M2150/M4000 Intrusion Guide

9.5.3 v1

SECURITY MANAGEMENT SYSTEM

9600-0540

M2150/M4000 Intrusion Guide
(9600-0540)

Issue 9.5.3v1 – 12th March 2024
Applies to version 9.5.3 or later of the Symmetry software, until superseded by a later issue of the manual.

Contents

About this Guide

This guide explains the purpose and benefits of M2150/M4000 intrusion systems, concepts of how the system operates, and how to install, configure and use the software. This guide is intended to be of use to:

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

For additional installation and configuration information, please refer to:

- *Symmetry Software User Guide*
- *M2150 Design Guide* or the *M4000 Commissioning Guide*
- *UL1076 Compliance Guide*

This manual should be read in conjunction with the *Symmetry Online Help*.

Chapter 1: Introduction

Overview of M2150/M4000 Intrusion

The Symmetry M2150/M4000 intrusion software allows users to configure, monitor and control M2150/M4000 intrusion systems. The software is an optional feature of the Symmetry software, which provides a common framework to monitor and control all security management systems from a single user interface.

The software can be tightly integrated with access-control, digital video and other security systems supported by Symmetry to provide greater flexibility and enhanced features. For example, an access-control transaction can automatically disarm the intrusion system, or an intrusion alarm can automatically start video recordings at a selected camera.

The Symmetry M2150/M4000 intrusion software operates in conjunction with Symmetry M2150/M4000 nodes that have been upgraded with intrusion firmware. Details of the hardware configurations, options and features are given in the *M2150 Design Guide* or *M4000 Commissioning Guide*, as applicable.

The M2150/M4000 intrusion software is enabled by adding a valid intrusion license to the "Maintenance/ Licensing/System Licenses" screen in Symmetry.

Areas and Zones

An M2150/M4000 Intrusion system is organized into one or more "areas". Each area can be independently armed or disarmed from the Symmetry user interface or from a reader defined as being an arming/disarming reader. This allows different parts of the building to be armed at different times.

Each area contains one or more "zones". A zone is a sensor such as Passive Infra-Red (PIR) detector, which is defined in Symmetry as a monitor point. Zones are assigned to areas in the "Setup/Device Groups/Intrusion Areas" screen:

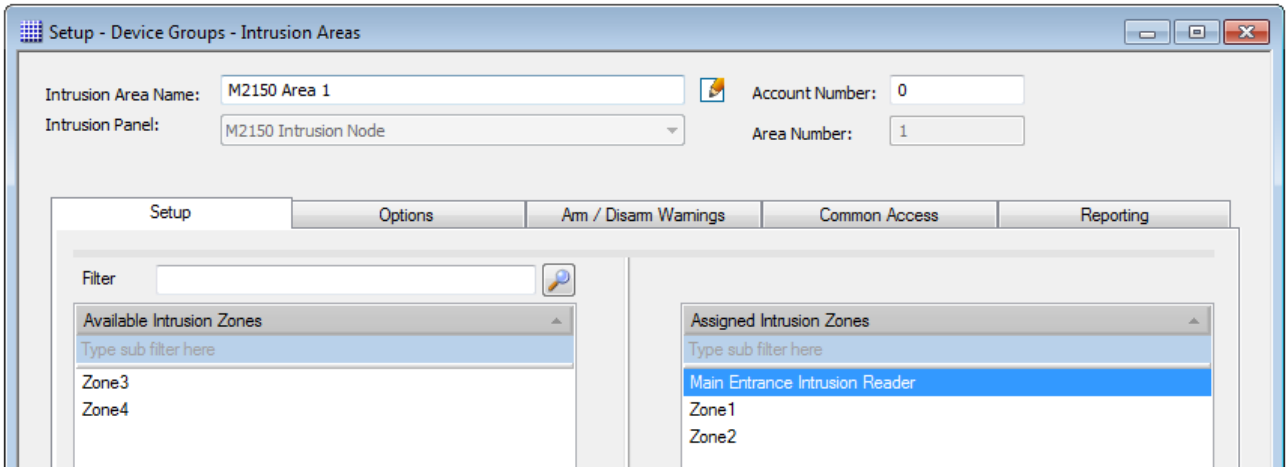


Figure 1-1: Intrusion Areas Screen

If required, zones can be defined as being on an entry/exit route. These do not cause an alarm while the entry/exit timer is running.

The termination resistor values used in zone sensors (to detect open circuit, short circuit and tamper conditions) are configurable in Symmetry (M2150) or in the web interface (M4000).

Note: Alarm sensors must not be wired in series or parallel[1]. Doing so prevents proper cable supervision and the ability to monitor the status of individual sensors.

Assigning Readers to an Area

You can assign readers, as well as zones, to areas. Assigning a reader to an area allows:

- An arming/disarming reader's sounder to operate while the area's entry or exit timer is running.
- An access-control transaction at the reader to disarm the area automatically (see Example 2 on page 8).
- The reader's door monitor to be used to start/stop the entry/exit timer. To enable this feature, the reader must be defined as being on the **Entry/Exit Route** (see Example 1 on page 7).
- The reader's door monitor to be used as a final exit sensor, so that the exit timer stops when the door is closed. To enable this feature, the reader must be defined as **Final Exit** (see Example 1 on page 7).
- You to choose whether or not to restrict all functions at the reader to the area the reader is in (see Example 5 on page 11). When **Restrict Keypad to assigned Area** is set in the "Install/Access Control/Readers" screen, a card holder is able to arm, disarm, select, change the arming time and view only the area the reader is assigned to (providing the area is also in the card holder's access rights). When the option is not set, the restriction is lifted, which means that an arming/disarming reader does not have to be assigned to an area to enable it to be used to arm or disarm that area.

Any type of reader can have **Final Exit** or **Entry/Exit Route** selected, even if it is not capable of being used as an arming/disarming reader. This allows standard access-control readers to finish the exit timer or start the entry timer.

Note: Any reader that is assigned to an area, but which is not defined as being an arming/disarming reader or on an entry/exit route is disabled once the area is armed. This allows standard access-control readers to be disabled, so that access is denied when a card holder presents a card.

Note: A card holder's area access rights determines which areas the card holder can arm/disarm.

M2150/M4000 Arming/Disarming Readers

Compatible Javelin readers allow operators to access intrusion options from the reader. Operators are able to carry out tasks such as to arm or disarm areas, view alarms and change auto-arm times. Chapter 5 starting on page 42 explains how to use the intrusion options at an S884-v2 reader, which can be used with M2150 intrusion systems. Depending on the application design, it is not necessary to have separate readers for both access control and intrusion, since a single reader can perform both tasks.

Note: For M2150 installations requiring Underwriters Laboratories (UL) UL1076 compliance, only the S844 keypad reader equipped with M2150 intrusion firmware can be used for arming and disarming functionality. See page 37 for details of S844 usage. M4000 systems are not approved by UL.

The reader must connect to the same node as the zones in the areas to be armed or disarmed. There can be more than one arming/disarming reader per node, which allows for cases where it is necessary to arm or disarm an area from different locations.

[1] An exception is in M2150 systems for door monitors that are used to finish the exit timer (reader configured as a Final Exit) or start the entry timer (reader configured as an Entry/Exit Route) when wired in a Door Loop. Door Loops have the door monitor wired in series with the exit-request switch and lock monitor, as described in the *M2150 Design Guide*.

Arming and Disarming

An area can be armed or disarmed from the Command Center in Symmetry, by scheduled commands, by trigger commands, or from arming/disarming readers using an IDS code or card (see the next section).

You can use the "Setup/Device Groups/Intrusion Areas" screen to set up alarms to occur if an area is armed or disarmed too late or early. A configurable grace period is allowed.

If a scheduled command is used to arm an area automatically at specified times, a pre-arm sounder operates to warn people to exit the area. The pre-arm period is configurable in Symmetry, and auto-arming can be delayed from an arming/disarming reader.

If required, you can choose to allow only certain Symmetry users the privileges to arm or disarm an area from Symmetry. This is achieved by selecting the **Permissions** button in the Intrusion Areas screen, and selecting the appropriate user roles.

Note: If arming/disarming reader is in view of the zone sensor, consider setting **Allow area arming with active zones on exit route** in the "Maintenance/User & Preferences/System Preferences" screen. This option allows you to start the arming sequence, even if a zone that is on the entry/exit route is active. If a zone remains active after the exit timer has expired, the affected area is not armed and an "Area Failed to Arm" alarm is generated.

Card Holders and Access Rights

To arm, disarm or perform other operations at an arming/disarming reader, each operator needs to be set up as a card holder in Symmetry using the "Home/Identity/Card Holders" screen.

The Card Holders screen allows you to specify area access rights, which determines the areas that the card holder is able to arm or disarm. Reader access rights, also set up in the Card Holders screen, are required only if the card holder needs to gain access through a door controlled by the reader.

Each card holder can have an intrusion PIN (IDS code), which can be entered at an arming/disarming reader to gain access to intrusion options, such as to arm or disarm an area. Alternatively, a card holder can present a card to access the intrusion options. The IDS code can be the same as the standard card PIN, or a different code can be used.

Monitoring and Controlling the Intrusion System

The intrusion system can be monitored and controlled from Symmetry using the Command Center, Graphics screen, Alarms screen, intrusion toolbar and other screens. The following pictures show examples.

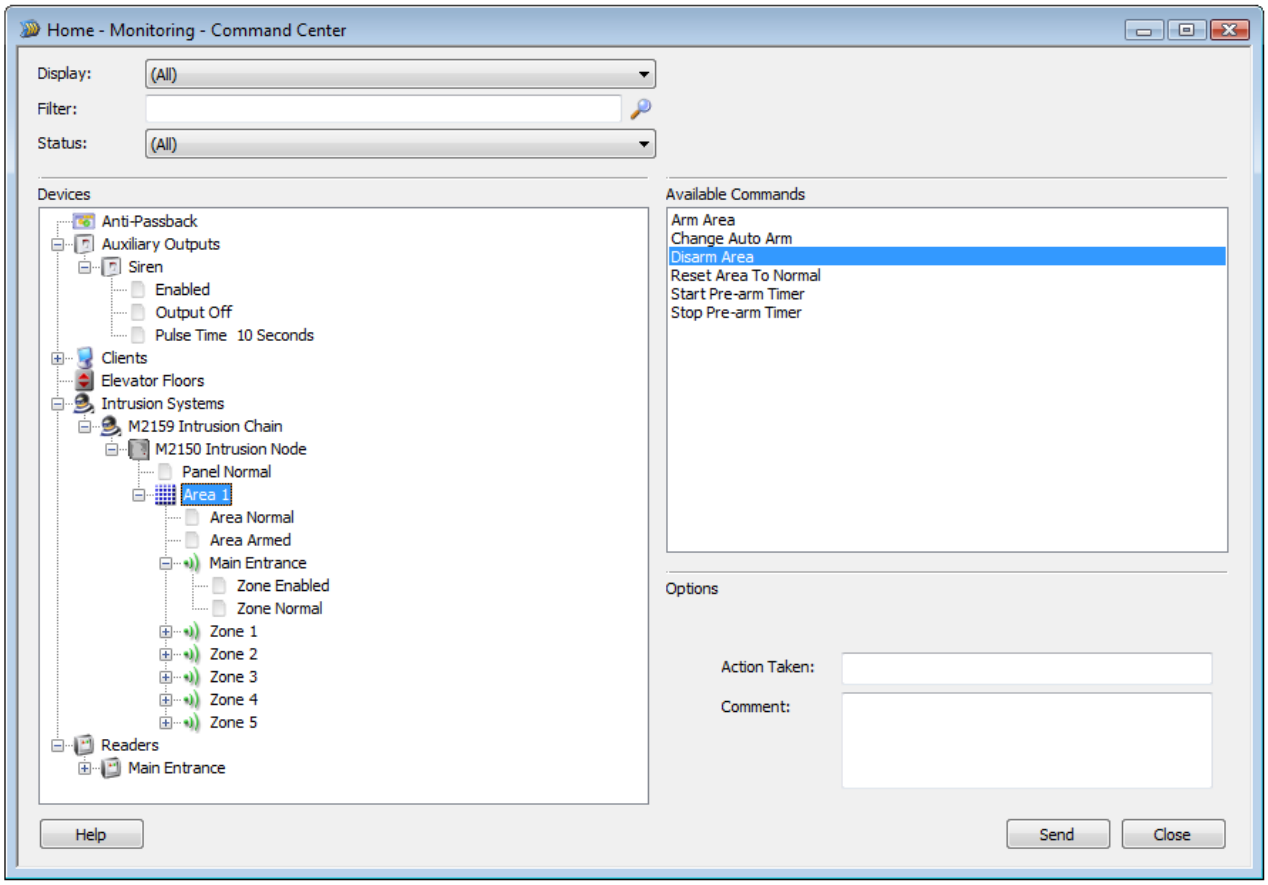


Figure 1-2: Command Center

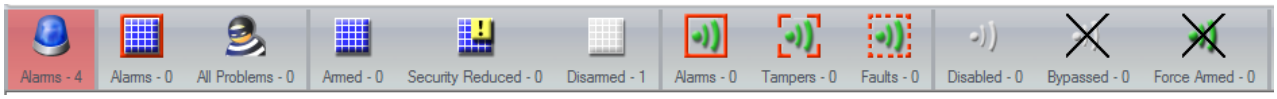


Figure 1-3: Intrusion Toolbar

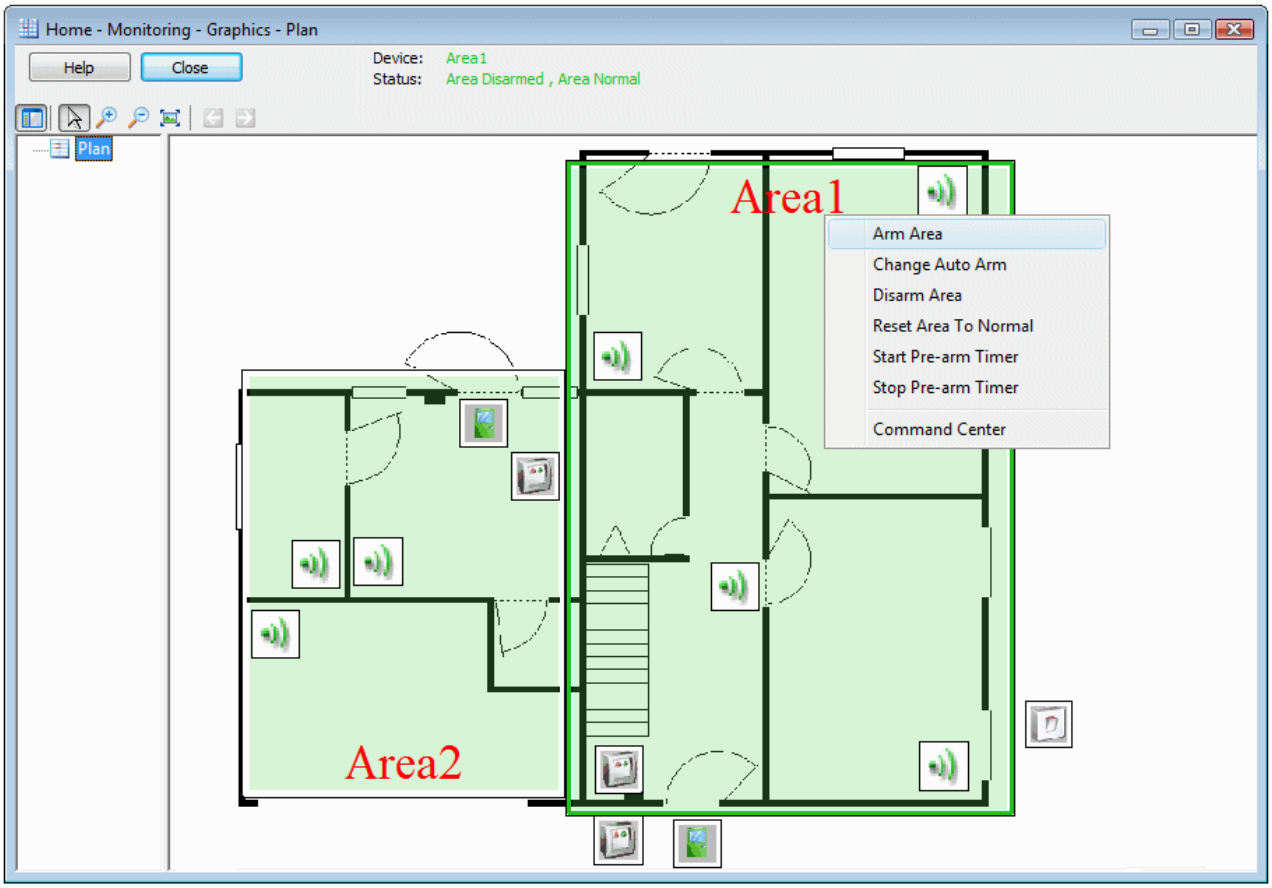


Figure 1-4: Graphics Screen

Alarm Siren and other External Devices

You can use auxiliary outputs to operate an alarm siren, entry/exit sounder, area armed indicator or area pre-arm sounder. Separate auxiliary outputs can be used for each area.

You can specify the auxiliary output to use for each function in the "Setup/Device Groups/Intrusion Areas" screen.

Communications Receiver (M2150 only)

If required, when using an M2150 system, Symmetry can send intrusion, reader and monitor point alarms over the network to a DMP SCS-1R communications receiver. This feature may, for example, be used to forward alarms to a centralized location during out-of-office hours.

Symmetry automatically maps Symmetry alarms to their DMP equivalents.

Note: The communications receiver and associated interfaces have not been evaluated by UL.

Lock-Out Mode

For M2150 systems, once the system is fully configured, a "Lock Out" feature can be used to prevent configuration changes being made to a node from Symmetry . You can choose which parts of the system configuration to lock.

Lock-out mode can be enabled from Symmetry or from an arming/disarming reader, but can be disabled only from an arming/disarming reader connected to the node. This feature provides added security when the reader is located inside the protected area.

Note: If a node is in lock-out mode, changes made in Symmetry may cause the node and the Symmetry database to be out of sync.

Maintenance Mode (M2150 only)

A user with installer privileges can place a node in "Maintenance Mode", which prevents unwanted alarms from occurring while an engineer is carrying out maintenance work.

Entry/Exit Routes and Final Exits

If required, monitor points and readers can be configured as:

- **Entry/Exit Route** - This prevents the monitor point or reader door monitor from causing an alarm if activated while the exit timer is running during the arming process. If the area is armed, activating the monitor point or door monitor starts the entry timer.

  If you set an arming/disarming reader to be on an entry/exit route, the exit timer starts when an operator uses the reader to arm the area that the reader is in.

- **Final Exit** - This causes the exit timer to finish during the arming process when the monitor point or reader door monitor is activated. Selecting **Final Exit** for a reader also selects **Entry/Exit Route**.

The duration of the entry/exit timer is defined in the "Install/Access Control/Node" screen.

Note: You can select the above options for a monitor point only if **Use as Intrusion Input** is selected in the "Install/Access Control/Monitor Point" screen. Any type of reader can have the above settings, even if it is not capable of being used as an arming/disarming reader. This allows standard access-control readers to finish the exit timer or start the entry timer.

System Configuration Examples

Example 1 – Internal Arming/Disarming Reader and External Access Reader

In this example, there is an arming/disarming reader inside the protected area, which is to arm and disarm the area. There is also an external access-control reader, which is used to gain entry to the protected area before disarming the system at the arming/disarming reader.

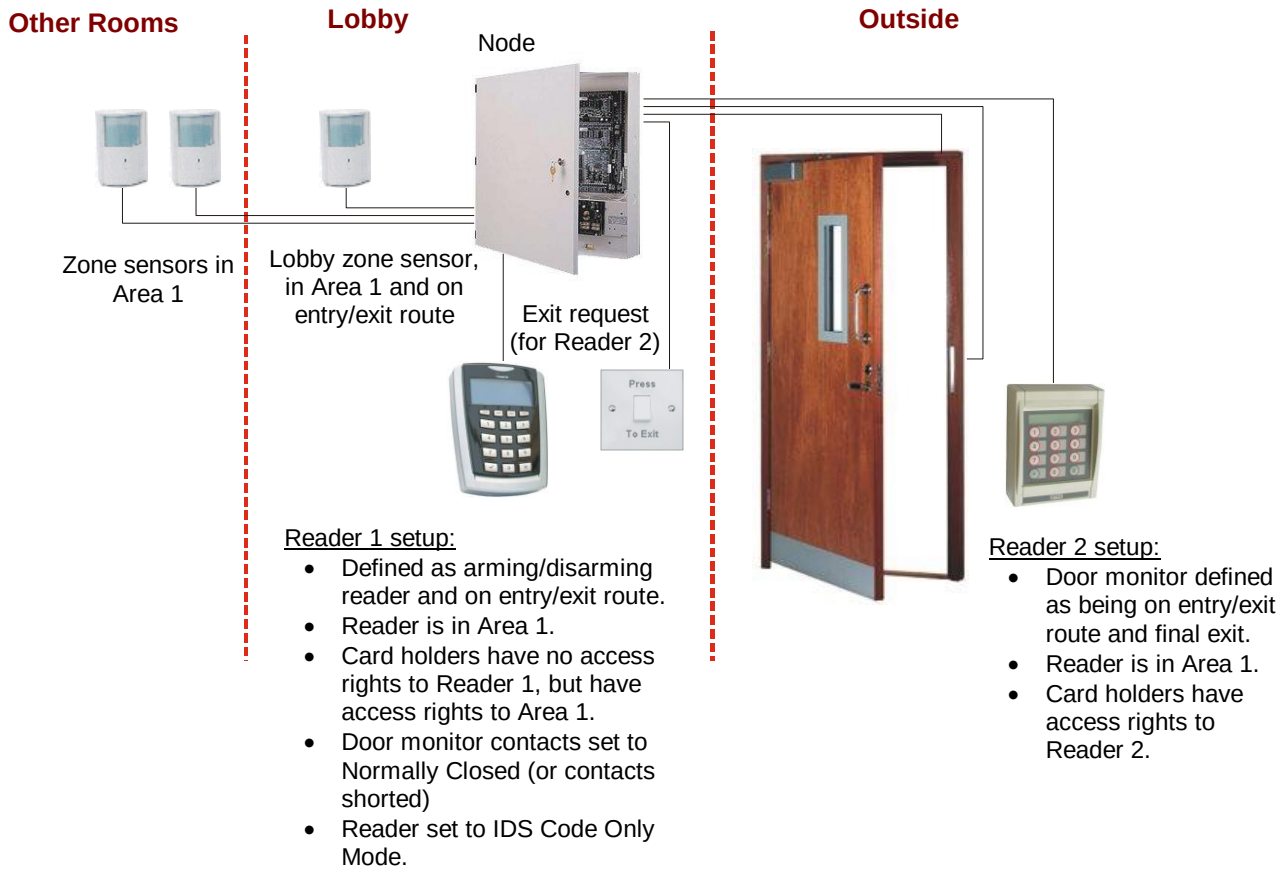


Figure 1-5: Example 1 - Arming/Disarming Reader Inside, with External Access-Control Reader

Example 1 Arming Sequence:

1. At Reader 1 (in the lobby), choose to arm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to arm and exit Area 1. The exit timer sounds.

2. Walk to the door. The Lobby sensor does not cause an alarm, since it is defined as being on the entry/exit route.

3. Press the exit-request switch to unlock the door.

4. Exit the lobby and close the door. The exit timer stops shortly after the door monitor detects that the door is closed, and the area arms.

Any reader that is assigned to Area 1, but which is not an arming/disarming reader, on an entry/exit route or used as a final exit is disabled once the area is armed, so that when you present a card, access is denied.

Example 1 Disarming Sequence:

1. Present your card to Reader 2 (the external reader) as a normal access-control transaction. The door unlocks.

2. Open the door and walk through. Since the door monitor is on the entry/exit route, the entry timer starts. The lobby zone sensor detects movement, but since it is on the entry/exit route, no alarm occurs.

3. Walk to Reader 1 and choose to disarm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to disarm Area 1. The area disarms and the entry timer stops.

Example 2 – External Reader Only

In this example, there is only an external reader, which is used to arm the area and to gain entry. The area disarms automatically when access is granted.

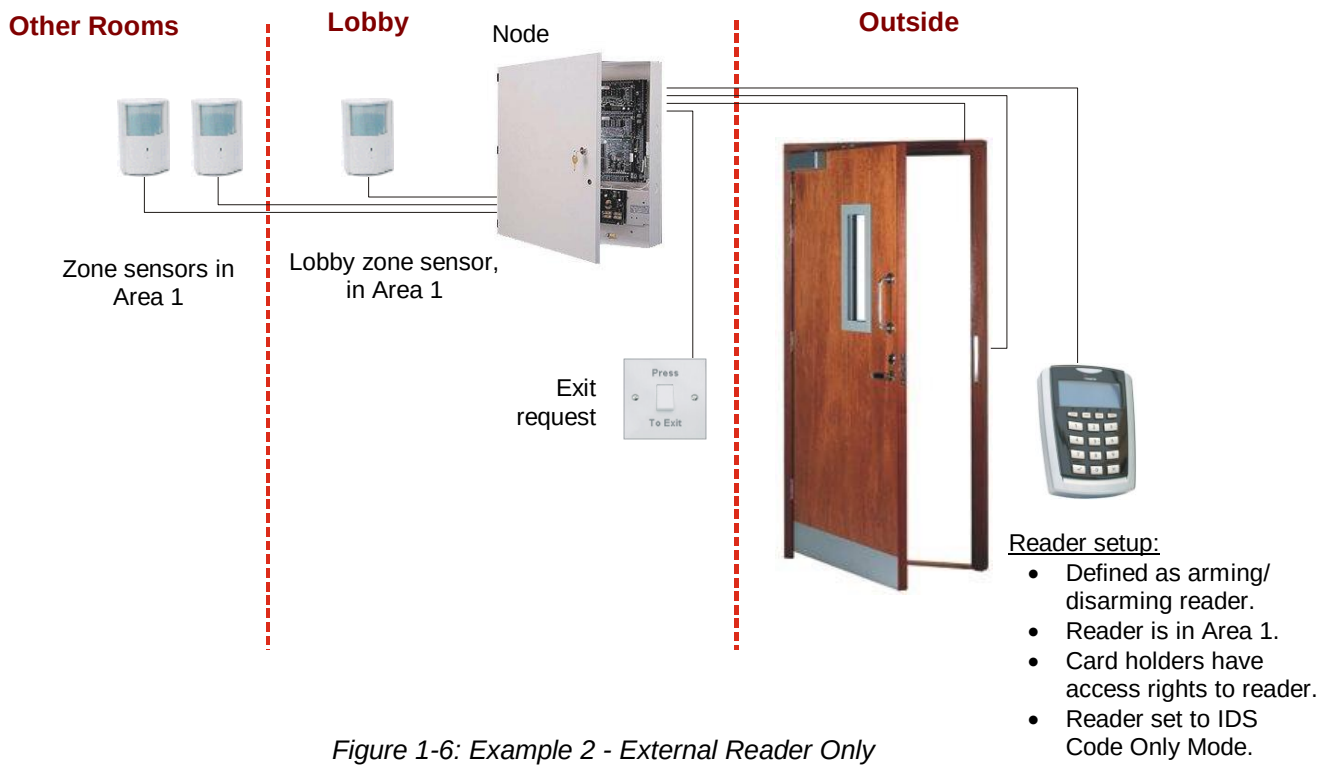


Figure 1-6: Example 2 - External Reader Only

Example 2 Arming Sequence:

1. Press the exit-request switch, exit the lobby and close the door.

2. At the reader, choose to arm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to arm and exit Area 1. There is no exit timer, since there is no entry/exit route.

Example 2 Disarming Sequence:

1. Present your card to the reader as a normal access-control transaction. The area associated with the reader disarms and the door unlocks.

2. Open the door and enter the lobby.

Example 3 – Internal Arming/Disarming Reader Only

In this example, there is only an internal arming/disarming reader. Access control is not used in this example.

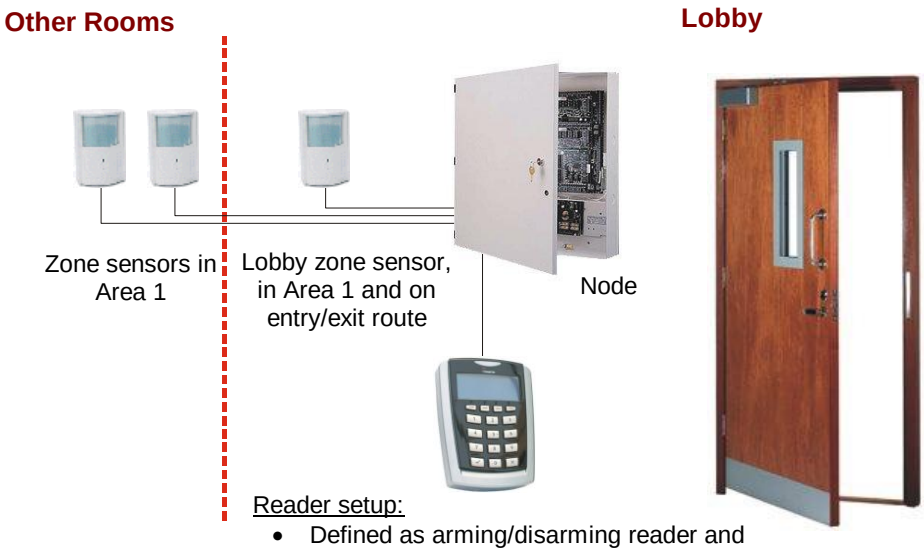


Figure 1-7: Example 3 - Internal Arming/Disarming Reader Only

Example 3 Arming Sequence:

1. At the reader, choose to arm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to arm and exit Area 1. The exit timer sounds.

2. Walk to the door. The Lobby sensor does not cause an alarm, since it is defined as being on the entry/exit route.

3. Open the door and exit.

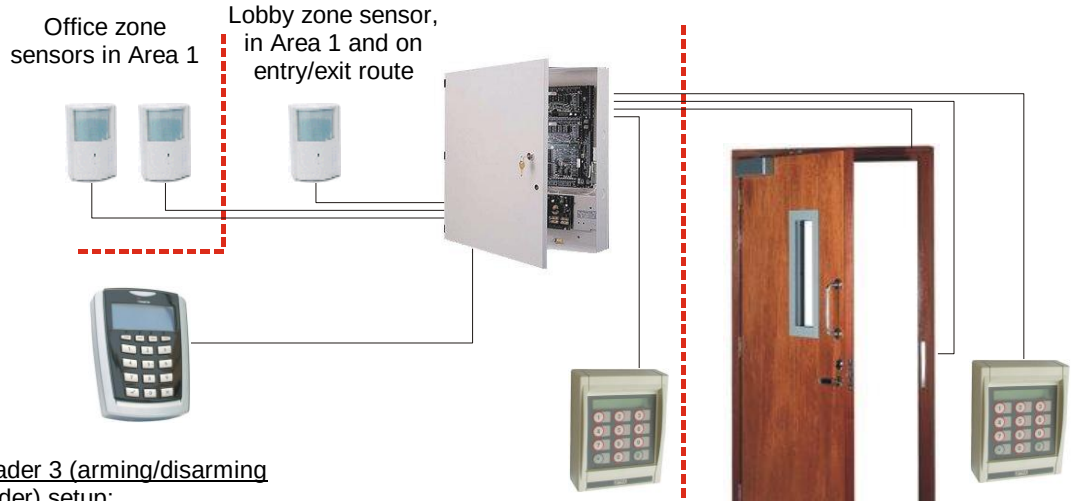
Example 3 Disarming Sequence:

1. Open the door and enter the lobby. The Lobby sensor detects movement and starts the entry timer.

2. Walk to the reader and choose to disarm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to disarm Area 1. The area disarms and the entry timer stops.

Example 4 – Internal Arming/Disarming Reader, with Entry and Exit Readers

This example uses a reader to arm and disarm the system, and two other readers for access control: one for entry and the other for exit, which may be used in some higher-security establishments to log when card holders exit as well as enter an area. These two readers use the "two readers at one door setting".



Reader 3 (arming/disarming reader) setup:

- Defined as arming/disarming reader and on entry/exit route.
- Reader is in Area 1.
- Card holders have no access rights to Reader 3, but have access rights to Area 1.
- Door monitor contacts set to Normally Closed (or contacts shorted).
- Reader set to IDS Code Only Mode.

Reader 2 (exit reader) setup:

- **NOT** set as an arming/disarming reader.
- Reader is in **NO** Area.
- Door monitor contacts set to Normally Closed (or contacts shorted).
- Card holders have access rights to Reader 2.

Reader 1 (entry reader) setup:

- Door monitor defined as being on entry/exit route and final exit.
- "Two readers at one door" set.
- Reader is in Area 1.
- Card holders have access rights to Reader 1.

Figure 1-8: Example 4 - Internal Arming/Disarming Reader, with Entry and Exit Readers

Example 4 Arming Sequence:

1. At Reader 3 (in the lobby), choose to arm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to arm and exit Area 1. The exit timer sounds.

2. Walk to the door. The Lobby sensor does not cause an alarm, since it is defined as being on the entry/exit route.

3. Present your access-control card to the exit reader (Reader 2). The door unlocks.

4. Exit the lobby and close the door. The exit timer stops when the door monitor detects that the door is closed, and the area arms.

Example 4 Disarming Sequence:

1. Present your card to Reader 1 (the entry reader) as a normal access-control transaction. The door unlocks.

2. Open the door and walk through. Since the door monitor is on the entry/exit route, the entry timer starts. The lobby zone sensor detects movement, but since it is on the entry/exit route, no alarm occurs.

3. Walk to Reader 3 and choose to disarm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to disarm Area 1. The area disarms and the entry timer stops.

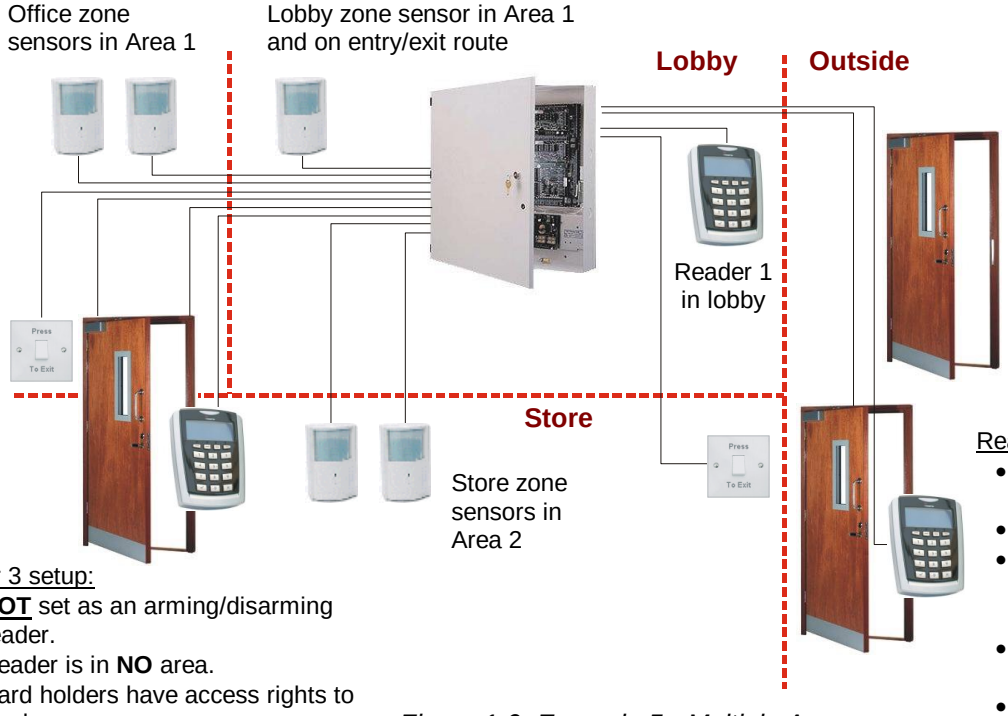
Example 5 – Multiple Areas

In this example, there is an internal arming/disarming reader (Reader 1) in the lobby, which can be used to arm and disarm Area 1 and/or Area 2. Reader 1 could be used for normal operation to arm/disarm the whole building at any time.

There is also an external arming/disarming reader (Reader 2), which in this example is used to gain access to a Store Room with sensors in Area 2 and arm/disarm that area. This could, for example, enable personnel to gain access to the store room at times when the main part of the building (Area 1) is not occupied, such as over the weekend or at night. Since Reader 2 is restricted to Area 2, personnel using Reader 2 are unable to arm/disarm Area 1.

Since access control is used at Reader 2, a successful access-control transaction at the reader also causes Area 2 to be automatically disarmed.

A standard internal access-control reader (Reader 3) provides access from the Store Room to offices protected by sensors in Area 1. A trigger command is set up to disable the reader when Area 1 is armed.



Reader 1 setup:
- Defined as arming/ disarming reader and on entry/exit route.
- Reader is in Area 1.
- Door monitor contacts set to Normally Closed (or contacts shorted)
- Reader set to IDS Code Only Mode.

Reader 2 setup:
- Defined as arming/ disarming reader.
- Reader is in Area 2.
- Reader has **Restrict Keypad to assigned Area** set.
- Card holders have access rights to reader.
- Reader set to IDS Code Only Mode.

Reader 3 setup:
- **NOT** set as an arming/disarming reader.
- Reader is in **NO** area.
- Card holders have access rights to reader.
- Trigger command disables reader when Area 1 is armed and enables reader when Area 1 is disarmed.

Figure 1-9: Example 5 - Multiple Areas

Example 5 Arming Sequence at Reader 1 (e.g. Monday-Friday, at end of day):

1. Ensure everyone has vacated both areas, except yourself. At the reader, choose to arm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to arm all areas and exit. The exit timer sounds.

2. Walk to the door. The Lobby sensor does not cause an alarm, since it is defined as being on the entry/exit route.

3. Open the door and exit.

Example 5 Disarming Sequence at Reader 1 (e.g. Monday-Friday, at start of day):

1. Open the door and enter the lobby. The Lobby sensor detects movement and starts the entry timer.

2. Walk to the reader and choose to disarm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to disarm all areas. The areas disarm and the entry timer stops. Standard access-control rules at Reader 3 allow access from the Store Room to offices protected by sensors in Area 1.

Example 5 Disarming Sequence at Reader 2 (e.g. Saturday, at start of day):

Assume Areas 1 and 2 are armed.

1. Present your card to Reader 2 (on the outside of the building) as a normal access-control transaction. The area associated with the reader (Area 2) disarms and the door unlocks. Area 1 remains armed. The **Restrict Keypad to assigned Area** option prevents you from disarming Area 1 through the intrusion menu.

2. Open the door and enter the room. Standard access-control rules at Reader 3 prevent you from gaining access from the Store Room to rooms with sensors in Area 1.

Example 5 Arming Sequence at Reader 2 (e.g. Saturday, at end of day):

1. Ensure everyone has vacated Area 2, except yourself. Press the exit-request switch, exit the room and close the door.

2. At the reader, choose to arm the system. When prompted, enter your unique IDS (intrusion) code or present your card, and choose to arm Area 2. There is no exit timer, since there is no entry/exit route. Area 1 remains armed.

Chapter 2: Configuring M2150/M4000 Intrusion in Symmetry

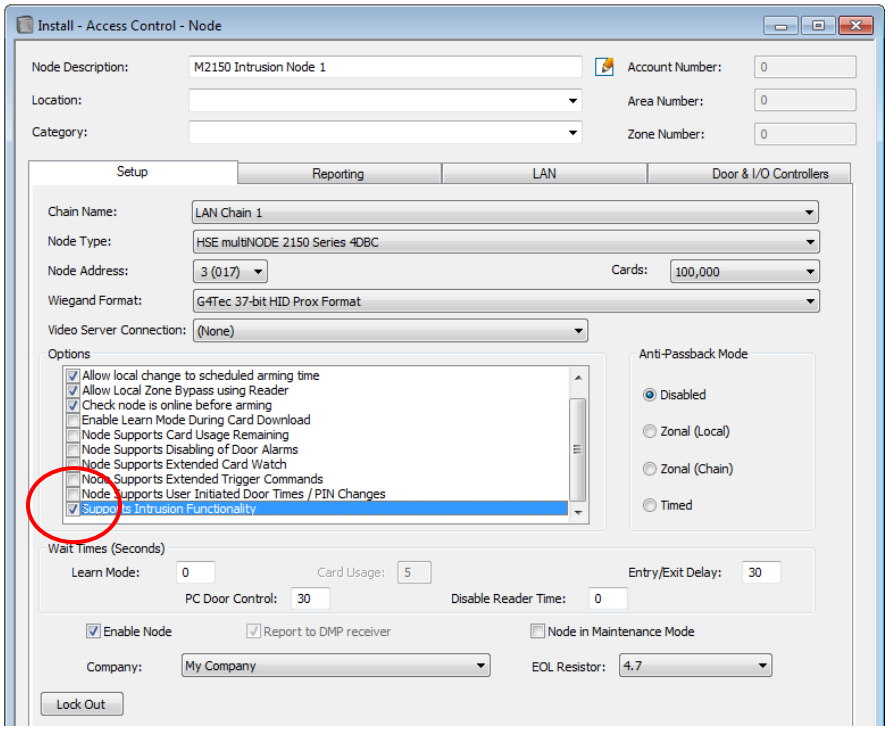
This chapter explains how to set up and configure an M2150/M4000 intrusion system in Symmetry. **Note:** Please refer to the *Online Help* for detailed information about the options in each screen.

Step 1 – Configure Client Ports and Chains

If you are using M2150 nodes and it is necessary for the node type you are using, configure the client ports and chains in the normal way using the "Install/System/Client Ports" and "Install/Access Control/Chains" screens in Symmetry.

Step 2 – Add the Intrusion Nodes

Use the Symmetry "Install/Access Control/Node" screen to add each intrusion node into Symmetry, and select **Supports Intrusion Functionality**:



Note: The screen layout is different for M4000.

Selecting **Supports Intrusion Functionality** enables additional intrusion options in the screen, including:

- **Entry/Exit Delay** – Specifies the duration of the entry and exit timers.

- **Node in Maintenance Mode (M2150 only)** – Prevents unwanted alarms from occurring while an engineer is carrying out maintenance work.

- **EOL Resistor (M2150 only)** – Specifies the resistor values (default values in kOhms) to use for cable supervision in monitor points (including zone sensors), door monitors and exit-request switches. Please refer to the *M2150 Design Guide* or *Online Help* for further information. For M4000, the resistor values are specified in the web interface.

  Note: The **Custom** option allows a non-default resistor value to be used. Please refer to your Technical Support representative if a custom resistor value is required.

  Note: To ensure proper line supervision, 3-state, 4-state or 6-state supervision must be used for installations requiring UL1076 compliance. Normally-open or normally-closed contacts can be used.

- **Lock Out (M2150 only)** – Once you have fully configured the system, you may want to lock certain types of data at the node for security reasons, such as card holder data or time codes. Once you have configured the type of data to lock using the **Lock Out** button, you can start lock-out mode by sending the **Lock Out Node** command from the "Home/Monitoring/Command Center screen" or from arming/disarming readers connected to the node. Lock-out mode can be switched off only from the arming/disarming reader connected to the node.

  Please refer to the *Online Help* for further information about lock-out mode.

Selecting **Supports Intrusion Functionality** also enables additional checkboxes in the **Options** area:

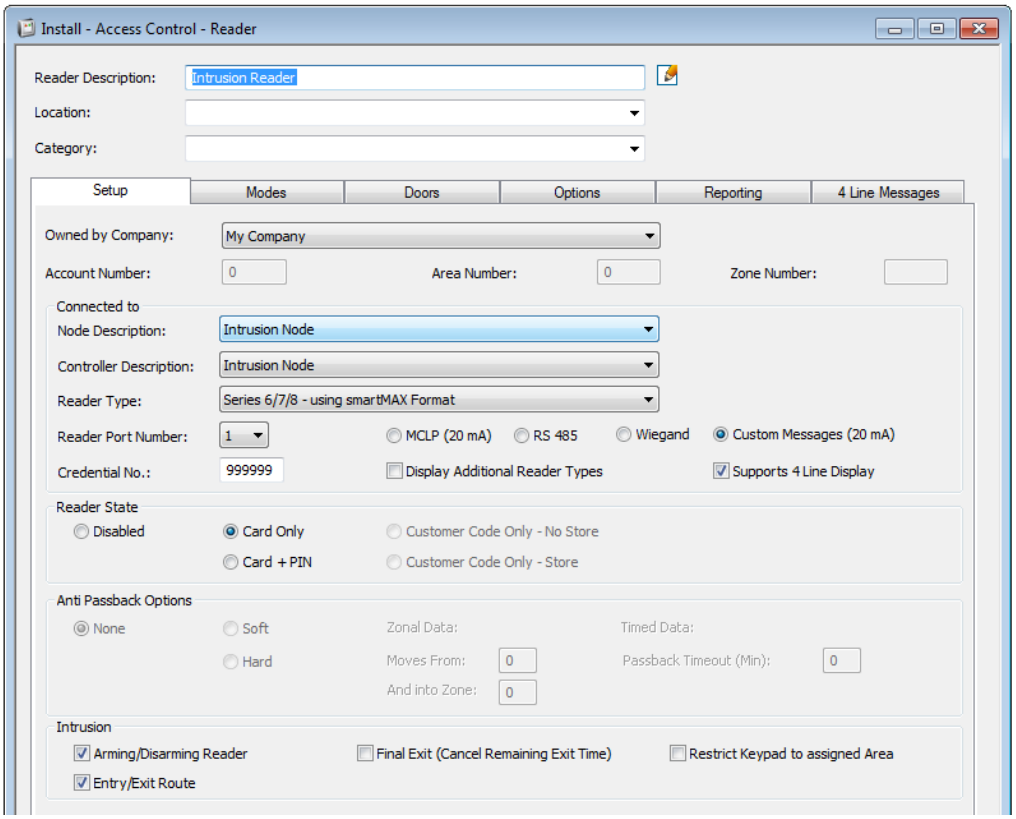
- **Allow local arming when node is offline** - Selecting this option allows a card holder at an arming/disarming reader to arm an area, irrespective of whether the node is online or offline. If the option is not selected, the node must be online to arm an area.

- **Allow local change to scheduled arming time** - If this option is set, card holders will be able to change the time of the next auto-arm at arming/disarming readers connected to this node. All subsequent auto-arms will occur at the scheduled time (unless changed again). Note: Card holders also need area access rights to change the auto-arm time of an area.

- **Allow Local Zone Bypass using Reader** - Selecting this option allows a card holder to bypass a zone that is in an alarm state. To bypass a zone, the zone must belong to an area that is in the card holder's access rights.

- **Check node is online before arming** - If selected, the Symmetry software checks the online/offline status of the node when an area is armed. This is used by **Allow local arming when node is offline**.

Step 3 – Add and Configure the Intrusion Readers



Note: The screen layout is different for M4000.

If you are using M2150, use the "Install/Access Control/Reader" screen to add each reader into Symmetry. If you are using M4000, readers are defined in the web interface and automatically import into Symmetry when you add the M4000 node.

For both M2150 and M4000, you need to configure each reader using the following options:

- **Arming/Disarming Reader** – This option is available only if an appropriate **Reader Type** is selected, and for M2150 the **Custom Messages (20mA)** communications protocol is selected. Select **Arming/Disarming Reader** if you want card holders to be able to arm and disarm intrusion areas at the reader. The area access rights (page 24) determine the areas that a card holder can arm and disarm.

- **Final Exit** – Select this option if you want the door monitor contact associated with the reader to cancel the exit timer when triggered.

- **Restrict Keypad to assigned Area** – Select this option if you want all functions at the reader to be restricted to the area the reader is assigned to.

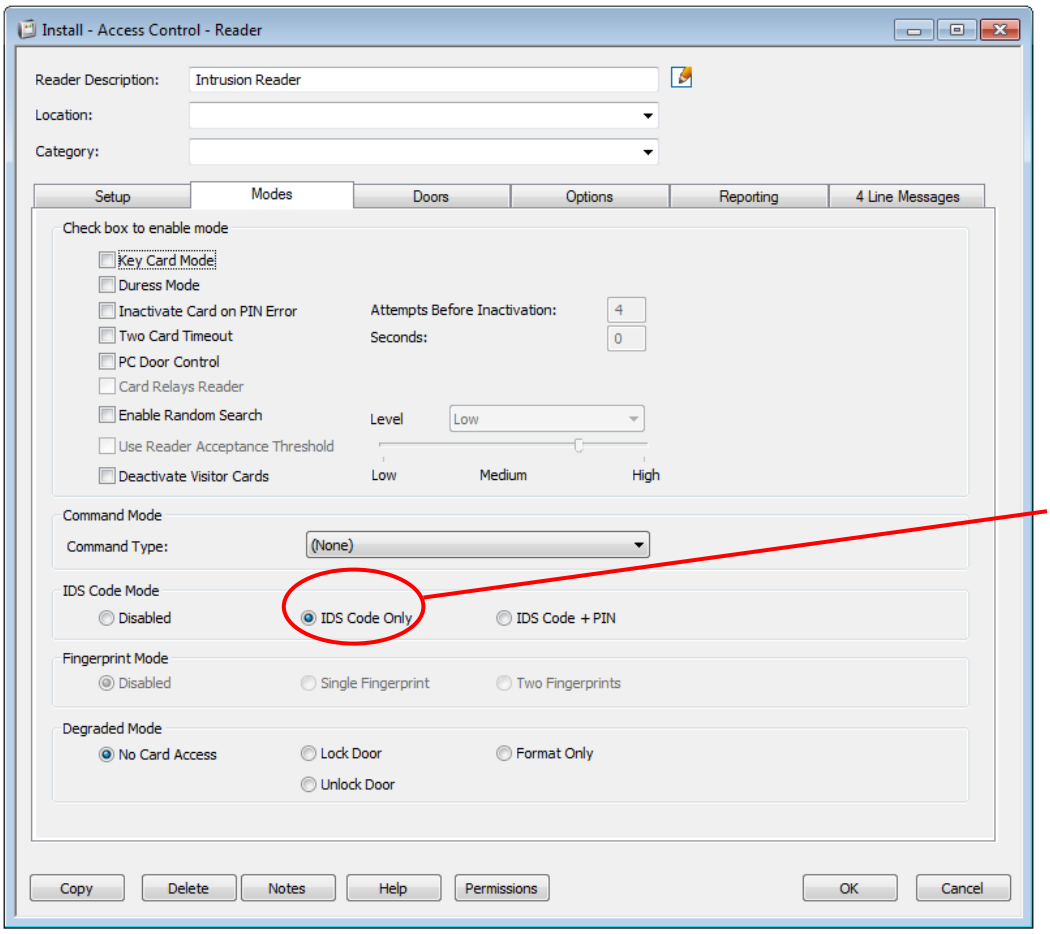
- **Entry/Exit Route** – Select this option if you require any of the following:
  - The exit timer to start when a card holder uses the reader to arm the area that the reader is in.
  - Valid activations of the door monitor to be ignored while the exit timer is running.
  - The entry timer to start if the door monitor is activated while the area the reader is in is armed.

Please see the examples from page 7.

Note: The Intrusion Areas screen (page 18) is used to assign the reader to an area.

Setting IDS Code-Only Mode

If the reader is an arming/disarming reader, select **IDS Code Only**, as shown in the following picture. This is necessary to enable IDS codes to be used at the reader.



Note: The screen layout is different for M4000.

Select **IDS Code Only** to enable IDS codes to be used at the reader.

Note: If a user enters the IDS code incorrectly three times in a row at a reader, the reader is blocked for IDS code entry for five minutes. The reader can be unblocked using the **Remove IDS Block** command.

S884 4-Line Messages Tab

For readers such as the Javelin S884-v2, selecting **Supports 4 Line Display** displays a **4 Line Messages** tab, which allows you to customize the text displayed at the reader. For information about how to use this tab, please refer to the Online Help.

Intrusion Zones Created by Reader Definitions

Each reader attached to an M2150/M4000 intrusion node automatically creates an intrusion zone for the door monitor contact.

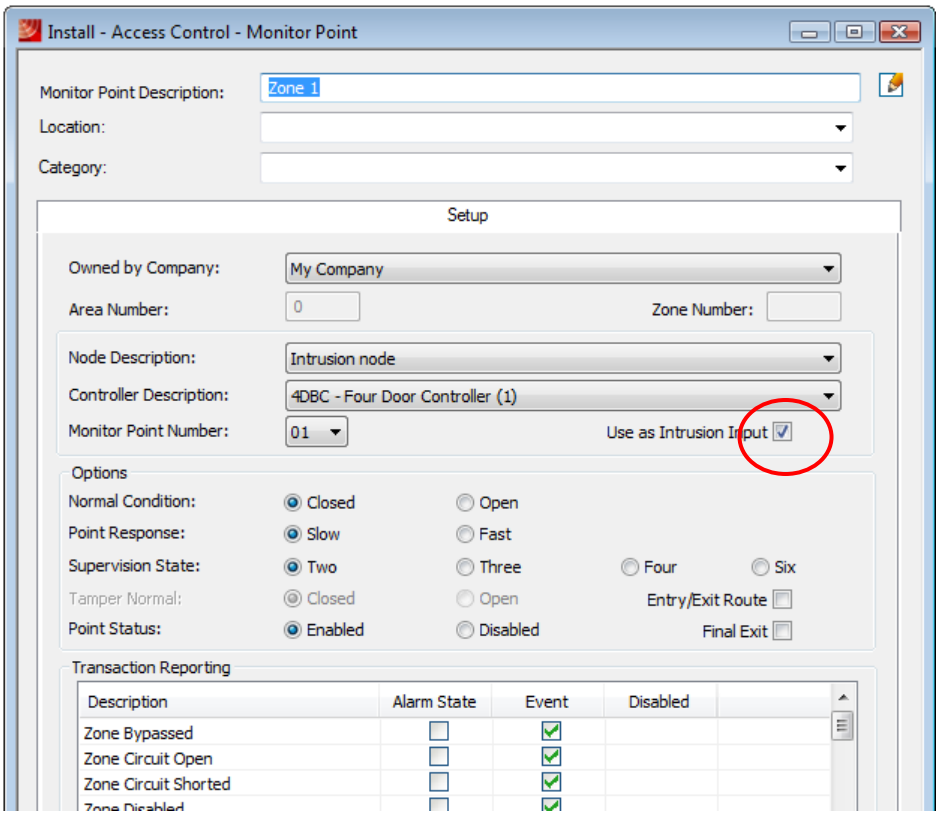
If, for example, the door is forced while the area is armed, the Symmetry software generates "Area in Alarm" and "Zone in Alarm" alarms, as well as the standard access-control "Door Forced" alarm.

You are able to monitor, bypass, enable or disable reader zones from the Command Center in the same way as other zones created using monitor points.

Step 4 – Add and Configure the Intrusion Zones

If you are using M2150, use the "Install/Access Control/Monitor Point" screen to add each monitor point (zone sensor) into Symmetry. If you are using M4000, monitor points are defined in the web interface and automatically import into Symmetry when you add the M4000 node.

For each M2150/M4000 zone sensor, select **Use as Intrusion Input**:

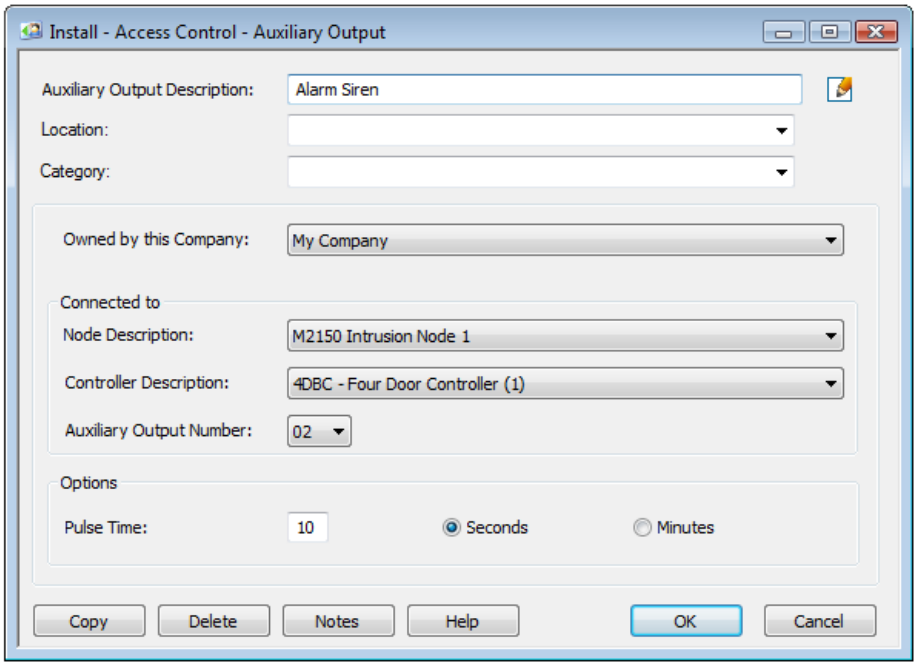


Note: The screen layout is different for M4000.

Select **Entry/Exit Route** if the zone is in an entry/exit route, and **Final Exit** if you want the zone to cancel any remaining exit period when the zone returns to its normal state after being triggered. Please refer to Chapter 1 for system examples.

Step 5 – Set Up the Auxiliary Outputs

If you are using M2150, use the "Install/Access Control/Auxiliary Output" screen to add each auxiliary output required for the intrusion system (such as an alarm siren or pre-arm warning buzzer). If you are using M4000, auxiliary outputs are defined in the web interface and automatically import into Symmetry when you add the M4000 node.



Note: The screen layout is different for M4000.

Step 6 – Set Up the Intrusion Areas

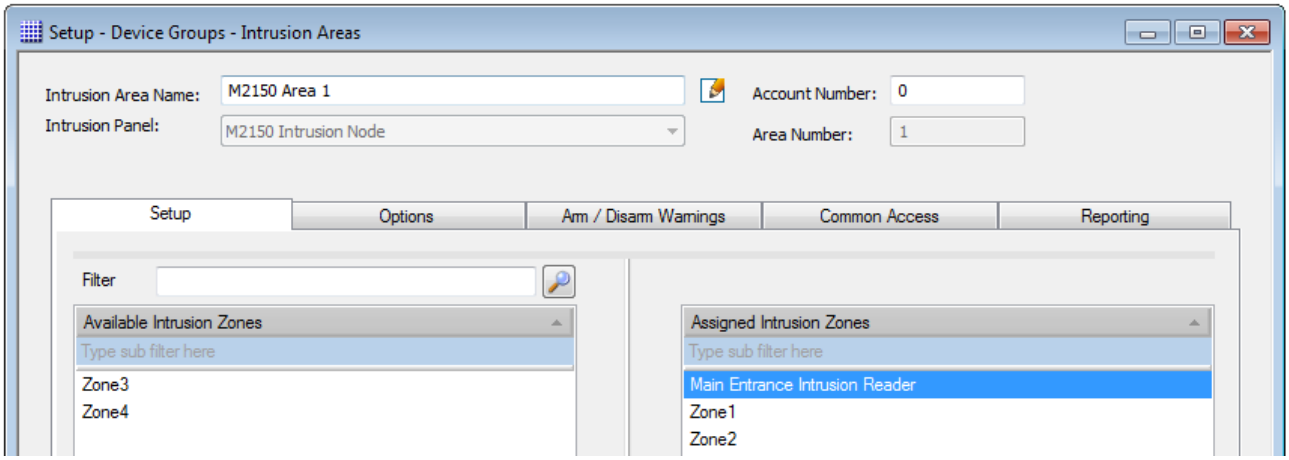
Set up each intrusion area using the "Setup/Device Groups/Intrusion Areas" screen, as described next. Each area you create belongs to the currently-selected company.

Note: You can use the **Permissions** button to allow only selected user roles to arm and/or disarm the area from the Symmetry software. You can assign separate arm and disarm privileges for each user role.

Please refer to page 1 for further information about setting up areas.

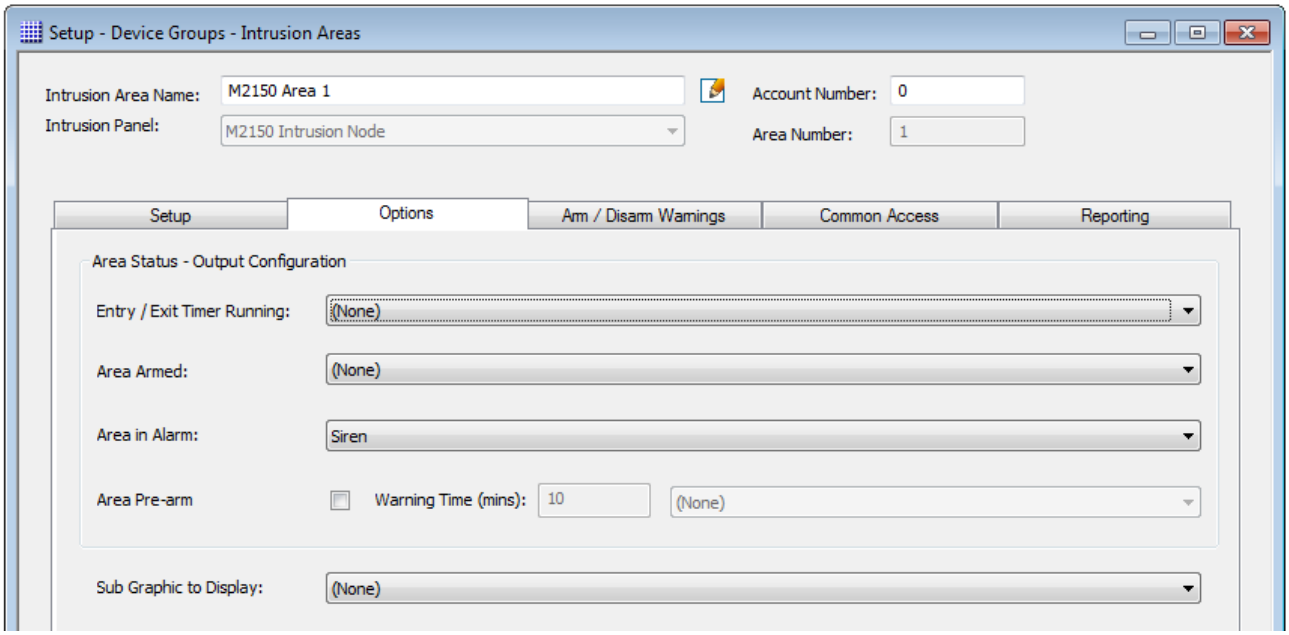
Setup Tab

In the Setup tab, choose the zones and readers to include in the area:



Options Tab

Choose the auxiliary outputs to switch on when specified conditions occur:



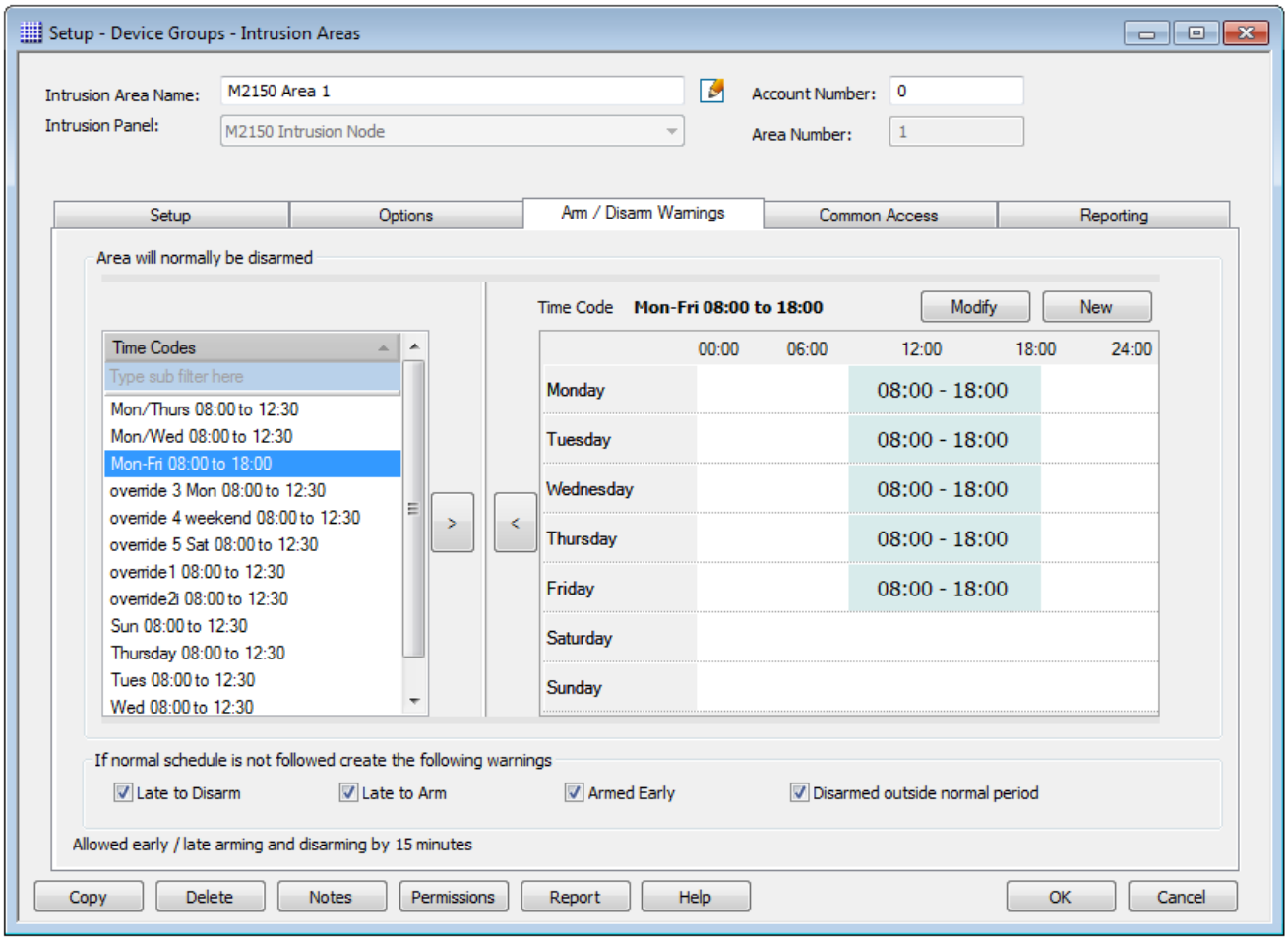
The auxiliary output selected by **Area in Alarm** operates when the area has an "Area in Alarm" alarm, and is normally used to activate the external alarm sounder (bell box). The auxiliary output returns to its normal state when you send a "Reset Area To Normal" command from the "Home/Monitoring/Command Center" screen, or when you disarm the area, or if you acknowledge the "Zone in Alarm" alarm (if **Zone resets area output** is selected in the "Maintenance/User & Preferences/System Preferences" screen).

The auxiliary output selected by **Area Pre-arm** operates immediately prior to an auto-arm of the area. The **Warning Time** field specifies the length of time before the auto-arm that the auxiliary output will operate for. You can set up auto-arms using scheduled commands (see page 22).

Sub Graphic to Display determines the graphic to display when a user double-clicks the icon representing the area in the "Home/Monitoring/Graphics" screen. This is useful if the site uses a top-level graphic that contains several areas; double-clicking the area could display a more detailed graphic that shows the locations of individual devices and building features.

Arm/Disarm Warnings Tab

You can use this tab to specify the periods when the intrusion system is expected to be disarmed and armed. The start time of the selected time code determines the time when the area should be disarmed. The end time determines the time when the area should be armed. The alarm/event messages selected in the lower area of the tab are generated automatically if the system is not in the expected armed/disarmed state.

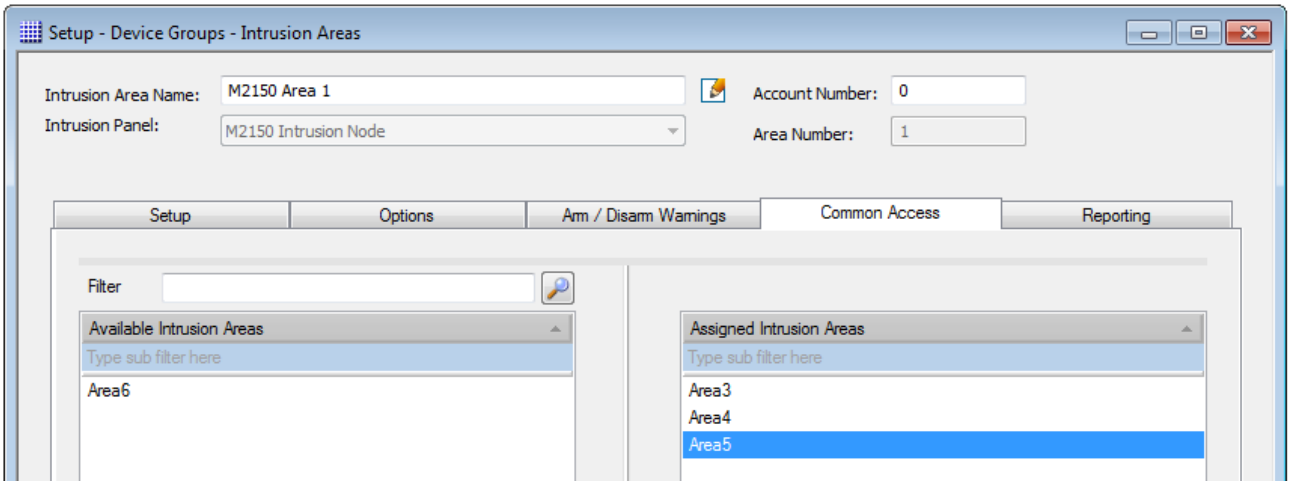


A grace period is allowed to arm or disarm the area late or early to prevent unnecessary alarm/event messages. The period is displayed near the bottom of the screen (**Allowed early / late arming and disarming by <n> minutes**), and is defined by **Intrusion Arm/Disarm Tolerance** in the "Maintenance/User & Preferences/System Preferences" screen. Please click the **Help** button in the Intrusion Areas screen for further information about the meaning of this setting for each alarm/event checkbox.

The area below the menu gives a graphical representation of the time intervals defined by the time code. You can use **Edit/View** to view or modify the selected time code, or **New** to create a new time code. The time code category used to define these periods is "Area Warning".

Common Areas Tab

You can use this tab for an M2150 system to define a common area such as a lobby or other part of the building that people can use to access several other areas.



By selecting areas in this tab, you are declaring that the area you are defining is a common area serving the selected areas.

A common area is automatically armed when the last area that is accessed through the common area is armed.

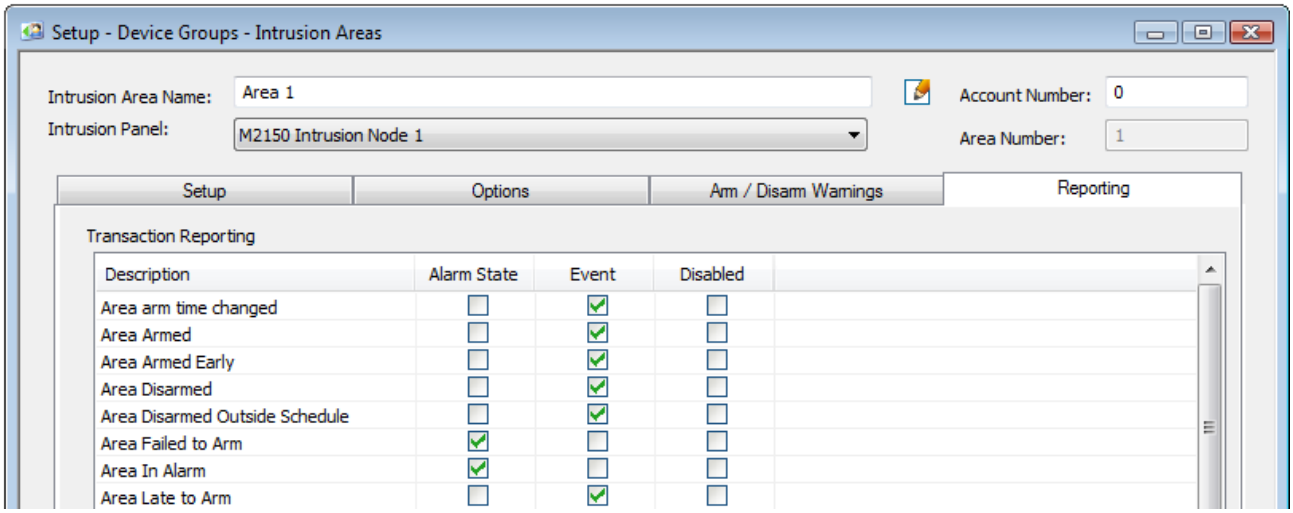
A common area and all its associated areas must be controlled by the same M2150 node.

For further information, please refer to the Symmetry *Online Help*.

Note: Common areas are not currently supported for M4000.

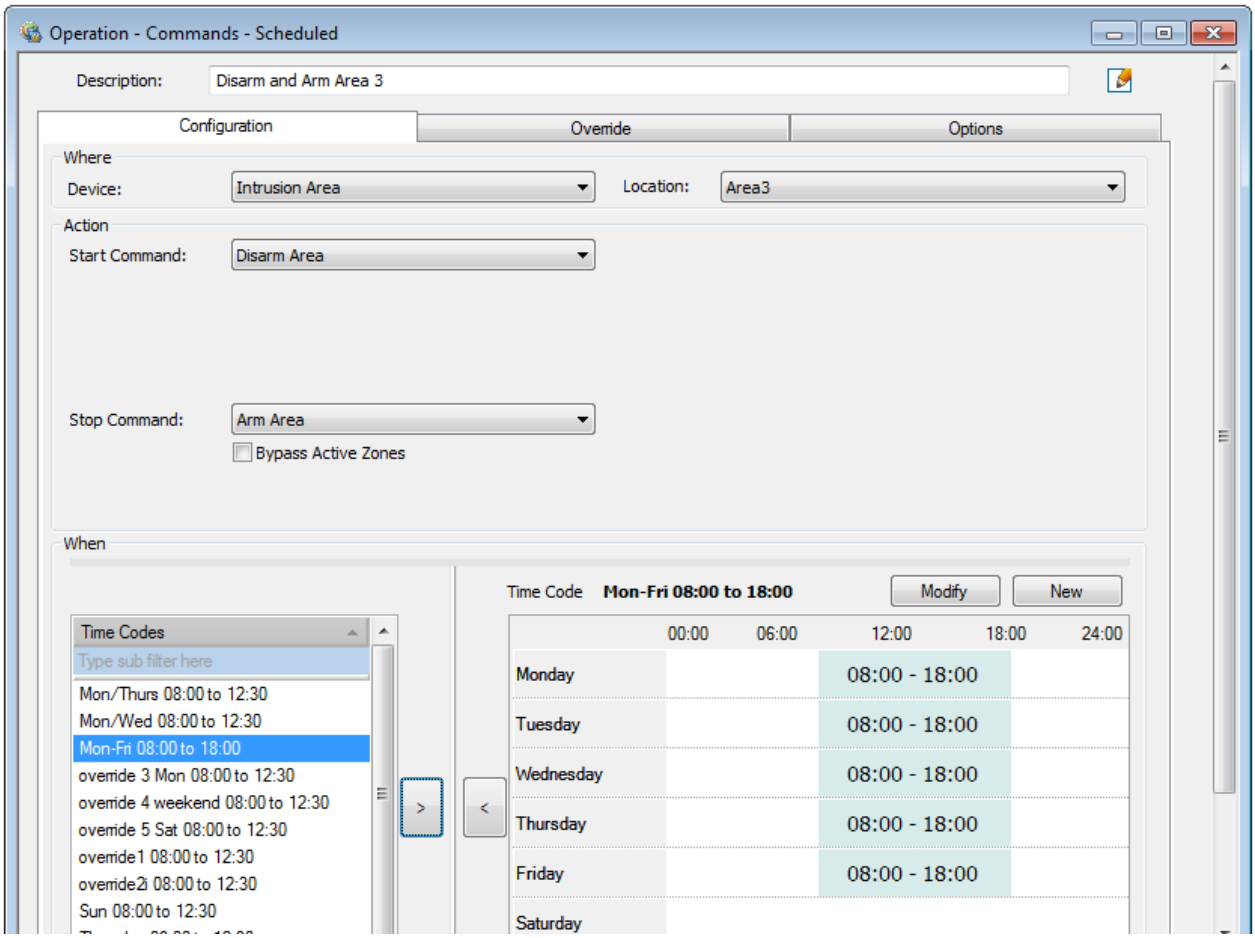
Reporting Tab

This tab specifies whether each message from the area causes an alarm, event or is not reported at all by the area's node. You should normally leave the default settings unchanged.



Step 7 – Set Up Auto-Disarming and Arming

You can disarm and arm the intrusion area automatically at specified times. To do this, set up a scheduled command using the "Operation/Commands/Scheduled" screen, as shown next.



The above example causes the area to disarm at 08:00 and arm at 18:00 Monday to Friday.

Note: By default, all arming/disarming readers in the area beep during the pre-arm period to warn people to exit the area. The pre-arm period is defined by **Warning Time** in the Options tab of the "Setup/Device Groups/Intrusion Areas" screen (see page 19). You can also use this tab to set up an auxiliary output to switch on during the pre-arm period.

Auto-arms can be delayed from the "Home/Monitoring/Command Center" screen or from an arming/disarming reader if **Allow local change to scheduled arming time** is set in the "Install/Access Control/Node" screen. The "Home/Monitoring/Command Center" screen can also be used to start or stop the pre-arm timer.

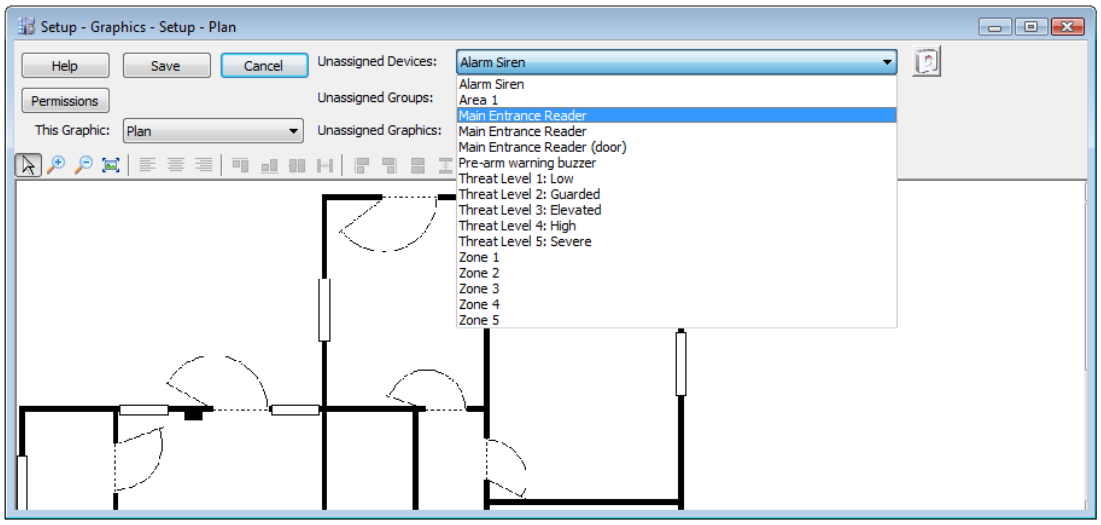
Step 8 – Set Up Graphics

You can monitor and control the intrusion system from a graphic displayed using the "Home/Monitoring/Graphics" screen. For example, you can monitor the current status of zones, and send commands to arm areas, disarm areas and bypass zones.

To configure a graphic in the Symmetry software:

1. Install the graphic using the "Setup/Graphics/Add" screen.

2. Add the required devices to the graphic using the "Setup/Graphics/Setup" screen. The following shows an example:



The following devices can be added to the graphic in the above example:

- **Alarm Siren** and **Pre-arm warning buzzer** – These are auxiliary outputs. Adding these allows a user to monitor and change their status from the "Home/Monitoring/Graphics" screen.
- **Area 1** – This is the name of the only area defined. Adding the area would allow a user to monitor and arm/disarm the area from the "Home/Monitoring/Graphics" screen. Double-clicking the area in the "Home/Monitoring/Graphics" screen causes the sub-graphic specified in the "Setup/Device Groups/Intrusion Areas" screen to be displayed.
- **Main Entrance Reader** – This is the name of the reader. There are three instances: one for the door monitor, one for the reader itself and the other for the door associated with the reader. Each has a different icon. The three different devices allow a user to monitor and control each function separately from the "Home/Monitoring/Graphics" screen.
- **Threat Level ...** – These are provided if the Threat Level Management option is installed (not specific to M2150/M4000 intrusion).
- **Zone <n>** – These are the names of the defined zones. Adding these to the graphic allows a user to monitor and control each zone separately from the "Home/Monitoring/Graphics" screen.

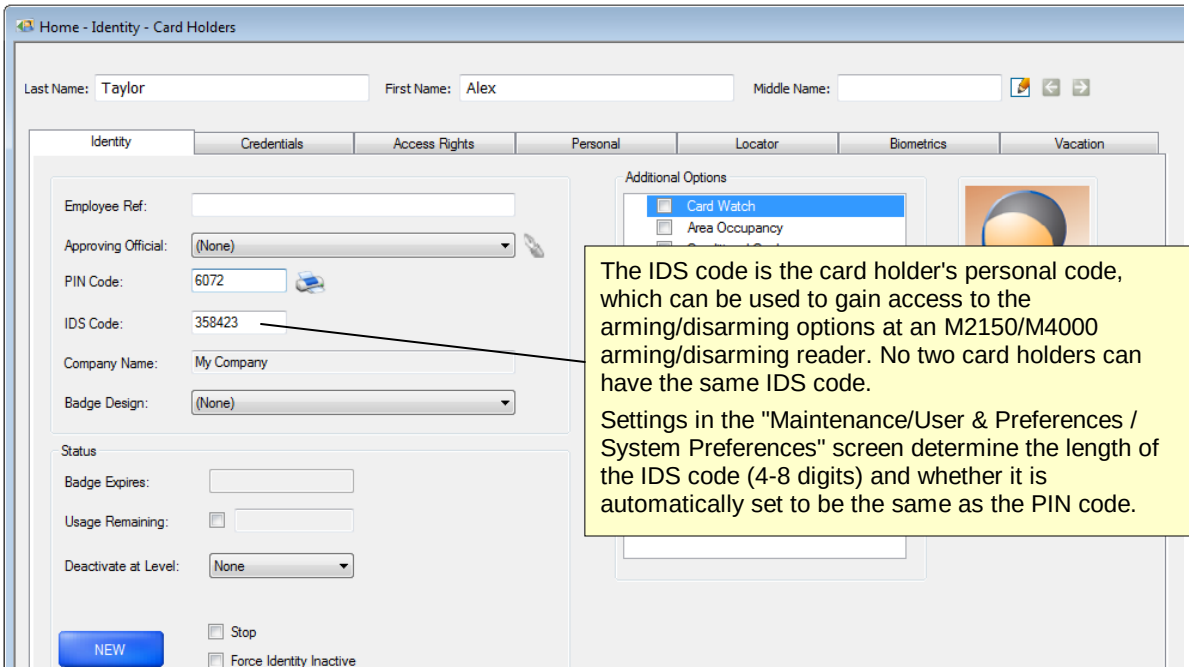
During the design of graphics, note that the **Sub Graphic to Display** option in the "Setup/Device Groups/Intrusion Areas" screen (see page 20) allows users to double-click an area graphic to display a sub-graphic, which could show further detail. You may want to set up several graphics and design a graphic hierarchy to take advantage of this feature.

Step 9 – Set Up Card Holders and Access Rights

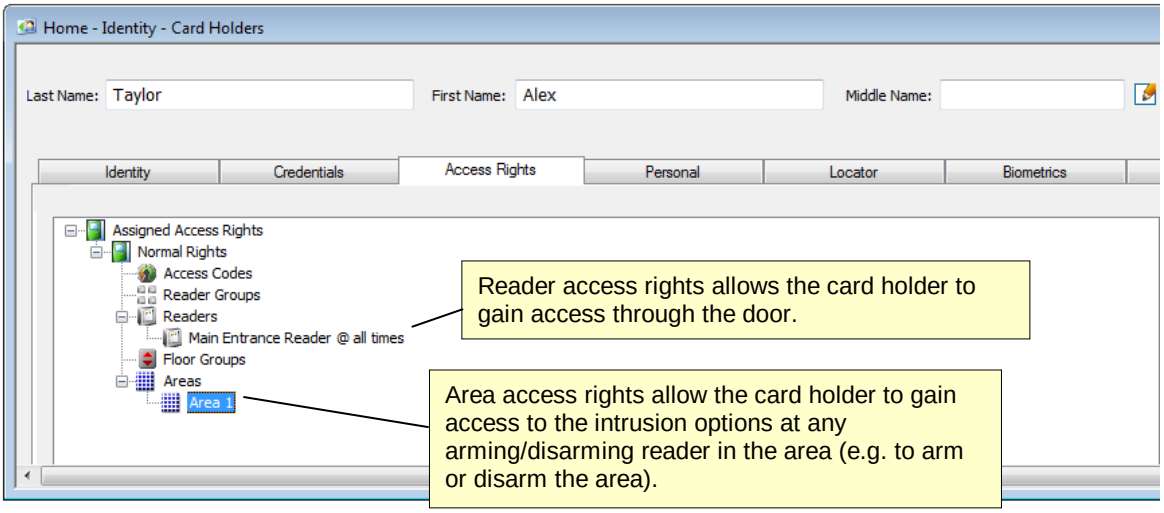
You need to use the "Home/Identity/Card Holders" screen to define a card holder for each person who is allowed to arm and/or disarm the intrusion system.

When defining the card holder:

1. Specify an **IDS Code**:



2. Define Reader and Area access rights:



Note: Reader access rights are not required to arm or disarm an area. However, if both reader and area access rights are assigned to the card holder, and the reader is an arming/disarming reader, performing a valid access-control transaction at the reader disarms the area and unlocks the door (see Example 2 on page 8).

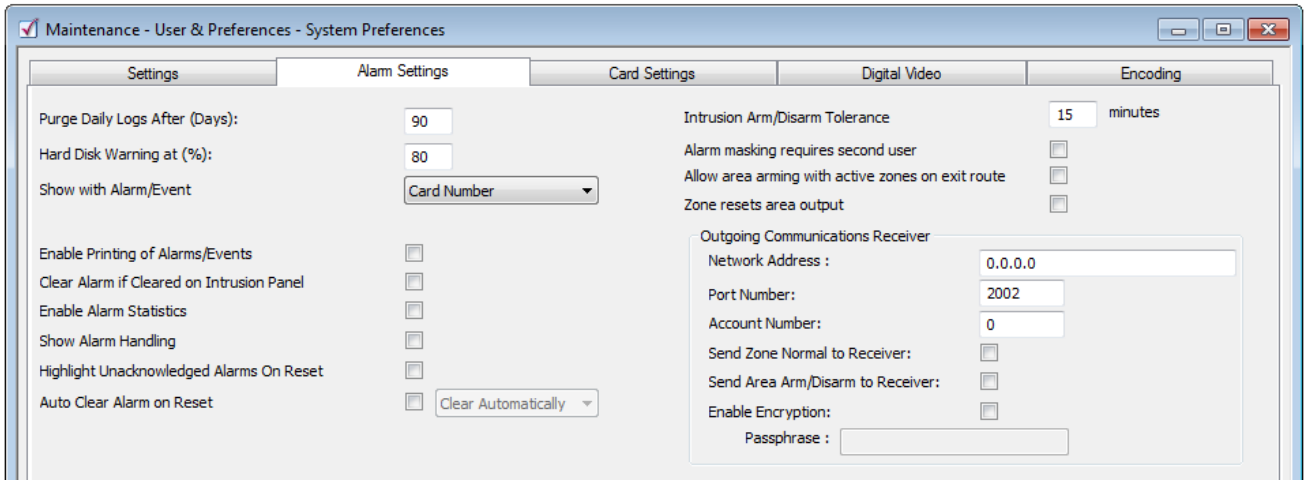
Step 10 – Set Up Communications Receiver Interface (Optional)

Use the following procedure if you want to send intrusion, reader and monitor point alarms over the network to a DMP SCS-1R communications receiver (M2150 only; not supported for M4000). See page 29 for details of the alarms that are sent.

Note: The communications receiver and associated interfaces have not been evaluated by UL.

Step 10a – Configure the Communications Receiver Settings

Configure the **Outgoing Communications Receiver** section of the "Maintenance/User & Preferences/System Preferences" screen:



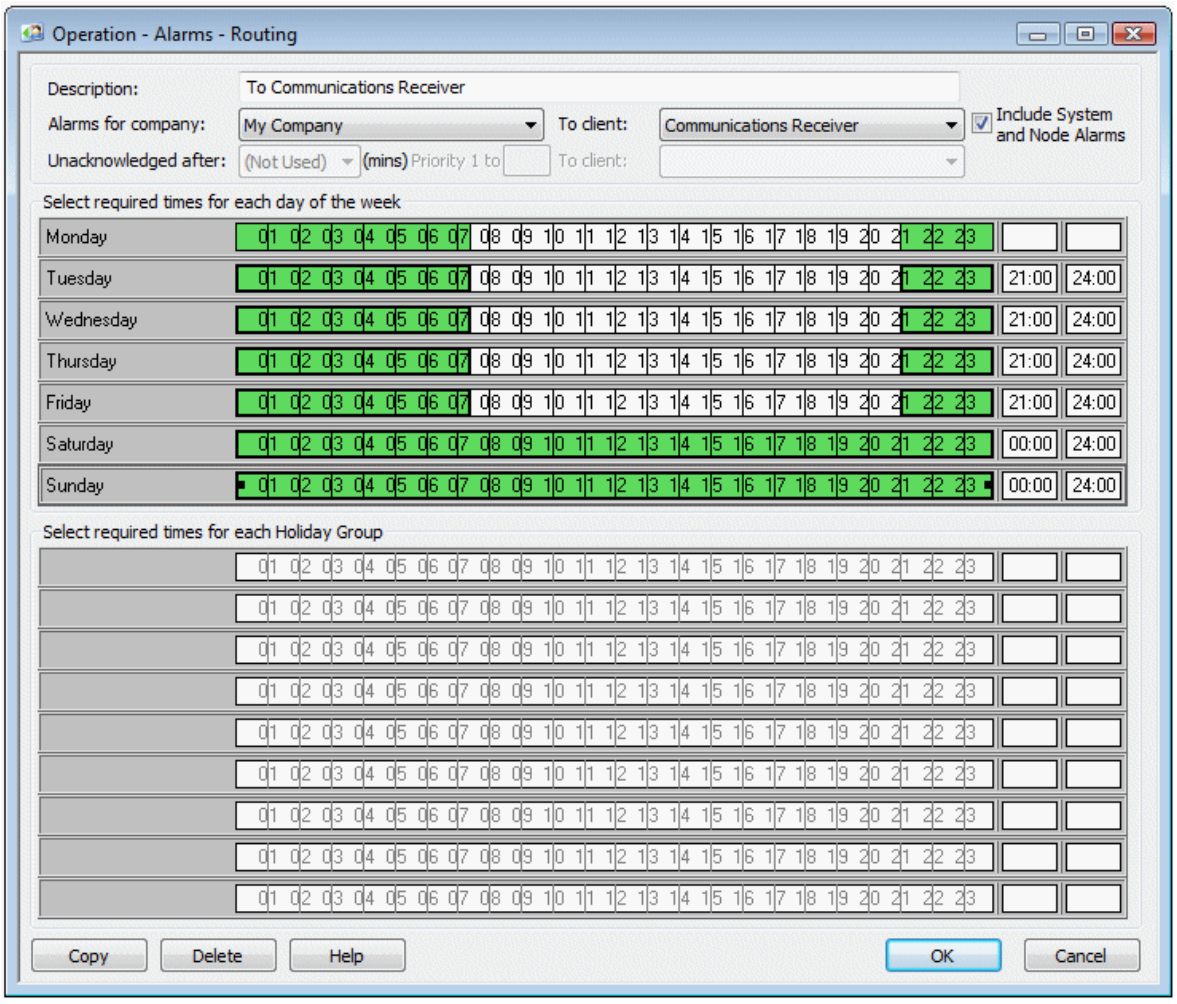
The following options are available:

- **Network Address** – Specify the IP address or network (DNS) name of the communications receiver.
- **Port Number** – Specify the port number of the communications receiver.
- **Account Number** – Details of any alarm sent to the communications receiver include the account number, which identifies the source of the alarm. The specified account number is used as the default for the "Setup/Device Groups/Intrusion Areas" screen, which is used for intrusion alarms. Reader alarms (see page 29) use the default account number. You can specify an account number for monitor point alarms (see page 29) in the "Install/Access Control/Monitor Point" screen.

  The Intrusion Areas screen also contains a read-only **Area Number**, which is unique to the area account number. The account number does not need to be unique to an area, but the combination of account number and area number is unique.
- **Send Zone Normal to Receiver** and **Send Area Arm/Disarm to Receiver** – Choose whether or not to send these messages to the communications receiver.
- **Enable Encryption** and **Passphrase** – If messages are to be sent encrypted, select **Enable Encryption** and specify the passphrase.

Step 10b – Set Up Alarm Routing

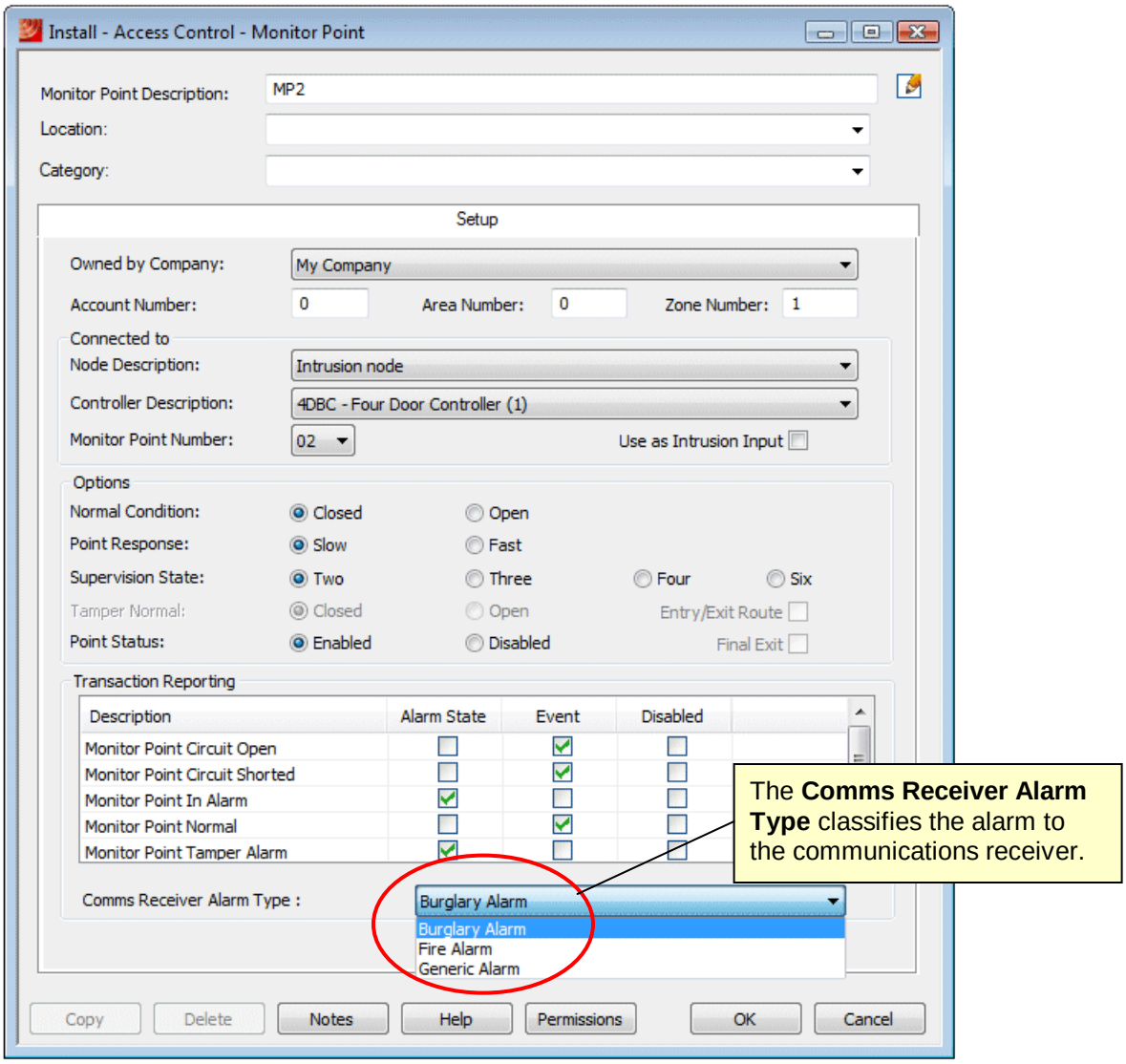
Route alarms to the communications receiver using the "Operation/Alarms/Routing" screen:



Select **Communications Receiver** in **To Client**, and choose the times to send alarms to the communications receiver.

Step 10c – Select an Alarm Type for each Monitor Point and Reader

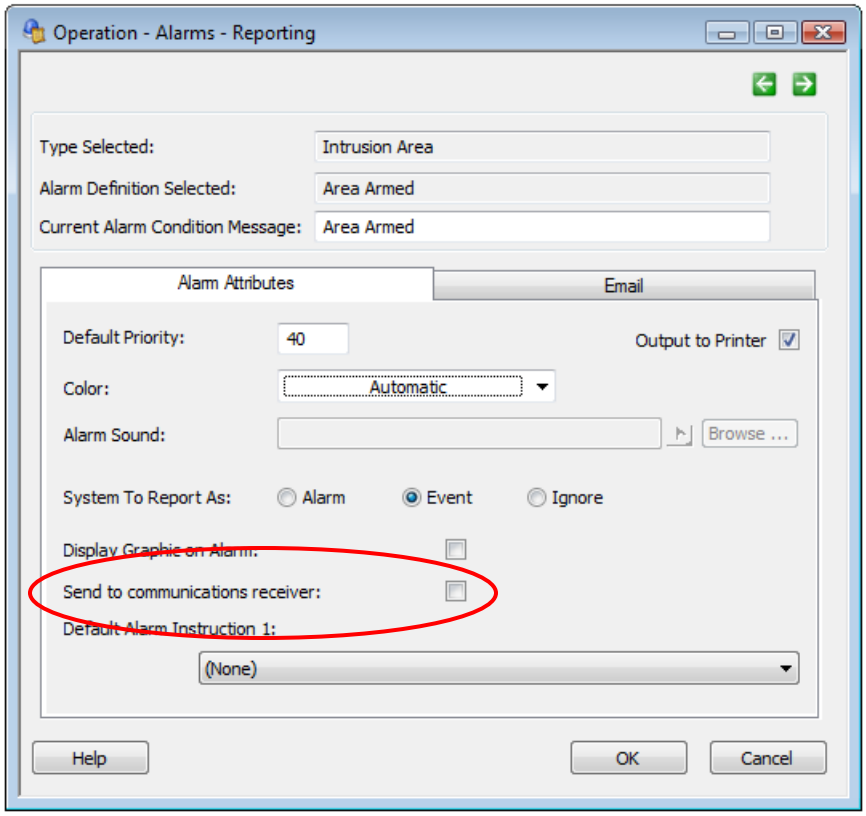
For each monitor point and reader, choose a **Comms Receiver Alarm Type**:



Note: The **Zone Number** field is available for each monitor point and reader. The **Account Number** and **Area Number** fields are available for monitor points only. These can be used to help an operator of a communications receiver to identify the location of the alarm.

Step 10d – Choose the Alarms/Events to Send to the Communications Receiver

For each message you want to send to the communications receiver, select **Send to communications receiver** in the "Operation/Alarms/Reporting" or "Operation/Alarms/Definitions" screen. The following shows an example.



Mapping of Symmetry Alarms to Communications Receiver Alarms

The following table shows the mapping between Symmetry alarms and DMP communications receiver alarms, and the type of information included with each alarm.

Note: The communications receiver and associated interfaces have not been evaluated by UL.

			Information Included						
	M2150 Message Generated by Symmetry Software	**Message Sent to DMP Receiver**	Account Number	Zone Number	Zone Description	Area Number	Area Description	User Name	User Number (IDS code)
Intrusion	Zone In Alarm	Zone Alarm	✓	✓	✓	✓	✓		
	Zone Normal	Zone Restore	✓	✓	✓	✓	✓		
	Zone Open Circuit Zone Closed Circuit	Zone Trouble	✓	✓	✓	✓	✓		
	Zone Tamper	Zone Fault	✓	✓	✓	✓	✓		
	Zone Bypass	Zone Bypass	✓	✓	✓	✓	✓	✓	
	Zone Reset	Zone/Area Reset	✓	✓	✓	✓	✓	✓	
	Area Armed (event)	Closing Report	✓			✓	✓	✓	
	Area Disarmed (event)	Opening Report	✓			✓	✓	✓	
	Area Late to Arm	Late to Close	✓			✓	✓		
Monitor Point	Monitor Point In Alarm	Zone Alarm	✓	✓	✓	✓	✓[1]		
	Monitor Point Closed	Zone Restore	✓	✓	✓	✓	✓[1]		
	Monitor Point Normal	Zone Restore	✓	✓	✓	✓	✓[1]		
	Monitor Point Tamper Normal	Zone Restore	✓	✓	✓	✓	✓[1]		
	Monitor Point Circuit Open	Zone Trouble	✓	✓	✓	✓	✓[1]		
	Monitor Point Circuit Shorted	Zone Fault	✓	✓	✓	✓	✓[1]		
	Monitor Point Tamper Alarm	Zone Fault	✓	✓	✓	✓	✓[1]		
Reader	Granted Access (event)	Door Access	✓	✓	✓			✓	✓
	At Wrong Door	Denied - Invalid Area	✓	✓	✓			✓	✓
	At Wrong Time	Denied - Invalid Time	✓	✓	✓			✓	✓
	All other Symmetry alarms	Generic text message							

Table 1: Mapping between Symmetry Alarms and DMP Communications Receiver Alarms

[1]The Area Description is the same as the Zone Description.

DMP SCS-1R Programming

The following settings were used during testing of the interface:

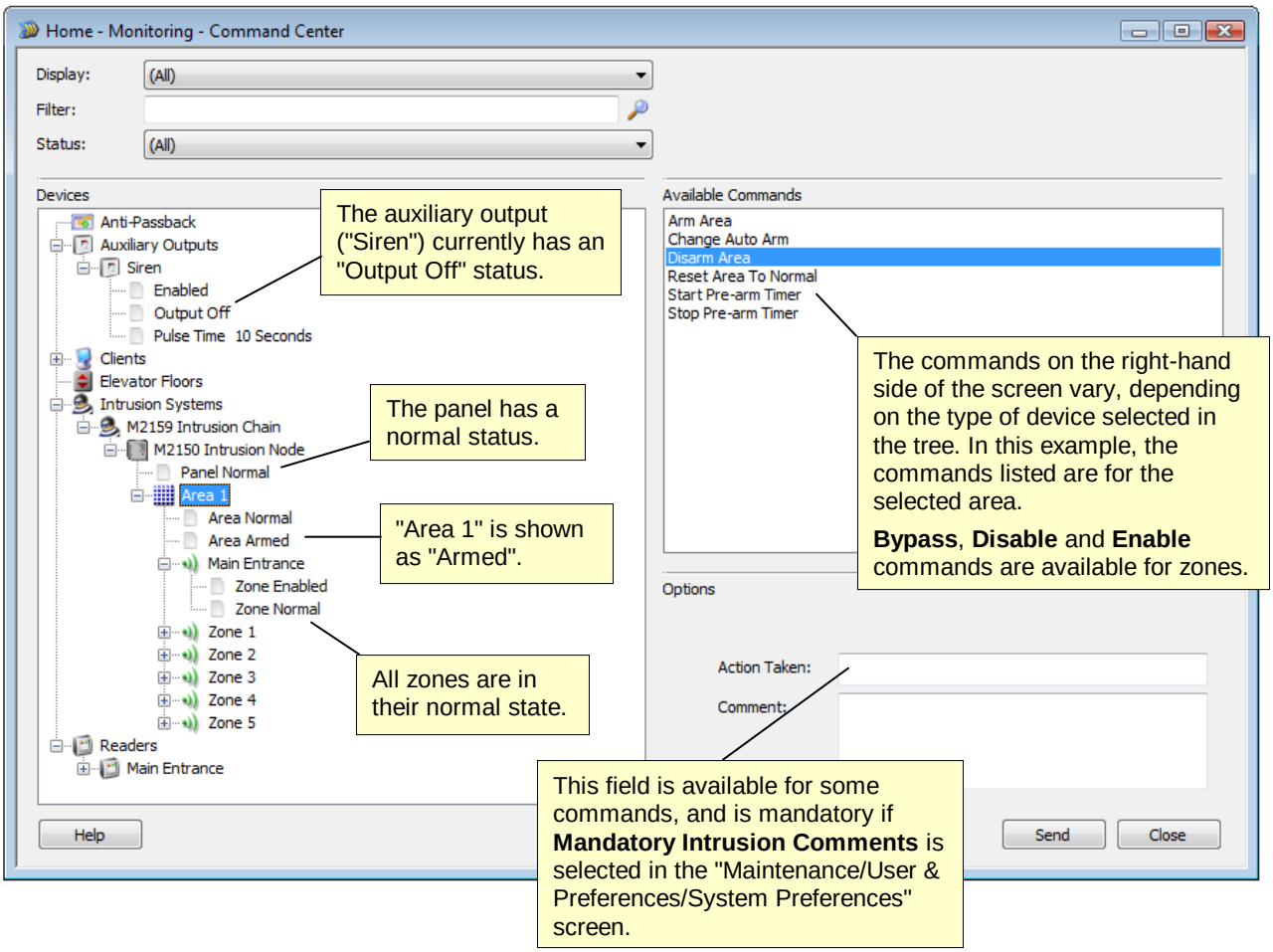
Line Type for Line Number 1 and 2 = Net (others set to NONE).
Test Interval = 1 minute
Acknowledge Timeout = 15 seconds
Line Number Length = 0
Zone Number Length = 3
User Number Length = 4
Baud Rate = 9600
Start Character STX
Area Format Decimal = YES
Retries to Failure = 5
Serial 3 Messages = YES
SCS-1R Printer Disable = YES
SCS-1R Print Always = NO
CRC Error Check = YES
Sequence Number = NO
Small "z" Zone Messages = YES
SCS-1R Time to Panels = NO
SCS-1R Hours from GMT = 0
Dialer Line Card Monitor = NO

Chapter 3: Monitoring and Controlling the Intrusion System

This chapter explains how to monitor and control an M2150/M4000 intrusion system from the Symmetry software.

Using the Command Center

You can use the "Home/Monitoring/Command Center" screen to monitor the current status of devices such as areas, zones, readers and auxiliary outputs. You can also access a wide range of commands to performs actions such as to arm and disarm areas, bypass zones and reset alarms. The following shows an example.



Note: Users are able to use only those commands that they have permission to use, as specified in the "Maintenance/User & Preferences/Command Roles" screen.

Area Commands

Commands available for an area include:

- **Arm Area** – Arms the area. This command arms the area immediately without starting the exit timer.

  When arming an area, a **Bypass zones in alarm** option is displayed if **Allow Zone Bypass when Arming** is selected in your user role. Selecting **Bypass zones in alarm** causes any zones that are in an alarm state to be automatically bypassed before the area is armed. This includes zones that are in a tamper state. An area cannot be armed if there is a zone that is in an alarm state that has not been bypassed. **Bypass zones in alarm** is available for scheduled and trigger commands, irrespective of the setting in your role.

- **Change Auto Arm** – Allows you to change the time of the next auto-arm of the area. Auto-arming is described on page 22.

- **Disarm Area** – Disarms the area.

- **Reset Area To Normal** – This command resets the alarm without disarming the area, and is intended to be used by personnel at a control center, after a guard has been dispatched to investigate the cause of the alarm. Before the command can be used, the zone alarm must have been acknowledged.

  Note: An area alarm can be cleared from the "Home/Monitoring/Alarms" screen only after disarming the area, or by sending this command if the area is still armed.

- **Start Pre-Arm Timer** – Starts the pre-arm period for an auto-arm of the area. The area arms at the next scheduled auto-arm time.

- **Stop Pre-Arm Timer** – Ends the pre-arm period for an auto-arm of the area. This does not cancel the auto-arm; it merely stops the actions that take place during the pre-arm period.

Zone Commands

Commands available for a zone include:

- **Bypass** – Prevents the zone from generating alarms. The bypass is cancelled when the area is next disarmed. You may want to bypass a zone if, for example, the zone is protecting a part of the building that will be occupied while the remaining zones in the building are armed.

- **Enable** – Cancels the effect of **Bypass** or **Disable**.

- **Disable** – Disables the zone until re-enabled. You may want to disable a zone if, for example, you suspect that the sensor is faulty.

Node Commands

The only command available for a node is **Lock Out Node** (M2150 only), which is used to prevent configuration changes in the node. Please refer to page 14 for further information.

Using the Intrusion Toolbar

The Intrusion Status toolbar, as shown below, provides status information about areas, zones and outputs. The toolbar can be displayed by selecting **Show Toolbar** in the "Maintenance/User & Preferences/Accounts" screen. From left to right, the toolbar provides the information shown in Table 2.

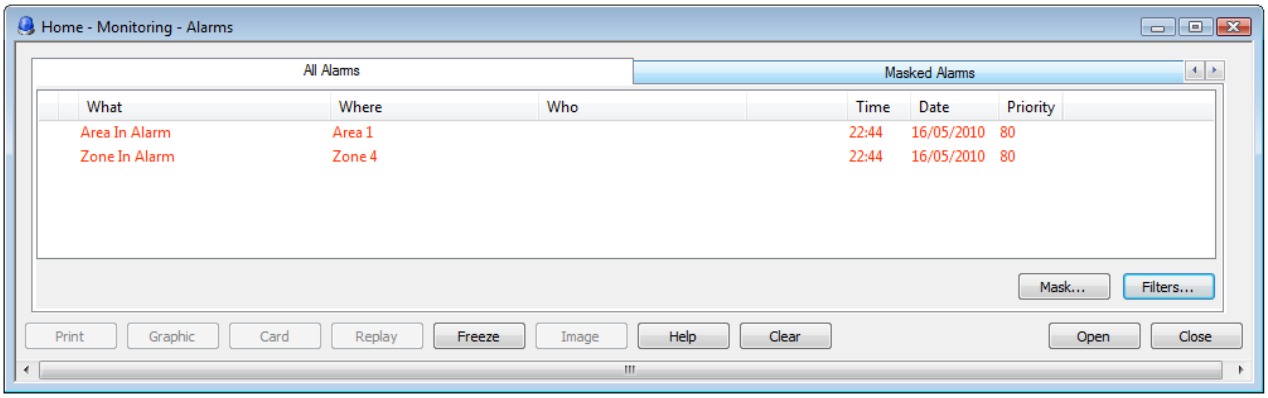
Icon	Meaning
	**Acknowledge Alarms** – Total number of unacknowledged alarms (from any source). The background is red when there is at least one unacknowledged alarm. Clicking the button displays the "Home/Monitoring/Alarms" screen.
	**Area Alarms** – Total number of areas that are currently in an alarm. An area alarm may occur only if the area is armed.
	**All Problems** – Total number of alarm, tamper, fault and panel offline conditions.
	**Areas Armed** – Total number of areas that are currently armed.
	**Areas Security Reduced** – Not applicable (only applicable to third-party intrusion systems).
	**Areas Disarmed** – Total number of areas that are currently disarmed.
	**Zone Alarms** – Total number of zones that are currently in an alarm condition.
	**Zone Tampers** – Total number of zones that are currently in a tamper condition.
	**Zone Faults** – Total number of zones that are currently in a fault or tamper condition.
	**Zones Disabled** – Total number of zones that are currently disabled.
	**Zones Bypassed** – Total number of zones that are currently bypassed.
	**Zones Force Armed** – Not applicable (only applicable to third-party intrusion systems).

Table 2: Icons in the Intrusion Status Toolbar

Note: Clicking any button other that the **Acknowledge Alarms** button opens the View/Command Center screen, with only the relevant objects displayed according to the button clicked.

Using the Alarms Screen

You can use the "Home/Monitoring/Alarms" screen to monitor and acknowledge alarms from the intrusion system. In the following example, Zone 4 has generated a "Zone In Alarm" alarm. Since Zone 4 is in Area 1, an "Area In Alarm" alarm is also generated.



Silencing an Alarm

The **Area in Alarm** siren (see page 19) can be silenced by sending a "Reset Area To Normal" command from the "Home/Monitoring/Command Center" screen or by disarming the area.

Clearing an Area Alarm

You can clear the "Area In Alarm" alarm by double-clicking the alarm and selecting **Clear**. Before you can clear an area alarm, you first need to:

1. Make sure that the zone that caused the alarm is in its normal state.

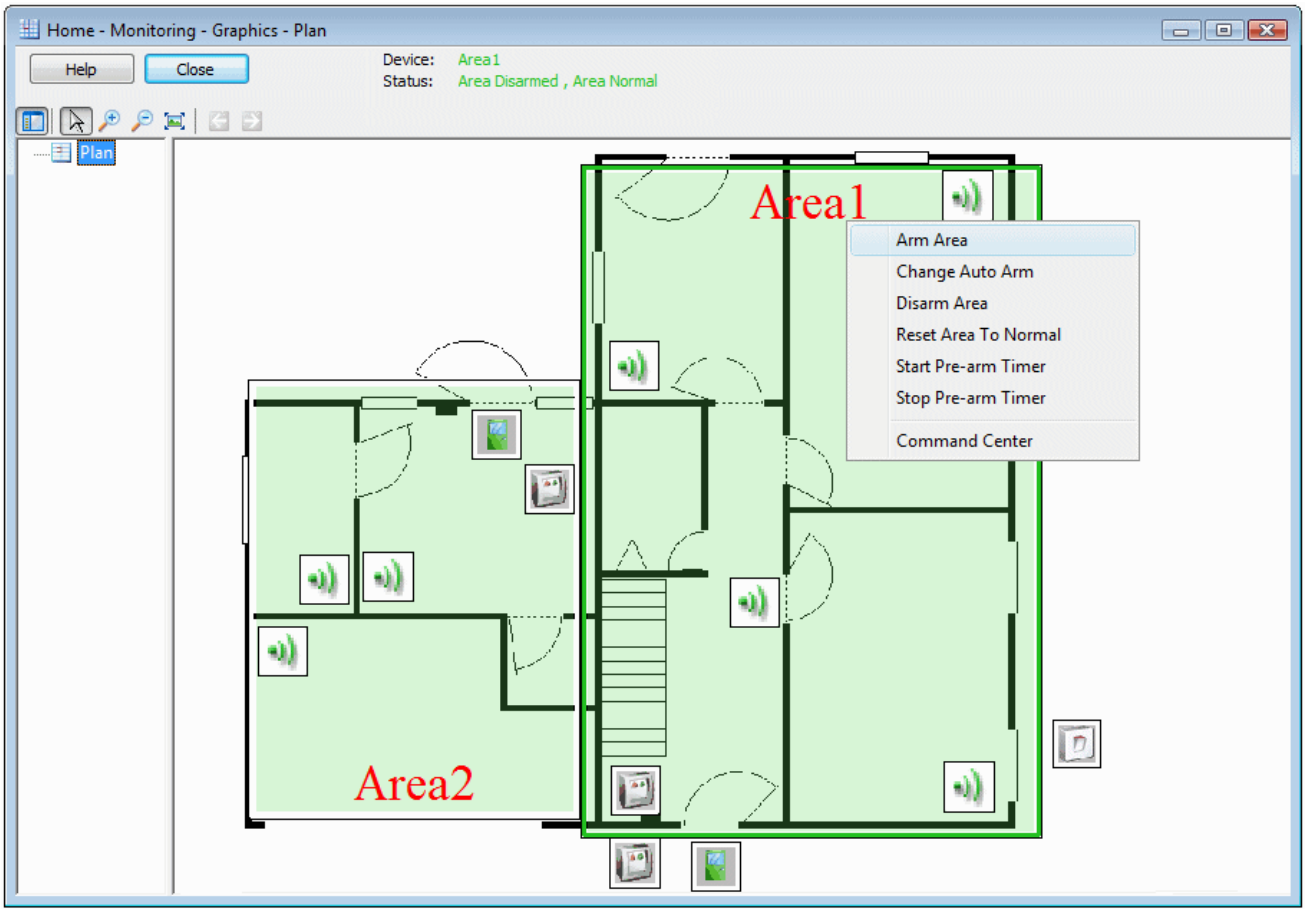
2. Disarm the area or send the **Reset Area To Normal** command from the Command Center (see page 32).

Using the Graphics Screen

You can use the "Home/Monitoring/Graphics" screen to monitor and control the intrusion system. The Graphics screen allows you to see any areas or zones that have an alarm, and send commands to perform actions such as to arm or disarm an area or bypass a zone.

The following example shows two areas (Area1 and Area2), and several readers and zones. The right-click menu shows the commands for Area1. Please refer to page 32 for details of the M2150/M4000 intrusion commands.

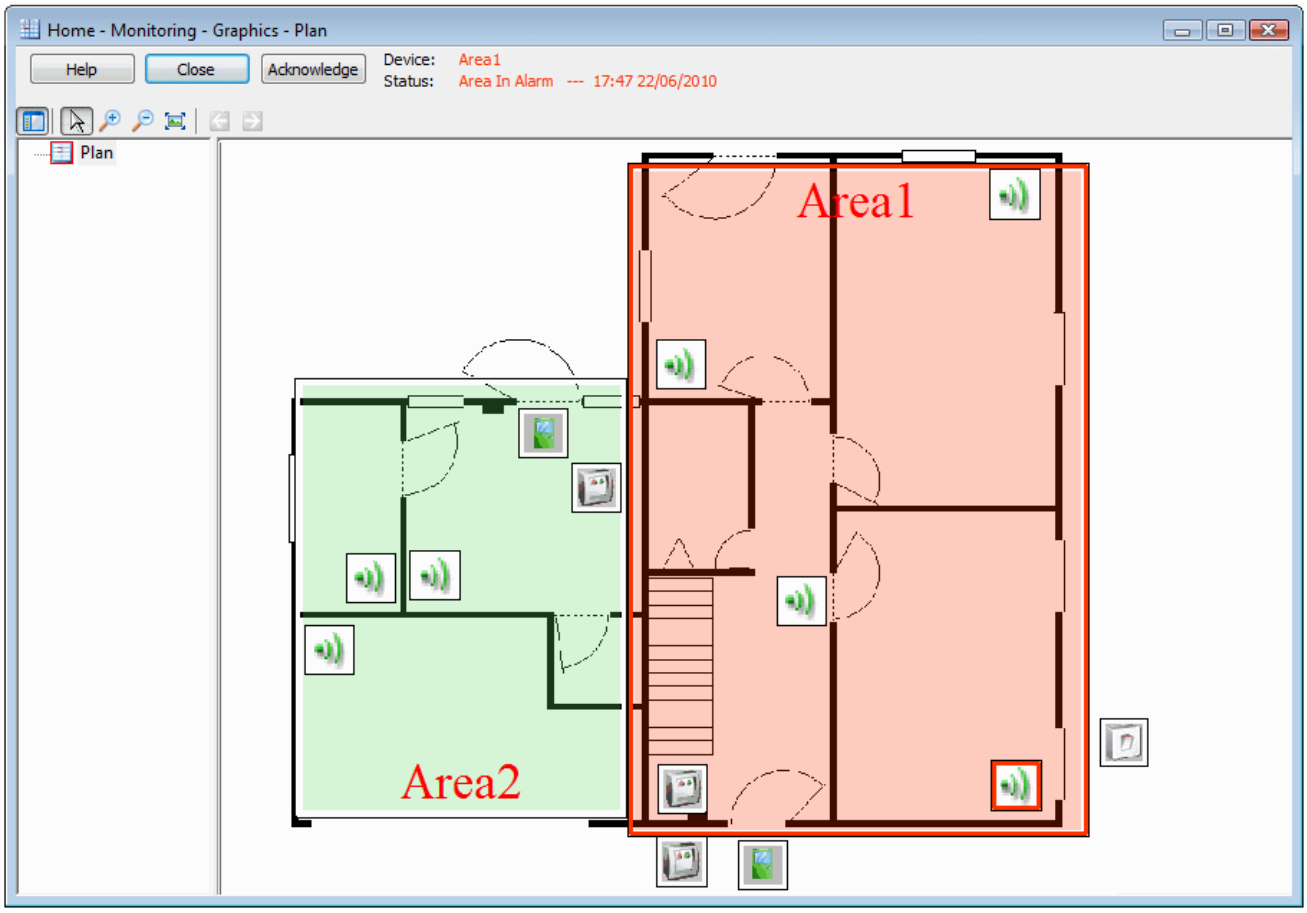
Note: An **Action Taken** prompt is displayed when for the **Bypass**, **Disable** or **Disarm** commands only if **Enable Comments on Graphic** is selected in the "Maintenance/User & Preferences/System Preferences" screen. Specifying the action taken is mandatory if **Mandatory Intrusion Comments** is selected in the "Maintenance/User & Preferences/System Preferences" screen.



The area near the top of the screen indicates the name and current status of a selected device. The color of the border of device icons, and the color of an area background also indicates the current status.

The following example shows that area and zone alarms have occurred. The **Acknowledge** button near the top of the screen allows you to acknowledge or clear an alarm for a selected device.

If an area has a sub-graphic defined (see page 20), double-clicking the area displays the sub-graphic.


Home - Monitoring - Graphics - Plan
Help
Close
Acknowledge
Device: Area1
Status: Area In Alarm --- 17:47 22/06/2010
Plan
Area1
Area2

Chapter 4: Using 843B and 844 Readers

This chapter explains how to use intrusion options at 843B and 844 readers (M2150 only).

Top-Level Menu

The top-level menu contain four options, as shown next. Press [#] to display each option in turn.

1. PRESENT CARD — This is the default prompt. ARMED is displayed if the system is armed.

2. ARM AREA — Allows you to arm one or more areas. See page 38.

3. DISARM AREA — Allows you to disarm one or more areas. See page 40.

4. AUTOARM TIME — Allows you to change the time of an auto-arm (see page 22).

5. NEW LOCKOUT — Allows you to start lock-out mode (see page 14). When lock-out mode is active, the option changes to ENTER LOCKOUT, which allows you to remove the lockout (requires entry of the lock-out code).

Arming Areas

To arm areas from an 843B/844 keypad:

1. 

   Press [#].

2. 

   Press [★].

3. 

   Present your card, or enter your IDS Code (set up in the "Home/Identity/Card Holders" screen) and press [★]. ENTER CODE is displayed if you start to enter an IDS code.

4. 

   This is displayed if the reader and you have access to more than one area. A flashing letter at the end of the line (e.g. "D") indicates the current status (see page 41).

   To arm all areas, press [★] followed by [#] and continue from step 6.

   To arm selected areas, press [#] and continue from step 5.

5. 

   The name of the first area is displayed.

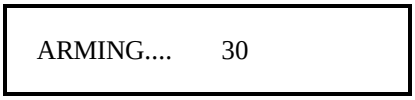
   To arm the area and display the next, press [★] followed by [#].

   To leave the area disarmed and display the next, simply press [#].

   Repeat this step for each area.

6. 

   This is displayed once you have scrolled through all areas. Press [★] to start the exit timer.

7. 

   The exit timer counts down if the reader is defined as being an entry/exit reader in an area you have armed.

   If applicable, exit the area.

8. 

   The area is armed. PARTLY ARMED is displayed if you have chosen not to arm the area that you are in.

Bypassing Zones while Arming

Bypassing a zone prevents it from generating alarms while the system is armed. If **Allow Local Zone Bypass using Reader** is selected in the "Install/Access Control/Node" screen, you can use the reader during the arming procedure to bypass zones that are active. A bypass is automatically removed when the zone is next disarmed.

FULLY ARM? !	A "!" is displayed if there are one or more zones active while you are attempting to arm the system.
Area1 !	This indicates that there are active zones in Area1.
Zone1 !	If you have chosen to arm an area that has active zones, the name of each active zone is displayed, followed by a BYPASS? prompt, as shown next.
BYPASS?	Press ★ to bypass the zone or # to exit the arming procedure.

Additional Messages when Arming

The following describes other messages you may see during the arming procedure.

NOT MONITORED	This indicates that the Symmetry server is currently offline from the node that the reader is connected to. In this condition, alarms will not be able to be monitored from Symmetry clients. This message can be generated only if **Check node is online before arming** is selected in the "Install/Access Control/Node" screen. Press ★ to continue.
ARM OFFLINE?	This prompts whether to arm the selected area(s), even though the Symmetry server cannot communicate with the node that the reader is connected to. This option is available only if **Allow local arming when node is offline** is selected in the "Install/Access Control/Node" screen. Press ★ to continue or # to exit.

Disarming Areas

To disarm areas from an 843B/844 keypad:

1. 

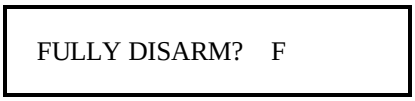
Press # **twice**. The reader may be bleeping if you set off the entry timer.

2. 

Press ★.

3. 

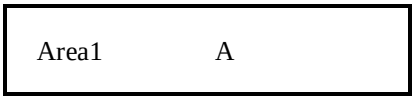
Present your card, or enter your IDS Code (set up in the "Home/Identity/Card Holders" screen) and press ★. ENTER CODE is displayed if you start to enter an IDS code.

4. 

This is displayed if the reader and you have access to more than one area. A flashing letter at the end of the line (e.g. "F") indicates the current status (see page 41).

To disarm all areas, press ★. No further input is required.

To disarm selected areas, press # and continue from step 5.

5. 

The name of the first area is displayed.

To disarm the area and display the next, press ★ followed by #. DISARMED is momentarily displayed.

To leave the area armed and display the next (if there is one), press #.

Repeat this step for each area.

6. 

This is displayed once you have scrolled through all areas. Press ★ to exit the menu or # to return to step 4.

7. 

Disarming an Area using an Access Control Transaction

If you have access rights to an arming/disarming reader (for normal access-control transactions), simply present your card to the reader and the area that the reader is in automatically disarms. Please see Example 2 on page 8 for further details.

Additional Messages when Disarming

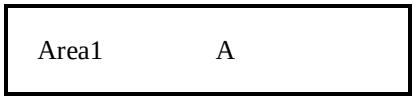
The following describes other messages you may see during the disarming procedure.

This is displayed if there was at least one zone alarm in an area you are disarming. Press ★ to show alarms or # if you do not want to see them.

If you continue with the disarming procedure, the name of each zone that has generated an alarm is displayed. Press ★ to display each zone in turn.

Viewing Area Status

The status of an area is indicated by a letter on the right-hand side of the display. In the following example, the status is indicated by the letter "A":



The meaning of each status is as follows:

A – Armed.

D – Disarmed.

E – Exit timer running/pending.

P – Partly armed.

F – Fully armed.

! – While arming: zone(s) active. While disarming: zone(s) caused alarms.

Chapter 5: Using the 884-v2 Reader

This chapter explains how to use the intrusion options on the 884-v2 reader (M2150 only).

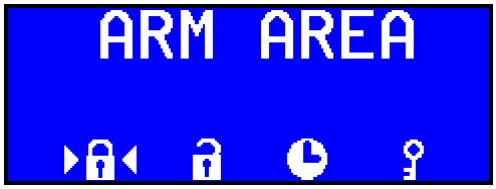
Introduction

The 884-v2 reader allows operators to operate M2150 intrusion systems. The reader displays status information and provides options for arming areas, disarming areas, changing the auto-arm time and setting lock-out mode.

Figure 5-1: 884-v2 Default Screen

The available options are represented by icons along the bottom line of the display. There are two methods of selecting an options:

- Simply select the hotkey button immediately below the icon on the keypad. This is the quickest method.
- Press the X button on the bottom-right of the keypad one or more times to select the required option, then press ✓. The selected option is indicated by an arrow on either side of the hotkey icon, and the name of the option on the screen. For example:



Note: When prompted, you must enter an Intrusion Detection System (IDS) code or present your card to access the intrusion options. The IDS code is set up in the "Home/Identity/Card Holders" screen.

Icons

The meaning of each icon that can appear on the display is given in the following table.

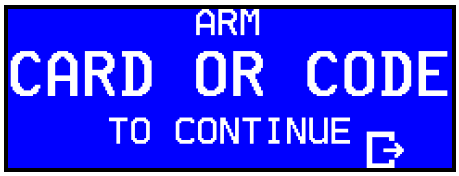
	Arm one or more areas. See page 44.
	Disarm one or more areas. See page 46.
	Change the time of an auto-arm. See page 48.
	Start or finish lock-out mode (see page 49). This is displayed when lock-out mode is active.
	Go back a step.
	Exit to the default screen.
	Display information such as alarms or zones to bypass.
	Cycle up through the options.
	Cycle down through the options.
	No external power is being supplied to the node.

Arming Areas

To arm areas from an 884-v2 keypad:

1. 

   Press .

2. 

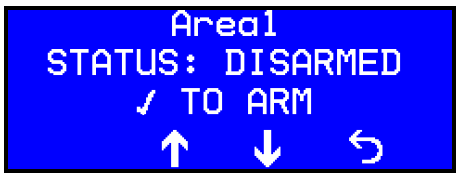
   Present your card, or enter your IDS Code and press ✓.

3. 

   This is displayed if the reader and you have access to more than one area.

   To arm all areas, press ✓ and continue from step 5.

   To arm selected areas, press x and continue from step 4.

4. 

   The name of the first area is displayed.

   To arm the area and display the next, press ✓.

   To leave the area disarmed and cycle up or down through the areas, simply press ↑ or ↓.

   Repeat this step for each area. Areas armed during this process are not listed.

5. 

   The exit timer counts down if the reader is defined as being an entry/exit reader in an area you have armed.

   If applicable, exit the area.

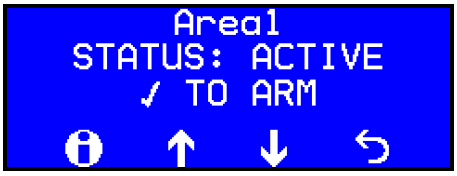
6. 

   The area is armed. PARTLY ARMED is displayed if you have chosen not to arm the area that you are in.

Bypassing Zones while Arming

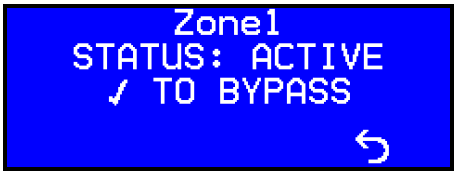
Bypassing a zone prevents it from generating alarms while the system is armed. If **Allow Local Zone Bypass using Reader** is selected in the "Install/Access Control/Node" screen, you can use the reader during the arming procedure to bypass zones that are currently active. A bypass is automatically removed when the zone is next disarmed.

STATUS: ACTIVE is displayed if there are one or more zones active while you are attempting to arm the system.



This indicates that there are active zones in Area1.

If required, you can press to view the names of the zones that are active.



If you have chosen to arm an area that has active zones, the name of each active zone is displayed.

Press ✓ to bypass the zone or not to arm the area.

After specifying which zones to bypass, the system starts the arming process.

Additional Messages when Arming

The following describes other messages you may see during the arming procedure.

This indicates that the Symmetry server is currently offline from the node that the reader is connected to. In this condition, alarms will not be able to be monitored from Symmetry clients.

Press ✓ to arm the system (available only if **Allow local arming when node is offline** is selected in the "Install/Access Control/Node" screen), or press x to exit.

This stops the user from arming the system, as the Symmetry server cannot communicate with the node that the reader is connected to. This screen is displayed only if **Allow local arming when node is offline** is turned off in the "Install/Access Control/Node" screen. Press x to exit.

Disarming Areas

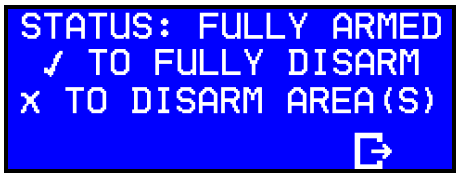
To disarm areas from an 884-v2 keypad:

1. 

   Press . The reader may be bleeping if you set off the entry timer.

2. 

   Present your card, or enter your IDS Code and press ✓.

3. 

   This is displayed if the reader and you have access to more than one area.

   To disarm all areas, press ✓. No further input is required.

   To disarm selected areas, press x and continue from step 4.

4. 

   The name of the first area is displayed.

   To disarm the area and display the next, press ✓. DISARMED is momentarily displayed.

   To leave the area armed and cycle up or down through the areas, press ↑ or ↓. Disarmed areas during this process are not listed.

   Repeat this step for each area.

   Press ↩ to exit.

5. 

   The default screen is displayed.

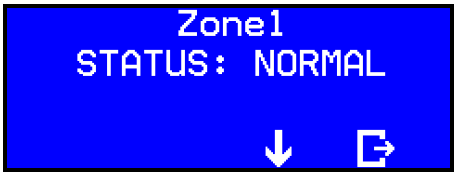
Disarming an Area using an Access Control Transaction

If you have access rights to an arming/disarming reader (for normal access-control transactions), simply present your card to the reader and the area that the reader is in automatically disarms. Please see Example 2 on page 8 for further details.

Additional Messages when Disarming

The following describes other messages you may see during the disarming procedure.

This is displayed if there was at least one zone alarm in an area you are disarming. Press to show alarms or if you do not want to see them.



If you press to show alarms, the name of each zone that has generated an alarm is displayed. Press to display each zone in turn.

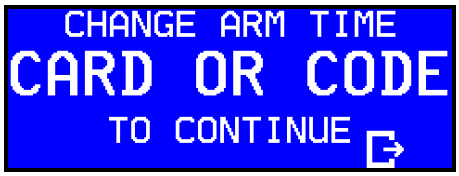
Changing the Auto-arm Time

This allows you to change the time of the next auto-arm (all subsequent auto-arm times are not affected). This option is available if **Allow local change to scheduled arming time** is set in the "Install/Access Control/Node" screen for the node that the reader is connected to. **Note:** You cannot change the auto-arm time if there is less than one minute to the time of the next auto-arm.

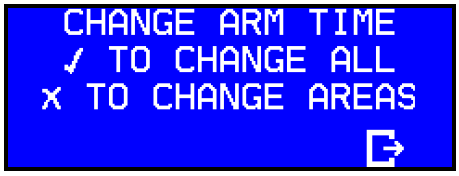
To change the time at which the system automatically arms:

1. 

Press .

2. 

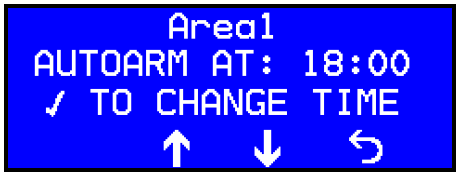
Present your card, or enter your IDS Code and press ✓.

3. 

This is displayed if the reader and you have access to more than one area.

To change the arm time for all areas, press ✓ and continue from step 5.

To change the arm time for selected areas, press x and continue from step 4.

4. 

The name of the first area is displayed.

To change the arm time for the area, press ✓ and continue from step 5.

To leave the arm time for the area and cycle up or down through the areas, press ↑ or ↓.

Press ↩ to exit.

5. 

Enter the auto-arm time and press ✓.

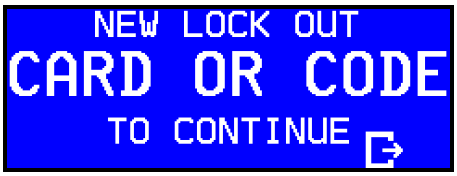
If you are changing the auto-arm time for one area out of several, continue from step 4.

Setting and Unsetting Lockouts

To set a new lockout:

1. 

Press ⚿.

2. 

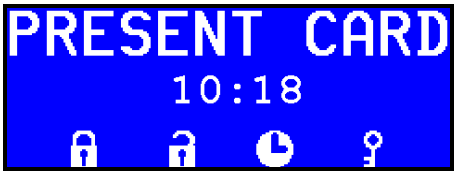
Present your card, or enter your IDS Code and press ✓.

3. 

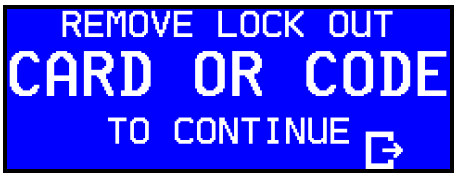
Enter a 5 digit lockout code and press ✓.

Note: Make sure you remember the code; you will need it to unset the lockout.

To unset a lockout:

1. 

Press ⚿.

2. 

Present your card, or enter your IDS Code and press ✓.

3. 

Enter the lockout code as entered when you set the lockout and press ✓.