTR</td>
<td>4 DTR</td>
<td>6 DSR</td>
<td>20 DTR</td>
<td>6 DSR</td>
</tr>
<tr>
<td>5 GND</td>
<td>5 GND</td>
<td>5 GND</td>
<td>7 GND</td>
<td>7 GND</td>
</tr>
<tr>
<td>6 DSR</td>
<td>6 DSR</td>
<td>4 DTR</td>
<td>6 DSR</td>
<td>20 DTR</td>
</tr>
<tr>
<td>7 RTS</td>
<td>7 RTS</td>
<td>8 CTS</td>
<td>4 RTS</td>
<td>5 CTS</td>
</tr>
<tr>
<td>8 CTS</td>
<td>8 CTS</td>
<td>7 RTS</td>
<td>5 CTS</td>
<td>4 RTS</td>
</tr>
<tr>
<td>9 RI (not used)</td>
<td>9 RI</td>
<td>22 RI</td>
<td>22 RI</td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** The DS7412 serial port is wired as a DTE device; therefore, if the printer is a DCE device (most common), a straight 9-pin to 9-pin or straight 9-pin to 25-pin cable may be used. If the printer is wired as a DTE device, a null modem 9-pin to 9-pin or a null modem 9-pin to 25-pin cable is required. Refer to the user guide provided with your printer for proper wiring requirements.

If you are using a non-standard printer configuration, you must make a custom cable using the table above.
Connections shown in **bold** are the minimum required connections when using XON/XOFF software flow control. If using the configuration, these are the only connections needed.

Connections in (parentheses) are optional.

---

### Configure the DS7412

The DS7412 serial interface module must be configured using the keypad connected to the DS7400Xi/DS7400XiV4.

**RS-232 Interface Control and Configuration**

If you are using the DS7400Xi

1. Enter programmers’ mode. The default programmers code is 9876. Enter this code followed by [#], [0].
2. Enter the program address 0206.
3. For data digit 1, enter [1].
4. For data digit 2, enter [0] followed by [#].
5. Enter the program address 0207.
7. For data digit 2, enter [5] followed by [#].
8. To exit programmers’ mode, press and hold the [*] key for a few seconds.

**Note:** For the DS7400Xi, the minimum firmware version is 3.09.

If you are using the DS7400XiV4

1. Enter programmers’ mode. The default programmers code is 9876. Enter this code followed by [#], [0].
2. Enter the program address 4019.
3. For data digit 1, enter [1].
4. For data digit 2, enter [0] followed by [#].
5. Enter the program address 4020.
7. For data digit 2, enter [5] followed by [#].
8. To exit programmers’ mode, press and hold the [*] key for a few seconds.

**Note:** For the DS7400XiV4, the minimum firmware version is 4.03.
Whenever the Bosch intrusion detection panel is online with the communication server and configured to report alarms to a central station, communication to the DS7412 serial interface device will cease until the dialing and event reporting to the central station has completed. This only happens in the case of alarm or panic report events sent to the central station. In addition, for any other events configured to report to a central station, such as open/close, when the panel is online with the communication server via the serial interface, these events will not cause the connection to drop. However, these events will not be reported to the central station immediately either. These events will only be reported to the central station once the communication session (with the communication server) has ended.

Bosch G Series Control Panels

Bosch G Series control panels (D9412GV3, D9412GV2, D9412G, D9412, D7412GV3, D7412GV2, D7412G, D7412) can be used for intrusion detection. To install the Bosch control panel and its components, refer to the product user guides.

The D8125 Addressable Expansion Module:
• provides point identification for initiating devices.
• supervises wiring to devices to ensure circuit integrity.
• is used to expand the control panel beyond its standard number of onboard initiating zones or points.

Connect the D8125 module to the Zonex ports. The D8125 is powered by the control panel.

The D8129 Octo-relay Module provides eight programmable Form-C relays. This module is also connected to the Zonex ports and powered by the control panel.

Keypads provide an alphanumeric display, and are capable of distinct fire and burglary tones. Connect the keypads to the data bus. Keypads are powered by the control panel.

Configure the Control Panel

Configuration of Bosch G Series control panels must be done using the RPS software provided by the manufacturer. Install the software using the RPS installation disc, and install the license dongle on the workstation running RPS.

Important: Do not install the RPS software on the same computer with OnGuard. Doing so might damage the computer.
In addition to RPS, one of several available Bosch interface modules is required. Refer to “Conettix DX4020 Ethernet Network Interface Module” on page 22 through “Serial Interface Module DX4010i” on page 25 for interface module information.

**Conettix DX4020 Ethernet Network Interface Module**

The DX4020 is used for bi-directional communications over ethernet networks. Use the DX4020 to establish a network connection with a compatible control panel, such as Bosch G Series control panels.

Before wiring the DX4020 to the control panel:

- Set the address to 80 for SDI automation.
  To communicate with the RPS through the network interface module, set the address to 88.

### SDI Bus Address DIP Switch Settings

<table>
<thead>
<tr>
<th>Module address</th>
<th>SDI DIP switches</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S1</td>
</tr>
<tr>
<td>80</td>
<td>ON</td>
</tr>
<tr>
<td>88</td>
<td>ON</td>
</tr>
</tbody>
</table>

**Note:** The DIP switch is on when it is in the down position. The address configuration is read only at power-up, so if a change is made, cycle power to the device.

**Wiring**

Connect the DX4020 to the Bosch control panel as follows:

<table>
<thead>
<tr>
<th>DX4020 connection</th>
<th>Panel connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>R terminal</td>
<td>POWER + (Terminal 32)</td>
</tr>
<tr>
<td>Y terminal</td>
<td>DATA A (Terminal 31)</td>
</tr>
<tr>
<td>G terminal</td>
<td>DATA B (Terminal 30)</td>
</tr>
<tr>
<td>B terminal</td>
<td>COMMON (Terminal 29)</td>
</tr>
</tbody>
</table>

Connect the DX4020 (RJ-45 connector) to the network.

**IP Programming**

The DX4020 is shipped with a default IP address (DHCP, port 7700).

Before using the network interface module, you must assign a unique IP address to it. In order to do this, locate the MAC address on the label. You must also obtain an IP address from your network administrator.
Set Up a Temporary IP Address

1. Verify that there is at least one entry in the ARP table. To do so, at the command prompt, type
   
   ```
   arp -g
   ```
   and press <Enter>.
   
   • If there are no entries other than the local machine, ping another machine (which must be a host other than the machine on which you are working) on the network to build the ARP table.

2. Use the ARP command to configure the IP address. Type
   
   ```
   arp -s [IP Address] [Ethernet/Hardware Address]
   ```
   and press <Enter>
   
   where the IP address is a numerical address and the Ethernet/Hardware Address is the MAC address found on the label attached to the DX4020.

3. Verify that the address was added to the table by typing
   
   ```
   arp -g
   ```

   The ARP command is used only to temporarily associate the IP address with the MAC address. To permanently assign the IP address, telnet to the device and set it in the server configuration.

Assign the IP Address

1. At the command prompt, telnet to port 1. Type
   
   ```
   telnet [IP Address] 1
   ```
   This first attempt at telnetting will fail.

2. Telnet to port 9999. Type
   
   ```
   telnet [IP Address] 9999
   ```
   This second attempt at telnetting will be successful.

3. Press <Enter> to go into setup mode.

4. Select 0 for Server Configuration.
   
   a. Configure the IP address of the DX4020. This is the same IP address used for the Intrusion Panel in System Administration
   
   b. If a gateway IP address is needed, select Y and enter the information. This is only needed when using a WAN. In a LAN, the gateway is not necessary and only needs to be changed if the gateway IP of the PC is different than that of the DX4020 host.
   
   c. If the netmask needs to be changed from the default, enter the number of bits that correspond to the netmask the network is using. Refer to the PC9133TTL-E Installation Guide for the available values.
   
   d. You may change the telnet configuration password. Select N to leave this at the default setting.

5. Select 1 for Channel 1 Configuration. Configure the serial port parameters.
   
   a. Set the baud rate to 9600.
   
   b. Set the interface mode (I/F Mode) to 4C (binary 0100 1100). This setting provides RS-232C, 8-bit, no parity, 1 stop bit.
   
   c. Set the flow control to 00 (no flow control).
d. Set the port number to 3001. The default port number is 7700. This must be changed to 3001.

e. Set the connect mode to C0.

f. The remote IP address can be left at 0.0.0.0 and the remote port can be left at 0 since these are not used.

g. The disconnect mode (DisConnMode) can be either 00 or 01. This determines the behavior of the state of the LED when there is a connection.

h. Set the flush mode to 00.

i. Set the disconnect time (DisConnTime) to 00:00.

j. For SendChar 1 and SendChar 2, set the values to 00.

   It is recommended that you set the TCP Keepalive time to 15 seconds. It is set to 0 by default. This option specified the amount of time (during a silent connection) before attempting to check if the network device is still online. If there is no response within this time period, the connection is dropped.

7. Select 9 to save and exit.

Program the control panel following the instructions in the Program Entry Guide.

**Enable Encryption**

To enable encryption on the DX4020:

1. Select 6 for Security Settings on the main menu. By default, encryption is disabled.

2. Press <Enter> until you see the menu option, **Enable Encryption**.

3. Press <Y> for yes.

4. When prompted for **Key length, in bits**, type 128 and press <Enter>.

5. For **Change Keys**, press <Y>.

6. Enter the key that will be used for encryption. This will consist of 32 hexadecimal characters.

   **Note:** The key entered here must match the active master key that is configured for the segment where the Intrusion Panel resides. Once the encryption key has been entered, you will advance to the next menu item. Configure this as needed and then exit from the Security menu item.

7. Once all other configuration has been performed for the DX4020, select 9 to save and exit the configuration session.

Once the DX4020 has been configured for encryption, you must also make sure that the intrusion panel that will be communicating with this device is enabled for encryption via the **Use an encrypted connection** checkbox on the Encryption tab of the Intrusion Detection Configuration form. If this is not done, communications will not be established with the intrusion panel.
Serial Interface Module DX4010i

The DX4010i facilitates serial communication between OnGuard and the Bosch D9412/D7412 control panels, or the Bosch DS7400Xi/DS7400XiV4 control panels. This module replaces the following communication interface modules: D9133, D9133DC, and DS7412.

Note: In order to use this device with the DS7400Xi/DS7400XiV4, the firmware on that unit should be version 2.02 or higher.

This device connects to a workstation serial port via a null modem cable (DTE to DTE device). A 9-pin to 9-pin or 9-pin to 25-pin null modem cable is required. If connecting to a DCE device (such as an external modem), a 9-pin to 9-pin or 9-pin to 25-pin straight through cable may be used.

**Connector Wiring**

<table>
<thead>
<tr>
<th>DX4010i 9-pin DTE connector</th>
<th>DCE 9-pin</th>
<th>DTE 9-pin</th>
<th>DCE 25-pin</th>
<th>DTE 25-pin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: DCD (not used)</td>
<td>1: DCD</td>
<td>1: DCD</td>
<td>8: DCD</td>
<td>8: DCD</td>
</tr>
<tr>
<td>2: RxD</td>
<td>2: RxD</td>
<td>3: TxD</td>
<td>3: RxD</td>
<td>2: TxD</td>
</tr>
<tr>
<td>3: TxD</td>
<td>3: TxD</td>
<td>2: RxD</td>
<td>2: TxD</td>
<td>3: RxD</td>
</tr>
<tr>
<td>5: GND</td>
<td>5: GND</td>
<td>5: GND</td>
<td>7: GND</td>
<td>7: GND</td>
</tr>
<tr>
<td>7: RTS</td>
<td>7: RTS</td>
<td>8: CTS</td>
<td>4: RTS</td>
<td>5: CTS</td>
</tr>
<tr>
<td>8: CTS</td>
<td>8: CTS</td>
<td>7: RTS</td>
<td>5: CTS</td>
<td>4: RTS</td>
</tr>
</tbody>
</table>
Note: For more information, refer to the DX4010i installation instructions.

For direct and LAN connections, set the DX4010i address to 80. The control panels (D9412/D7412) must be running firmware version 6.50 or later.

To communicate with the RPS through the DX4010i serial interface module, set the address to 88 for the enhanced direct communication type.

When establishing communication with the DS7400Xi/DS7400XiV4, the address should be set to 13.

### SDI Bus Address DIP Switch Settings

<table>
<thead>
<tr>
<th>Module address</th>
<th>SDI DIP switches</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>S1</td>
</tr>
<tr>
<td>80</td>
<td>ON</td>
</tr>
<tr>
<td>88</td>
<td>ON</td>
</tr>
<tr>
<td>13</td>
<td>off</td>
</tr>
</tbody>
</table>

Note: The DIP switch is on when it is in the down position.

### G Series Panel Firmware

Bosch firmware version 7.07 or later for a G Series intrusion panel (connected to the DX4020/DX4010i interface modules) allows communication with OnGuard (5.11.216 or later) through a serial or Ethernet connection. Earlier versions of the firmware are not supported. The following software is also required:

- Bosch RPS software version 5.7 or later
- D1260 keypad firmware version 1.04 or later
- DX4020/DX4010 firmware version 2.23 or later

To ensure reliable communications, verify that the following lines are under the [Radionics] section of the ACS.INI file on the computer running the Communication Server. If they are not, then add them.

```
[Radionics]
LanTimeoutseconds=4
ReadTotalTimeoutConstant=4000
```

All settings in OnGuard and RPS are the same for the D9412GV3/D7412GV3, D9412GV2/D7412GV2, and the D9412G/D7412G.
**Downstream Devices**

For any additional downstream devices supported, refer to the product user guide for wiring and configuration.
Galaxy Intrusion Controllers

The following Galaxy controllers are supported:

- Galaxy 8
- Galaxy 18
- Galaxy 60
- Galaxy 128
- Galaxy 500
- Galaxy 504
- Galaxy 512
- Galaxy 3 Series (3-520, 3-144, and 3-48)
- Galaxy Dimension GD48
- Galaxy Dimension GD520

The minimum firmware required for Galaxy panels is version 4.39.

Notes:  
Limitation in the Galaxy panel firmware (Is not a limitation with the Galaxy 3 panels or Galaxy Dimension panels):

When communicating with the Galaxy panel via the access control software, several “COPY SITE” events will be generated and placed in the Galaxy internal event log. This makes it difficult to use the Galaxy keypad to look at past events that have occurred in the panel since the Galaxy internal event log only stores a small number of events, anywhere from 250 - 1000, based on the different panel types.

This is a limitation in the Galaxy panel firmware.

Serial Connection

The Galaxy RS232 module provides full duplex serial communication between the Galaxy control panels and PCs.

This module requires firmware version 1.20 or higher.
RS232 module PCB

- 25 Way Sub-D type RS232 Connector
- SW 2 (Tamper)
- SW 3 (Copy)
- SW 4 (Overwrite)
- LD 1
- LD 3 (Copy)
- LD 4 (Overwrite)
- IC 1
- IC 2
- IC 3
- PROM 1
- SW 1 (MEM BK)
- Link 1 (Cut to enable tamper)

DIP Switches – For information on DIP Switch settings see Pages 10 and 11
The RS-232 module must be connected to the controller on the AB data line. If using a Galaxy 128, 500, 504, 512, 3-48, 3-144, or 3-520, the RS-232 module must be connected to data line 1 for successful communications.

Also note that a keypad with address D cannot be connected to data line 1 when using the RS-232 module.

Use a null modem cable to connect to the 25-pin male connector on the back of the RS-232 module.

DIP switches 1 through 5 should be off.

**DIP switch settings**

<table>
<thead>
<tr>
<th>DIP switch</th>
<th>Setting</th>
<th>ON</th>
<th>OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>parity</td>
<td>yes</td>
<td>none</td>
</tr>
<tr>
<td>4</td>
<td>parity</td>
<td>odd</td>
<td>even</td>
</tr>
<tr>
<td>3</td>
<td>data bits</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>stop bits</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>transmission</td>
<td>printer</td>
<td>RS-232 (9PC)</td>
</tr>
</tbody>
</table>

The baud rate must be set to match that of the host machine communicating with the controller.

**Baud rate**

<table>
<thead>
<tr>
<th>Baud rate</th>
<th>DIP switch setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>1200</td>
<td>off</td>
</tr>
<tr>
<td>2400</td>
<td>off</td>
</tr>
<tr>
<td>4800</td>
<td>ON</td>
</tr>
<tr>
<td>9600</td>
<td>ON</td>
</tr>
<tr>
<td>19200</td>
<td>ON</td>
</tr>
<tr>
<td>38400</td>
<td>ON</td>
</tr>
</tbody>
</table>

Using the DIP switches, configure the following communication settings.

- Data bits: 8
- Stop bits: 1
- Parity: None
- Flow control: none
The Galaxy 3 series and Galaxy Dimension panels have an onboard RS232 serial port that can be used for serial communications. The configuration of the onboard RS232 port is all performed via the keypad.

The following settings must be used in order to communicate with a Lantronix adapter:

- Access = remote
- Parity = none
- Stop bits = 1
- Byte size = 8
- Flow control = none
- Baud rate = 1200, 2400, 4800, 9600, 19200, or 38400

Currently, OnGuard does not support 300 or 600 baud.

To configure the RS232 module and interface the Galaxy control panel with a PC, refer to the Galaxy RS232 Module Operating Instructions and the Galaxy Programming manual included with the unit for specific information regarding the configuration of the Galaxy panel.

Configure the Galaxy Panel for Serial Communications

In order to use the RS-232 module, enable Event Reporting in order to receive alarm transmissions from the Galaxy panel.

The following will vary depending on whether you are configuring a Galaxy classic panel (i.e. Galaxy 60, 128, 504, etc...) vs. a Galaxy 3 series or Galaxy Dimension panel.

1. Access engineer mode by entering 112233 at the keypad followed by the [ent] key. This must be done twice, the first entry of this PIN activates a tamper alarm and the second entry cancels the alarm and accesses engineer mode. If the menu is not currently displayed (10 = SETTING), you may have to enter the engineer PIN code (112233) once more. If using a Galaxy 3 or Galaxy Dimension panel do the following:
   a. Engineer mode is authorized by a user with access to menu option 48.1 = ACCESS Auth. Engineer.
   b. Select this option and press key [1] to enable engineer access.
   c. The keypad sequence used to enable engineer access is: User Code (12345) + [ent] + 48 + [ent] + [ent] + 1 + [ent].
d. Keypad Sequence used to access engineer mode is: Engineer code (112233) + [ent].


3. Press the [A] button until RS-232 is displayed. Then press [ent]. If using the Galaxy 3 panels, the user must either select 2 = Ext RS232 (if using an external RS232 serial interface module or 6 = Int RS232 (if using the onboard RS232 serial interface port).

4. 1 = MODE is displayed. Press ent and ensure DIRECT is selected. If it is not already selected press [1] for DIRECT communication, then Press [ent]. (If configuring a Galaxy 3 panel and option 6=Int RS232 was selected then press [2] for DIRECT.

5. Press [esc] to exit this menu.


7. If the format is not already selected and displayed, press [2] for Microtech. Press [ent].

8. At this point, all the event triggers that can be configured to report events using RS-232 communication will be displayed. If you wish to have events that occur on the controller reported to Alarm Monitoring, each of these triggers must be set to ON.
   a. Scroll through the event triggers by using the [A] key.
   b. If an event trigger is set to OFF, turn it ON by pressing [ent] followed by [1]. Press [ent] again. You can now scroll to the next event trigger.
   c. If Areas (or Groups) have been enabled for the panel, make sure that the event trigger has been enabled for each area that is configured and in use on the panel. Otherwise, it will not be reported in Alarm Monitoring.

9. Press [esc] to exit the menu, and continue to do so until you reach the 2=FORMAT menu option.


11. If an account number has not been entered, enter one now. Press [ent] when you are done. If configuring a Galaxy 3 panel do the following:
   a. If configuring a Galaxy 3 panel and option 6=Int RS232 (i.e. onboard RS232 serial port) Press [A] to get to the COMMS SET-UP menu option.
   b. Press [ent]. 1 = BAUD RATE should now be displayed.
   c. Press [ent]. The baud rate selected must be set to match that of the host machine communicating with the controller. Valid entries include 3=1200, 4=2400, 5=4800, 6=9600, 7=19200 and 8=38400. Note that this must also match the baud rate selected in the Baud Rate combo box on the Connection tab of the Intrusion Detection Configuration form from System Administration. Press [ent] when done.
   d. Press [A] to advanced to 2 = DATA BITS, Press [ent].
   e. Make sure the appropriate data bit size is selected, press [ent] when done. Valid entries include 1=5; 2=6; 3=7; 4=8.
   f. Press [A] to advanced to 3 = STOP BITS, Press [ent].
g. Make sure the appropriate number of stop bits are selected, press [ent] when done. Valid entries include 1=1 STOP BIT, 2=2 STOP BITS.

h. Press [A] to advanced to 4 = PARITY, Press [ent].

i. Make sure the appropriate parity is selected, press [ent] when done. Valid entries include 1=No Parity, 2=Odd Parity and 3 = Even Parity.

j. Press [esc] to exit the COMMS SET-UP sub-menu.

12. Press [esc] to exit this menu.

13. Press [esc] until you are back to the ENGINEER MODE.

14. Exit this mode by entering the engineer PIN code (112233), followed by [esc].

---

**Ethernet Connection for Galaxy Classic Panels**

Instead of using a direct or LAN connection, with a Lantronix adapter, you can also communicate to the panel via the Galaxy Ethernet module. Configuration for an Ethernet connection is completely separate from direct or LAN connections.

This module requires firmware version 1.00 or higher.

In order to use this method of communication, some configuration must done in the panel via the keypad. Below is a list of the steps required to communicate to the controller using the Ethernet module. Use the Galaxy control panel to configure the Ethernet module. Refer to the Galaxy User Guide for instructions on how to access the menu.

---

**Note:** This configuration must be done while in engineer mode. In order to access engineer mode, the user must enter **112233** at the keypad followed by the <ent> key. This must be done twice, the first entry of this PIN activates a tamper alarm and the second entry cancels the alarm and accesses engineer mode. If the menu is not currently displayed (10 = SETTING) you may have to enter the engineer PIN code (112233) once more.

---

1. Enter the communications menu option 56 (COMMUNICATIONON) and select **4 = Ethernet**.

2. The first option should be MODULE CONFIG. Select this option and the following items must be configured. (Some or all of this information should be provided by a network administrator.)
   - 1 = IP address: This is the unique address used to identify the Ethernet module on the network. The default is 0.0.0.0.
   - 2 = Site Name: This is a text description used to identify the Galaxy panel. By default, it is blank.
   - 3 = Gateway IP: This option must be specified for communication to other LAN segments. This address should be the IP address of the router
connected to the same LAN segment as the Ethernet module. The default is 0.0.0.0.

- 4 = Network Mask: The network mask defines the number of bits taken from the IP address that are assigned for the host section. The default is 255.255.255.000.

3. Next, configure alarm reporting. This step is required in order to have events reported in Alarm Monitoring. When using the Galaxy Ethernet module, the IP address and port number, as well as some additional settings, must be configured in the Galaxy control panel.

   Enter the COMMUNICATIONS / ETHERNET menu (56.4) and select 2 = Alarm Report. From this option, the following can be configured.

   - 1 = Format: Choices include SIA and Microtech. Select Microtech. You MUST ensure that all appropriate event triggers have been set to ON upon selecting this format. If some of the triggers are not set to ON, events belonging to this trigger will not be reported in Alarm Monitoring.

   - 2 = IP Address: (Must be 15 digits) Make sure the IP address entered is correct. This must match the IP address of the machine running the Communication Server application. The [*] key can be used to end each block of three numbers.

   - 4 = Port No.: (Default is 10002). Every TCP connection is defined by a destination IP address and port number. If the default port is not available on the workstation running the Communication Server, the following ACS.INI setting can be used to specify the port number to listen on:

     ```
     [Galaxy]
     BindingPort = XXX
     ```

     (Where XXX is the numerical value of the port for the Communication Server to listen for incoming events.)

### Ethernet Connection for Galaxy 3 Series Panels

Follow these steps to configure a Galaxy 3 panel for use with the Galaxy Ethernet module.

**Note:** The Galaxy Ethernet module is not supported for the Galaxy Dimension panels.
Use the following keypad sequence to access engineer mode is: (12345) + [ent] + 48 + [ent] + [ent] + 1 + [ent].

1. Enter the communications menu option 56 (COMMUNICATIONON) and select 4 = Ethernet.

2. The first option should be MODULE CONFIG. Select this option and the following items must be configured. (Some or all of this information should be provided by a network administrator.)
   - 1 = IP address: This is the unique address used to identify the Ethernet module on the network. The default is 0.0.0.0.
   - 2 = Site Name: This is a text description used to identify the Galaxy panel. By default, it is blank.
   - 3 = Gateway IP: This option must be specified for communication to other LAN segments. This address should be the IP address of the router connected to the same LAN segment as the Ethernet module. The default is 0.0.0.0.
   - 4 = Network Mask: The network mask defines the number of bits taken from the IP address that are assigned for the host section. The default is 255.255.255.000.

   Press [esc] to exit the MODULE CONFIG sub-menu.

3. Next, configure alarm reporting. This step is required in order to have events reported in Alarm Monitoring. When using the Galaxy Ethernet module, the IP address and port number, as well as some additional settings, must be configured in the Galaxy control panel. Enter the COMMUNICATIONS / ETHERNET menu (56.4) and select 2 = Alarm Report. From this option, the following can be configured.

4. “Select 1 = Format.” Choices include SIA and Microtech. Select Microtech. You MUST ensure that all appropriate event triggers have been set to ON upon selecting this format. If some of the triggers are not set to ON, events belonging to this trigger will not be reported in Alarm Monitoring.

5. “Select 2 = Primary IP.” Press [ent]. The Primary IP defines the receiver destination details for the primary alarm transmission path. The Communication Server will be treated as the receiver destination. If groups are enabled the information programmed for the primary IP and port numbers is automatically copied to all groups.

6. Enter the IP address of the workstation running the Communication Server, this will be treated as the primary receiver. The IP address will be in the format XXX.XXX.XXX.XXX. The dot separator will be automatically added after each sequence of three numbers or can be manually added by pressing the * key. To save the address and return to the previous menu level press [ent].

7. Configure the port number by pressing [ent] at 2 = PORT NO.

8. Press [esc] to exit the PRIMARY IP sub-menu.


---

**Note:** The Galaxy 3 panels support alarm signaling to more than one receiver destination. If this is desired the same configuration noted above can also be configured using either menu options 2 = SECONDARY IP or 6 = ALARM.
MON. Any of these alarm transmission paths may be used; however, OnGuard will only utilize one of these alarm transmission paths. Also note that the panel treats the Primary IP alarm signaling path with the highest priority.

10. Select “4 = Port No.” (Default is 10002). Every TCP connection is defined by a destination IP address and port number. If the default port is not available on the workstation running the Communication Server, the following ACS.INI setting can be used to specify the port number to listen on:

   [Galaxy]
   BindingPort = XXX
   (Where XXX is the numerical value of the port for the Communication Server to listen for incoming events.)

11. Skip menu options 5, 6 and 7. these are not required and/or not supported.

12. Configure the Protocol by pressing [ent] at 8 = PROTOCOL. It is important to ensure that this option is configured to 1=TCP. If 2=UDP is selected, OnGuard will not receive alarms transmitted from the panel.


14. 1 = ACCESS PERIOD should be displayed, press [ent]. Make sure 4=ANY TIME is selected, press [ent] when done.

15. Press [A] to advance to the 2 = MODE menu and press [ent].


17. Press [esc] to exit the REMOTE ACCESS sub-menu.

18. Press [A] and skip the next few menu options (4, 5, 6, 7 and 8).

19. Press [ent] when you have arrived at 9 = ENCRYPT.

20. 1 = ALARM REPORT should be displayed, press [ent].

21. Make sure 0 = OFF is selected. If this is not selected, OnGuard will not be able to process alarm transmissions sent from the Galaxy panel. Press [ent] when done.

22. Press [esc] to exit the ENCRYPT sub-menu.

23. Press [A] to advance to the 10 = BACKUP MODULE menu and press [ent].

24. Make sure 1 = OFF is selected. OnGuard does not currently support the use of backup modules at this time. Press [ent] when done.

25. Press [esc] to exit the ETHERNET sub-menu. At this point the Ethernet module should not be configured to receive alarm transmission sent by the Galaxy panels.

**Lantronix UDS-10/UDS-100 Connection**

A NULL modem cable is required that is connected from the Galaxy RS-232 module to the UDS-10/100.
Connect to the UDS-10/100 using telnet on port 9999.

Once the telnet session has been established, you will see the following text in the window:

*** Lantronix Universal Device Server ***
Serial Number 6400191 MAC address 00:20:4A:64:00:BF
Software version 04.5 (011025)

Press <Enter> to access the Setup Mode menu.

Once in Setup Mode you will see a menu with the following options:

Change Setup : 0 Server configuration
1 Channel 1 configuration
5 Expert settings
6 Security
7 Factory defaults
8 Exit without save
9 Save and exit

At the prompt, type 1 for Channel 1 configuration and press <Enter>.

Configure the following settings:

- **Baudrate** = 1200 - 38400
  This must match the baud rate configured for the Galaxy panel. Valid range: 1200 through 38400.
- **I/F mode** = 4C
  This stands for RS-232 communication with 1 Stop bit, No parity and 8 bit data size.
- **Flow** = 0
  No flow control is used.
- **Port Number** = 3001
- **Connection Mode** = C0
- **Remote IP Address** = (000).(000).(000).(000)
- **Remote Port** = 00000
- **DisConnMode** = 00
- **FlushMode** = 00
- **DisconnectTime** = 00:00
- **Send Char 1** = 00
- **Send Char 2** = 00

Once these settings have been properly configured, type 9 at the prompt to save the changes and exit.

Exit the telnet session.
You can now communicate to the Galaxy panel using the UDS-10/100 connected to the Galaxy RS-232 module via the Communication Server.

**Galaxy Terminology**

Terminology used by Galaxy differs from that used by OnGuard. Please note the following differences.

<table>
<thead>
<tr>
<th>OnGuard term</th>
<th>Galaxy equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Areas</td>
<td>Groups</td>
</tr>
<tr>
<td>Relays</td>
<td>Outputs</td>
</tr>
<tr>
<td>Bypass</td>
<td>Omit</td>
</tr>
<tr>
<td>Unbypass</td>
<td>Unomit</td>
</tr>
<tr>
<td>Arm</td>
<td>Set</td>
</tr>
<tr>
<td>Disarm</td>
<td>Unset</td>
</tr>
<tr>
<td>Partial arm</td>
<td>Partial set</td>
</tr>
</tbody>
</table>

**Galaxy 3 and Galaxy Dimension Configuration**

Galaxy 3 and Galaxy Dimension Zone / Relay Addressing with Onboard RIO Switch:

The RIO switch (SW3, DIP switch 8) controls the ordering and availability of the onboard RIO’s. This DIP switch must be set before powering up the panel.

---

**Note:** The RIO switch is not functional on the 3-48. It defaults to the Switch off configuration.

---

A new panel option, “Onboard input /output module uses line 0 addressing,” has been added for the Galaxy 3-144 and 3-520 in the Intrusion Detection Configuration form in System Administration. This option must be set to match the Dip Switch setting on the panel (unchecked = DIP SWITCH 8 OFF, Checked = DIP SWITCH 8 ON).

**Switch off (default)**

When the switch is set to this mode, the onboard RIO’s configure to the following addresses:

Onboard RIO0: Zone address range: 1001-1008; Onboard Relays: 1001-1004

Onboard RIO1: Zone address range: 1011-1018; Onboard Relays: 1011-1014
Switch on

When the switch is set to this mode, the onboard RIO’s configure to the following addresses:

Onboard RIO0: Zone address range: 1001-1008: Onboard Relays: 1001-1004

Onboard RIO1: Zone address range: 0011-0018: Onboard Relays: 0011-0014

Please refer to the Galaxy 3 or Galaxy Dimension documentation that should have come with your panel for more information.
Configuration
Chapter 3: System Administration Configuration

Implementation of Bosch products and Galaxy products requires the configuration using their respective keypads as well as the configuration of OnGuard components using OnGuard software. Refer to the manufacturer manuals when configuring the panel with the keypad.

Implementation of Bosch products requires the configuration of the Bosch components using Bosch software as well as the configuration of OnGuard components using OnGuard software. Refer to the Bosch manuals when working with Bosch software.

OnGuard Configuration Sequence

System Administration Application - device procedures

1. Configure panel user groups.
2. Add intrusion panels.
3. Configure intrusion detection zones.
4. Configure intrusion detection onboard relays.
5. Configure intrusion detection offboard relays.
6. Configure intrusion detection doors.
7. Configure intrusion detection areas.
System Administration Application - procedures to monitor alarms

1. Set up operator permissions.
2. Add intrusion devices to monitor zones.
3. Customize intrusion alarms.
4. Create instructions to display with intrusion alarms.*
5. Create pre-configured acknowledgment notes.*
6. Create intrusion detection maps.*

Note: Procedures for * items are located in the Alarm Monitoring User Guide, System Administration User Guide or MapDesigner User Guide. These procedures are common procedures and do not change if you are configuring an intrusion detection alarm.
OnGuard Configuration Procedures

Configure Panel User Groups

The Panel User Groups link cardholders to user events.

OnGuard cardholders can be assigned to panel user groups. Each panel user group can store up to 1000 panel users. Bosch supports up to 300 panel users; Galaxy supports up to 1000 panel users.

1. From the Additional Hardware menu in System Administration, select Intrusion Detection Devices.
2. Click the Panel User Groups tab.
3. Click [Add].
4. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this panel user group will be assigned to.
   b. Click [OK].
5. In the User group name field, type a name for the panel user group.
6. In the table located on the right half of the form, double-click a panel user.

8. Specify your search criteria by typing full or partial entries in the fields.
9. Click [Next]. One of the following happens:
   • If the system locates only one cardholder record based on your search criteria, the Panel User Assignment Wizard: Summary form opens.
   • If the system locates more than one cardholder record matching your search criteria, the Panel User Assignment Wizard: Select Person window opens.
     a. Select a cardholder from the listing window.
b. Optional - Click [Personal] to display information on the selected cardholder. Click [OK] to return to the Wizard.

c. Click [Next]. The Panel User Assignment Wizard: Summary form opens.

10. Click [Finish] to make the assignment display in the summary window.

11. Repeat steps 6 - 10 for each panel user name you want to configure.

12. Click [OK].

**Add Intrusion Panels**

1. From the Additional Hardware menu in System Administration, select Intrusion Detection Devices. The Intrusion Detection Configuration folder opens.

2. On the Intrusion Panels tab, click [Add].

3. If segmentation is enabled:
   a. The Segment Membership window opens. Select the segment that this intrusion panel will be assigned to.
   b. Click [OK].

4. In the Name field, type a name for the intrusion panel.

5. Select whether the receiver is online or offline. When an intrusion panel is online, the Communication Server attempts to communicate with the device.

6. On the Location sub-tab, select the Workstation to which the intrusion panel is connected to. The Communication Server must be running on the specified workstation.

<table>
<thead>
<tr>
<th><strong>Note:</strong></th>
<th>The workstation name is obtained from Microsoft Windows by right-clicking the My Computer desktop icon and selecting Properties. The workstation name is located on the Computer Name tab.</th>
</tr>
</thead>
</table>

| **Intrusion panel names can be up to 32 characters.** |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

7. Select an intrusion panel type that is valid for the installed software license.

8. Click the Connection sub-tab.

9. Select the method that will be used to communicate with the intrusion panel.
   • Select the Direct radio button if communication with the intrusion panel will be via a direct serial connection to the specified Workstation. You must also specify the workstation’s COM port and Baud rate.

<table>
<thead>
<tr>
<th><strong>Important:</strong></th>
<th>Bosch panels (DS7400Xi Version 3+ and 4+) both have 2400 and 9600 baud rates, with 2400 being the default. Bosch panels (D7412 and D9412) have a</th>
</tr>
</thead>
</table>
fixed baud rate of 9600. Galaxy default baud rate is 1200 and supports baud rates of 1200, 2400, 4800, 9600, 19200, and 38400.

- Select the **LAN** radio button if communication with the intrusion panel will be over a Local Area Network. You must also specify the panel or Lantronics IP address.

10. Click the **Options** sub-tab.

11. Select the **Panel user group** assigned to the panel. The panel user group is used to map the user ID in the panel to a cardholder. For more information please refer to Configure Panel User Groups on page 45.

12. **Bosch only** - require the Agency and Pass code. These fields are automatically populated with default values when you click [OK]. It is recommended you use the default values.

   **Galaxy** is capable of a Pass code but it is not required. If the panel has been configured with a pass code then the pass code entered must matched the pass code in the panel in order to communicate with the panel. Configure the Galaxy panel pass code using the Ademco Galaxy Gold software application.

   **Galaxy 3-144, 3-520, and Dimension GD520 only**: Check or uncheck the **Onboard input/output module uses line 0 addressing** check box. This much match the Dip Switch 8 setting on the panel. Unchecked, this option equals DIP Switch 8 is off. Checked, the option equals DIP Switch 8 = on.

   - If the **Onboard input/output module uses line 0 addressing** check box is not checked then a number of zones, onboard relays, and offboard relays will be non-configurable.

**Note:** The agency and pass code are five digit hexadecimal codes (similar to a login ID) used by the LS Communication server. For Galaxy panels the pass code can include any characters and be 24 characters long.

13. Click [OK].

**Enter Notes for a Panel**

1. In the listing window, select the entry you want to edit.
2. Click [Modify].
3. Type the information in the Notes field. This note will be able to be displayed in Alarm Monitoring.
4. Click [OK].
Configure Intrusion Detection Zones

A zone is an input to a panel and is sometimes referred to as a point (e.g. smoke detector or motion detector).

The number of zones you can configure per panel depends on the panel type. Refer to the following table.

<table>
<thead>
<tr>
<th>Zones per panel</th>
<th>Panel type</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>Bosch DS7400Xi Version 3+</td>
</tr>
<tr>
<td>248</td>
<td>Bosch DS7400Xi Version 4+</td>
</tr>
<tr>
<td>75</td>
<td>Bosch D7412</td>
</tr>
<tr>
<td>246</td>
<td>Bosch D9412</td>
</tr>
<tr>
<td>8</td>
<td>Galaxy 8</td>
</tr>
<tr>
<td>18</td>
<td>Galaxy 18</td>
</tr>
<tr>
<td>48</td>
<td>Galaxy 3-48</td>
</tr>
<tr>
<td>60</td>
<td>Galaxy 60</td>
</tr>
<tr>
<td>128</td>
<td>Galaxy 128</td>
</tr>
<tr>
<td>144</td>
<td>Galaxy 3-144</td>
</tr>
<tr>
<td>504</td>
<td>Galaxy 500</td>
</tr>
<tr>
<td>512</td>
<td>Galaxy 504 and 512</td>
</tr>
<tr>
<td>520</td>
<td>Galaxy 3-520</td>
</tr>
<tr>
<td>48</td>
<td>Galaxy Dimension GD48</td>
</tr>
<tr>
<td>520</td>
<td>Galaxy Dimension GD520</td>
</tr>
</tbody>
</table>

Intrusion detection zones are configured in both Bosch software and Lenel software (OnGuard). Configuring intrusion detection zones in OnGuard allows you to view the zones in the Alarm Monitoring system hardware tree as well as view zone names (instead of the Bosch zone number) when the zone is in alarm.

1. From the Additional Hardware menu in System Administration, select Intrusion Detection Devices.
2. Click the Zones tab.
3. Select the intrusion panel that you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the Name column to activate the field. A cursor appears in the active field. Enter the name of this intrusion zone.
   b. Double-click the Enabled cell to toggle between Yes (enabled) and No (disabled). If you enable the zone, its name appears (instead of its Bosch configured number) in Alarm Monitoring when the zone is in alarm.
   c. Bosch only. Double-click the Output cell to toggle between Yes and No. Yes indicates the zone is an output zone and has hardware associated with it. No indicates the zone is an input.
Note: If the zone is an output zone then you can activate the output from Alarm Monitoring.

d. Repeat step 5 for each zone you want to configure.

6. Click [OK].

**Configure Intrusion Detection Onboard Relays**

The number of relays you can configure per panel depends on the panel type. Refer to the following table.

<table>
<thead>
<tr>
<th>Onboard relays per panel</th>
<th>Panel type</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Bosch DS7400Xi Version 3+</td>
</tr>
<tr>
<td>5</td>
<td>Bosch DS7400Xi Version 4+</td>
</tr>
<tr>
<td>3</td>
<td>Bosch D7412</td>
</tr>
<tr>
<td>3</td>
<td>Bosch D9412</td>
</tr>
<tr>
<td>6</td>
<td>Galaxy 8, 18, and 60</td>
</tr>
<tr>
<td>4</td>
<td>Galaxy 128, 500, 504, 512</td>
</tr>
<tr>
<td>8</td>
<td>Galaxy 3-48, 3-144, 3-520</td>
</tr>
<tr>
<td>8</td>
<td>Galaxy Dimension GD48</td>
</tr>
<tr>
<td>12</td>
<td>Galaxy Dimension GD520</td>
</tr>
</tbody>
</table>

Onboard relays are configured in both Bosch software and Lenel software (OnGuard). Configuring onboard relays in OnGuard allows you to view the relay
in the Alarm Monitoring system hardware tree as well as view relay names (instead of the Bosch relay number) when the onboard relay is in alarm.

1. From the **Additional Hardware** menu in System Administration, select **Intrusion Detection Devices**.
2. Click the Onboard Relays tab.
3. Select the intrusion panel you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the name of this onboard relay.
   b. Double-click the **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the relay, its name appears (instead of its Bosch configured letter) in Alarm Monitoring when the relay is in alarm.
6. Repeat step 5 for each relay that you want to configure.
7. Click [OK].

**Configure Intrusion Detection Offboard Relays**

The number of relays you can configure per panel depends on the panel type. Refer to the following table.

<table>
<thead>
<tr>
<th>Offboard relays per panel</th>
<th>Panel type</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>Bosch DS7400Xi Version 3+</td>
</tr>
<tr>
<td>16</td>
<td>Bosch DS7400Xi Version 4+</td>
</tr>
<tr>
<td>64</td>
<td>Bosch D7412</td>
</tr>
<tr>
<td>128</td>
<td>Bosch D9412</td>
</tr>
<tr>
<td>0</td>
<td>Galaxy 8</td>
</tr>
</tbody>
</table>
Offboard relays are configured in both Bosch software and Lenel software (OnGuard). Configuring offboard relays in OnGuard allows you to view the relay

<table>
<thead>
<tr>
<th>Offboard relays per panel</th>
<th>Panel type</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Galaxy 18</td>
</tr>
<tr>
<td>16</td>
<td>Galaxy 3-48</td>
</tr>
<tr>
<td>24</td>
<td>Galaxy 60</td>
</tr>
<tr>
<td>64</td>
<td>Galaxy 128</td>
</tr>
<tr>
<td>250</td>
<td>Galaxy 500, 3-144</td>
</tr>
<tr>
<td>252</td>
<td>Galaxy 504, 3-520</td>
</tr>
<tr>
<td>256</td>
<td>Galaxy 512</td>
</tr>
<tr>
<td>16</td>
<td>Galaxy Dimension GD48</td>
</tr>
<tr>
<td>252</td>
<td>Galaxy Dimension GD520</td>
</tr>
</tbody>
</table>
in the Alarm Monitoring system hardware tree as well as view relay names (instead of the Bosch relay number) when the offboard relay is in alarm.

1. From the **Additional Hardware** menu in System Administration, select **Intrusion Detection Devices**.
2. Click the Offboard Relays tab.

3. Select the intrusion panel you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the name of the offboard relay.
   b. Double-click an **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the relay, its name appears (instead of its Bosch configured letter) in Alarm Monitoring when the relay is in alarm
6. Repeat step 5 for each relay that you want to configure.
7. Click [OK].

**Configure Intrusion Detection Doors**

The following procedure applies to **Bosch devices only**. You can configure up to eight (8) doors with Bosch D9412 devices and up to two (2) doors with Bosch D7412.

**Note:** The Door Control Module (DCM) for Galaxy Dimension panels is not supported.
Intrusion detection doors are configured in both RPS software and Lenel software (OnGuard). Configuring doors in OnGuard allows you to view the door in the Alarm Monitoring system hardware tree as well as view the name of the door (instead of its Bosch number) when the door is in alarm.

1. From the Additional Hardware menu in System Administration, select Intrusion Detection Devices.
2. Click the Doors tab.
3. Select the intrusion panel you want to configure.
4. Click [Modify].
5. In the table located on the bottom half of the form:
   a. Double-click a cell in the Name column to activate the field. A cursor appears in the active field. Enter the name of the door.
   b. Double-click the Enabled cell to toggle between Yes (enabled) and No (disabled). If you enable the door, its name appears (instead of its Bosch configured number) in Alarm Monitoring when the door is in alarm.
6. Repeat step 5 for each intrusion door that you want to configure.
7. Click [OK].

**Configure Intrusion Detection Areas**

Areas can have multiple zones assigned to them. The number of configurable areas available depend on the panel type. Refer to the following table.

<table>
<thead>
<tr>
<th>Areas per panel</th>
<th>Panel type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Bosch DS7400Xi Version 3+</td>
</tr>
<tr>
<td>8</td>
<td>Bosch DS7400Xi Version 4+</td>
</tr>
</tbody>
</table>
Intrusion detection areas are configured in both Bosch software and Lenel software (OnGuard). Configuring areas in OnGuard allows you to view the area

<table>
<thead>
<tr>
<th>Areas per panel</th>
<th>Panel type</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Bosch D7412</td>
</tr>
<tr>
<td>8</td>
<td>Bosch D9412</td>
</tr>
<tr>
<td>0</td>
<td>Galaxy 8</td>
</tr>
<tr>
<td>3</td>
<td>Galaxy 18</td>
</tr>
<tr>
<td>4</td>
<td>Galaxy 60, 3-48</td>
</tr>
<tr>
<td>8</td>
<td>Galaxy 128, 3-144</td>
</tr>
<tr>
<td>16</td>
<td>Galaxy 500</td>
</tr>
<tr>
<td>32</td>
<td>Galaxy 54, 512, 3-520</td>
</tr>
<tr>
<td>8</td>
<td>Galaxy Dimension GD48</td>
</tr>
<tr>
<td>32</td>
<td>Galaxy Dimension GD520</td>
</tr>
</tbody>
</table>
in the Alarm Monitoring system hardware tree as well as view area names (instead of the Bosch area number) when the area is in alarm.

1. From the **Additional Hardware** menu in System Administration, select **Intrusion Detection Devices**.

2. Click the Areas tab.

3. Select the intrusion panel you want to configure.

4. Click [Modify].

5. In the table located on the bottom half of the form:
   - Double-click a cell in the **Name** column to activate the field. A cursor appears in the active field. Enter the name of the intrusion area. Each name can contain no more than 64 characters.
   - Double-click the **Enabled** cell to toggle between Yes (enabled) and No (disabled). If you enable the area, its name appears (instead of its Bosch configured number) in Alarm Monitoring when the area is in alarm.

6. Repeat step 5 for each intrusion area that you want to configure.

7. Click [OK].

**Add Intrusion Devices to Monitor Zones**

You can create new monitor zones for intrusion detection devices or add intrusion detection devices to existing monitor zones. The procedures below describe how to add devices to existing monitor zones. To add a new monitor
zone, refer to the Monitor Zones Folder chapter of the System Administration User Guide.

1. From the Monitoring menu in System Administration, select Monitor Zones.
2. Select the monitor zone you want to add the intrusion panel to.
3. Click [Modify]
4. Select Intrusion Panels, Intrusion Zones, Intrusion Doors, Onboard, or Offboard Relays from the Select drop-down list.
5. Select the Intrusion Device.
6. Click [Assign].
7. Click [OK].
Customize Intrusion Alarms

1. From the Monitoring menu in System Administration, select Alarms.
2. Select the Alarm Definitions tab.
3. Select the desired alarm.
4. Click [Modify].
5. Optional - Modify the name of the alarm.
6. Set the priority of the alarm.
7. Select the Display Alarm checkbox. This ensures the alarm will display in Alarm Monitoring.
8. Select any other checkboxes you want. For more information, refer to Alarm Definitions on page 79.
9. Optional - Assign a device-event linked pair to this alarm:
   a. Select the name of the device(s).
   b. Select the event you wish to link to the selected device(s).
   c. If the event you selected is parameter-based, the Event Parameters display field will appear below it. In the Event Parameters display field, select the event parameter you want to be linked with the device-event linked pair.
   d. Click [>>]. The Assigned Event(s) window will display one entry for each hardware device-event pair you selected.
10. Repeat step 9 for each additional device-event you want to assign to this alarm.
Notes:  You cannot remove any of the **Assigned Events** from default system alarms, which are included in the database at the time of installation.

You cannot remove all of an alarm’s assigned device-events (even if it’s a custom alarm). An alarm must have at least one entry in the **Assigned Events** window.

11. Click [OK].
Chapter 4: License and Permissions

Licenses for Intrusion Detection

Licenses are based, not on the type of controller, but instead the number of controllers for a given panel class. One license, SWG-1450, is issued per panel.

Important: The maximum number of devices allowed per Communication Server is 255. Past that, the maximum number of devices is limited only by the license.

User Permissions for Alarm Monitoring

The System Administrator should create a unique account for each OnGuard user. For each user, the System Administrator can also create a list of permissions, which specifies precisely which screens, fields and buttons the user can access.

With the introduction of Intrusion Detection, additional permissions are available:

• Arm areas
• Disarm areas
• Silence area alarms
• Trace areas
• Trace readers and doors
Set Permissions for Intrusion Detection

1. From the Administration menu in System Administration, select Users.
2. Click the Monitor Permission Groups tab and then the Monitor sub-tab.
3. Refer to the table below for the checkboxes you should select to enable intrusion detection user permissions.

<table>
<thead>
<tr>
<th>Checkboxes to select</th>
<th>User permission enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trace, Controllers</td>
<td>Trace an intrusion controller</td>
</tr>
<tr>
<td>Trace, Inputs and outputs</td>
<td>Trace an intrusion onboard or offboard relay and intrusion zone.</td>
</tr>
<tr>
<td>Trace, Areas</td>
<td>Trace an intrusion area</td>
</tr>
<tr>
<td>Trace, Readers and doors</td>
<td>Trace an intrusion door</td>
</tr>
</tbody>
</table>

4. Click the Control sub-tab.
5. Refer to the table below for the checkboxes you should select to enable user permissions.

<table>
<thead>
<tr>
<th>Checkboxes to select</th>
<th>User Permission enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control, Set panel clock</td>
<td>Set an intrusion controller clock</td>
</tr>
<tr>
<td>Control, Execute function lists</td>
<td>Execute a custom function on a Bosch intrusion controller</td>
</tr>
<tr>
<td>Control, Mask alarms and inputs</td>
<td>Bypass an intrusion zone</td>
</tr>
<tr>
<td>Control, Unmask alarms and inputs</td>
<td>Unbypass an intrusion zone</td>
</tr>
<tr>
<td>Control, Relay and reader outputs</td>
<td>Activate, Deactivate, or Toggle an intrusion zone output, intrusion onboard relay or intrusion off-board relay</td>
</tr>
<tr>
<td>Control, Arm areas</td>
<td>Arm an intrusion area</td>
</tr>
<tr>
<td>Control, Disarm areas</td>
<td>Disarm an intrusion area</td>
</tr>
<tr>
<td>Control, Silence area alarms</td>
<td>Silence alarms for an intrusion area</td>
</tr>
<tr>
<td>Control, Open doors</td>
<td>Pulse open an intrusion door</td>
</tr>
<tr>
<td>Control, Access modes</td>
<td>Change the door mode of an intrusion door.</td>
</tr>
</tbody>
</table>
Operator Procedures
Chapter 5: Alarm Monitoring Operator Procedures

The following procedures can be used to handle intrusion detection events in Alarm Monitoring.

Intrusion Detection in Alarm Monitoring

Monitor Intrusion Detection Devices/Alarms

Refer to the following checklist when preparing to monitor intrusion detection devices/alarms.

1. Select events to monitor (filter events).
2. Select column configuration.
3. Filter the hardware view.
4. Verify the status of areas, zones and devices.

Respond to Intrusion Detection Alarms

Refer to the following checklist when responding to intrusion detection alarm.

1. Display alarm details.
2. View live video associated with an alarm.*
3. View or listen to stored instructions for a specific alarm.*
4. Display an intrusion detection map.
5. Acknowledge an intrusion alarm.
6. Execute intrusion detection commands (change the status of intrusion detection devices).
7. Send an e-mail and/or page.*
8. Print an intrusion detection report.*
9. Trace an intrusion detection device.*
10. Delete an alarm.*

Note: Procedures for * items are located in the Alarm Monitoring User Guide. These procedures are common procedures for responding to any alarm and do not change if you are responding to an intrusion detection alarm.
Monitor Intrusion Detection Devices/Alarms Procedures

Select Events to Monitor (filter events)

You can control the types of events displayed in various Alarm Monitoring windows. Each window can display a different set of event types. For example, you may wish to display all events for Trace windows, but you may to exclude “Access Granted” alarms in the Main Alarm Monitoring window.

1. In Alarm Monitoring make the window, for which you want to choose event types, the active (topmost) window.
2. From the Configure menu select Alarm Filter. The Alarm Filter window displays.
3. By default, all event types are selected (have a checkmark). If you do not want to display a particular category of events, click that option to deselect it (remove the checkmark). Click the option again to select it.

Note: Bosch events are associated with System, Trouble, Fire, Temperature, Open/Close, Access Denied, Access Granted, Emergency and Relay/Sounder event types.

4. Click [OK] to close the Alarm Filter window.

Select Column Configuration

Additional columns have been added, to Alarm Monitoring Windows, for Intrusion Detection Devices. The new columns include a Text column and an Intrusion Area column. The Text column indicates whether there is additional text associated with the alarm (yes or blank). The Intrusion Area column indicates the name of the area associated with the alarm and is only displayed when the controller reports an area number along with the alarm.

You can rearrange the order of the columns in any window as well as add or remove columns that display. This is done independently for each type of window (e.g. the Main Alarm Monitoring, Video Verification, etc.).
If the column configuration is changed for an alarm window, this becomes the default for all the alarm windows. For example, if the column configuration is changed for a given reader trace, this will become the default configuration for all reader traces.

1. In Alarm Monitoring open the window from which you want to configure the columns displayed. Verify this window is the active (topmost) window.

2. From the **Configure** menu select **Columns**. The Column Configuration window displays.

![Column Configuration for Main Alarm Monitor](image)

3. In the **Select columns** display field, click/highlight the name of a column, then click [>>]. The column name appears in the **Columns to view** display field.

4. Arrange the column names in the order you want them to appear.
   - Click/highlight a column name in the **Columns to view** display box. Then use [Up] and [Down] to change the column's relative position.

**Note:** The order the column names appear in the **Columns to view** display field is the same order the columns will display in Alarm Monitoring.

5. Click [OK]. The window displays the new column configuration.
Filter the Hardware View

The System Hardware window displays intrusion detection devices and their device status. Operators can filter the types of devices displayed.

1. Display the System Hardware window, in Alarm Monitoring.
2. From the **Configure** menu select **System Hardware Options**. The System Hardware Options form displays.

3. Specify the types of devices to be displayed (all devices or specific devices) and how they will be viewed (tree or detailed list).

**Note:** The filter option, “Areas in alarm” is available for Bosch controllers. This support does not exist for former Detection Systems controllers.

4. If desired, select the **Lock display updates** checkbox. The Lock display updates feature prevents items from being added or deleted from the view as their status changes. For more information, refer to the System Hardware Window chapter in the Alarm Monitoring User Guide.

Verify the Status of Areas, Zones and Devices

Alarm Monitoring is the only OnGuard application that displays the status of devices. Alarm Monitoring obtains the status of a device from the Communication Server which in turn obtains device status from hardware controllers. Alarm Monitoring displays the status of a device via icons and text in the hardware and map views.

1. Display the hardware or map view, in Alarm Monitoring.
2. If necessary, select **Control > Update hardware status**.
For more information on the different status types, refer to the Intrusion Detection Device Statuses Appendix in this manual.

**Respond To Intrusion Detection Alarm Procedures**

**Display Alarm Details**

Right-click an intrusion alarm (in Alarm Monitoring) and select **Alarm Details**. Alarm Details include the following information:

- Alarm description
- Time/date associated with an alarm
- Controller associated with an alarm
- Device associated with an alarm
- Area associated with an alarm
- The user id reported from the controller as well as the cardholder name to which it is linked to (if any).
- Additional text associated with the alarm - you can right click an intrusion alarm and select **Associated Text** to view just this component of the alarm details.

**Display an intrusion detection Map**

Intrusion Detection areas, like any other anti-passback area, are configured in System Administration and can be added to any map. To view an intrusion detection area right-click an intrusion alarm and select **View Map**. If multiple maps are associated with an alarm, select a map and click [OK].

The following are intrusion detection icons that you may see on maps:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Intrusion Detection Device</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Intrusion Area</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Intrusion Door</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Intrusion Panel</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>Intrusion Zone</td>
</tr>
</tbody>
</table>
Acknowledge an Intrusion Alarm

1. Display the Alarm Acknowledgment window by double-clicking an alarm in the Main Alarm Monitoring window.

2. If the alarm has text instructions associated with it the information displays in the Instructions sub-window. To print the instructions click [Print].

3. If the alarm has voice instructions click [Audio].

4. To select pre-configured acknowledgment note(s) click [Select]. The Select Acknowledgment Notes dialog appears. Select the name of the pre-configured note and click [OK].

5. If you have permission to add notes to the alarm, type your comments in the Notes sub-window. If this is a canceling alarm, any notes carried forward from the associated initiating alarm display in the Original Notes field.

6. Click [Acknowledge] to acknowledge the alarm.
   - If this alarm type has been configured for “Require Login On Ack.” in the System Configuration software, you must first log in before this alarm can be acknowledged.
   - If this is an initiating alarm, the corresponding canceling alarm may not display until you acknowledge this alarm. Whether this happens depends upon how your system is configured.
   - Your System Administrator may have set up some types of alarms to be automatically deleted from the Main Alarm Monitoring window after you acknowledge them. If an alarm is not removed from the Main Alarm Monitoring window after you acknowledge it, you will have to delete it manually. To delete an alarm entry, refer to the Main Alarm Monitoring Window chapter in the Alarm Monitoring User Guide.

7. You can acknowledge multiple alarms without closing the Alarm Acknowledgment window. Repeat step 2 through step 6 for each alarm displayed in the Alarm Acknowledgment window. Use the navigation buttons to move through the list of alarms.

8. To close the Alarm Acknowledgment window, click [Close].

Note: For information on using the Fast/Group Acknowledge Feature, refer to the Alarm Acknowledgment Window chapter in the Alarm Monitoring User Guide.

Intrusion Detection Command Procedures

With OnGuard you can respond to an intrusion alarm by changing the status of a device. This is done by executing commands through a variety of right-click options.
Note: All the commands for intrusion devices are also available as action types through the Global I/O, Scheduler and Guard Tour. For more information, refer to the Actions appendix in the Alarm Monitoring User Guide.

Execute Panel Commands

1. Right-click an intrusion panel alarm.
2. Refer to the table below to select the appropriate command.

<table>
<thead>
<tr>
<th>Right-click option</th>
<th>Detection Systems</th>
<th>Bosch</th>
<th>Galaxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Controller Clock</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Execute Custom Functions</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Execute Zone Commands

1. Right-click an intrusion panel alarm.
2. Refer to the table below to select the appropriate command.

<table>
<thead>
<tr>
<th>Right-click option</th>
<th>Detection Systems</th>
<th>Bosch</th>
<th>Galaxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Unbypass</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Activate Zone Outputs</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Deactivate Zone Outputs</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Note: The Activate/Deactivate right-click options are dependent on the firmware in the Bosch panel.

Execute Area Commands

A new area command exists for arming/disarming areas and alarms.

1. Right-click an intrusion panel alarm.
2. Refer to the table below to select the appropriate command.

<table>
<thead>
<tr>
<th>Right-click option</th>
<th>Description</th>
<th>Detection Systems</th>
<th>Bosch</th>
<th>Galaxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter Arm</td>
<td>Arms the perimeter of an area</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Some Detection Systems panels can be used as fire panels. With this in mind using the right-click Silence Alarms option could be dangerous. System Administrators should check the local fire codes to determine who if anyone in the company should have permission to silence alarms. For more information, refer to User Permissions for Alarm Monitoring on page 59.

### Onboard/Offboard Relay Commands

1. Right-click an intrusion panel alarm.
2. Refer to the table below to select the appropriate command

<table>
<thead>
<tr>
<th>Right-click option</th>
<th>Detection Systems</th>
<th>Bosch</th>
<th>Galaxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deactivate</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Toggle an Offboard Relay Output</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Note: The Toggle an Offboard Relay Output right-click option is only available for offboard relays.

## Execute Door Commands

1. Right-click an intrusion panel alarm.
2. Refer to the table below to select the appropriate command.

<table>
<thead>
<tr>
<th>Right-click option</th>
<th>Description</th>
<th>Detection Systems</th>
<th>Bosch</th>
<th>Galaxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open door</td>
<td>Opens or cycles a door</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Change door mode</td>
<td>Door modes include:</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td><strong>Lock</strong> - locks a door and requires a proper user ID to allow access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Unlock</strong> - unlocks the door allowing free access to everyone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Secure</strong> - locks the door prohibiting access by anyone</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendices
Appendix A: Intrusion Detection Device Statuses

Alarm Panel Statuses

- Firmware Version (Bosch, Galaxy)
- Online status (Bosch, Galaxy)
- Set Controller Clock (Bosch)
- Internal Event Log Threshold Reached (Bosch)
- Internal Event Log Wrapped (Bosch)
- Point Bus Failed since it Last Reported (Bosch)
- Valid Local Access (Bosch)
- RF Receiver Trouble (Bosch)
- Failed to Call RAM (Bosch)
- User Code Tamper (Bosch)
- SDI Device is Failed (Bosch)
- Receiver Communications Has Failed (Bosch)
- AC Failure (Bosch)
- Battery is Missing (Bosch)
- Battery is Low (Bosch)
- Parameter Checksum Failed (Bosch)
- Phone Line Failed (Bosch)
- Extra RF point (Bosch) - This means an RF zone was detected by the panel at an address that should not be used. It may indicate that a point is incorrectly addressed.
- Report Failure (Bosch)
- Control Fault (Bosch)
- MPX Bus Fault (Bosch)
- Radio RX Fault (Bosch)
- AUX Power Fault (Bosch)
- Option Fault (Bosch)

Note: Other than firmware revision, the above status values are only indicated in Alarm Monitoring when they are active/apply. If a given condition is not currently in effect, nothing is indicated.
Zone Statuses

- Bypassed / Unbypassed (Bosch) - Indicates if the zone has been bypassed out of the system.
- Forced / Not Forced (Bosch) - Indicates if the zone has been forced out of the system. Implementation.
- Normal, Shorted, Open, Missing (Not Responding), Not Defined (Not Programmed).
- Normal, Open, Short Circuit, Open Circuit, Low Resistance, High Resistance, Bypassed, Alarm (unrestored), Suspended, RF (Galaxy)
- Unacknowledged / Acknowledged (Bosch) - Indicates if the alarm point is not normal and has not been acknowledged.
- Explicit Trouble (Bosch)
- Tamper (Bosch)
- Low Battery [Radio Zone] (Bosch)
- Motion Masked
- No Signal Strength [Radio Zone] (Bosch)
- Alarm (unrestored) (Bosch)
- Trouble (unrestored) (Bosch)
- Untested (Bosch)
- Day Monitor Alarm (Bosch)
- Output Latched (Bosch)
- Soak Test

Note: The above status values are only indicated in Alarm Monitoring when they are active/apply. If a given condition is not currently in effect, nothing is indicated.

Area Statuses

- Arm/Disarm (Bosch)
- Disarmed (Galaxy)
- Not In Use - (Bosch)
- Entire Partition Armed (Bosch, Galaxy)
- Perimeter Armed (Bosch)
- Master Armed (Bosch)
- Setting, Unsetting, Suspend, Partial Arm (Galaxy)
- Perimeter Instant Armed (Bosch)
• Alarm (Galaxy)
• System (Galaxy)
• PA Tamper (Galaxy)
• Tamper (Galaxy)
• Perimeter Delay (Bosch)
• Area Entry Delay (Bosch)
• Perimeter Entry Delay (Bosch)
• Area Exit Delay (Bosch)
• Perimeter Exit Delay (Bosch)
• Master Armed Instant (Bosch)
• Additional Area Status - Values will be indicated in alarm monitoring when they are active/apply. If a given condition is not currently in effect, nothing is indicated.
  – Not Ready To Arm (Bosch) - Indicates the area is not ready to be armed (perimeter or interior points are off normal)
  – Area Points Bypassed (Bosch) - Indicates if area has bypassed points.
  – Area Forced Points (Bosch) - Indicates if area has forced points.
  – Alarm Status (Bosch) - indicates if area is in alarm as well as the type of alarm (the bits are set until the alarm is acknowledged).
    – Fire
    – Non Fire
    – Fire Trouble
    – Fire Supervisory
    – Non Fire Trouble
    – Non Fire Supervisory

**Onboard and Offboard Relay Statuses**

On / Off (Bosch, Galaxy) - The status will only be indicated when the output is on/active.

**Door Statuses**

Alarm Monitoring will indicate the mode of the door as one of three mutually exclusive states: locked, unlocked, or secured. If Monitoring has not been told the mode of the door, no door mode will be indicated. This does not apply to Galaxy intrusion detection.

• Unlocked / Locked (Bosch)
• Secured / Not Secured (Bosch)
• Not Used (Bosch)
• In Learn Mode / Not in Learn Mode (Bosch) - A reader (door) is ready to accept new token data.
• In Diagnostic Mode / Not in Diagnostic Mode (Bosch)
• In SDI Failure / Not in SDI Failure (Bosch)
• Held Open / Not Held Open (Bosch)

Note: Other than unlocked, secured and not used, the above status values are only indicated in Alarm Monitoring when they are active/apply. If a given condition is not currently in effect, nothing is indicated.
Appendix B: Alarm Definitions

Refer to the following table when customizing Intrusion Detection Alarms. The Form Elements are options that you can select when customizing an alarm. For more information, refer to Customize Intrusion Alarms on page 57.

<table>
<thead>
<tr>
<th>Form Element</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm description</td>
<td>(view mode only)</td>
</tr>
<tr>
<td></td>
<td>Lists currently defined alarms and the type (alarm category) and priority of each alarm.</td>
</tr>
<tr>
<td>Name</td>
<td>Indicates the alarm’s name. This is the name that will appear in the listing window. Note that some names are paired. For example, “Door Held Open” and “Door Held Open Canceled”. These are, respectively, an initiating alarm and a canceling alarm. Some options selected on this form affect these paired alarms, as noted in this field table. You can also use this form to create custom alarms with more distinctive names.</td>
</tr>
<tr>
<td>Priority</td>
<td>Indicates a priority level for this alarm. You can choose a value from 0 to 255. The priority is highlighted in the color assigned to the value, as specified on the Priority form of this folder. You can view priority assignments and colors for alarms by clicking the Priority column heading in the alarm description field on this form. This sorts the entries in priority order.</td>
</tr>
<tr>
<td>Display Alarm</td>
<td>If selected, the alarm will be displayed on an alarm monitoring workstation when the corresponding event is triggered. If this box is not selected, alarms will not be displayed.</td>
</tr>
<tr>
<td>Must Ack.</td>
<td>If selected the alarm must be acknowledged before it can be deleted. For initiating alarms, the canceling alarm won’t display until the initiating alarm is acknowledged.</td>
</tr>
<tr>
<td>Print Alarm</td>
<td>If selected, a one-line entry automatically prints when the corresponding event is triggered. An activity printer must be configured for the monitoring workstation via the Workstations form in the System Configuration folder.</td>
</tr>
<tr>
<td>Visual Notification</td>
<td>When the alarm arrives, the Main Alarm Monitor window displays in the foreground. This feature can also be disabled in the Alarm Monitoring module.</td>
</tr>
<tr>
<td>Video Verification</td>
<td>If selected the video verify view displays upon arrival of the alarm. The video verify view is only displayed if the alarm is so configured and if the instance of the alarm deals with a reader. A video board must be configured for the monitoring workstation via the Workstations form in the System Configuration folder.</td>
</tr>
<tr>
<td>Show Cardholder</td>
<td>Select if you want to show the cardholder view for a given alarm upon arrival. If the cardholder screen is already being displayed when such an alarm comes in, it is brought to the foreground and the new cardholder associated with the alarm is searched. The cardholder screen is shown only if the alarm is so configured AND the instance of the alarm deals with a badge ID.</td>
</tr>
<tr>
<td>Must Enter Response on Ack.</td>
<td>If selected, the operator must enter an alarm response in the Notes field of the Alarm Acknowledgment window before the alarm can be acknowledged.</td>
</tr>
</tbody>
</table>
### B: Alarm Definitions

<table>
<thead>
<tr>
<th>Form Element</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don't Delete on Ack.</td>
<td>By default, an alarm is automatically deleted from the Main Alarm Monitor window upon acknowledgment. If this checkbox is selected, an acknowledged entry will be marked with a checkmark (✓), but won't be deleted automatically. The operator must manually remove it by selecting <strong>Delete</strong> from the <strong>Edit</strong> menu. It is important to note, however, that a canceling alarm will always automatically delete its corresponding initiating alarm (unless the operator deletes it first). The exception to this is an alarm for which the “Must Ack.” checkbox is selected. A canceling alarm won’t delete such a Must Ack. initiating alarm if it is unacknowledged.</td>
</tr>
<tr>
<td>Display Map on Arrival</td>
<td>If selected, when this alarm arrives, the monitoring map containing the associated device will be displayed. If the device is represented on more than one map, the first map found will be displayed. This automatic map display feature can be disabled in the Alarm Monitoring module.</td>
</tr>
<tr>
<td>Operator Can Change Response</td>
<td>If selected, the operator will be able to change the information entered in the Alarm Acknowledgment window.</td>
</tr>
<tr>
<td>Active Alarm</td>
<td>Selecting this checkbox produces the following effects in the Alarm Monitoring module:</td>
</tr>
<tr>
<td></td>
<td>This alarm, when it occurs, will be highlighted in the Main Alarm Monitor window. The color of the highlight is determined by the priority value associated with the particular alarm. Priority values are specified on this form, but the color displayed for a given value is assigned on the Priority form of this folder.</td>
</tr>
<tr>
<td></td>
<td>When this alarm occurs, animation displayed on the monitoring map for the associated device will indicate the location of the alarm. Next to the device icon, the word “Alarm” will grow to a maximum size, then the animation will pause before restarting.</td>
</tr>
<tr>
<td>Require Login On Ack.</td>
<td>If selected, the operator will be required to log in when (s)he attempts to acknowledge this alarm. The operator can log in using the same or a different user ID from that which was used at initial login. This login is used only for logging transactions related to the acknowledgment of the alarm.</td>
</tr>
<tr>
<td>Assigned Event(s)</td>
<td>Lists all event-hardware assignments for the current alarm. Each entry is preceded by an <img src="image" alt="icon" /> icon, and includes the name of the event, name of the specific hardware device and the device type.</td>
</tr>
<tr>
<td>Link Summary</td>
<td>(displays only in view mode)</td>
</tr>
<tr>
<td></td>
<td>Displays the Link Summary View window, which lists all currently defined event-hardware-alarm assignments.</td>
</tr>
<tr>
<td>Form Element</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hardware Devices</td>
<td>(displays only in modify mode)</td>
</tr>
<tr>
<td></td>
<td>Lists currently defined hardware devices by name and device type. The icon that precedes each entry indicates the device type, as follows:</td>
</tr>
<tr>
<td></td>
<td>access panel</td>
</tr>
<tr>
<td></td>
<td>alarm panel</td>
</tr>
<tr>
<td></td>
<td>alarm input or reader auxiliary input</td>
</tr>
<tr>
<td></td>
<td>alarm output or reader auxiliary output</td>
</tr>
<tr>
<td></td>
<td>reader</td>
</tr>
<tr>
<td>Access Control</td>
<td>(displays only in modify mode)</td>
</tr>
<tr>
<td>Events</td>
<td>Lists all currently defined events by name and event type. An icon precedes each entry.</td>
</tr>
<tr>
<td>Event Parameters</td>
<td>(displays only in modify mode for parameter-based events)</td>
</tr>
<tr>
<td></td>
<td>Lists all currently defined event parameters by description and parameter number. An icon precedes each entry.</td>
</tr>
<tr>
<td></td>
<td>(displays only in modify mode)</td>
</tr>
<tr>
<td></td>
<td>Assigns device-event pairs to the current alarm. The pairs are added to the Assigned Event(s) window.</td>
</tr>
<tr>
<td></td>
<td>(displays only in modify mode)</td>
</tr>
<tr>
<td></td>
<td>Removes device-event assignments from the current alarm. The pairs are removed from the Assigned Event(s) window.</td>
</tr>
<tr>
<td>Add</td>
<td>Adds a custom alarm.</td>
</tr>
<tr>
<td>Modify</td>
<td>Changes an Alarm Description entry.</td>
</tr>
<tr>
<td>Delete</td>
<td>Removes an Alarm Description entry.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays online assistance for this form.</td>
</tr>
<tr>
<td>Mode</td>
<td>In view mode, indicates the record/selection count (such as “1 of 42 selected”). In modify mode, indicates the current operation, such as “Modify Mode.”</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the Alarm Configuration folder.</td>
</tr>
</tbody>
</table>
# Index

**A**  
Add...................................................................... 55  
monitor zones ............................................... 55  
panels ........................................................... 46  
Alarm panel statuses ........................................... 75  
Alarms................................................................... 57  
acknowledge ................................................ 68  
customization options .................................. 79  
definitions .................................................... 79  
details ................................................................ 67  
display details .............................................. 67  
monitor ........................................................... 4  
respond to ..................................................... 63  
Areas  
configure ...................................................... 53  
execute commands....................................... 69  
status ............................................................ 66  
statuses ......................................................... 76  
verify statuses .............................................. 66  

**B**  
Bosch .................................................................. 17  
D7412G/D9412G configuration .................. 21  

**C**  
Column configurations ....................................... 64  
Configure ............................................................ 52  
areas ............................................................. 53  
doors ............................................................ 52  
monitor zones............................................... 55  
offboard relays............................................. 50  
onboard relays............................................... 49  
panel user groups ......................................... 45  
zones ............................................................ 48  
Customize alarms................................................ 57  

**D**  
DB9 socket layout............................................... 19  
Detection Systems  
serial interface module................................. 17  
Device status ....................................................... 66  
Devices - monitor............................................. 4  
Display  
alarm details................................................. 67  
maps.................................................................. 67  
Doors  
commands .................................................... 71  
configure ...................................................... 52  
modes ............................................................ 77  

**E**  
Ethernet connection ..................................... 33, 34  
Events- monitoring/filtering ............................... 64  

**F**  
Filter  
events ........................................................... 64  
hardware view.............................................. 66  
Functions of intrusion devices ............................ 11  

**G**  
Galaxy intrusion controllers................................. 28  
serial connection ........................................... 28  
Galaxy terminology ............................................ 38  

**H**  
Hardware  
view - filter .................................................. 66  

**I**  
Intrusion alarms .................................................. 57  
acknowledge ................................................ 68  
Intrusion detection functions .............................. 11  
Intrusion detection hardware .............................. 17  

**L**  
Licenses .............................................................. 59  

**M**  
Maps  
display.......................................................... 67  
Monitor ............................................................. 64  
alarms ........................................................... 4  
devices .......................................................... 63  
events ............................................................ 64  
Monitor zones - add ........................................... 55
Index

N
Network interface module ........................................ 22

O
Onboard and offboard relays .............................. 77
commands ................................................................ 70
configure .......................................................... 50
statuses .............................................................. 77
Operator checklist .................................................. 4
Operator procedures
  monitor devices .................................................... 63

P
Panel user groups - configure ............................... 45
Panels
  configure .......................................................... 46
  execute commands ............................................ 69
  statuses .......................................................... 75
  types of .......................................................... 12
Permissions
  control permissions ........................................... 60
  tracing permissions ........................................... 60

R
Relay statuses ..................................................... 77
Right-click options ............................................. 68
RS-232
  Cable ground ................................................... 20
  RS-232 interface ............................................... 20

S
Select
column configuration ........................................ 64
events to monitor .............................................. 64
Serial interface module
  DS7412 .......................................................... 18
  DX4010i .......................................................... 25
Set user permissions ............................................. 60
Software configuration checklist ........................... 3
Statuses
  area .............................................................. 76
door ............................................................... 77
  onboard and offboard relays ............................ 77
  panel ............................................................. 75

U
User permissions .................................................. 59

V
Verify status of areas, zones, and devices .............. 66

Z
Zones
  configure ....................................................... 48
  execute commands ........................................... 69
  status ........................................................... 66
  statuses ......................................................... 76
  verify status .................................................. 66