REMOTE *LINK*

Help File

Remote Link Help

Exported on 06/18/2025

Table of Contents

2 Welcome to Remote Link

Remote Link offers an interface that is simple to navigate and provides easy access to the information you need. Remote Link can be used with the following panels:

- XR Series Control Panels
- XT30/XT50 Control Panels
- XTL Series Control Panels
- Com Series Communicators

2.1 Remote Link Quick Reference

- To close the account file and all open windows, select **File > Close Panel**.
- To close all open windows, disconnect from all panels, and exit Remote Link, select **File > Exit**.
- To switch between open windows or organize them in Remote Link, select **Window**. To quickly switch between windows, press **Ctrl + Tab**.
- To apply all current changes in a window when creating or editing information, select **Apply**.
- To save any changes you have made in a window and to close the window, select **OK**.
- To access context-sensitive help for the window currently open in Remote Link, press **F1**.

2.2 Copyright Statement

The information in this help file is subject to change without notice. The software program described herein is furnished under the included license agreement (LT-1920). The software may be used or copied only in accordance with the terms of the agreement.

No part of this document may be reproduced or transmitted in any form or by any means, electronic, or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the express written permission of Digital Monitoring Products, Inc.

- IBM is a trademark of International Business Machines Corporation
- Windows™ is a trademark of Microsoft® Corporation
- Unless otherwise noted, all names of companies, street addresses, and persons contained herein are part of a completely fictitious scenario and are designed solely to document the use of Remote Link

Remote Link™ © 2025 Digital Monitoring Products, Inc.

2.3 Related Documentation

Before using Remote Link, read and familiarize yourself with the required panel documents. All programming and installation guides are available on DMP.com and can be downloaded for free in pdf format. For more information, refer to the following resources:

- DMP Technical Documents: DMP.com/technical-documentation
- Contact Information: DMP.com/company/contact-support

3 Install Remote Link

This section covers how to install Remote Link, including system requirements, installation, and logging on and off. Before installing Remote Link, review the system requirements and additional documentation in this section.

3.1 System Requirements

Before installing Remote Link, ensure your computer system meets the minimum specifications. Ensure you have Administrator permissions or select **Run as Administrator** to install Remote Link software.

> ℹ **Note:** Although Remote Link is compatible with versions of Windows that have surpassed their end-of-support dates, DMP recommends using versions of Windows that currently have mainstream or extended support. For more information, refer to Microsoft's Windows lifecycle documentation.

Operating System	Minimum Requirements
Windows 2000	Pentium 150 Mhz processor 64 MB RAM
Windows XP	Pentium II 300 MHz processor 128 MB RAM
Windows Vista	1 GHz processor 1 GB RAM (32-bit) 16 GB disk space available DirectX 9 Graphics
Windows 7	1 GHz processor 1 GB RAM (32-bit) 16 GB disk space available DirectX 9 Graphics
Windows Server 2008 R2	1 GHz processor 1 GB RAM (32-bit) 16 GB disk space available DirectX 9 Graphics
Windows 10	1 GHz processor 1 GB RAM (32-bit) 16 GB disk space available DirectX 9 Graphics

3.1.1 Additional Requirements

- 800 x 600 or higher resolution monitor

- CD-ROM drive
- One available COM port if connecting to an SCS-1R or SCS-105, or directly connecting to a panel. To use the passthru feature, ensure you have COM ports available.

3.1.2 Using a Virtual Environment

Remote Link may be installed and used in a virtual environment, provided that the virtual machine is running an operating system listed in the System Requirements table. When running in a virtual environment, additional configuration of the virtual machine's TCP and serial ports may be required.

3.2 Install on Windows

This section outlines specific steps to install and use Remote Link on Windows. A Workstation Administrator should perform installation of Remote Link and Link Server. A Workstation Administrator should also perform any version upgrades to Remote Link or Link Server.

3.2.1 Registry Keys

Once Remote Link and all modules are installed, the Workstation Administrator should give Remote Link Administrators Full Control access to modify the DMP key shown and its sub-keys. An operator does not require any additional registry privileges. The primary registry key that Remote Link uses to store application data is: \HKEY_LOCAL_MACHINE\SOFTWARE\Digital Monitoring Products\

3.2.2 Database Setup

If a Link Administrator is not a Workstation Administrator, then the Link database should not be located in a system drive, such as C:\ or C:\Program Files. Locating the Link database in a non-system directory allows the Link Administrator to manage and move the database without requiring the assistance of the Workstation Administrator.

The Workstation Administrator should grant Link Administrators and Link Operators full access to the database folder (and sub-folders) and the Link installation folder (and sub-folders). This should be done irrespective of the database location.

3.2.3 Link Server

Link Server allows multiple Remote Link client workstations to use a single database. After Link Server is installed by a Workstation Administrator, it may be used in day-to-day operation by a Link Operator.

The primary component that differentiates Link Server from other Link installations is the DBISAM Database Server, a SQL database service. Once Link Server is installed, the DBISAM Database Server should automatically start when the workstation is started. A Workstation Administrator can start and stop the service using the Services tool. A Link Operator should not be able to stop the service. All Link Operator workstations that run Remote Link should be able to establish a TCP/IP connection to the DBISAM Database Server address and port.

3.3 System Connection Options

To use Remote Link, ensure you have a connection to the panel. For information about configuring software connection options, refer to Configure Remote Link Options and Manage Panels. Select one of the following hardware configurations:

- **SCS-1 / SCS-105:** Communicate through a receiver using dial-up.
- **Network (standard)**: Connect to a panel over a network. The workstation can be connected to a panel on the same LAN or an external LAN. Connection to a panel on an external LAN requires that port forwarding is enabled on the panel's network.
- **Network (Ethernet):** Connect directly to the panel with an Ethernet cable. This method creates a temporary LAN between the panel and Remote Link workstation.

> **ⓘ Note:** This connection method requires advanced network configuration. Use standard connection methods when possible.

- **Direct:** Connect directly to the panel with a Model 399 cable.
- **Modem:** Connect to the panel with a computer modem.

> **ⓘ Note:** Use this method only when connecting directly to a modem. To connect to a receiver with a phone line, select **SCS-1/SCS-105**.

- **Modem Special:** Connect to the panel with a computer modem when a slow, constant baud rate is required to maintain connection data integrity.
- **Cellular:** Connect to the panel over cell. This method requires that the Remote Link workstation is connected to a network.

3.4 Safeguarding Your Remote Link Database

Your Remote Link database contains your subscriber account information, password information, and other valuable data. Protect this information by performing regular database backups.

3.4.1 Location

To locate the Remote Link database, select **System > Configure > Remote Link**, then open the **Database** tab. The **Database Location** field displays the path to your database. If you would like to store your Remote Link database in a different location than the default folder, change the location before setting up any accounts.

> ℹ **Note:** Do not attempt to move an existing database by changing the location listed in the **Database Location** field.

If you change the location listed in the **Database Location** field without first moving the database manually, **Do you wish to create a new database?** displays. If you select **OK**, Remote Link creates a new database at the location that you just assigned and ignores the previous database. This means you will not have access to any account information and configurations settings from the previous database.

> ℹ **Note:** If you are using Remote Link on a computer connected to a network, run Remote Link from your local hard drive instead of a network drive. Remote Link accesses the database faster if it is located on the local workstation. Unless Link Server is installed, only one workstation at a time may use a Remote Link database.

3.5 Log ON/OFF

Before using Remote Link, log into the program with a username and password. When you open the program, the **Remote Link Login** window automatically displays. To log off then log on with a different user, go to **System > LOG ON/OFF**. To prevent unauthorized system access, DMP recommends changing default usernames and passwords for all software.

3.5.1 Default Remote Link Login

Username: **new**

Password: **new**

4 Configure Remote Link Options

Before adding operators or panels, ensure you configure global Remote Link settings, such as connection options, receivers, and databases, as needed.

4.1 Receiver Tab

The **Receiver** tab allows you to configure receivers used with Remote Link. This section covers how to configure receiver options and settings for specific receiver models.

4.1.1 Configure Receiver Options

To access the **Receiver** tab, go to **System > Configure > Remote Link > Receiver**. After configuring the tab, select **OK** to save your settings.

4.1.2 Select the Receiver Model

In **Model**, select your receiver model.

4.1.3 Configure Communication Options

To automatically configure communication, select **Auto**. To manually configure communication, complete the following steps:

1. In **Communication Options**, go to **COM Port** and select the communications port connected to the receiver from the drop-down menu. The SCS-1R can be configured when using the SCS-150 Processor Board.

> ℹ️ **Note**: Ensure you select a setting that does not interfere with your mouse, modem, or any other device on your computer. The COM Port cannot be used for any other purpose while Remote Link is running.

2. In **Baud Rate**, set your baud rate to the same setting as your receiver. The default setting is **9600 baud**.
3. In **Dial Out Line #**, enter the number of the line card that your current receiver will use to dial out.
4. For any receiver except the SCS-150 that you wish to tone dial, select **Tone Dial**. To pulse dial, clear **Tone Dial**.

> ℹ️ **Note:** The SCS-1R always pulse dials, regardless of this setting.

4.1.4 Configure General Options

Available options differ by receiver type. Configure the following options as needed:

1. In **Areas**, select which reporting format you want Remote Link to communicate with panels.
    - **Bin:** 2-character binary mode. Use this mode with SCS-105 Receivers.
    - **Dec:** 2-character decimal mode. Select this mode if the SCS-1R Receiver has been programmed to require Decimal mode.
2. In **Start Character**, select the appropriate option and enter the character programmed in the LSU Host Configuration in the field next to the dropdown.
3. If the SCS-1R Receiver CRC option in the LSU Host Options is set to **YES**, select **CRC**.
4. If the Sequence Numbers option in the SCS-1R Receiver LSU Host Setup is set to **YES**, select **Sequence Numbers**.

4.1.5 Configure Lengths

Configure the following lengths for specific portions of messages sent to the receiver:

1. In **Line#**, select the number of digits assigned to report the line number.
2. In **Zone#**, select the number of digits assigned to report a zone number. This number should correlate with the number of digits of the zones that report to the panel.
3. In **User#**, select the number of digits used to report a user number. For SCS-1R receivers, match the User number programmed in the Host setup programming on the receiver.

4.1.6 Set Up Hardware Receivers

The SCS-1R Receiver is a rack-mountable receiver that accepts up to eight line cards. For more information, refer to the SCS-1R Installation Guide (LT-1037).

The SCS-105 receiver is a single line receiver that acts as an external modem, allowing you to communicate with a single alarm panel over a standard telephone line. For more information, refer to the SCS-105 Installation Guide (LT-0153).

4.1.7 SCS-105 Firmware Requirements

To be compatible with Remote Link, the SCS-105 Receiver requires firmware Version 204 or higher. If your SCS-105 has firmware lower then Version 204, contact DMP Customer Service for an SCS-105 Firmware Update kit. If you are not sure which revision level your SCS-105 is currently running, complete the following steps:

1. Remove power from the SCS-105 and disconnect all cables.
2. Open the front of the SCS-105 by removing the two machine screws.
3. Gently tilt the SCS-105 face down and hold the processor board as it slides out.

The SCS-105 firmware chip is located about two inches above the internal speaker. The firmware version number is on a label on top of the chip.

4.1.8 SCS-1R System Configuration

The SCS-1 System Configuration window allows you to configure Remote Link to communicate through an attached receiver. If you are communicating with panels through either an SCS-1R or SCS-105 receiver, complete the following steps:

1. Go to **System > Configure > SCS 1 System**.
2. Enter information in the following fields:
   - **System Number:** If your monitoring center has more than one receiver, enter the number of the appropriate receiver.
   - **Company Name:** Enter the name of the company operating the central station receiver.
   - **Receiver Key:** The Receiver Key is a number that the receiver uses as a password to confirm its identity to panels. Enter the number that you will use as a key to identify the receiver.

> ℹ **Note:** Record the receiver key and store it in a secure location for future reference.

If the key numbers programmed into the panel and the receiver match, the receiver and the panel will communicate. If the numbers do not match, you will receive an Invalid receiver number error.

4.1.9 Line Configuration

Go to **System > Configure > SCS 1 Line**. Complete the following steps to configure each line card used in the SCS-1R Receiver:

1. In **Line Number**, enter the number of the communication line assigned to the line card in the SCS-1R Receiver that you are programming. Enter a single digit from **1 to 9**.
2. In **Line Type**, select one of the following communication line types for the receiver:
    • Select **None** to clear all programmed information for the line prior to programming.
    • Select **Multiplex (MPX)**, if you are using multiplex communication over a polled communication line.
    • Select **Digital Dialer (DD)** if you are using Digital Dialer for communication over standard telephone lines.
    • Select **DDMX** if the line card is configured for multiplex or Digital Dialer accounts. You may have up to **128 DDMX** accounts on one line card.
    • Select **ASYNCH** if the line card is configured for asynchronous network communications.
3. In **Phone Number**, enter the phone number of the telephone line connected to the receiver.
4. In **Billing Number**, enter the billing number that the telephone company has assigned to the telephone line connected to this line card.
5. In **Comment**, if necessary, enter any comments that might assist you in billing or system maintenance.
6. Select the checkboxes next to the number that corresponds to each multiplex account connected to this line card.

4.2 Modem Tab

Use the **Modem** tab to configure Remote Link to connect to a panel that has a modem installed or when connecting to an XR Series panel for programming at 2400 baud through the panel dialer.

To access the **Modem** tab, go to **System > Configure > Remote Link > Modem**. After configuring the tab, select **OK** to save your settings. Complete the following steps to configure Modem options:

1. Go to the **Communication Options** section.
2. In **COM Port**, select the **COM Port** that is connected to your local computer modem.
3. In **Baud Rate**, select the baud rate for Remote Link to communicate with the computer modem. The default setting is **9600 Baud**.
4. In **Flow Control**, select the flow control option recommended by your modem manufacturer. The default setting is **Hardware**. If the modem does not operate correctly with the default Hardware setting, select **Xon/ Xoff** for software flow control. If neither setting operates correctly, select **None**. For more information, refer to your modem documentation.
5. Select **Tone Dial** to enable tone dial. Clear **Tone Dial** to enable pulse dial.
6. Go to the **General Options** section.
7. In **Dial Timeout**, enter the length of time Remote Link waits for the XR Series panel to pick up. Enter a range from **1 to 255** seconds. The default is **60** seconds.
8. If an initialization string is required for a standard modem connection, enter the string in **Modem Initialization String**. The string can be up to 32 characters.
9. If an initialization string is required for Modem Special connection, enter the string in **Special Initialization String**. The string can be up to 32 characters long.

> ℹ **Note:** Only one initialization string can be used. Select the correct one for your operation. Refer to Panel Information in the appropriate panel programming guide.

4.3 Database Tab

The **Database** tab allows you to change the location where Remote Link stores data on your computer's hard drive. It also allows you to backup and purge your database, merge another database into the existing one, or import your Remote Access database into Remote Link. You may move your database to a folder on your computer hard drive, or to any connected network drive.

> ⓘ **Note:** Before performing any database maintenance function, it is recommended that you backup the Remote Link database folder to prevent possible data loss.

4.3.1 Configure a Database

> **ⓘ Note:** When using Remote Link with Microsoft SQL Server, ensure all backup and repair operations are performed by the database administrator using SQL Server management tools. Remote Link does not perform these operations.

To access the **Database** tab, go to **System > Configure > Remote Link > Database**. After configuring the options in the following steps, select **OK** to save your settings.

Select a Database Location

To change the default database location, complete the following steps:

1. Select **Require Admin Login for Database Update** to require operators to have Administrator privileges to update the database location,
2. To select a new location for the database, go to **Database Location**, then select **More**. Select a folder for the database, then select **OK**. The default database location is **C:\Link\Db**.

Backup the Database

To avoid potential data loss, backup your Remote Link database regularly.

> **ⓘ Note:** Only a Remote Link Admin operator can backup the database.

To backup the database, complete the following steps:

1. Go to **Backup Options** and select **Options**.
2. In **Backup Location**, select **More** and double-click the directory to select it. To create a new folder, append the folder name on the end of the path. For example, C:\Link\backup_db.
3. Select **OK**. If creating a new folder, a dialog displays to confirm that you want to create the directory. Select **Yes**.
4. Select **Remind me to backup after** to set a backup reminder, then enter a number of days in the days field.
5. Select **Backup** to immediately backup the database. When the backup has completed, select **OK**.

Merge Databases

Merge allows you to combine another Remote Link database with an existing database.

> **ⓘ Note:** Only a database located on a local or network drive can be merged. A database located on a remote server cannot be merged. The Merge option is not available if using Remote Link with the SQL Server module. If an account being merged has the same receiver and account number as one in the existing Remote Link database, an error message displays and the account is not merged.

To merge databases, complete the following steps:

1. Go to **Merge Database**.
2. Select **Merge**.
3. Select **More** to choose a database to merge into the current database. Double click the database folder, then select **OK**.

4. Select **Merge**. The **Result Log** displays the results of the merge.

Purge the Database

Occasionally purging your database of old data can improve Remote Link performance, decrease the amount of time it takes to backup a database, and reduce storage space taken up by unnecessary files. If necessary, print the Activity, Acknowledged Messages, or Events lists (Advanced Reporting add-on module) before purging the database.

To purge databases, complete the following steps:

1. Go to **Purge Options**.
2. In **Start Date**, select the beginning of the purge range.
3. In **End Date**, select the end of the purge range.
4. To purge activity logs, select **Activity**.
5. To purge acknowledged message logs, select **Acknowledged Messages**.
6. To purge events (Advanced Reporting add-on module), select **Events**.
7. Select **Purge**.
8. A dialog displays to confirm your decision. To purge the database, select **Yes**. When the purge operation is complete, select **OK**. Repeat this step for each selected purge option.

Repair a Database

Databases may be damaged if your computer experiences a power outage or a hardware or software problem that causes Remote Link to stop unexpectedly. The Repair feature attempts to repair corrupted account information, activity, panel programming, and configuration files in your Remote Link database.

> ℹ **Note:** When using Remote Link with Microsoft SQL Server, ensure all backup and repair operations are performed by the database administrator, using SQL Server management tools. Remote Link does not perform these operations.

To repair a database, complete the following steps:

1. Close **Remote Link**.
2. Go to **Start > Programs > Remote Link**.
3. Select **Repair Database**.
4. A log window displays files being repaired. After Remote Link restarts, log in with your credentials.

Restore a Database

> ℹ **Note:** When using Remote Link with Microsoft SQL Server, ensure all backup and repair operations are performed by the database administrator using SQL Server management tools. Remote Link does not perform these operations.

Automatically Restore a Database

The Restore from Backup window automatically prompts you to restore your database if Remote Link determines that the data is corrupted and needs to be restored. To automatically restore a database, complete the following steps,

1. To restore the database from a .cab backup file, select **Use old backup file (.cab)**.
2. Next to **Restore from file**, select **More**, then select the database backup (.bkp) file.
3. Next to **Restore Location**, select **More**, then select your Remote Link database folder.
4. Select **Restore**. After the database restores, select **OK**.
5. After Remote Link restarts, log in with your credentials.

Manually Restore a Database

If Remote Link doesn't prompt you to restore a damaged database, manually restore it by completing the following steps:

1. Close Remote Link.
2. Go to **Start > Programs > Remote Link**.
3. Select **Restore Database**.
4. To restore the database from a .cab backup file, select **Use old backup file (.cab)**.
5. Next to **Restore from file**, select **More,** then select the database backup (.bkp) file.
6. Next to **Restore Location**, select **More,** then select your Remote Link database folder.
7. Select **Restore**. After the database restores, select **OK**.
8. After Remote Link restarts, log in with your credentials.

4.4 Other Tab

The **Other** tab allows you to configure general Remote Link options like time zone, pass through, auto account archive, and admin reader settings.

4.4.1 Configure Other Settings

To access the **Other** tab, go to **System > Configure > Remote Link > Other**. After configuring the tab, select **OK** to save your settings.

Configure General Options

In Time Zone, select the time zone of the Remote Link workstation.

In Logging Threshold, select one of the following issue types to record in the Remote Link error log file:

> ℹ️ **Note:** All messages with a severity equal to or greater than the threshold setting are logged. For example, selecting Warning will log Warning, Exception, and Critical events.

- **Debug:** Detailed information that does not indicate an error, including communication strings. Debug logging is verbose and significantly increases the size of the log file.
- **Information:** General information detail about program operations.
- **Warning:** Default value. An error condition such as minor communication problems, timeouts, etc. that can be handled without operator intervention. A warning message may or may not be displayed to the operator.
- **Exception:** Requires operator action to recover or restore normal operation such as an invalid COM Port selection for the receiver.
- **Critical:** Causes Remote Link to stop responding. For example, access violations or database corruption.

Select any of the following checkboxes as needed:

- **Enable Debug Logging:** Allow all communication between the panel, receiver, and Remote Link to be saved in the debug table for diagnostic purposes. When this feature is disabled, communication is not visible on the diagnostics screen.
- **Enable Alarm/Event Monitoring:** Display panel alarms and system event messages in the Alarm List. Disable this feature when Remote Link is used for programming purposes with a shared database without displaying panel messages. If using the Alarm/Event add-on module, enable this option.
- **Exit App After:** Enable and edit the number of minutes of inactivity by the logged in user before the application displays a warning to close the application. Once the Warning dialog box displays, the user will have one minute to choose Yes to extend their Remote Link session.
- **Update Time Default:** Enables the Time Update checkbox in Panel > Send to be automatically selected. This allows a time update to be sent to the panel anytime programming is sent.

Configure Pass Through Options

Use pass through mode when passing reports through Remote Link to a host automation computer.

1. Go to **Pass Through Options**.
2. In **Mode**, select **Pass Through**.

3. In **Outgoing COM Port**, select the COM port that Remote Link will use to communicate with your host automation computer.
4. In **Baud Rate**, leave the rate defaulted at **9600** Baud unless your automation software requires a different setting.

Configure Auto Account Archive

Auto Account Archive allows panel account programming to be automatically saved separately when connecting to a panel with programming that is different than the programming on file.

1. Select **Enable Auto Account Archive**.
2. In **Max Per Account**, enter the maximum number of archive versions allowed to be stored per account. Range is 1 - 20.
3. To manually archive programming, go to **File > Panel Information**. Select the appropriate system, then select **Archive**.

Configure Admin Reader Settings

During configuration, refer to the device installation guide as needed.

1. In **COM Port**, select the port that the reader is connected to.
2. In **Baud Rate**, select a rate for communication between Remote Link and the reader. The default is **9600 Baud**.
3. In **Reader Model**, select **Serial** for readers connected to a serial port (RS232), or select **USB 6081** for readers connected to a USB port.
4. In **Max Code Length**, select the number of characters for the code. Range is 5 - 10.
5. In **Wiegand Length**, specify the total number of Wiegand bits to be received, including parity bits. Range is 0 - 255. Default is **26**.
6. In **User Code Position**, specify the user code start bit position. Range is 0 - 255. Default is **9**.
7. In **User Code Length**, specify the number of user code bits. Range is 16 - 32. Default is **17**.
8. To set the proximity reader fields based on the current value of the Max Code Length, select **Set Card Defaults**.
9. To test communication between the Remote Link workstation and the admin reader, select **Test**.

4.5 Network Tab

The **Network** tab allows you to configure TCP trap, cellular network, and SOCKS proxy settings

4.5.1 Configure Network Options

To access the **Network** tab, go to **System > Configure > Remote Link > Network**. After configuring the tab, select **OK** to save your settings.

Configure TCP Trap Settings

1. Go to **TCP Trap**.
2. To enable traps, select **TCP Trap Enabled**.
3. In **Programming App Address**, enter the IP address of the Remote Link workstation used to program panels. If the workstation is behind a firewall, enter the IP address of the network router. This address is sent to the network panel to use for connection to Remote Link for a remote upload/download session.
4. In P**rogramming App Port**, enter the port number that the Remote Link workstation uses to connect to the panel. The default is **2001**.
5. In **Trap Server Address**, enter the IP address of the central station receiver. This address is used by Remote Link to send trap messages.
6. In **Trap Server Port**, enter the central station receiver port.

Configure Traps to Send Automatically

Auto Send Traps enables Remote Link to resend the trap command continuously to the SCS-1R receiver. This prevents the receiver from discarding the trap after a four-hour period. The trap is sent according to the configured delay time.

1. Go to **Auto Send Traps**.
2. To enable automatic sending, select **Auto Send Traps**.
3. In **Delay**, enter the number of seconds that Remote Link waits between resetting traps. The default is **180 seconds**. The minimum is **30 seconds**.
4. In **Customer**, specify any customers to send traps.

Configure a SOCKS Proxy

A SOCKS proxy server is a server-based application used to transfer data between client computers using a set of filtering rules for enhanced security. A user's workstation requires a SOCKS client to be installed, either in the application (such as PuTTY, Firefox) or in the TCP/IP where the client software redirects packets into a SOCKS tunnel.

The SOCKS client initiates a connection to a SOCKS server while the protocol handles authentication and logs connection requests. The SOCKS server acts as the IP Client for the connection request so the external server is only aware of the proxy.

1. Go to **SOCKS Proxy**.
2. In **Version**, select the appropriate SOCKS Proxy version.
3. In **Host**, enter the IP address of the SCS-101 or SCS-104 installed in the SCS-1R receiver.
4. In **Port**, enter the port through which you will connect to the panel. The valid range is **1-65535**. Default is **1080**.

Enable a Cellular Network

This feature enables a cellular backup connection for Remote Link.

To enable cellular network, go to **Cellular Network** and select **Direct Cell**.

4.6 Modules Tab

The **Modules** tab allows you to configure settings for add-on modules.

4.6.1 Configure Monitoring Options

To access the Modules tab, go to **System > Configure > Remote Link > Modules**. After configuring the tab, select **OK** to save your settings.

> ℹ **Note:** The following options are only visible if additional modules are installed

Host Monitoring

- **Host Monitoring:** To allow the module to receive signals from network enabled panels, select **Host Monitoring Enabled**.
- **UDP Port:** Enter the data network UDP port number through which the module will use to monitor for incoming alarm signals. **2001** is the default port.

Direct Monitoring

- **COM Port:** Select the COM port that is connected to your panel.
- **Baud Rate:** Set the baud rate to **9600**.

Command Center

- **Track Armed Status:** Select **Track Armed Status** to allow the Command Center to display the armed/disarmed status of all monitored accounts.

4.7 Custom Fields Tab

The **Custom Fields** tab enables you to rename field titles and maintain selections in dropdown lists located on the Panel Information window and the **User Codes** window.

4.7.1 Configure Custom Fields

To access the **Custom Fields** tab, go to **System > Configure > Remote Link > Custom Fields**. After configuring the tab, select **OK** to save your settings.

Edit List

Create, edit, or delete selections available for account configuration dropdowns in **Panel Information > General Information** and **User Codes > Custom**.

Add a Custom Field

1. Select a field and select **Edit List**.
2. Select **New**.
3. In the text field, enter a name for the custom field.
4. Select **OK**.

Edit a Custom Field

1. Select a field and select **Edit List**.
2. Select the custom field name that you want to edit.
3. Edit the field, then select **OK**.

Delete a Custom Field

1. Select a custom field and select **Edit List**.
2. Select the custom field that you want to delete, then select **Delete**.
3. A dialog pops up to confirm your decision. Select **OK**.

Edit Caption and Make Selections

To edit a **Caption**, double-click the entry or press F2. Rename the caption, then press **Enter**. The **Limit to List** and **Admin Add** selections work together to determine how entries that use a dropdown list of items are handled. Make these selections as needed. The following table describes the effect of the possible combinations:

Limit to List	Admin Add	Description
Unselected	Unselected	All operators can enter text for custom fields. Entries are not added to the dropdown list, but the values entered for the panel are stored in the database.
Unselected	Selected	All operators can add to the list of custom fields. A prompt confirms addition of the item to the dropdown list.

Limit to List	Admin Add	Description
Selected	Unselected	Custom field selections are limited to items in the dropdown list. Additions can only be made in the **Custom Fields** tab.
Selected	Selected	Entries for non-admin operators are limited to items in the dropdown list. Admins can enter text not in the dropdown list.

4.8 Configure the Toolbar

Remote Link provides a customizable toolbar to assist you when performing common tasks. The toolbar is displayed just below the menu bar.

By placing a button on the toolbar, you can quickly open the needed window without using the menu bar and drop-down menus. For example, if you frequently arm and disarm panels, you could place an Arm/Disarm button on the toolbar.

Some toolbar buttons only display when the panel is open, when the panel is connected, or when the panel supports a specific feature. For example, the Arm/Disarm button does not display and enable until you are connected to a panel.

1. Go to **System > Toolbar Configuration**.
2. To add an item to the toolbar, select it in **Available Menus**, then select **Add**.
3. To reorder the toolbar items, select the item in Toolbar and select **Move Up** or **Move Down**.
4. To insert a separator for toolbar sections, select **Separator**, then move the separator up or down.
5. To remove an item from the toolbar, select it in **Toolbar**, then select **Remove**.
6. To make the toolbar visible, select **Show Toolbar**. To show text labels for toolbar items, select **Show Caption**. To show icons on the toolbar, select **Show Images**.
7. Select **OK**.

5 Operators

There are three roles discussed in this section:

- **Workstation Administrator:** Has administrator access to the workstation operating system. The workstation administrator is generally a member of your company's IT team or a system administrator.
- **Remote Link Administrator:** Has limited operating system privileges and administrator operator privileges within Remote Link.
- **Remote Link Operator:** Has limited operating system privileges and may also have limited operator privileges.

The remainder of this section assumes a 'typical' organizational structure and configuration. This is defined as the following:

- There are one or more Workstation Administrators who perform maintenance of the workstations. Workstation Administrators only interact with Remote Link for installation and maintenance.
- There is at least one Remote Link Administrator who performs operator management tasks within Remote Link. The Remote Link Administrator interacts with Remote Link as needed.
- There are one or more Remote Link Operators who use Remote Link daily. Remote Link Operators cannot perform installation, maintenance, or management tasks.

> **ⓘ Note:** An individual may serve more than one role for an organization

5.1 Configure Operators

To prevent unauthorized system access, DMP recommends changing default usernames and passwords for all software.

To configure operators, go to **System > Operator Configuration**.

5.1.1 Change the Default Admin Login

Maintain at least one admin user for Remote Link. To create other users, refer to "Add an Operator".

1. Select **new**, then go to the **Login Information** section.
2. In **Login**, enter a new username such as *admin*.
3. In **Password**, enter a password, then enter the password again in **Re-enter Password**.
4. Leave all options selected in each tab. Select **OK**.

5.1.2 Add an Operator

1. Select **New**.
2. In **Login**, enter a username for the account.
3. In **Password**, enter a password for the operator, then enter the password again in **Re-enter Password**.
4. If necessary, enter the operator's first and last name in the **Personal Information** section.
5. Go to the **Account Access** section. To allow the operator to access all accounts, select **All**. To restrict the operator's access to specific accounts, select **Restrict**, select **More**, then select accounts as needed.
6. Select **User Restrictions** and **Special Permissions** as needed.
7. Select options in the **Panel Programming** tab, **User Status and Programming** tab, and **Receiver** tab as needed.
8. Select **OK**.

5.2 Configure Authentication

When configuring Single Sign-On or Windows Credentials authentication, the Remote Link admin account maps to the Windows account that is currently signed in. Ensure you map existing operators to their Windows account before they can sign in. After an operator account is mapped to a Windows account, the operator's Remote Link password is deleted.

> ℹ️ **Note:** Authentication types apply to all Remote Link operator accounts. Only one authentication type can be used at a time.

Remote Link supports the following operator authentication methods:

- **Classic Login:** Operators log in with their Remote Link username and password. This method relies on Remote Link for operator authentication.
- **Single Sign-On:** Operators are automatically logged in to Remote Link. This method uses a directory service and authentication tokens that allow operators to automatically sign in to multiple programs.
- **Windows Credentials:** Operators log in with their Windows password. This method uses Windows Active Directory to authenticate Remote Link operators

5.2.1 Configure Classic Authentication

1. Go to **System > Operator Configuration**.
2. Select **Authentication**.
3. Select **Next**.
4. Select **Classic Login**, then select **Next**.
5. Enter a new password for the operator account.
6. Select **Finish**.
7. Create passwords for each operator. To create classic Remote Link operator logins, refer to "Configure Operators".

5.2.2 Configure Single Sign-On or Windows Credentials Authentication

1. Go to **System > Operator Configuration**.
2. Select **Authentication**.
3. Select **Next**.
4. Select **Single Sign-On** or **Windows Credentials**, then select **Next**.
5. Select **Finish**.
6. In the **Windows Account Information** section, go to **Windows User Account** and select **Edit**.
7. In **Enter the object name to select**, enter the operator's Windows username or LDAP, then select **Check Names** to find the user in the Active Directory.
8. Select **OK**.
9. Repeat steps 6-8 for each operator account, then restart Remote Link on each workstation.

6 Manage Receivers

The following topics cover how to add and program receivers in Remote Link.

6.1 Add a Receiver

1. Go to **File > Panel Information** and open the **Receiver** tab.
2. Select **New**.
3. Select a **Model** and enter a firmware **Version** if necessary.
4. In **Receiver**, enter the receiver number. Range is 1-99. Default is **1**.
5. In **Account**, enter the account number. Range is 1-65535. The account number is needed to maintain database integrity and is not used by the system.
6. Select **OK**.
7. If necessary, enter a **Receiver Name**.
8. Select a **COM Port**.
9. Select **OK**.

6.2 Program a Receiver

The options available in programming depend on the receiver model and whether communication has been established with the receiver. The following topics cover receiver programming options in each window.

6.2.1 Receiver System Options

1. Go to **Program > Receiver Sys Options**.
2. To retrieve existing programming from the receiver, select **Retrieve**.
3. In **Company Name**, enter your company name.
4. In **Receiver Number**, enter the receiver number. Range 0-9. Default is **1**.
5. If necessary, enter the receiver key in **Receiver Key**. Receiver keys are eight-character alphanumeric codes that are requested when using remote programming.
6. If a service code is required, enter it in **Service Code**. A service code is a 5-digit service authorization code used to authenticate service personnel before allowing access to panel programming or performing any user operations. The valid range for the 5-digit code is **00000-65535**. Entering 00000 for the Service Code disables this feature and access to panel programming is always granted. The default is **00000**.
7. To set the receiver time zone, enter the appropriate value from **Hours From GMT**. Default is **6**.
8. To enable monitoring of DD line cards for failed communication with panels, select **Dialer Line Monitor**. The default is disabled.
9. To send the system options to the receiver, select **Send**.
10. Select **OK**.

6.2.2 Print Operation

This section assigns the activity log and printer programming for the SCS-1R. Connect the printer to the Activity Log port on the back of the SCS-1R Receiver.

1. Go to **Program > Print Operation**.
2. To retrieve existing programming from the receiver, select **Retrieve**.
3. In **Print**, select one of the following options:

- **Never**: Suppresses all printing o
- **Always**: Default. Prints all messages from the receiver.
- **Primary Fail**: Prints only when communication to the primary host fails.

4. In **Port Type**, select the printer communication type.
5. To send the system options to the receiver, select **Send**.
6. Select **OK**.

6.2.3 Receiver Line Cards

1. Go to **Program > Receiver Line Cards**.
2. To retrieve existing programming from the receiver, select **Retrieve**.
3. To add a new line card, select **New**.
4. In **Card Number**, enter the card number. The valid range is **1-8**.
    - **Note:** Lines 6-8 can only be used with SCS-104 Line Cards using SCS-150 Version 101 and updated SCS-RACK hardware.
5. In Card Model, select one of the following options:
    - **None**
    - **SCS-104**
    - **SCS-101 o**
    - **SCS-100**
6. To allow the receiver to update the panel's clock, select **Send Time to Panels**.
7. For SCS-104 cards, select options as needed. Refer to SCS-104 Option Reference.
8. To send the system options to the receiver, select **Send**.
9. Select **OK**.

SCS-104 Option Reference

SCS-104 Dialer

- **Dialer Line Enable:** Enable Dialer Lines 1-4 on each card number.
- **Send ANI/DNIS Information:** ANI sends the phone number that the panel is using to call. DNIS sends information about the phone number the panel dialed.
- **Send Caller ID Information:** Sends information to host automation.
- **Echo Cancel Disable:** If echo cancellation is interfering with alarm signals, select this option.

SCS-104 Network

- **Net Line Enable:** Enable network for the selected line card.
- **Local IP Address:** Enter the local receiver IP address. Ensure the address is unique and cannot be duplicated. The default value is 192.168.000.250.
- **Local Port:** Enter the local port number. The valid range is **1 to 65,535**. The default value is **2001**.
- **Gateway IP Address:** Enter the Gateway IP Address to exit your local network. The default value is **000.000.000.000**.
- **Subnet Mask:** Enter the subnet mask assigned to the receiver. The default value is **255.255.255.000**.
- **o Passphrase**: To communicate using encryption, ensure the panel, SCS-104, and receiver has a matching passphrase programmed. If a passphrase is not entered, the receiver communicates with panels, but the data is not encrypted.

> ⚠️ **Caution**: Do not lose the passphrase. A lost or forgotten passphrase requires that every panel reporting in to the SCS-104 at the receiver be individually reprogrammed with a new passphrase.

- **S16 and S17 Always:** When selected, S16 Panel Not Responding messages are always sent to the automation computer for each supervised account that has stopped sending check-in messages without regard to the number of accounts generating S16 messages. S17 Panel Response Restored messages are sent to the automation computer each time a supervised account checks in for the first time after installation. This also occurs at an account's first check-in after the receiver or SCS-104 is powered-up.
- **Ack Substituted Message:** When selected, the SCS-104 replies with an acknowledgment to messages sent by substituted panels. The SCS-104 generates only one S58 Alarm Panel Substitution message to the host automation computer and receiver printer for each substituted panel. Subsequent messages from substituted panels do not generate additional S58 messages.

> ℹ️ **Note:** Do not select this option when compliance regulations require that panel substitution messages be manually acknowledged.

SCS-104 Check-in Table

The optional SCS-CTM Check-in Table Manager software is used to backup the records of supervised network accounts on up to 32 different SCS-104 line cards. Use SCS-CTM to repopulate the list of supervised network accounts when one SCS-104 or SCS-101 line card is replaced by another SCS-104 or SCS-101. The list of supervised network accounts used by an SCS-104 or SCS-101 on a primary receiver can be mirrored by the SCSCTM for use by an SCS-104 or SCS-101 card on a second receiver. Refer to the following list:

> ℹ️ **Note:** The list of supervised network accounts on an SCS-104 line card is automatically populated when each panel sends its supervisory check-in message to the line card.

- **Check-in Table IP Address:** Enter the IP address for the computer where SCS-CTM is installed. The default is **000.000.000.000**.
- **Check-in Table Port:** Enter the IP port used to communicate messages to SCS-CTM. The valid range is **1 to 65,535**. The default is **2005**.
- **Check-in Table ID:** Enter the table ID number to be used to identify the check-in table. The valid range is **1-255**. The default is **1**.

6.2.4 Receiver Host Programming

This section assigns programming to the Receiver Host that is connected to the SCS-1R. Connect the host computer to the Host Output port on the back of the SCS-1R Receiver.

1. Go to **Program > Receiver Hosts**.
2. To retrieve existing programming from the receiver, select **Retrieve**.
3. In **Host Number**, enter the host number. The default is **1**.
4. In **Host Name**, enter a name for the receiver host. The max is **16 characters**.
5. In **Host Type**, select a type. The default is **Primary**.
6. In **Port Type**, select a communication port type. The default is **Serial**.
7. In **Start Character**, select a character to precede all host messages. The default is **None**.
8. To enable CRC error checking on each message sent to the host, select **Use CRC**.
9. To enable numbering of messages sent to the host (1-99), select **Use Sequence**.

10. In Test Interval (Minutes), enter the number of minutes between message tests. The valid range is **1-60**. The default is **1 minute**.
11. In **Acknowledge Timeout**, enter the number of seconds that a receiver should wait for an acknowledgment before re-sending the message. The valid range is **1-15**. The default is **3 seconds**.
12. In **Retries to Failure**, enter the number of retries allowed without acknowledgment before entering a failed state. Retry number includes the initial message sent to the host. The valid range **1-15**. The default is **3**.
13. In **Line Number Length**, enter the number of digits used to report the receiver signal line number. The valid range is **0-2**. The default is **0**.
14. To send the system options to the receiver, select **Send**.
15. Select **OK**.

6.3 Receiver Status

To view the Receiver Model, Version Number, and Firmware Date, go to **Program > Receiver Status**.

6.4 Serial Ports

1. Go to **Program > Serial Ports**.
2. To retrieve existing programming from the receiver, select **Retrieve**.
3. In Auxiliary (A2), set Usage to Auxiliary. In **Baud Rate**, select **9600 Baud**.
4. In **Host Output (A3)**, set **Usage** to **Host Output**. In **Baud Rate**, select the appropriate Baud rate. Default is **9600 Baud**.
5. In **Activity log/Printer (A1)**, set Usage to Printer. In **Baud Rate**, select the appropriate Baud rate. Default is **1200 Baud**.
6. To send the system options to the receiver, select **Send**.
7. Select **OK**.

6.5 Receiver Diagnostics

To view detailed receiver information for troubleshooting, go to **Program > Receiver Diagnostics**.

7 Manage Panels

The following topics cover how to add, program, and connect to a panel in Remote Link.

7.1 Add a Panel

1. Go to **File > Panel Information**.
2. Select **New**.
3. In **Model**, select the panel model number.
4. If necessary, enter a firmware version number in **Version**.
5. In **Receiver**, enter the receiver number. The valid range is **1-99**. The default is **1**.
6. In **Account**, enter the panel account number. The valid range is **1-65535**.
7. Select **OK**.
8. In the **General Information** section, configure the **Panel Name**, **Customer**, and **Region** as needed.
9. In **Connection Information**, select a connection type.
10. Enter the panel remote key.
11. Enter connection information as needed for the connection type. For more information, refer Connection Type Reference.
12. In **Backup Connection Information**, configure a secondary connection as needed.
13. In **Location**, enter panel location information as needed.
14. Select **OK**.

7.1.1 Connection Type Reference

The connection type determines how Remote Link connects to the panel. Appropriate global connection options should be configured before attempting to connect. For more information, refer to Configure Remote Link.

SCS-1/SCS-105 Receiver or Modem

Communicate with the panel through a receiver using dial-up or connect to the panel with a computer modem, especially when a slow, constant baud rate is required to maintain connection data integrity.

- **Phone:** Enter the panel phone number.

> ℹ **Note:** If you need to dial a number to access an outside line, enter that number before the panel's phone number. Enter a **P** for a pause after dialing the number to access the outside line. For example, if you need to dial 9 to get an outside line, enter **9P**, then the panel's phone number. Modems from some manufacturers require a comma (,) for a pause rather than the letter P. Refer to your modem's documentation.

- **Dial:** To dial the phone number, select **Yes**. To not dial the phone number, select **No**. To configure Remote Link to seize the panel when it calls in to the receiver, select **Pickup Only**.

Network (Standard)

Connect over a standard network.

- **IP Address:** Enter the panel IP address. Do not enter leading zeros. If the Remote Link workstation and panel are in the same LAN (internal), enter the panel's local IP in **NETWORK OPTIONS**. If the workstation is on a separate LAN (external), enter the panel network's public IP. When connecting to a panel on an external LAN, configure port forwarding on the panel's network.
- **IP Port:** Enter the panel network port. The default is **2001**.

Network (Ethernet)

Connect directly to the panel with an Ethernet cable. This method creates a temporary LAN between the panel and Remote Link workstation.

> ⓘ **Note:** This connection method requires advanced network configuration. Use standard connection methods whenever possible.

In **NETWORK OPTIONS**, disable **DHCP**. Set the **LOCAL IP ADDRESS** to the default **192.168.0.1**. In **REMOTE OPTIONS**, ensure **ALLOW NETWORK REMOTE** is set to **YES**, then set **NETWORK PROG PORT** to the default **2001**.

On the Remote Link workstation, turn off DHCP. Configure the workstation's IP address to be in the same subnet as the panel. For example, *192.168.0.251*. Ensure the workstation's gateway and subnet mask match the settings in panel **NETWORK OPTIONS**.

- **IP Address:** Enter the panel IP address **192.168.0.1**. Do not enter leading zeros.
- **IP Port:** Enter the panel network port **2001**.

Direct

Connect directly to the panel with a Model 399 cable.

- **COM Port:** Select the workstation port connected to the panel.
- **Baud Rate:** Enter the Baud rate. If the workstation has trouble connecting to the panel, set the Baud rate to a lower value. The default is **9600 Baud**.

Cellular

Connect to the panel over cell. This method requires that the Remote Link workstation is connected to a network.

- **Phone Number:** Enter the Mobile ID Number that you received when the SIM/MEID card was activated.

7.1.2 Seize the Panel with Pickup Only (SCS-1 / SCS-105) Example

Using the same phone line as the SCS-105, a monitoring center operator calls the installing technician. Using the same phone line as the panel, the installing technician answers the call.

Using Remote Link, the monitoring center operator goes to **Panel Information > Connection Information > Type and selects SCS-1 / SCS-105**. In **Dial**, the operator selects **Pickup Only**. The operator goes to **Panel > Connect** and presses **Connect**.

When the SCS-105 goes on-line, the amber OL LED lights. The monitoring center operator tells the technician to enter **984 + CMD** at the keypad. The technician selects **NBR** and enters any number other than zero (0). Remote Link seizes the phone line and the operator and technician hang up their phones.

7.1.3 Extra Information Reference

Go to **File > Panel Information**. In the Location section, select **Extra Information**. Configure the following settings as needed:

- **Site Password:** Enter any site password that is required for emergency personnel to enter the building.
- **Response:** Enter a type of response for the operator to send in case of alarm.
- **Notes:** Enter additional information, such as special details about the building and premises, that may be useful for the operator or response team.
- **Emergency Call List:** Enter contact information for individuals to call in case of alarm.
- **Auto Recall Frequency:** Enter the number of days the panel is expected to send at least one Automatic Recall Test. The valid range is **0-60** days. By default, this field is blank. When the field is blank or 0, Remote Link does not look for an Automatic Recall Test for the account.

> ⓘ **Note**: Auto Recall Frequency and Allow Test Deferrals should have the same value as the **Test Frequency** and **Defer Test** fields in **Program > Communications > Test Timer**.

- **Allow Test Deferrals:** To allow Remote Link to acknowledge any incoming message from the account as the Automatic Recall Test, select **Allow Test Deferrals**. When enabled, Remote Link accepts the opening signal as the Automatic Recall test and the timer is reset after the opening signal is received.
- **Hyperlink** (requires the Alarm Monitoring or Command Center module): Enter a URL or filepath to open. For example, D:\Documents\sitemap.jpeg. Select **Test** to verify that the **Hyperlink** button in **Alarm List** opens the correct URL or file. The maximum number of hyperlinks allowed per account is 1.

7.2 Filter Panels

Filtering options are configured and applied in **File > Panel Information**.

> ℹ **Note:** The Filtering Accounts option is not available if using the SQL Server module.

7.2.1 Quick Filter

In **Panel Information**, tabs near the top of the window allow you to quickly filter panels alphanumerically by **Name**, **City**, **Account**, **Panel Phone**, **Customer**, and **Region**.

Selecting a column header further sorts the results on the grid. For example, to sort results alphabetically by city name, select **City**. To hide a column, right-click an item in the column that you want to hide, then select **Hide Grid Field**. To show all grid options, right-click any value and select **Show All Fields**.

To quickly filter data with a specific value, right-click the value that you want to filter, then select **Filter By Selection**. To add a value to the filter as an additional condition, right-click the value and select **Add to Filter**. To clear all filtering, right-click any value in the grid and select **Clear Filter**.

7.2.2 Create a Custom Panel Filter

> ℹ **Note:** To access the Panel Information Filter window, ensure operator accounts have Advanced Filtering privileges enabled.

To create a custom panel filter, complete the following steps:

1. In **Panel Information**, select **Panel Filter**.
2. To create a panel filter, select **Panel Filter**. To create a user filter, select **User Filter**.
3. To view all active filters, select **View Summary**. To clear the search, select **New Search**.
4. In **Fields**, select a field to filter.
5. To filter results with a specific value, open the **By Value** tab. In **Field Value**, enter the value that you want to filter. In **Search Type**, select an option that matches the field value to results.
6. To filter results with a literal alphanumeric range, open the **By Range** tab. Enter values in **Starting Range** and **Ending Range** as needed.
7. Select **OK**.

7.2.3 Export Filter Results

Remote Link allows filter results to be exported as a tab-delimited text file. To export data, go to **File Name** and select **More**. Choose a location and name the file. To export panel filter results, clear **Export Selected Users**. To export user filter results, select **Export Selected Users**. To export results to the file, select **Export**.

7.3 SecureCom Wireless Activations

SecureCom Wireless Activations are used for managing control panel cellular service using SecureCom Wireless, LLC.

7.3.1 Establish Cellular Service

To establish cellular service with SecureCom Wireless, visit SecureComWireless.com and download the Network Service Agreement. This contract only needs to be completed once per company.

7.3.2 Register the SecureCom Wireless Module in Remote Link

Once SecureCom Wireless service has been established, a Certificate of Authentication is emailed that contains a serial number. The serial number is needed to register and activate a SecureCom Wireless service module in Remote Link. The serial number and activation are required for each installation of Remote Link. Contact SecureCom Customer Service at 877-300-8030 for activations.

To register the SecureCom Wireless Module in Remote Link, complete the following steps:

1. Select **System** and select **Operator Configuration**.
2. Ensure **Cellular Activations** in the **Special Permissions** box is enabled. This option must be enabled for an operator to manage SecureCom Wireless SIM/MEIDs.
3. Select **OK**.
4. Select **Help** and select **Registration**.
5. Select **Add**.
6. Type the module's serial number as it appears on the certificate.
7. Select **OK**. A message box will appear reminding you to activate the module within 7 days.

7.3.3 Activate the SIM/MEID

The **Activate SIM/MEID** window allows changes, activation, and deactivation of the selected SIM/MEID. Remote Link automatically populates the **Rate Plan** field with a suggested rate plan that most closely matches the communication path programming for the panel.

To activate the SIM/MEID, complete the following steps:

1. Select **System**, then select **SecureCom Wireless Activations**.
2. Choose a panel and select **Edit** to open the **Activate SIM** window. Select **New** to add a SIM/MEID. You can also select **Transfer** if you would like to transfer an existing and activated SIM/MEID to a new panel. The **Activate SIM** window can also be accessed by selecting **Program**, then selecting **Communication**.
3. Choose the path programmed for cell communication and select **Activate**.
4. When the **Activate SIM/MEID** screen displays, enter all information before selecting **Activate**. Complete all panel programming before activating the cellular path to ensure the correct rate plan is calculated for usage. The activation process could take up to 24 hours to complete.

The following list explains the fields that appear on the **Activate SIM/MEID** screen.

- **SIM Type:** Select the type of **SIM/MEID** you are activating. Select **200, 400, MEID**, or **LTE SIM**.
- **SIM/MEID Card#:** Enter the **SIM** (Subscriber Identity Module) or **MEID** (Mobile Equipment Identifier) number from the SecureCom AT&T Wireless SIM/MEID, SecureCom T-Mobile Wireless SIM/MEID, or the

263LTE Series Cellular Communicator. The SIM number can be found on the label of the 263LTE Series device.

- **Rate Plan:** Remote Link automatically populates this field with a suggested rate plan that most closely matches the communication path programming for the panel. If you choose to override the suggested rate plan, you could experience overage fees from SecureCom Wireless, LLC.

> ℹ️ **Note:** SMS functionality is not compatible with LTE cellular modules

Available rate plans may include the following options:

Rate Plan	Primary Path	Data Cap (KB)	Daily Test	O/C Reports	Check-In Compatible	Door Access[3]	Panic Test[3]
Backup	N	Flat Rate	Y	Y	N	N/A	N/A
CellComSL	Y	Flat Rat	Y	Y	N	N/A	N/A
XTL	Y	Flat Rate	Y	Y	N	N/A	N/A
XT	Y	Flat Rate	Y	Y	N	N/A	N/A
XR	Y	Flat Rate	Y	Y	N	N	N
Fire	Y	Flat Rate	Y	Y (8 Areas)	58 Min	Y	Y
406	Y	50 KB	Y	N	N	N	N
408	Y	200 KB	Y	Y (4 Areas)	60 Min	Y[2]	Y[2]
416	Y	1000 KB	Y	Y (8 Areas)	5 Min	Y[2]	Y[2]
425	Y	2000 KB	Y	N	3 Min	Y[2]	Y[2]

[1] A backup path is only used when the primary path is unable to connect.

[2] Some setting combinations may require a higher tier plan to avoid overages.

[3] These options refer to reports in communication programming and do not reflect panel capabilities.

Heading

- **Status:** This displays the current status of the SIM/MEID. To update the status of the current SIM/MEID, elect Update Status.
- **Unused:** The SIM/MEID number is currently not assigned to an active panel account.
- **Pend Act:** A request for activation has been sent and is pending.
- **Activated:** This is an active digital cellular SIM/MEID.
- **Pend DeAct:** A request to deactivate this SIM/MEID has been sent and is pending.
- **Deactivated:** This SIM/MEID has been deactivated.
- **Invalid:** The SIM/MEID number entered is not a valid number. Re-enter the number from the SIM/MEID and retry the activation process.
- **Text Plan:** Select the text plan for the SIM/MEID. Available text plans may include the following options:

Text Plans Available	SIM/MEID	Available Plans
None: Messaging is not included	Level 400	• XT30/XT50 • XTL Series • XR Series
SMS100: 100 Messages per month	Level 400	• XT30/XT50 • XTL Series • XR Series
SMS200: 200 Messages per month	Level 400	• XT30/XT50 • XTL Series • XR Series
MyAccess: Unlimited messages	Level 400	• XT30/XT50 • XTL Series • XR Series

7.3.4 Deactivate the SIM/MEID

From the **Activate SIM** or **SecureCom Wireless** window, select **Deactivate** to request deactivation.

7.3.5 Transfer the SIM/MEID

To transfer the SIM/MEID, complete the following steps:

1. Navigate to the **SecureCom Wireless Activations** window or open the edit window for the SIM or MEID you would like to transfer.
2. Select **Transfer**. Remote Link connects to SecureCom Wireless and retrieves the SIM or MEID's current information.
3. Enter the new panel's account number in the **New Account** field and select **Next**.
4. The **Select Rate and Text Plans** window displays. Remote Link suggests a rate and text plan based on the new panel's type. If you would like to make a different selection, use the **Rate Plan** and **Text Plan** drop-down menus. If you choose a rate plan that is likely to cause overages, Remote Link notifies you. Select **Next** when you've made your selections.

5. The **Transfer Summary** window displays. If the information looks correct, select **Finish**. When the transfer completes, the **Success** window displays. Select **Done** to close the **Transfer SIM or MEID** window.

7.4 Connect a Panel

To connect to a panel, go to **File > Panel Information** and double-click the panel that you want to connect. Go to **Panel > Connect**, then select **Connect**. To troubleshoot connection errors, refer to "Connection Error Reference" in this topic.

To disconnect from a panel, go to **Panel > Disconnect,** then select **Disconnect.**

> ⓘ **Note:** An inactivity timeout occurs if no data transfer activity is detected within 4.5 minutes. At timeout, a message box appears and allows an operator to extend the connection. If an extension is not performed, Remote Link will disconnect from the panel in 1 minute.

7.4.1 Connection Error Reference

Connection canceled: Action aborted by user—The connection attempt was manually canceled by an operator. Reattempt connection.

Error connecting, invalid connection information—Connection information is missing or incorrect. Depending on connection type, this may include cellular phone number, IP address, Port number, COM port, phone number, or remote key.

Error connecting, please make sure TCP/IP is installed—The computer is not properly configured for network communication. Refer to operating system documentation.

Error requesting max partitions—Could not retrieve the max partitions from the panel.

Panel Connection Error: Connection closed—Connection was closed while Remote Link was trying to send data to the panel.

Panel Connection Error: Invalid connect response—Remote Link did not receive a proper reply from the panel. Reattempt connection.

Panel Connection Error: Invalid connect response while calling panel—(Phone line connections) Remote Link did not receive a proper reply from the panel. Reattempt connection.

Panel Connection Error: Invalid connect sequence—Data being passed from the panel to Remote Link has been lost or corrupted. Reattempt connection.

Panel Connection Error: Invalid receiver number—The receiver key programmed in the receiver does not match the key stored in panel or Alarm Receiver/Service Receiver are not enabled in panel programming. In Remote Link, check the receiver key in **System > Configure > SCS-1 System**.

Panel Connection Error: Invalid remote key—The panel remote key does not match the one configured in Remote Link. Change the remote key in **File > Panel Information > Connection Information**, then reattempt connection.

Panel Connection Error: Panel busy with other communication—Panel communication paths are busy. Reattempt connection.

Panel Connection Error: Panel not connected—Connection lost with panel. Reattempt connection.

Panel Connection Error: Receiver not authorized to connect—In panel programming, go to **REMOTE OPTIONS** and ensure that **SERVICE RECEIVER AUTH** is set to **YES**. Check local firewall settings and ensure the proper ports are open. Check port configurations in the panel and Remote Link.

Panel Connection Error: Timeout—Remote Link did not receive a reply from panel within the allowed time frame. Check wiring connections and traffic, then reattempt connection.

Panel Connection Error: Timeout trying to call panel—If connecting through a receiver on a phone line, ensure the receiver is getting dial tone and the Phone Number is correct in Panel Information. For receiver connections, check wiring connections, cable types, connector pinouts, power connections, and COM port configuration in **File > Panel Information and System > Configure > Remote Link > Receiver**.

Unable to Connect to Panel—For network systems, the IP address is missing or incorrect.

To view diagnostic messages associated with failed connections, go to **System > Diagnostics**. The following error strings are appended to the end of the failed connection messages.

Error String	Meaning
-VA	Not allowed
-VB	Panel busy
-VC	Invalid remote key
-VD	Bad data
-VN	Not connected
-VR	Invalid receiver
-VU	Invalid account

7.5 Program the Panel

The following topics cover how to program each section in the Program menu. The programming options available in each section depend on panel type and configuration. Refer to the appropriate panel programming guide from DMP.com/resources when programming in Remote Link.

For listed installations, refer to DMP's product Compliance Guides and Compliance Notes.

7.5.1 Retrieve Programming from Panel

> ℹ **Note:** When you retrieve from a panel, any programming changes made in Remote Link that have not yet been sent to the panel are overwritten by the panel programming information that you retrieve from the panel.

1. Close all programming and configuration windows.
2. Ensure Remote Link is connected to the panel.
3. Go to **Panel > Retrieve**.
4. To automatically request the panel's events after programming is retrieved, select **Request Events**.
5. To update the panel time after programming is retrieved, select **Update Time**.
6. To automatically disconnect from the panel after programming is retrieved, select **Disconnect on Completion**.
7. To retrieve only the programming that has changed since the last connection with the panel, select **Changes Only**.
8. Select **Retrieve**.

7.5.2 Quick Programming Reference

Refer to the following tables when programming DMP accessories. For complete programming guides, refer to DMP.com/resources.

7.5.3 XR150

The following table columns are arranged to follow the typical panel programming order and values required for each item. For example, you should first program a wireless keypad in Device Setup, where you give it a device number, select a device type, select a device communication type, then enter the wireless serial number before programming other options.

For additional installation requirements and programming options, refer to the model's installation guide.

- **Models:** The accessory item's model number and name, linked to its installation guide.
- **Program In:** The menu where you program the accessory: Device Setup, Zone Information, Output Information, or Key Fobs.
- **Device, Zone, or Output Number:** The range of numbers for the accessory, depending on where it is programmed. See above. Keep in mind that although any device can be programmed as device 1 in the panel, that address should be reserved for the primary system keypad in most cases.
- **Device Type:** If the accessory is programmed in Device Setup, this lists possible device types.
- **Device Communication Type:** If the accessory is programmed in Device Setup, this lists possible communication types.
- **Zone Type:** If the accessory is programmed in Zone Information, this lists possible zone types.
- **Wireless SN Range:** For a wireless device, the typical serial number range of its class.

Models	Program In	XR150 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
630F Fire Keypad	Device Setup	1-8	FI	n/a	n/a	n/a
714N-POE Zone Expander Module	Device Setup	1-8	EXP & NET	NET	n/a	n/a
734 Access Control Module	Device Setup	1-8	DOOR	KPD or AXBUS	n/a	n/a
734B BIN Access Control Module	Device Setup	1-8	DOOR	KPD or AXBUS	n/a	n/a

Models	Program In	XR150 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
734N/734N-POE Network Access Control Module	Device Setup	1-8	DOOR	KPD or NET	n/a	n/a
736V V-Plex Module	Device Setup	501	VPX	n/a	n/a	n/a
7000 Series Thinline Keypads	Device Setup	1-8	KPD or DOOR	KPD	n/a	n/a
7300 Series Icon Keypads	Device Setup	1-8	KPD	KPD	n/a	n/a
7463 Network Thinlilne Keypads	Device Setup	1-8	KPD	NET	n/a	n/a
7800 Series Graphic Touchscreen Keypad	Device Setup	1-8	KPD or DOOR	KPD	n/a	n/a
1100R Repeater	Zone Information	Consecutive if more than one per panel: 500-599	AUX1	n/a	AUX1	13000000-13999999
1100T Wireless Translator	Device Setup	2-8	1100T	n/a	n/a	13000000-13999999

Models	Program In	XR150 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1100T Wireless Translator	Zone Information	500-599	n/a	n/a	Any	Non-DMP SN
1101 Universal Transmitter	Zone Information	500-599	n/a	n/a	Any	01000000-01999999
1102 Universal Transmitter, external contact	Zone Information	500-599	n/a	n/a	Any	01000000-01999999
1103 Universal Transmitter	Zone Information	Consecutive: 500-599	n/a	n/a	Any	01000000-01999999
1106 Universal Transmitter, internal/ external contact	Zone Information	500-599	n/a	n/a	Any	01000000-01999999
1107 Micro Window Transmitter	Zone Information	500-599	n/a	n/a	NT	02000000-02999999
1108 Doorbell Module	Zone Information	500-599	n/a	n/a	DB	02000000-02999999
1114 Four-Zone Expander Module	Zone Information	Consecutive: 500-599	n/a	n/a	Any	08000000-08999999

Models	Program In	XR150 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1115 Temperature Sensor and Flood Detector	Zone Information	500-599	n/a	n/a	SV	08000000-08999999
1116 Relay Output	Output Information	450-474 (slow); 480- 499 (fast)	n/a	n/a	n/a	15100000-15199999
1117 LED Annunciator	Output Information	450-474 (slow); 480- 499 (fast)	n/a	n/a	n/a	15100000-15199999
1118 Remote Indicator Light	Output Information	450-474 (slow); 480- 499 (fast)	n/a	n/a	n/a	15100000-15199999
1119 Door Sounder	Zone Information	500-599	n/a	n/a	NT or DY	02000000-02999999
1119 Door Sounder (Output)	Output Information	450-474 (slow); 480- 499 (fast)	n/a	n/a	n/a	15100000-15199999
1122 PIR	Zone Information	500-599	n/a	n/a	NT	09500000-09999999
1126R Ceiling Mount PIR	Zone Information	500-599	n/a	n/a	NT	09100000-09499999
1127 Wall Mount Curtain PIR	Zone Information	500-599	n/a	n/a	NT	09100000-09499999
1128 Glassbreak	Zone Information	500-599	n/a	n/a	NT	03000000-03999999

Models	Program In	XR150 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1131 Recessed Contact	Zone Information	500-599	n/a	n/a	Any	02000000-02999999
1134 Access Control Module	Device Setup	1-8	DOOR	n/a	WLS	14300000-14499999
1135 Siren	Output Information	450-474 (slow); 480- 499 (fast)	n/a	n/a	n/a	15200000-15999999
1136 Remote Chime	Output Information	450-474 (slow); 480- 499 (fast)	n/a	n/a	n/a	15200000-15999999
1137 LED Emergency Light	Output Information	450-474 (slow); 480- 499 (fast)	n/a	n/a	n/a	15200000-15999999
1139 Bill Trap	Zone Information	500-599	n/a	n/a	PN	02000000-02999999
1141 Wall Button	Zone Information	500-599	n/a	n/a	Any	04000000-04999999
1142 Two-button HoldUp	Zone Information	500-599	n/a	n/a	PN	04000000-04999999
1144 Key Fob	Key Fobs Zone Information	400-449 500-599	n/a n/a	n/a n/a	n/a n/a	05900000-59999999 05900000-59999999
1148 Personal Pendant	Zone Information	500-599	n/a	n/a	EM	04000000-04999999

Models	Program In	XR150 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1154 Four-Zone Input Module	Zone Information	500-599	n/a	n/a	Any	08000000-08999999
1158 Eight-Zone Input Module	Zone Information	500-599	n/a	n/a	Any	08000000-08999999
1164 Smoke Detector with Sounder	Zone Information	500-599	n/a	n/a	FI	07000000-07999999
1166 Smoke Ring	Zone Information	500-599	n/a	n/a	FI	06000000-06999999
1168 CO/Smoke/Low Temp Combo Detector Zone	Zone Information	Consecutive: 500-599	n/a	n/a	FI + CO + SV	07000000-07999999
1183 Heat Detector	Zone Information	500-599	n/a	n/a	FI	06000000-06999999
1184 Carbon Monoxide Detector	Zone Information	500-599	n/a	n/a	CO	06000000-06999999
9000 Series Thinline Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14000000-14299999
9800 Graphic Touchscreen Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14500000-14999999

7.5.4 XR550

XR550

The following table columns are arranged to follow the typical panel programming order and values required for each item. For example, you should first program a wireless keypad in Device Setup, where you give it a device number, select a device type, select a device communication type, then enter the wireless serial number before programming other options. For additional installation requirements and programming options, refer to the model's installation guide.

- **Models:** The accessory item's model number and name, linked to its installation guide.
- **Program In:** The menu where you program the accessory: Device Setup, Zone Information, Output Information, or Key Fobs.
- **Device, Zone, or Output Number:** The range of numbers for the accessory, depending on where it is programmed. See above. Keep in mind that although any device can be programmed as device 1 in the panel, that address should be reserved for the primary system keypad in most cases.
- **Device Type:** If the accessory is programmed in Device Setup, this lists possible device types.
- **Device Communication Type:** If the accessory is programmed in Device Setup, this lists possible communication types.
- **Zone Type:** If the accessory is programmed in Zone Information, this lists possible zone types.
- **Wireless SN Range:** For a wireless device, the typical serial number range of its class.

Models	Program In	XR550 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
630F Fire Keypad	Device Setup	1-16	FI	n/a	n/a	n/a
714N-POE Zone Expander Module	Device Setup	1-16	EXP and NET	NET	n/a	n/a
734 Access Control Module	Device Setup	1-16	DOOR	KPD or AX-BUS	n/a	n/a
734B BIN Access Control Module	Device Setup	1-16	DOOR	KPD or AX-BUS	n/a	n/a
734N/734N-POE Network Access Control Module	Device Setup	1-16	DOOR	KPD or AX-BUS	n/a	n/a

Models	Program In	XR550 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
736V V-Plex Module	Device Setup	501, 601, 701, 801, 901	VPX	n/a	n/a	n/a
7000 Series Thinline Keypads	Device Setup	1-16	KPD or DOOR	KPD	n/a	n/a
7300 Series Icon Keypads	Device Setup	1-16	KPD	KPD	n/a	n/a
7463 Network Thinline Keypads	Device Setup	1-16	KPD	NET	n/a	n/a
7800 Series Graphic Touchscreen Keypad	Device Setup	1-16	KPD	NET	n/a	n/a
1100R Repeater	Zone Information	Consecutive if more than one per panel: 500-999	AUX1	n/a	AUX1	13000000-13999999
1100T Wireless Translator	Device Setup	2-16	1100T	n/a	n/a	13000000-13999999
1100T Wireless Translator	Zone Information	500-999	n/a	n/a	Any	Non-DMP SN
1101 Universal Transmitter	Zone Information	500-999	n/a	n/a	Any	01000000-01999999

Models	Program In	XR550 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1102 Universal Transmitter, external contact	Zone Information	500-999	n/a	n/a	Any	01000000-01999999
1103 Universal Transmitter	Zone Information	Consecutive: 500-999	n/a	n/a	Any	01000000-01999999
1106 Universal Transmitter, internal/ external contact	Zone Information	500-999	n/a	n/a	Any	01000000-01999999
1107 Micro Window Transmitter	Zone Information	500-999	n/a	n/a	NT	02000000-02999999
1108 Doorbell Module	Zone Information	500-999	n/a	n/a	DB	02000000-02999999
1114 Four-Zone Expander Module	Zone Information	Consecutive: 500-999	n/a	n/a	Any	08000000-08999999
1115 Temperature Sensor and Flood Detector	Zone Information	500-999	n/a	n/a	SV	08000000-08999999
1116 Relay Output	Output Information	450-474 (slow); 480-499 (fast)	n/a	n/a	n/a	15100000-15199999

Models	Program In	XR550 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1117 LED Annunciator	Output Information	450-474 (slow); 480-499 (fast)	n/a	n/a	n/a	15100000-15199999
1118 Remote Indicator Light	Output Information	450-474 (slow); 480-499 (fast)	n/a	n/a	n/a	15100000-15199999
1119 Door Sounder	Zone Information	500-999	n/a	n/a	NT or DY	02000000-02999999
1119 Door Sounder (Output)	Output Information	450-474 (slow); 480-499 (fast)	n/a	n/a	n/a	15100000-15199999
1122 PIR	Zone Information	500-999	n/a	n/a	NT	09500000-09999999
1126R Ceiling Mount PIR	Zone Information	500-999	n/a	n/a	NT	09100000-09499999
1127 Wall Mount Curtain PIR	Zone Information	500-999	n/a	n/a	NT	09100000-09499999
1128 Glassbreak	Zone Information	500-999	n/a	n/a	NT	03000000-03999999
1131 Recessed Contact	Zone Information	500-999	n/a	n/a	Any	02000000-02999999

Models	Program In	XR550 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1134 Access Control Module	Device Setup	1-16	DOOR	n/a	WLS	14300000-14499999
1135 Siren	Output Information	450-474 (slow); 480-499 (fast)	n/a	n/a	n/a	15200000-15999999
1136 Remote Chime	Output Information	450-474 (slow); 480-499 (fast)	n/a	n/a	n/a	15200000-15999999
1137 LED Emergency Light	Output Information	450-474 (slow); 480-499 (fast)	n/a	n/a	n/a	15200000-15999999
1139 Bill Trap	Zone Information	500-999	n/a	n/a	PN	02000000-02999999
1141 Wall Button	Zone Information	500-999	n/a	n/a	Any	04000000-04999999
1142 Two-button HoldUp	Zone Information	500-999	n/a	n/a	PN	04000000-04999999
1144 Key Fob	Key Fobs	400-449	n/a	n/a	n/a	05900000-59999999
	Zone Information	500-999	n/a	n/a	PN or HU	05900000-59999999

Models	Program In	XR550 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1148 Personal Pendant	Zone Information	500-999	n/a	n/a	EM	04000000-04999999
1154 Four-Zone Input Module	Zone Information	500-999	n/a	n/a	Any	08000000-08999999
1158 Eight-Zone Input Module	Zone Information	500-999	n/a	n/a	Any	07000000-07999999
1164 Smoke Detector with Sounder	Zone Information	500-999	n/a	n/a	FI	07000000-07999999
1166 Smoke Ring	Zone Information	500-999	n/a	n/a	FI	06000000-06999999
1168 CO/Smoke/ Low Temp Combo Detector	Zone Information	Consecutive: 500-999	n/a	n/a	FI + CO + SV	07000000-07999999
1183 Heat Detector	Zone Information	500-999	n/a	n/a	FI	06000000-06999999
9000 Series Thinline Keypad	Device Setup	1-16	KPD or DOOR	WLS	n/a	14500000-14999999
9800 Graphic Touchscreen Keypad	Device Setup	1-16	KPD or DOOR	WLS	n/a	14500000-14999999

7.5.5 XT50

The following table columns are arranged to follow the typical panel programming order and values required for each item. For example, you should first program a wireless keypad in Device Setup, where you give it a device number, select a device type, select a device communication type, then enter the wireless serial number before programming other options. For additional installation requirements and programming options, refer to the model's installation guide.

Models: The accessory item's model number and name, linked to its installation guide.

Program In: The menu where you program the accessory: Device Setup, Zone Information, Output Information, or Key Fobs.

Device, Zone, or Output Number: The range of numbers for the accessory, depending on where it is programmed. See above. Keep in mind that although any device can be programmed as device 1 in the panel, that address should be reserved for the primary system keypad in most cases.

Device Type: If the accessory is programmed in Device Setup, this lists possible device types.

Device Communication Type: If the accessory is programmed in Device Setup, this lists possible communication types.

Zone Type: If the accessory is programmed in Zone Information, this lists possible zone types.

Wireless SN Range: For a wireless device, the typical serial number range of its class.

Models	Program In	XT50 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
734 Access Control Module	Device Setup	1-8	DOOR	KPD or AX-BUS	n/a	n/a
734N/734N-POE Network Access Control Module	Device Setup	1-8	DOOR	KPD or NET	n/a	n/a
7000 Series Thinline Keypads	Device Setup	1-8	KPD or DOOR	KPD	n/a	n/a
7300 Series Icon Keypads	Device Setup	1-8	KPD	KPD	n/a	n/a

Models	Program In	XT50 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
7463 Network Thinline Keypads	Device Setup	1-8	KPD	NET	n/a	n/a
7800 Series Graphic Touchscreen Keypad	Device Setup	1-8	KPD or DOOR	KPD	n/a	n/a
1100R Repeater	Zone Information	Consecutive if more than one per panel: 11-14, 21-24, 31-34, 41-44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	AUX1	n/a	AUX1	13000000-13999999
1100T Wireless Translator	Device Setup	2-8	1100T	n/a	n/a	13000000-13999999
1100T Wireless Translator	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	Non-DMP SN
1101 Universal Transmitter	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	01000000-01999999
1102 Universal Transmitter, external contact	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	01000000-01999999

Models	Program In	XT50 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1103 Universal Transmitter	Zone Information	Consecutive: 11-14, 21- 24, 31-34, 41-44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	01000000-01999999
1106 Universal Transmitter, internal/ external contact	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	01000000-01999999
1107 Micro Window Transmitter	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	NT	02000000-02999999
1108 Doorbell Module	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	DB	02000000-02999999
1114 Four-Zone Expander Module	Zone Information	Consecutive: 11-14, 21- 24, 31-34, 41-44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	08000000-08999999
1115 Temperature Sensor and Flood Detector	Zone Information	11-14,21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	SV	08000000-08999999

Models	Program In	XT50 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1116 Relay Output	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999
1117 LED Annunciator	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999
1118 Remote Indicator Light	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999
1119 Door Sounder	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	NT or DY	02000000-02999999
1119 Door Sounder (Output)	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999
1122 PIR	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	NT	09500000-09999999
1126R Ceiling Mount PIR	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	NT	09100000-09499999
1127 Wall Mount Curtain PIR	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	NT	09100000-09499999

Models	Program In	XT50 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1128 Glassbreak	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	NT	03000000-03999999
1131 Recessed Contact	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	02000000-02999999
1134 Access Control Module	Device Setup	1-8	DOOR	n/a	WLS	14300000-14499999
1135 Siren	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15200000-15999999
1136 Remote Chime	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15200000-15999999
1137 LED Emergency Light	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15200000-15999999
1139 Bill Trap	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	PN	02000000-02999999
1141 Wall Button	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	04000000-04999999

Models	Program In	XT50 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1142 Two-button Hold-Up	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	PN	04000000-04999999
1144 Key fob	Key Fobs	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	05900000-59999999
1148 Personal Pendant	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	EM	04000000-04999999
1154 Four-Zone Input Module	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	08000000-08999999
1158 Eight-Zone Input Module	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	Any	08000000-08999999
1164 Smoke Detector with Sounder	Zone Information	11-14, 21-24, 31-34, 41-44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	FI	07000000-07999999
1166 Smoke Ring	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	FI	06000000-06999999

Models	Program In	XT50 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1168 CO/ Smoke/Low Temp Combo Detector	Zone Information	Consecutive: 11-14, 21- 24, 31-34, 41-44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	FI + CO + SV	07000000-07999999
1183 Heat Detector	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	FI	06000000-06999999
1184 Carbon Monoxide Detector	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 80; 81-84; 85-99	n/a	n/a	CO	06000000-06999999
9000 Series Thinline Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14000000-14299999
9800 Graphic Touchscreen Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14500000-14999999

7.5.6 XT30

The following table columns are arranged to follow the typical panel programming order and values required for each item. For example, you should first program a wireless keypad in Device Setup, where you give it a device number, select a device type, select a device communication type, then enter the wireless serial number before programming other options.

For additional installation requirements and programming options, refer to the model's installation guide.

- **Models:** The accessory item's model number and name, linked to its installation guide.
- **Program In:** The menu where you program the accessory: Device Setup, Zone Information, Output Information, or Key Fobs.
- **Device, Zone, or Output Number:** The range of numbers for the accessory, depending on where it is programmed. See above. Keep in mind that although any device can be programmed as device 1 in the panel, that address should be reserved for the primary system keypad in most cases.
- **Device Type:** If the accessory is programmed in Device Setup, this lists possible device types.
- **Device Communication Type:** If the accessory is programmed in Device Setup, this lists possible communication types.
- **Zone Type:** If the accessory is programmed in Zone Information, this lists possible zone types.
- **Wireless SN Range:** For a wireless device, the typical serial number range of its class.

Models	Program In	XT30 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
734 Access Control Module	Device Setup	1-8	DOOR	KPD or AX-BUS	n/a	n/a
734N/734N-POE Network Access Control Module	Device Setup	1-8	DOOR	KPD or NET	n/a	n/a
7000 Series Thinline Keypads	Device Setup	1-8	KPD or DOOR	KPD	n/a	n/a
7300 Series Icon Keypads	Device Setup	1-8	KPD	KPD	n/a	n/a

Models	Program In	XT30 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
7463 Network Thinlilne Keypads	Device Setup	1-8	KPD	NET	n/a	n/a
7800 Series Graphic Touchscreen Keypad	Device Setup	1-8	KPD or DOOR	KPD	n/a	n/a
1100R Repeater	Zone Information	Consecutive if more than one per panel: 11-14, 21-24, 31-34, 41-44, 51- 54, 61-64, 71-74, 81-84	AUX1	n/a	AUX1	13000000-13999999
1100T Wireless Translator	Device Setup	2-8	1100T	n/a	n/a	13000000-13999999
1100T Wireless Translator	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	Non-DMP SN
1101 Universal Transmitter	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	01000000-01999999
1102 Universal Transmitter, external contact	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	01000000-01999999

Models	Program In	XT30 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1103 Universal Transmitter	Zone Information	Consecutive: 11-14, 21- 24, 31-34, 41-44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	01000000-01999999
1106 Universal Transmitter, internal/ external contact	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	01000000-01999999
1107 Micro Window Transmitter	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	NT	02000000-02999999
1108 Doorbell Module	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	DB	02000000-02999999
1114 Four-Zone Expander Module	Zone Information	Consecutive: 11-14, 21- 24, 31-34, 41-44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	08000000-08999999
1115 Temperature Sensor and Flood Detector	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	SV	08000000-08999999
1116 Relay Output	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999

Models	Program In	XT30 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1117 LED Annunciator	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999
1118 Remote Indicator Light	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999
1119 Door Sounder	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	NT or DY	02000000-02999999
1119 Door Sounder (Output)	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15100000-15199999
1122 PIR	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	NT	09500000-09999999
1126R Ceiling Mount PIR	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	NT	09100000-09499999
1127 Wall Mount Curtain PIR	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	NT	09100000-09499999
1128 Glassbreak	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	NT	03000000-03999999

Models	Program In	XT30 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1131 Recessed Contact	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	02000000-02999999
1134 Access Control Module	Device Setup	1-8	DOOR	n/a	WLS	14300000-14499999
1135 Siren	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15200000-15999999
1136 Remote Chime	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15200000-15999999
1137 LED Emergency Light	Output Information	31-34 (slow); 41-44 (fast)	n/a	n/a	n/a	15200000-15999999
1139 Bill Trap	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	PN	02000000-02999999
1141 Wall Button	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	04000000-04999999
1142 Two-button Hold-Up	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	PN	04000000-04999999

Models	Program In	XT30 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1148 Personal Pendant	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	EM	04000000-04999999
1154 Four-Zone Input Module	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	08000000-08999999
1158 Eight-Zone Input Module	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	Any	08000000-08999999
1164 Smoke Detector with Sounder	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	FI	07000000-07999999
1166 Smoke Ring	Zone Information	11-14, 21-24, 31-34, 41-44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	FI	06000000-0 6999999
1168 CO/ Smoke/Low Temp Combo Detector	Zone Information	Consecutive: 11-14, 21- 24, 31-34, 41-44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	FI + CO + SV	07000000-07999999
1183 Heat Detector	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	FI	06000000-06999999

Models	Program In	XT30 Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1184 Carbon Monoxide Detector	Zone Information	11-14, 21-24, 31-34, 41- 44, 51-54, 61-64, 71-74, 81-84	n/a	n/a	CO	06000000-06999999
9000 Series Thinline Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14000000-14299999
9800 Graphic Touchscreen Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14500000-14999999

7.5.7 XTL

The following table columns are arranged to follow the typical panel programming order and values required for each item. For example, you should first program a wireless keypad in Device Setup, where you give it a device number, select a device type, select a device communication type, then enter the wireless serial number before programming other options. For additional installation requirements and programming options, refer to the model's installation guide.

- **Models**: The accessory item's model number and name, linked to its installation guide.
- **Program In**: The menu where you program the accessory: Device Setup, Zone Information, Output Information, or Key Fobs.
- **Device, Zone, or Output Number**: The range of numbers for the accessory, depending on where it is programmed. See above. Keep in mind that although any device can be programmed as device 1 in the panel, that address should be reserved for the primary system keypad in most cases.
- **Device Type**: If the accessory is programmed in Device Setup, this lists possible device types.
- **Device Communication Type**: If the accessory is programmed in Device Setup, this lists possible communication types.
- **Zone Type**: If the accessory is programmed in Zone Information, this lists possible zone types.
- **Wireless SN Range**: For a wireless device, the typical serial number range of its class.

Models	Program In	XTL Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
7463 Network Thinline Keypads	Device Setup	1-8	KPD	NET	n/a	n/a
1100R Repeater	Zone Information	Consecutive if more than one per panel: 1-99	AUX1	n/a	AUX1	13000000-13999999
1100T Wireless Translator	Device Setup	2-8	1100T	n/a	n/a	13000000-13999999
1100T Wireless Translator	Zone Information	1-99	n/a	n/a	Any	Non-DMP SN
1101 Universal Transmitter	Zone Information	1-99	n/a	n/a	Any	01000000-01999999

Models	Program In	XTL Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1102 Universal Transmitter, external contact	Zone Information	1-99	n/a	n/a	Any	01000000-01999999
1103 Universal Transmitter	Zone Information	Consecutive: 1-99	n/a	n/a	Any	01000000-01999999
1106 Universal Transmitter, internal/ external contact	Zone Information	1-99	n/a	n/a	Any	01000000-01999999
1107 Micro Window Transmitter	Zone Information	1-99	n/a	n/a	NT	02000000-02999999
1108 Doorbell Module	Zone Information	1-99	n/a	n/a	DB	02000000-02999999
1114 Four-Zone Expander Module	Zone Information	Consecutive: 1-99	n/a	n/a	Any	08000000-08999999
1115 Temperature Sensor and Flood Detector	Zone Information	1-99	n/a	n/a	SV	08000000-08999999
1116 Relay Output	Output Information	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	15100000-15199999

Models	Program In	XTL Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1117 LED Annunciator	Output Information	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	15100000-15199999
1118 Remote Indicator Light	Output Information	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	15100000-15199999
1119 Door Sounder	Zone Information	1-99	n/a	n/a	NT or DY	02000000-02999999
1119 Door Sounder (Output)	Output Information	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	15100000-15199999
1122 PIR	Zone Information	1-99	n/a	n/a	NT	09500000-09999999
1126R Ceiling Mount PIR	Zone Information	1-99	n/a	n/a	NT	09100000-09499999
1127 Wall Mount Curtain PIR	Zone Information	1-99	n/a	n/a	NT	09100000-09499999
1128 Glassbreak	Zone Information	1-99	n/a	n/a	NT	03000000-03999999
1131 Recessed Contact	Zone Information	1-99	n/a	n/a	Any	02000000-02999999
1134 Access Control Module	Device Setup	1-8	DOOR	n/a	WLS	14300000-14499999

Models	Program In	XTL Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1135 Siren	Output Information	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	15200000-15999999
1136 Remote Chime	Output Information	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	15200000-15999999
1137 LED Emergency Light	Output Information	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	15200000-15999999
1139 Bill Trap	Zone Information	1-99	n/a	n/a	PN	02000000-02999999
1141 Wall Button	Zone Information	1-99	n/a	n/a	Any	04000000-04999999
1142 Two-button HoldUp	Zone Information	1-99	n/a	n/a	PN	04000000-04999999
1144 Key Fob	Key Fobs	51-54 (slow); 61-64 (fast)	n/a	n/a	n/a	05900000-59999999
1148 Personal Pendant	Zone Information	1-99	n/a	n/a	EM	04000000-04999999
1154 Four-Zone Input Module	Zone Information	1-99	n/a	n/a	Any	08000000-08999999
1158 Eight-Zone Input Module	Zone Information	1-99	n/a	n/a	Any	08000000-08999999

Models	Program In	XTL Device, Zone, or Output Number	Device Type	Device Communication Type	Zone Type	Wireless SN Range
1164 Smoke Detector with Sounder	Zone Information	1-99	n/a	n/a	FI	07000000-07999999
1166 Smoke Ring	Zone Information	1-99	n/a	n/a	FI	06000000-06999999
1168 CO/ Smoke/Low Temp Combo Detector	Zone Information	Consecutive: 1-99	n/a	n/a	FI + CO + SV	07000000-07999999
1183 Heat Detector	Zone Information	1-99	n/a	n/a	FI	06000000-06999999
1184 Carbon Monoxide Detector	Zone Information	1-99	n/a	n/a	CO	06000000-06999999
9000 Series Thinline Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14000000-14299999
9800 Graphic Touchscreen Keypad	Device Setup	1-8	KPD or DOOR	WLS	n/a	14500000-14999999

7.5.8 Communication Paths

To program communication paths, go to **Program** > **Communication Paths** > **Path** and select **New**. After configuring relevant settings, select **Apply** to save changes.

Configure Paths

1. In **Account Number**, enter the 1-5 digit number used to identify the panel.
2. In **Transmit Delay**, enter the number of seconds the panel waits to send burglary zone reports to the receiver. Other zone types are sent immediately and alarms are not delayed during this period. The valid range is **15-45** seconds. The default is **30 seconds**.
3. In **Path**, select the number of the path. The valid range is **1-8**. Path 1 is reserved for primary communication.
4. In **Comm Type**, select the communication type for the path used to report events to receivers.
5. In **Path Type**, select **Primary** or **Backup**.

Configure Supervision

1. In **Test Report**, select one of the following options:
    - **Yes:** Allows the programmed test report to be sent on the path currently being programmed
    - **No:** Does not allow test reports to be sent on this path
    - **Defer:** Does not allow test reports to be sent on this path if the panel communicates any message to the receiver within the time set in **Test Frequency**
2. In **Test Frequency**, enter a number from **1-60**.
3. In **Frequency Unit**, select the unit for test frequency.
4. If testing occurs on more than one day, select the day to send the report from **Test Day**.
5. If test frequency is set to days, enter the time of day in **Test Time**. To disable Test Time, enter **0:00 AM**.

Configure Checkin

1. In **Use Checkin**, select one of the following options:
    - **Yes:** Enables checkin
    - **No:** Disables checkin
    - **Random:** Allows panel to checkin at random times. Range is 6-60 minutes.
    - **Adaptive:** Allows a backup path to adapt to primary communication failure by adopting the checkin programming from the primary path
    - **Adaptive 3:** Allows a backup path to adapt to primary communication failure by adopting a 3 minute checkin and fail time
2. If applicable, enter the number of checkin minutes In **Check-In (Minutes)**. The valid range is **2-240** minutes for network or **3-240** minutes for cellular.
3. If applicable, enter the number of fail time minutes in **Fail Time (Minutes)**. The valid range is **0-240** minutes and should be equal or greater to the checkin time.

Configure Comm Type Details (Network, Cellular, Wi-Fi)

1. To enable communication path encryption on compatible panels, select **Encryption**.
2. For encrypted systems, select an **Encryption Scheme**. 256-bit encrypted messages to the SCS-1R receiver only communicate when using SCS-104 Receiver Line Cards with Version 102 or higher software.
3. To use IPv6 on network panels, select **IPv6**.

4. In **Receiver IP**, enter all digits of the receiver address with periods. For example, 192.168.0.1.
5. If using IPv6, enter all digits of the receiver address with colons in **Receiver IPv6**. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
6. **In Receiver Port**, enter the receiver port number. The default is **2001**.

Configure DD/CID Details (Digital Dialer, Contact ID)

In **1st Phone No**, enter the primary phone number. Phone numbers can have two lines of 16 characters each to equal up to 32 characters. To program a 3 second pause, enter P. Enter R as the first character for rotary (pulse) phone function. To cancel call waiting, enter ***70P** in the first position.

> ⚠ **Caution:** Canceling call waiting on a non-call waiting telephone line would prevent communication to the central station.

In **2nd Phone No**, enter the backup phone number. If attempts fail on the primary and backup phone line, the panel continues to attempt sending the message using the next programmed path.

7.5.9 Advanced Tab

Configure the following advanced settings according to your communication path type defined in the Path tab.

Configure Details

None

Send Comm Trouble: Determines if communication trouble on the path is sent to the receiver. A trouble message indicates both the path number and communication type that failed. Default is **Yes**.

Digital Dialer

Send Comm Trouble: Determines whether communication trouble on the path is sent to the receiver. A trouble message indicates both the path number and communication type that failed. Default is **Yes**.

Send Path Information: If communication troubles are sent, determines whether the path information such as path number, communication type, and path type are appended to the message. Default is **No**.

Network

Retry Seconds: Enter the number of seconds the panel should wait before retrying to send a message to the receiver if an acknowledgment was not received. The panel retries as many times as possible for a period of one minute before sending a network trouble message. Range is 6-15 seconds.

Substitution Code: Increases the level of security by helping to ensure that the panel sending the message to the receiver has not been substituted by another panel. To send a substitution code with every message, select **Yes**. To use the same substitution code as operating in the previous path, select **Shared**. To prevent substitution codes from being sent, select **No**. The default is **No**.

Send Comm Trouble: Determines if communication trouble on the path is sent to the receiver. A trouble message indicates both the path number and communication type that failed. Default is **Yes**.

Send Path Information: If communication troubles are sent, determines whether the path information such as path number, communication type, and path type are appended to the message. Default is **No**.

Protocol: Determines the protocol for communication. Select **TCP** or **UDP**. Default is **TCP**.

Contact ID

Send Comm Trouble: Determines if communication trouble on the path is sent to the receiver. A trouble message indicates both the path number and communication type that failed. Default is **Yes**.

893A: Allows reports to be sent to the receiver on a second DD line using the 893A module. If enabled, Test Report messages are sent to the receiver at the frequency configured in **Test Frequency** on the **Path** tab, alternating between the first and second phone line.

Second Line Prefix: If **893A** is enabled, enter a 3-digit prefix to be dialed before the second phone number. If no prefix is entered, the second phone number is dialed as originally entered.

Alarm Switchover: Enter the number of attempts to send an alarm message before switching to the next path. All non-alarm messages are sent for 10 attempts on the dialer before a switch is initiated. If the path immediately following this channel is not a backup path, this option has no effect. Range is 1-10 attempts. Default is **1**.

Cellular Network

Substitution Code: Increases the level of security by helping to ensure that the panel sending the message to the receiver has not been substituted by another panel. To send a substitution code with every message, select **Yes**. To use the same substitution code as operating in the previous path, select **Shared**. To prevent substitution codes from being sent, select **No**. The default is **No**.

First GPRS APN: Enter the first APN (Access Point Name). This allows an access point for cellular communication and is used to connect to a DNS network. The APN may contain two lines of 16 characters to equal 32 characters. Default is **SECURECOM400**. This option is not used when CDMA modems are used for communication.

Send Communication Trouble: Determines if communication trouble on the path is sent to the receiver. A trouble message indicates both the path number and communication type that failed. Default is **Yes**.

Send Path Information: If communication troubles are sent, determines whether the path information such as path number, communication type, and path type are appended to the message. Default is **No**.

Wi-Fi

Retry Seconds: Enter the number of seconds the panel should wait before retrying to send a message to the receiver if an acknowledgment was not received. The panel retries as many times as possible for a period of one minute before sending a network trouble message. Range is **6-15 seconds**.

Substitution Code: Increases the level of security by helping to ensure that the panel sending the message to the receiver has not been substituted by another panel. To send a substitution code with every message, select **Yes**. To use the same substitution code as operating in the previous path, select **Shared**. To prevent substitution codes from being sent, select **No**. The default is **No**.

Send Comm Trouble: Determines if communication trouble on the path is sent to the receiver. A trouble message indicates both the path number and communication type that failed. Default is **Yes**.

Send Path Information: If communication troubles are sent, determines whether the path information such as path number, communication type, and path type are appended to the message. Default is **No**.

Protocol: Determines the protocol for communication. Select **TCP** or **UDP**. Default is **TCP**.

RS232 (XR100/XR00 only)

Retry Seconds: Enter the number of seconds the panel should wait before retrying to send a message to the receiver if an acknowledgment was not received. The panel retries as many times as possible for a period of one minute before sending a network trouble message. Range is **6-15 seconds**.

Substitution Code: Increases the level of security by helping to ensure that the panel sending the message to the receiver has not been substituted by another panel. To send a substitution code with every message, select Yes. To use the same substitution code as operating in the previous path, select **Shared**. To prevent substitution codes from being sent, select **No**. The default is **No**.

232 Port: If using the panel's onboard RS232 connection, select **Onboard**. If using a Model 461 Adapter Card, select the appropriate port. If using a 462N Network Interface Card, select **Port A**. Reset the panel to initiate communication over RS232.

232 Setup String: Enter the destination address. The setup string can contain a maximum of 32 characters. For example, an address including an IP and port number is entered as **AT#UC192.168.000.001#2001**.

Send Comm Trouble: Determines if communication trouble on the path is sent to the receiver. A trouble message indicates both the path number and communication type that failed. Default is **Yes**.

Send Path Information: If communication troubles are sent, determines whether the path information such as path number, communication type, and path type are appended to the message. Default is **No**.

Configure Reports

Alarm

This option is available for primary path types. All backup paths within the group follow the same programming. Default is **Yes**.

When **Yes** is selected, the following reports are sent for all zone types:

- Alarm
- Bypass
- Reset
- Restore

When **Fire** is selected, the following reports are sent for Fire, Fire Verify and Supervisory Zones:

- Alarm
- Bypass
- Reset
- Restore

Supv/Trouble Reports (Supervisory and Trouble)

This option is available for primary path types. All backup paths within the group follow the same programming. Default is **Yes**. Serviceman reports are sent regardless of the selection made.

When **Yes** is selected, the following reports are sent for all zone types:

- Trouble
- Low
- Battery
- Missing
- Fault
- Restorals
- System Troubles
- System Restoral

When Fire is selected, the following reports are sent for Fire, Fire Verify and Supervisory Zones:

- Trouble
- Low Battery
- Missing
- Fault
- Restorals
- System Troubles
- System Restoral

O/C_User Reports (Opening, Closing, and User)

This option is available for primary path types. All backup paths within the group follow the same programming. The default is **Yes**.

When **Yes** is selected, the following reports are sent for all zone types:

- Opening
- Code changes
- Closing
- Schedule changes
- Bypass
- Holiday date changes
- Reset

Door Access

This option is available for primary path types. All backup paths within the group follow the same programming. The default is **Deny**.

To enable both Door Access Granted and Door Access Denied reports, select **Yes**. To enable Door Access Denied reports, select **Deny**. To disable Door Access reports, select **No**.

Door Access Granted reports are only sent if the keypad number has also been selected in Access Keypads in the **SYSTEM REPORTS** menu.

Panic Test (Network only)

To enable Panic Test reports, select **Yes**. To disable Panic Test reports, select **No**. The default is **No**.

7.5.10 Network Options

To program network options, go to **Program** > **Network Options**. After configuring relevant settings, select **OK**.

Configure Options

1. To enable DHCP, select **DHCP**. To enter network options manually, clear **DHCP**. When using a hardwired connection on XR panels, users can program the specific DNS the panel should use even when DHCP is enabled.
2. In **Local IP Address**. enter the local IP of the panel with periods. The default is **192.168.0.250**.
3. In **Gateway Address**, enter the panel gateway address with periods. The default is **192.168.0.1**.
4. In **Subnet Mask**, enter the panel subnet mask with periods. The default is **255.255.255.0**.
5. In **DNS Server**, enter the address of the DNS (Domain Name System) used by the panel to resolve domain names into IP addresses. The default is **192.168.0.1**.
6. In **Passphrase**, enter the passphrase for encrypted network communication with the receiver. If you leave the Passphrase blank, the panel communicates with the receiver, but the data is not encrypted. The valid range is 8-16 alphanumeric characters. The default is blank. Do not lose the passphrase. A lost or forgotten passphrase requires that the panel and every line card at the receiver be individually reprogrammed with a new passphrase.
7. In **734N Listen Port**, enter the port number that the 734N/734N-POE uses to send communication to the panel. Ensure this is the same port that is programmed in Panel IP Port within the 734N/734N-POE Communication programming menu. The 734N Listen Port cannot be the same as the panel network programming port.
8. In **734N Passphrase**, enter a passphrase to encrypt communication with the734N/734N-POE module. Ensure the passphrase matches the one in communication programming of the 734N. The valid range is 8-16 alphanumeric characters. The default is blank. A passphrase is required for operation.
9. **Enable XR/X1 Communication Communication**: Select **Yes** to enable XR to XR communication. Select **No** to leave this option disabled.
10. **DDP Passphrase**: This option only displays if XR/X1 Communication is set to **Yes**. Enter a passphrase to encrypt XR to XR communication. The valid range is 8-16 characters.

Configure Wi-Fi Settings (Wi-Fi only)

1. In **SSID**, enter the name of the wireless network.
2. In **Security**, select **WEP**, **WPA**, or **None**. When possible, use **WPA** for wireless communication.
3. In **Passphrase**, enter the network password.

Enable IPv6

To enable IPv6, select **DHCP**, then select **IPv6**. IPv6 information is automatically populated when connected to a panel.

7.5.11 Messaging Setup

Messaging Setup allows you to configure information for sending SMS messages between the panel and mobile devices. Messaging setup is only shown for panels that have firmware version 202 and lower.

1. Go to **Program > Messaging Setup**.
2. To enable SMS messaging, select **Enable Messaging**.
3. In **System Name**, enter a name to be used as the sender of the message. If this field is blank, the panel account number is sent.
4. In **Destination**, enter a mobile device number in each destination field. In the accompanying destination **User Num** field, enter the user number for the account.
5. To allow the panel to send opening and closing messages over SMS, select **SMS O/C**.
6. In **Monthly Limit**, enter the limit of your rate plan. A monthly limit of 0 (zero) is unlimited. The valid range is **0-999**. The default is **0**.

7.5.12 Device Setup

When programming devices, consult the Quick Programming Reference as needed. To add a device, complete the following steps:

1. Go to **Program** > **Device Setup** > **Path** and select **New**.
2. In **Device Number**, enter the device's number:
      - The range for keypad, fire, and expander devices is 1-16 for XR550 panels and 1-8 for all other panels.
      - The range for doors is 1-16 and 501-961 for XR550 panels and 1-8 for all other panels.
      - The valid V-Plex device numbers are 501, 601, 701, 801, and 901. On XR150 panels, device 501 is reserved for a V-Plex device.
      - The valid range for 1100T is 2-16 for XR Series panels or 2-8 for all other compatible panels.
      - The valid range for a XR panel integration is 1-16.
3. In **Name**, enter a name for the device.
4. In **Device Type**, select one of the following types:
      - Door (DOOR)
      - Fire (FI)
      - Keypad (KPD)
      - Zone Expander (EXP)
      - 1100T Wireless Translator (TLR)
      - Vplex PL-500 (VPX)
      - Secondary XR panel (PNL)
      - Camera (CAM)
5. In **Device Communication Type**, select **Keypad Bus**, **AX-Bus**, **Network**, or **Wireless**.
6. For wireless devices, enter the device **Serial Numbe**r and select a **Supervision Time**.
7. For 1100T Wireless Translators, select an 1100T Frequency: o **HWL** (345 MHz) (Honeywell 5800) o **2GIG** (345 MHz) (2GIG) o **INT** (319.5 MHz) (Interlogix) o **DSC** (433 MHz) (DSC)
8. Configure additional options as needed.
9. If necessary, enter a description for the device installation.
10. To configure 734 options for doors, go to the **734 Options** tab. To configure card formats, select **Card Formats**.
11. Select **Apply**. Repeat steps 1-10 to add more devices as needed.
12. Select **OK**.

7.5.13 Z-Wave Setup

To view, rename, backup, and restore Z-Wave devices, go to **Program > Z-Wave Setup**.

If your panel has existing devices programmed, they will be displayed here after the panel has been retrieved. Device types include Lights, Locks, Thermostats, Controllers or Other. If the retrieved device is not a Light, Lock, Thermostat or Controller, they will be displayed as Other.

The device name may be edited. To edit a device, open the tab for the device type, select the text in **Name**, rename the device, then select **Apply**.

Remote Link can store a copy of all Z-Wave programming in case there is a data loss at the panel or an associated 738Z Z-Wave Interface module. This allows programming to be sent back to the panel or the 738Z if either is damaged. You can back up Z-Wave settings by selecting **Backup**. If a backup exists, restore the device from backup by selecting **Restore**.

7.5.14 Favorites

Z-Wave devices must be added to the panel and then retrieved using Remote Link before they can be added to a Favorite. To add a favorite, complete the following steps.

1. Go to **Program > Favorites**.
2. In **Number**, enter a number for the Favorite.
3. In **Name**, enter a name for the Favorite.
4. In the Z-Wave section, select **Add**.
5. Open the tab of the device for the favorite, then select the specific device from **Device**.
6. Select actions for the Favorite.
7. Select **Apply**. Repeat steps 1-7 to add more favorites as needed.
8. Select **OK**.

7.5.15 Remote Options

The Remote Options window allows you to enter the information needed for connecting to the panel with Remote Link, Dealer Admin, Tech APP, and Virtual Keypad.

1. Go to **Program > Remote Options > Standard**.
2. In **Remote Key**, enter the remote key programmed in the panel. The remote key is required for connection to Remote Link.
3. To allow users to disarm the system from Virtual Keypad, select **Remote Disarm**.
4. In the **Dialer**, **Network**, **Cellular**, and **RS232** sections, configure settings as needed for the panel connection type. For field descriptions, refer to "Standard Fields Reference".
5. To allow users to connect to the panel with Virtual Keypad, enter your app key in **App Key**.
6. In **Send Local Changes**, select one of the following options:
   - **None:** Does not allow the panel to automatically update remote programming workstations.
   - **NET:** Allows the panel to update remote programming workstations over network.
   - **DD:** Allows the panel to update remote programming workstations over dialer.
7. In **Remote Change IP**, enter the IP address for the workstation to send changes for **NET**.
8. In **Remote Change Port**, enter the port for the workstation to send changes for **NET**.
9. In **Remote Phone Number**, enter the phone number to send changes to for **DD**.
10. Select **OK**.

Standard Fields Reference

Dialer

- **Armed Answer Rings:** Enter the number of times to allow the phone line to ring before it answers when all areas of the system are armed. Range is 0-15. Default is **8**. If 0 (zero) is entered, the panel does not answer the phone when all system areas are armed.
- **Disarmed Answer Rings:** Enter the number of times to allow the phone line to ring before it answers when any areas of the system are disarmed. Range is 0-15. Default is **8**. If 0 (zero) is entered, the panel does not answer the phone when any system areas are disarmed.
- **PC Modem:** Allows panel dialer connection for remote programming at 2400 baud. Enable this option to allow communication through an SCS-105.
- **Alarm Receiver:** Select **Yes** to enable the panel to accept remote commands and programming from the alarm receiver. If you select **No**, the panel will not accept remote commands and programming from the alarm receiver.
- **Service Receiver:** Select **Yes** to enable the panel to accept remote commands and programming from a secondary service receiver other than the alarm receiver. This option must be **Yes** to allow programming from a directly connected computer using Remote Link. If you select **No**, the panel will not accept remote commands and programming from a secondary service receiver.

Network

- **Allow Network Remote:** Allow remote programming over network connection.
- **Encrypt Network Remote:** Encrypt data sent over network.
- **Network Programming Port:** Enter the panel port. Default is 2001.

Cellular

- **Allow Cell Remote:** Allow remote programming over cellular connection.
- **Encrypt Cell Remote:** Encrypt data sent over cell.

- **First GPRS APN:** Enter the first APN (Access Point Name). This allows an access point for cellular communication and is used to connect to a DNS network. Default is **SECURECOM400**.

RS232

- **Allow RS-232 Remote:** Enable to allow remote programming over the onboard RS-232 port. Default is enabled.

7.5.16 Entre

For connection to Entré, configure the following settings as needed:

Entré Connection: Select the connection type.

Entré IPv6: Select this option to enable IPv6.

Entré Incoming TCP Port: Enter the port number for the incoming Entré connection. The port identifies the port used to communicate with the Entré software. Default is **2011**.

Entré IP: Enter the Entré IP address where the panel sends network messages. Default is **0.0.0.0**.

Entré IPv6 Address: Enter the Entré IPv6 address where the panel sends network messages. Default is **0:0:0:0:0:0:0:0**.

Entré Outbound TCP Port: Enter the port number for the outbound Entré connection. The port identifies the port used to communicate messages to the Entré software. Default is **2001**.

Entré Backup Connection: Select a backup connection type. Entré Backup IP: Enter the backup Entré IP address where the panel sends network messages. Default is 0.0.0.0.

Entré Backup IPv6: Enter the backup Entré IPv6 address where the panel sends network messages. Default is **0:0:0:0:0:0:0:0**.

Entré Backup TCP Port: Enter the backup port number for the outbound Entré connection. The port identifies the port used to communicate messages to the Entré software. Default is **2001**.

Entré Arm/Disarm Reports: Sends arming, disarming and Late to Close events. Includes the area number, name and action, the user number and name, and the time and date the event occurred.

Entré Zone Reports: Sends changes in the status of active zones. Includes the zone number, name, type, the action (alarm, trouble, bypass, etc.), user number (if applicable), and area name. For a Walk Test, Verify and Fail messages are sent for each zone.

Entré User Command Reports: Sends user code changes, schedule changes, and door access denied events.

Entré Door Access Reports: Sends door access activity: door number, user number and name, and time and date the event occurred.

Entré Supervisory Reports: Sends system monitor reports, such as AC and battery, and system event reports. If this feature is enabled, the panel also sends Abort, Exit Error, Ambush, System Recently Armed, Alarm Bell Silenced, Unauthorized Entry, and Late to Close reports.

Entré Check-In Minutes: Select the rate at which check-in messages are sent over the Entré connection. Select 0 (zero) to disable check in messages. Range is 0, 3-240 minutes. Default is **0**.

Entré Passphrase: To enable encryption, enter the alphanumeric Entré passphrase. If you leave the passphrase blank, the panel communicates with Entré, but the data is not encrypted. Default is blank.

7.5.17 Integrator Path

For connection to an integrator path, configure the following settings as needed:

Connection: Select the connection type. Incoming TCP Port: Enter the port number for the incoming connection. The port identifies the port used to communicate with the integrator software. Default is **2011**.

Integrator IP: Enter the IP address where the panel sends network messages. Default is **0.0.0.0**.

Outbound TCP Port: Enter the port number for the outbound integrator connection. The port identifies the port used to communicate messages to the integrator. Default is **2001**.

Backup Connection: Select a backup connection type.

Backup IP: Enter the backup IP address where the panel sends network messages. Default is **0.0.0.0**.

Backup TCP Port: Enter the backup port number for the outbound connection. The port identifies the port used to communicate messages to the software. Default is **2001**.

Arm/Disarm Reports: Sends arming, disarming and Late to Close events. Includes the area number, name and action, the user number and name, and the time and date the event occurred.

Zone Reports: Sends changes in the status of active zones. Includes the zone number, name, type, the action (alarm, trouble, bypass, etc.), user number (if applicable), and area name. For a Walk Test, Verify and Fail messages are sent for each zone.

User Cmd Reports: Sends user code changes, schedule changes, and door access denied events.

Door Access Reports: Sends door access activity: door number, user number and name, and time and date the event occurred.

Supervisory Reports: Sends system monitor reports, such as AC and battery, and system event reports. If this feature is enabled, the panel also sends Abort, Exit Error, Ambush, System Recently Armed, Alarm Bell Silenced, Unauthorized Entry, and Late to Close reports.

Check-In Minutes: Select the rate at which check-in messages are sent over the connection. Select 0 (zero) to disable check in messages. Range is 0, 3-240 minutes. Default is **0**.

Passphrase: To enable encryption, enter the alphanumeric passphrase. If you leave the passphrase blank, the panel communicates with the integrator, but the data is not encrypted. Default is blank.

7.5.18 System Reports

The System Reports window allows you to select the reports the panel can send to the central station receiver. You can also enable keypad door access reports by device address and enable the panel Ambush code option. The options available in System Reports depend on the panel type and firmware version.

1. Go to **Program > System Reports**.
2. In **Zone Restorals**, select **Yes** to enable zone restoral reports, or No to disable zone restoral reports. To send zone restoral reports when a zone is disarmed, select **Disarm**.
3. In **Open / Close Enable**, select **Yes** to enable opening and closing reports. Select **No** to disable opening and closing reports.
4. In **Access Keypad Enable**, enter the keypad addresses that you want to include in access reports.
5. To send specific reports to the receiver, select the following reports as needed:
    - **Abort Reports:** Sent any time an area is disarmed after an alarm report has been sent and the bell cutoff time has not expired
    - **Bypass Reports:** Sends all zone bypasses, resets, and force arm reports to the receiver
    - **Schedule Change Reports:** Sends all schedule changes to the receiver
    - **Code Change Reports:** Sends all code additions, changes, and deletions to the receiver
    - **Ambush Reports:** Sends an ambush report to the central station whenever user code number one is entered at a keypad
    - **Send Stored Messages:** If a panel loses communication with the receiver, it will store any messages that are not able to be sent while communication was down.
    - **Entry Check-In Protection:** Enables the panel to send a check-in message when an Entry Delay begins.
6. In **Late To Open**, enter the number of minutes that the system can be disarmed after the scheduled opening time before a Late to Open message sent. Range is 0-240 minutes
7. In **Early To Close**, enter the number of minutes that the system can be armed before the scheduled closing time. Range is 0-240 minutes
8. Select **OK**.

7.5.19 System Options

System Options allows you to program how the areas operate for arming and disarming.

1. Go to **Program > System Options**.
2. Program settings in **Options**, **Miscellaneous Options**, **Languages**, **Time Change**, **Delays**, **Wireless**, and **Advanced Options** as needed. Refer to "System Options Programming Reference" for details.
3. Select **OK**.

System Options Programming Reference

The following reference provides basic descriptions of each field in System Options. Configure each setting as needed.

Options

System Arming Type (XR, XT, XTL)

Area: All areas are programmed and controlled independently

All/Perimeter: Areas are divided into perimeter and interior

Home/Sleep/Away: Areas are divided into Home (perimeter), Sleep (perimeter and interior non-bedroom areas), and Away (all areas)

HSA with Guest: Areas are divided into one main Home/Sleep/Away system and two guest Home/Sleep/ Away systems

Instant Arm (XR)

Enabled: Ignore arming delays, arm instantly

Disabled: Arming delays are unaffected

Closing Wait (XR)

Enabled: Wait for acknowledgment from receiver and perform bell test (if enabled) before arming

Disabled: Arm without waiting for acknowledgment

Closing Code (XT, XTL)

Enabled: A code is required to arm the system

Disabled: A code is not required to arm the system

Closing Check (XT, XTL)

Enabled: Panel verifies that all areas are armed after a scheduled closing time passes

Disabled: Panel does not verify that all areas are armed after a scheduled closing time passes

Reset Swinger Bypass (XR, XT, XTL, Com)

Enabled: An automatically bypassed zone is reset if it remains in normal condition for one hour after bypass
Disabled: An automatically bypassed zone is not reset based on condition and time elapsed

Time Display (XT, XTL)

Enabled: Keypads display the time and day in the status list

Disabled: Keypads do not display the time and day

Telephone Access (XT)

Enabled: Allow DTMF telephones to arm, disarm, and check armed status

Disabled: Do not allow DTMF telephones to arm, disarm, and check armed status

Enable Keypad Panic Keys (XR, XT, XTL)

Enabled: Allow keypad panic keys to send panic messages to central station receivers

Disabled: Does not allow keypad panic keys to send panic messages to central station receivers

Enhanced Zone Test (XR)

Enabled: Send verification messages and detailed zone information with walk, panic, and burglary tests Disabled: Send standard information during walk, panic, and burglary tests

Send 16 Character Names (XR)

Enabled: Sends the first 16 characters of the name field to the central station

Disabled: Send the exact number of characters in the name field to the central station

Allow Own User Code Change (XR)

Enabled: Allow users without user code permissions to change only their own user code

Disabled: Users without user code permissions cannot change their own user code

Panic Supervision (XR)

Enabled: Allow 30-day supervision of 1144-1P-PSV

Disabled: Does not allow 30-day supervision of 1144-1P-PSV. Use this setting if key fob is taken off site

Keypad Armed LED (XR)

All: Requires all areas to be armed before keypad LED lights

Any: Keypad LED lights when any area is armed

CID Message Format (Com)

DMP: Sends messages to the monitoring standard in standard DMP format with any CID messages appended.

CID: Sends messages to the monitoring center in raw CID format.

4-2: Sends messages to the monitoring center in 4-2 format.

SIA: Sends messages to the monitoring center in SIA format.

Miscellaneous Options

Swinger Bypass Trips (XR, XT, XTL, Com)

Enter the number of times a zone can go into an alarm or trouble condition within one hour without being automatically bypassed. Range is 1-6. Default is **2**.

Bypass Limit (XR)

Enter the maximum number of zones that can be bypassed in an area when the area is being armed. Range is 1-8. Entering 0 disables bypass limit. Default is **0**.

Weather Zip Code (XR, XT, XTL, Com)

Enter the panel zip code to display weather on keypads. Entering 0 disables weather. Default is **0**.

Keypad Input (Com)

To enable ECP passthru, select **ECP**.

To enable DSC passthru, select **DSC**.

To disable passthru, select **None**. Default is **None**.

Occupied Premises (XR, XT, XTL)

Enabled: Allow the panel to automatically disarm potentially occupied (perimeter zone is not tripped during the exit delay)

Disabled: Does not allow the panel to automatically disarm potentially occupied areas

Languages

Primary Programming Language (XR)

Select the language displayed in the programming menu.

Secondary Programming Language (XR)

Select a secondary language option to display in programming. Allows installers to choose between two languages. None disables secondary programming language.

Primary User Language (XR)

Select the language displayed in the user menu

Secondary User Language (XR)

Select a secondary language option to display in the user menu. Allows users to choose between two languages. None disables secondary programming language

Time Zone Changes (XR, XT, XTL, Com)

Select **NO** to not request time changes.

Select **SCS** to request time changes from the SCS-1R or SCS-VR Receiver.

Select **SCW** to request time changes from SecureCom Wireless.

Daylight Saving Time

This option only displays if you selected **SCW**. The default is **YES**.

Select **NO** to not observe daylight saving time.

Select **YES** to observe daylight saving time.

Hours from GMT (XR, XT, XTL, Com)

Enter the number of the panel time zone. Range is 0-23. Default is **6**. For more information, refer to "Time Zone Table"

Delays

Zone Activity Hours (XR, XT, XTL)

Enter the number of hours for the system to check for zone inactivity. Range is 0-9 hours. Entering 0 disables this feature. Default is **0** hours.

Arm/Disarm Activity Days (XT, XTL)

Enter a number of days a countdown timer is set for area arming and disarming activity. Range is 0-99 days. Default is **0** days.

Entry Delay (XR, XT, XTL, Com)

Enter a number of seconds for all exit type zones to use when an exit zone is faulted. Range is 30-250 seconds. Default for **Entry Delay 1** is **30 seconds**. Default for **Entry Delay 2** is **60 seconds**. Default for **Entry Delay 3** is **90 seconds**. Default for **Entry Delay 4** is **120 seconds**.

Exit Delay (XT, XTL, Com)

Enter a number of seconds for an exit delay. Range is 45-250 seconds. Default is **60 seconds**.

Cross Zone Time (XR, XT, XTL, Com)

Enter a number of seconds allowed between zone faults. Range is 4-250 seconds. Entering 0 disables this feature. Default is **4 seconds**.

Zone Retard Delay (XR)

Enter a number of seconds for a retard time assign to Fire, Supervisory, Auxiliary, Arming, and Panic zones. Range is 1-250 seconds. Entering 0 disables this feature. Default is **10 seconds**.

Power Fail Delay (XR, XT, XTL, Com)

Enter a number of hours that power should be disconnected before sending a power failure message to the receiver. Range is 1-15 hours. Entering 0 sends power failure reports in 15 seconds. Default is **1 hour**.

Wireless

Wireless House Code (XR, XT, XTL)

Enter a house code that allows the panel and peripheral wireless devices to identify each other. Ensure that buildings in close proximity are not programmed with the same house code. Range is 1-50. Entering 0 disables this feature. Default is **0**.

Use Built-In 1100 (XT)

Enabled: Allows use of the onboard module for wireless communication.

Disabled: Does not allow the use of the onboard module for wireless communication

Detect Wireless Jamming (XR, XT, XTL)

Enabled: The system monitors wireless signals for jamming.

Disabled: The system does not monitor wireless signals for jamming.

Trouble Audibles (XR, XT, XTL)

Any: Allows annunciation any time for wireless low battery and missing messages.

Day: Allows annunciation for wireless low battery and missing messages only between the hours of 9 AM and 9 PM.

Min: Allows annunciation for wireless low battery and missing messages only for Fire and Fire Verify zones between the hours of 9 AM and 9 PM.

1100 Wireless Encryption (XR, XT)

None: Does not allow encryption.

Both: Allows encryption only for selected wireless devices.

All: Allows encryption for all wireless devices.

1100 Passphrase (XR, XT)

Enter a passphrase for wireless communication that sets the panel encryption key. Passphrase must be an 8-digit hexadecimal string.

Advanced Options

Latched Supervisory (XR)

Enabled: Allows latching supervisory zone alarms on the keypad display until a sensor reset is performed.
Disabled: Does not allow latching supervisory zones.

7.5.20 Time Zone Table

GMT	City/Time Zone
0	London, Monrovia, Lisbon, Dublin, Casablanca, Edinburgh
1	Cape Verde Island, Azores
2	Mid-Atlantic, Fernando de Noronha
3	Buenos Aires, Georgetown, Brasilia, Rio de Janeiro
4	Atlantic Time (Canada), Caracas, La Paz, Santiago, Puerto Rico*, Virgin Islands*
5	Eastern Time (US, Canada), Bogota, Lima, Arequipa, Puerto Rico*, Virgin Islands*
6	Central Time (US, Canada), Mexico City, Saskatchewan, Cancun
7	Mountain Time (US, Canada), Edmonton, Arizona*
8	Pacific Time (US, Canada), Tijuana, Arizona*
9	Alaska
10	Hawaii*
11	Midway Island, American Samoa*, Hawaii*
12	Fiji, Marshall Island, Wellington, Auckland, Kwajalein, Kamchatka
13	Guam*, New Caledonia
14	Guam*, Sydney
15	Tokyo, Seoul
16	Hong Kong, Singapore

GMT	City/Time Zone
17	Bangkok, Hanoi
18	Dhaka, Almaty
19	Islamabad, Karachi
20	Abu Dhabi, Kazan, Dubai, Cairo
21	Moscow, Bagdad
22	Eastern Europe, Cape Town, Bangui
23	Rome, Paris, Berlin

7.5.21 Bell Options

The Bell Options window allows you to specify what type of alarm output the panel initiates for different types of alarms.

1. Go to **Program** > **Bell Options**.
2. Available actions include: Steady, Pulse, and Temporal 3, Temporal 4, and None. Selecting None for an alarm event will cause no alarm to sound for the specified type of alarm. Select actions as needed in each of the following options:
   - Fire Bell Action
   - Burglary Bell Action
   - Supervisory Bell Action
   - Panic Bell Action
   - Emergency Bell Action
   - Aux 1 Bell Action
   - Aux 2 Bell Action
   - Carbon Monoxide Action
3. In Bell Cutoff Time, enter the maximum number of minutes for the bell output to remain on. Range is 1-99 minutes. Default is **15 minutes**.
4. To enable an automatic 2 second bell test each time an area is completely armed from a keypad, select **Automatic Bell Test**.
5. In Bell Output, enter the output number to follow the panel bell output operation for all actions and off conditions. To disable the output, enter 0. Default is **0**.

> ℹ **Note:** Bell Output should not be programmed for a Model 1135/1135DB Wireless Siren when programmed in **Output Information** with **Trip with Panel Bell** enabled.

7.5.22 Output Options

Output Options allows you to assign individual outputs to activate for various events.

1. Go to **Program > Output Options**.
2. Program settings in **Options**, **Energy Saving**, and **Outputs** as needed. Refer to "Output Options Programming Reference" for details.
3. Select **OK.**

Output Options Programming Reference

The following reference provides basic descriptions of each field in Output Options. Configure each setting as needed.

Options

Cutoff Outputs (XR, XT, Com)

Enter outputs to turn off after the cutoff time. Range is 1-6.

Cutoff Time Minutes (XR, XT, Com)

Enter a number of minutes for outputs to remain on. Range is 1-99 minutes. Entering 0 results in continuous output. Default is **0 minutes**.

Energy Saving

Heat Saver Temperature (XR, XT, XTL, Com)

Enter a temperature for Z-Wave thermostat (heating) when the system is armed All or Away. Range is 1-99 degrees. Enter 0 to disable this feature. Default is **0**.

Cool Saver Temperature (XR, XT, XTL, Com)

Enter a temperature for Z-Wave thermostat (cooling) when the system is armed All or Away. Range is 1-99 degrees. Enter 0 to disable this feature. Default is **0**.

Outputs

Communication Fail Output (XR, XT, XTL, Com)

Enter the output to turn on when communication fails. Enter 0 to disable this feature. Default is **0**.

Fire Alarm Output (XR, XT, XTL)

Enter the output to turn on when a fire zone goes into alarm. Enter 0 to disable this feature. Default is **0**.

Fire Trouble Output (XR, XT)

Enter the output to turn on when a fire zone reports trouble. Enter 0 to disable this feature. Default is **0**.

Panic Alarm Output (XR, XT, XTL)

Enter the output to turn on when a panic zone goes into alarm. Enter 0 to disable this feature. Default is **0**.

Ambush Output (XR, XT)

Enter the output to turn on when an ambush code is entered at the keypad. Enter 0 to disable this feature. Default is **0**.

Entry Output (XR, XT, XTL)

Enter the output to turn on at the start of the entry delay time. Enter 0 to disable this feature. Default is **0**.

Begin Exit Output (XR, XT, XTL)

Enter the output to turn on at the start of the exit delay time. Enter 0 to disable this feature. Default is **0**.

End Exit Output (XR, XT, XTL)

Enter the output to turn on when an exit delay ends. Enter 0 to disable this feature. Default is **0**.

Ready Output (XR, XT, XTL)

Enter the output to turn on when all disarmed burglary zones are in a normal state. Enter 0 to disable this feature. Default is **0**.

Phone Trouble Output (XR)

Enter the output to turn on when phone trouble is reported. Enter 0 to disable this feature. Default is **0**.

Late to Close Output (XR, XT)

Enter the output to turn on when a closing schedule expires. Enter 0 to disable this feature. Default is **0**.

Device Fail Output (XR)

Enter the output to turn on when a device fails to respond to the panel. Enter 0 to disable this feature. Default is **0**.

Armed Output (XT, XTL, Com)

Enter the output to turn on when the system is armed. Enter 0 to disable this feature. Default is **0**.

Remote Arming Output (Com)

Enter the output to turn on when the system is armed from Virtual Keypad. Enter 0 to disable this feature. Default is **0**.

Sensor Reset Output (XR)

Enter the output to turn on when a sensor reset is performed. Enter 0 to disable this feature. Default is **0**.

Closing Wait Output (XR)

Enter the output to turn on when closing wait is initiated. Enter 0 to disable this feature. Default is **0**.

Disarmed Output (XR, XT, XTL)

Enter the output to turn on when the system is disarmed. Enter 0 to disable this feature. Default is **0**.

Burglary Output (XT, XTL)

Enter the output to turn on when a burglary zone goes into alarm. Enter 0 to disable this feature. Default is **0**.

Arm-Alarm Output (XR, XT, XTL)

Enter the output to turn on when the system is armed. If the system goes into alarm, the output pulses. Enter 0 to disable this feature. Default is **0**.

Supervisory Alarm Output (XR)

Enter the output to turn on when a supervisory zone goes into alarm. Enter 0 to disable this feature. Default is **0**.

Home/Perimeter Output (XR, XT)

Enter the output to turn on when a system is armed Home or Perimeter. Enter 0 to disable this feature. Default is **0**.

All/Away Output (XR, XT)

Enter the output to turn on when a system is armed All or Away. Enter 0 to disable this feature. Default is **0**.

Sleep Output (XR, XT)

Enter the output to turn on when a system is armed Sleep. Enter 0 to disable this feature. Default is **0**.

Carbon Monoxide Output (XR, XT)

Enter the output to turn on when a carbon monoxide detector goes into alarm. Enter 0 to disable this feature. Default is **0**.

Lockdown Output (XR)

Enter the output to turn on when a lockdown is initiated. Enter 0 to disable this feature. Default is **0**.

Zone Monitor Output (XR, XT)

Enter the output to turn on when a zone monitor tone is activated on a keypad. Enter 0 to disable this feature. Default is **0**.

7.5.23 Output Information

When programming outputs, consult the Quick Programming Reference as needed. To add output information, complete the following steps.

1. Go to **Program > Output Information** and select **New**.
2. In **Output Number**, enter the number of the output according the panel model.
3. In **Output Name**, name the output.
4. To enable Real-time status for the output, select **Real-time Status**.
5. If necessary, add a description of the output information.
6. Select **Apply**. Repeat steps 1-6 to add more outputs as needed.
7. Select **OK**.

7.5.24 Output Groups

This function allows you to group outputs to turn an entire group of outputs on and off together. You may assign output groups to areas of programming, such as Output Options, the same way that you assign single outputs. To add output groups, complete the following steps.

1. Go to **Program > Output Groups**. Select **New**.
2. In **Output Group Number**, enter the number of the output group. Range is 1-20.
3. In **Output Group Name**, enter a name for the output group.
4. In each **Output Number** field, enter the number of the outputs that you want to assign to a group separated by commas. Max is 8 outputs.
5. If necessary, add a description about each output group.
6. Select **Apply**. Repeat steps 1-6 to add more output groups as needed.
7. Select **OK**.

7.5.25 Menu Display

Menu Display allows you to select which keypad addresses display Armed Area status, Time, and Arm/Disarm status.

1. Go to **Program > Menu Display**.
2. In **Armed Area Status Display**, enter the keypad addresses that can display the armed areas for their partitions. For example, if address 1 is enabled here, it can display the armed areas within its partition.
3. In **Time Display**, enter the keypad addresses that can display the time and day of the week.
4. In **Arm Disarm Display**, enter the keypad addresses from which users can arm and disarm the system.
5. Select OK.

7.5.26 Status List

To configure the status list, complete the following steps.

1. Go to **Program > Status List**.
2. Enter the addresses of keypads to display each status as needed. For details, refer to "Status List Programming Reference".
3. Select **OK**.

Status List Programming Reference

The following reference provides basic descriptions of each field in Status List. Configure each setting as needed.

System Trouble Status Monitors

Enter the addresses of keypads that must display system troubles. This includes AC power, low battery, closing check, panel box tamper, phone line troubles, and wireless troubles. Range is 1-16. Default is **1-16**.

Fire Zone Keypads

Enter the addresses of keypads that must display fire zone alarms and troubles. Range is 1-16. Default is **1-16**.

Carbon Monoxide Zone Keypads

Enter the addresses of keypads that must display carbon monoxide zone alarms and troubles. Range is 1-16. Default is **1-16**.

Burglary Zone Keypads

Enter the addresses of keypads that must display burglary zone alarms and troubles. Range is 1-16. Default is **1-16**.

Supervisory Zone Keypads

Enter the addresses of keypads that must display supervisory zone alarms and troubles. Range is 1-16. Default is **1-16**.

Panic Zone Keypads

Enter the addresses of keypads that must display panic zone alarms and troubles. Range is 1-16. Default is blank.

Emergency Zone Keypads

Enter the addresses of keypads that must display emergency zone alarms and troubles. Range is 1-16. Default is blank.

Auxiliary 1 Zone Keypads

Enter the addresses of keypads that must display auxiliary 1 zone alarms and troubles. Range is 1-16. Default is blank.

Auxiliary 2 Zone Keypads

Enter the addresses of keypads that must display auxiliary 2 zone alarms and troubles. Range is 1-16. Default is blank.

Comm Path Trouble

Yes: Display communication trouble on keypads when any communication path fails

No: Does not display communication trouble on keypads when any communication path fails

All: Displays communication trouble on keypads when all communication paths collectively fail

7.5.27 PC Log Reports

PC Log Reports allows you to configure the types of reports that are sent from a panel to a workstation over network.

1. Go to **Program > PC Log Reports**.
2. Configure **Options** and **Net Options** as needed. For details, refer to "PC Log Reports Programming Reference".
3. Select **OK**.

PC Log Reports Programming Reference

The following reference provides basic descriptions of each field in PC Log Reports. Configure each setting as needed.

Options

Arm/Disarm Reports

Enabled: Sends arming, disarming, and late to close events

Disabled: Does not send arming, disarming, or late to close events

Zone Reports

Enabled: Sends zone status changes

Disabled: Does not send zone status changes

User Command Reports

Enabled: Sends user code changes, schedules changes, and door access denied events

Disabled: Does not send user code changes, schedule changes, or door access denied events

Door Access Reports

Enabled: Sends door access events

Disabled: Does not send door access events

Supervisory Reports

Enabled: Sends system monitor reports along with abort, exit error, system recently armed, late to close, ambush, alarm bell silenced, and unauthorized entry events

Disabled: Does not send system monitor and supervisory events

Real-time Status Reports

Enabled: Sends real-time status events for zones, doors, and outputs

Disabled: Does not send real-time status events

Net Options

Net IP Address

Enter the local IP of the workstation that receives panel reports separated by periods. Default is **0.0.0.0**.

Net Port

Enter the port of the workstation that receives panel reports. Default is **2001.**

7.5.28 Area Information

When programming area information, refer to device installation and panel programming guides as needed. To add area information, complete the following steps.

1. Go to **Program > Area** Information and select **New**.
2. Configure settings in Global Settings and standard area information as needed. For details, refer to "Area Information Programming Reference" in this article.
3. Select **Apply**. Repeat steps 1-3 to add more areas as needed.
4. Select **OK**.

Area Information Programming Reference

The following reference provides basic descriptions of each field in Area Information. Configure each setting as needed.

Global Settings

Global settings apply to all system areas.

Exit Delay (XR)

Enter the number of seconds for the global exit delay. Range is 30-250. Default is **60 seconds**.

Early Morning Ambush (XR)

Enter the number of minutes before a silent alarm is sent to the central station. Range is 1-15 minutes. Entering 0 disables this feature. Default is 0 seconds.

Closing Check (XR)

Enabled: Panel verifies that all areas are armed after a scheduled closing time passes.

Disabled: Panel does not verify that all areas are armed after a scheduled closing time passes.

Closing Code (XR)

Enabled: A code is required to arm the system.

Disabled: A code is not required to arm the system.

Any Bypass (XR)

Enabled: Allows zones to be bypassed without a code during the arming sequence. A code is always required to use the Bypass Zones option from the User Menu on the keypad.

Disabled: Does not allow zones to be bypassed without a code during the arming sequence.

Area Schedules (XR)

Enabled: Allows each area to follow individual sets of schedules.

Disabled: Allows one set of schedules for the system.

Area Information

Area (XR, XT, XTL, Com)

Enter the number of the area to program.

Area Name (XR, XT, XTL, Com)

Enter a name for the area. Max is 32 characters.

Account Number (XR)

Enter the panel account number.

Bad Zones (XR, XT, XTL, Com)

Bypass: All bad zones are bypassed automatically.

Force Arm: All bad zones are force armed automatically.

Refuse Arm: No zones are armed until the zone is restored.

Burglary Bell Output (XR)

Enter the output number that is turned on when a burglary zone goes into alarm. Entering 0 disabled this feature. Default is **0**.

Armed Output (XR)

Enter the output number that is turned on when the area is armed. Entering 0 disabled this feature. Default is **0**.

Late Output (XR)

Enter the output number that is turned on when area late or closing time displays on the keypad. Entering 0 disabled this feature. Default is **0**. Requires that **Closing Check** is enabled.

Late/Arm Delay (XR)

Enter the number of minutes before an area is automatically rearmed after the area is disarmed outside a schedule. Range is 4-250 minutes. Default is **60 minutes**.

Dual Authority (XR)

No: Disables Dual Authority.

Arm: Require two user code entries to arm this area.

Disarm: Require two user code entries to disarm this area.

All: Require two user code entries to arm or disarm this area.

Open/Close Reports (XR)

Enabled: Allows an opening/closing report to be sent to the receiver when this area is armed or disarmed.
Disabled: Does not allow opening/closing reports to be sent when this area is armed or disarmed.

Auto Arming (XR, XT, XTL, Com)

Enabled: Allow this area to arm automatically according to schedules.

Disabled: Does not allow this area to arm automatically.

Auto Disarm (XR, XT, XTL, Com)

Enabled: Allow this area to disarm automatically according to schedules.

Disabled: Does not allow this area to disarm automatically.

Bank Safe and Vault (XR)

Enabled: Allow this area to only be disarmed during scheduled times.

Disabled: Does not allow Bank Safe and Vault.

Common Area (XR)

Enable: Allows this area to arm/disarm automatically when the last area is armed or disarmed.

Disable: Does not allow automatic arming/disarming of this area based on arming sequence.

Arm First (XR)

Enabled: Allow this area to arm automatically when other areas are armed.

Disabled: Does not automatically arm this area when other areas are armed.

Card Plus PIN (XR)

Enabled: Require users to swipe a credential and enter a code before area access is granted.

Disabled: Do not require users to swipe a credential and enter a code before area access is granted.

Description (XR, XT, XTL, Com)

If necessary, add a description for the area.

7.5.29 Zone Information

When programming zones, consult the Quick Programming Reference as needed. To add zone information, complete the following steps.

1. Go to **Program > Zone Information** and select **New**.
2. Configure settings in the **Standard**, **Action**, **Wireless/VPlex**, and **Advanced** tabs as needed. For details, refer to Zone Information Programming Reference.
3. Select **Apply**. Repeat steps 1-3 to add more zones as needed.
4. To save a zone as a template, select the zone from the table, enter a name Zone Template, then select **Save**.
5. Select **OK**.

Zone Information Programming Reference

The following reference provides basic descriptions of each field in Zone Information. Configure each setting as needed.

Standard

Zone Number

Enter the zone number.

Zone Name

Enter a name for the zone.

Type

Blank (--): Customizable zone type

Night (NT): Controlled instant zone for perimeter doors, windows, PIRs, and glassbreaks

Instant (IN): Controlled instant zone for perimeter doors, windows, PIRs, and glassbreaks; also causes alarm if tripped during exit/entry delay

Day (DY): For emergency doors or fire doors

Exit (EX): Initiates the entry delay timer when area is armed

Fire (FI): For any type of powered or mechanical fire detection device

Panic (ON): For panic buttons or key fobs with panic

Emergency (EM): For non-panic emergencies

Supervisory (SV): Provides 24-hour zone supervision to devices associated with fire systems

Auxiliary 1 (A1) and Auxiliary 2 (A2): Controlled instant zone for restricted zones within a protected area

Fire Verify (FV): For verifying existence of a fire condition

Arming (AR): For connecting a keyswitch to arm or disarm areas

Carbon Monoxide (CO): For carbon monoxide detectors Doorbell (DB): For video or mechanical doorbells

Area

Select areas programmed in **Area Information**.

Follow Area

Enter the number of an area to follow in exit or entry delay. Entering 0 disabled this feature. Default is **0**.

Expander Serial Number

Enter the serial number if this is a zone expander.

Armed Areas

Enter the keypad addresses to display armed areas.

Action

Configure the following messages, outputs, and output actions.

DO: Disarmed Open

DS: Disarmed Short

AO: Armed Open

AS: Armed Short

Message

None (-): No message is sent to receiver

Alarm (A): Send an alarm report to the receiver and activate the bell output according to zone type

Trouble (T): Send a trouble report to the receiver

Local (L): Does not send an alarm to the receiver-local notification only

Door Propped Open (D): Allow Entry Delay 4 to begin countdown without displaying on the keypad. If the door is not closed after the countdown has expired, a faulted zone report is sent to the receiver.

Sensor Reset (S): When a zone state changes, the bell is silenced, a sensor reset is performed, and an alarm bell silenced message is sent to the receiver

Cancel Ambush (C): Cancel the ambush timer and prevent an ambush message from being sent to the receiver

Output

Enter the output number.

Output Action

None: No output action.

Pulse: Output alternates on one second and off one second.

Steady: Output turns on and remains on until the area is disarmed, an output cutoff expires, or the output is reset.

Momentary: Output turns on once for one second.

Follow: Output is turned on and remains on while the zone is in an off normal or bad condition. When the zone restores, the output is turned off.

Wireless / VPlex

Wireless

Wireless

Enabled: Allows the zone to be programmed as a wireless zone.

Disabled: Does not allow the zone to be programmed as a wireless zone.

VPlex

Enabled: Allows the zone to be programmed as a V-Plex zone.

Disabled: Does not allow the zone to be programmed as a V-Plex zone.

Competitor Wireless

Enabled: Allows the zone to be programmed as a competitor wireless zone for the 1100T.

Disabled: Does not allow the zone to be programmed as a competitor wireless zone for the 1100T.

DMP Wireless

Serial Number

Enter the serial number of the wireless device.

Two Button (XR Only)

This option only displays when programming 1144 Key Fobs as wireless panic zones.

Select **Yes** to use the key fob as a 2-button panic. Select **No** to use the key fob as a 1-button panic. The default is **No.**

Contact

Internal: Used for devices with internal reed switch contacts.

External: Used for devices with wired external contacts.

Normally Open

Enabled: Allows external contact to operate as normally open.

Disabled: Allows external contact to operate as normally closed.

Supervision Time

Select a supervision time for the device: **None, 3 min, 60 min**, or **240 min**. Default is **240 min**.

LED Enabled

Enabled: The 1142 Hold-Up Transmitter LED to turns on during panic or emergency operation.

Disabled: The 1142 Hold-Up Transmitter LED does not turn on during panic or emergency operation.

Disarm Disable

Enabled: When the system is disarmed, transmitters and PIRs do not send zone tripped messages.

Disabled: When the system is disarmed, transmitters and PIRs send zone tripped messages.

Wireless PIR Pulse Count

Select either **2** or **4** infrared pulses to be sensed before sending a message to an 1100 Series receiver. Default is **4**.

Wireless PIR Sensitivity

Low: Lowers PIR sensitivity (75%)

High: Maximum PIR sensitivity (100%)

Wireless PIR Pet Immunity

Off: Pet immunity is disabled. PIR detects all movement.

On: Pet immunity is enabled. PIR ignores movement from animals up to 55 pounds.

Advanced

Swinger Bypass

Enabled: Allows zone to be swinger bypassed.

Disabled: Does not allow zone to be swinger bypassed.

Retard

Enabled: Allows zone to operate with retard delay.

Disabled: Does not allow zone to operate with retard delay.

Fast Response

Enabled: Allows zone response time of 167 ms.

Disabled: Allows zone response time of 500 ms.

Cross Zone

Enabled: Allows cross zoning.

Disabled: Does not allow cross zoning.

Priority Zone

Enabled: Area won't arm until the zone is in normal condition.

Disabled: Area can be armed with zone in any condition.

Fire Panel Slave

Enabled: Zone transmits restoral immediately when restored by a monitored fire panel

Disabled: Zone does not automatically transmit restoral

Real-time Status

Enabled: Allows real-time status reports such as door open or door closed.

Disabled: Does not allow real-time status reports.

Traffic Count

Enabled: When disarmed, report the number of zone trips.

Disabled: Does not report the number of zone trips.

Lockdown

Enabled: Allows panic operation to initiate zone lockdown.

Disabled: Panic operation does not initiate zone lockdown.

Zone Audit Days

Enter the number of days allowed to pass without zone trips before a fault message is sent to the receiver. Range is 0-365 days. Entering 0 disables this function. Default is **0** days.

Report with Acct # for Area

Enter the area to assign as a 24-hour type. If the area doesn't exist, the account number is sent to the receiver instead. Range is 1-32. Entering 0 disables this feature. Default is **0**.

Chime Sound

Select one of the following chimes for the zone: **Off**, **Doorbell**, **Ascend**, **Descend**.

Prewarn Keypads

Enter the keypad addresses to display the enter code prompt when an entry delay starts.

Entry Delay Number

Enter the entry timer selected as default in System Options for this zone. Range is 1-4. Default is **1**.

7.5.30 Key Fobs

When programming key fobs, consult the Quick Programming Reference as needed. To add a key fob, complete the following steps.

> ℹ️ **Note**: For XR Series Control Panels, key fobs can also be programmed as wireless panic zones in **Zone Information**. The valid zone range is 500-599 for XR150 panels and 500-999 for XR550 panels.

1. Go to **Program > Key Fobs** and select **New**.
2. In **Number**, enter a zone number for the key fob. Refer to the Key Fob Zone Numbers table for acceptable ranges.
3. In **User**, select More and choose a user.
4. In **Serial Number**, enter the 8-digit serial number. Key fob range is 05000000-05999999.
5. In **Supervision Time**, select a supervision time for the key fob. For key fobs that are taken off-site, select **None**. Default is **None**.
6. In **Number of Buttons**, enter **1**, **2**, or **4**.
7. Select **Apply**.
8. Program the button **Action**, **Select Time**, **Areas**, **Output**, and **Output Action** as needed.
9. Repeat steps 1-8 to add more key fobs as needed.
10. Select **OK**.

Panel Model	Zone Numbers
XR150/XR550 Series	400-449
XT30/XT50 Series	31-34 (fast) 41-44 (slow)
XTLplus and XTLtouch	51-54 (fast) 61-64 (slow)

7.5.31 XR Schedules

Learn how to program Output/Door/Favorite Schedules, Area Schedules, Time Schedules, and Holiday Dates for XR Series systems.

Output/Door/Favorite Schedules

Output/Door/Favorite Schedules allows you to assign up to 16 schedules to an output, door, or favorite.

1. Go to **Program > Output/Door/Favorite Schedules** and select **New**.
2. In **Output**, enter an output, door, or favorite number for the schedule.
3. In **Schedules**, select **More** in the row of each schedule, then double-click the appropriate schedule to assign it to the output, door, or favorite.
4. Select **Apply**. Repeat steps 1-4 to add more schedules as needed.
5. Select **OK**.

Area Schedules

Area Schedules allows you to assign up to 8 schedules to an area.

1. Go to **Program > Area Schedules** and select **New**.
2. In **Area Number**, enter an area number for the schedule.
3. In **Schedules**, select **More** in the row of each schedule, then double-click the appropriate schedule to assign it to the area.
4. Select **Apply**. Repeat steps 1-4 to add more area schedules as needed.
5. Select **OK**.

Time Schedules

Time Schedules allows you to program up to 99 access, arm/disarm, and holiday schedules. When programming schedules, refer to device installation and panel programming guides as needed. To add a schedule, complete the following steps.

1. Go to **Program > Time Schedules** and select **New**.
2. In **Number**, enter a number for the schedule. Range is 1-99.
3. In **Name**, enter a name for the schedule.
4. To make the schedule temporary, select **Temporary Schedule**, then select a **Begin Date** and **End Date**.
5. Configure settings in **Open/Begin/Activate** and **Close/End** as needed.
6. Select **Apply**. Repeat steps 1-6 to add more schedules as needed.
7. Select **OK**.

Holiday Dates

Holiday Dates provides the system with dates in the year when the normal opening and closing schedules are not used and superseded by one of the holiday schedules: A, B, or C. When the panel determines that it is a holiday, the holiday schedule supersedes the current schedule for that day.

When programming holiday dates, refer to device installation and panel programming guides as needed. To add a holiday date, complete the following steps.

1. Go to **Program > Holiday Dates** and select **New**.

2. In **Number**, enter a number for the holiday.
3. In **Name**, enter a name for the holiday.
4. In **Class**, choose **A**, **B**, or **C**.
5. In **Holiday**, select the holiday date from the calendar.
6. If necessary, enter a description of the holiday.
7. Select **Apply**. Repeat steps 1-7 to add more holiday schedules as needed.
8. Select **OK**.

7.5.32 XT30/XT50 Schedules

Learn how to program an Arming schedule, Output Schedules, and Favorite Schedules for XT30/XT50 systems.

Schedules (Arming)

An Arming Schedule, also known as a Permanent Schedule, automatically arms and disarms a system at times that you program. You can create one Arming Schedule per XT30/XT50 system. To program an Arming Schedule, complete the following steps:

1. Go to **Program > Schedules**.
2. Select **New**.
3. In **Opening**, enter the time for each day when you want the system to disarm. If you don't want the system to disarm for a day, leave its field blank.
4. In **Closing**, enter the time for each day when you want the system to arm. If you don't want the system to arm for a day, leave its field blank.
5. Select **Apply**.
6. Select **OK**.

Output Schedules

An Output Schedule turns a programmed output on or off at the time that you choose. Output Schedules can also use Sunrise and Sunset times to turn outputs on or off. You can create up to 4 output schedules per XT30/XT50 system.

We recommend that you program outputs in **Program > Output Information** before creating output schedules. If you plan on using **Sunrise** and **Sunset** times, go to **Program > System Options** and enter the system's ZIP code in **Weather Zip Code**. To program an Output Schedule, complete the following steps:

If Using Sunrise/Sunset Times

1. Go to **Program > Output Schedules**.
2. Select **New**.
3. In **Output**, enter the number of the output that you want to schedule.
4. In **On**, skip to **Sunrise/Sunset** and select whether the output turns on at **Sunrise** or **Sunset**.
5. Select days for the **On** schedule. If you don't want the output to turn on for a day, leave it unselected.
6. In **Off**, skip to **Sunrise/Sunset**, select whether the output turns off at **Sunrise** or **Sunset**.
7. Select days for the **Off** schedule. If you don't want the output to turn off for a day, leave it unselected.
8. Select **Apply**.
9. Select **OK**.

If Using Custom Times

1. Go to **Program > Output Schedules**.
2. Select **New**.
3. In **Output**, enter the number of the output that you want to schedule.
4. In **On**, enter the time for each day when you want the output to turn on. If you don't want the output to turn on for a day, leave its field blank.
5. In **Off**, enter the time for each day when you want the output to turn off. If you don't want the output to turn off for a day, leave its field blank.
6. Select **Apply**.

7. Select **OK**.

Favorite Schedules

A Favorite Schedule activates a favorite at the time that you choose. Favorite Schedules can also use Sunrise and Sunset times to activate favorites. You can create up to 20 favorite schedules per XT30/XT50 system.

We recommend that you program favorites in **Program > Favorites** before creating favorite schedules. If you plan on using **Sunrise** and **Sunset** times, go to **Program > System Options** and enter the system's ZIP code in **Weather Zip Code**.

To program a Favorite Schedule, complete the following steps:

If Using Sunrise/Sunset Times

1. Go to **Program > Favorite Schedules**.
2. Select **New**.
3. In **Favorite**, enter the number of the favorite that you want to schedule.
4. In **Activate**, skip to Sunrise/Sunset, select whether the favorite activates at Sunrise or Sunset.
5. Select days for the schedule.If you don't want the favorite to activate for a day, leave it unselected.
6. Select **Apply**.
7. Select **OK**.

If Using Custom Times

1. Go to **Program > Favorite Schedules**.
2. Select **New**.
3. In **Favorite**, enter the number of the favorite that you want to schedule.
4. In **Activate**, enter the time for each day when you want the favorite to activate. If you don't want the favorite to activate for a day, leave its field blank.
5. Select **Apply**.
6. Select **OK**.

7.6 Profiles

Profiles allows you to add, delete, or change user profiles.

1. Go to **Program > Profiles** and select **New**.
2. In **Profile**, enter a number for the profile.
3. In **Name**, enter a name for the profile.
4. In **Arm/Disarm Areas**, enter the number for the areas that you want to authorize this profile to arm and disarm
5. In **Access Areas**, enter the number for the areas you want to authorize access for this profile.
6. If necessary, go the **Output Group** field and assign each profile to an output group number. Range is 1-20. Default is **0**.
7. If necessary, go to the **ReArm Delay** field and enter a number of minutes to be used to delay automatic rearming when the user disarms an area outside of schedule. Range is 0-720 minutes. Default is **0**.
8. If necessary, go to the **Inactive User Audit Days** field and set the number of days a user code can remain unused before the panel sends an Inactive User Code message to the receiver and changes the user code status to inactive. Range is 0-425 days. Default is **0**.
9. Select access privileges as needed.
10. To assign an existing schedule to the profile, go to the **Schedules** section, select **More** in the row of each schedule, and double-click the appropriate schedule.
11. To assign private doors to the profile, go to **Private Doors** and select the appropriate doors configured in the system's **Device Setup** menu. Up to 4 private doors can be assigned to a profile.
12. If necessary, add a description for the profile.
13. Select **Apply**. Repeat steps 1-12 to add more profiles as needed.
14. Select **OK**.

7.7 User Codes

User Codes allows you to enter or change to the user code information in the panel or database file.

1. Go to **Program > User Codes** and select **New**.
2. Open the **Panel** tab. In Number, enter a number for the user.
3. In **User Code**, enter the user's code.
4. In **User Name**, enter the user's name.
5. Select **Active User**.
6. Configure credential information, areas, and temp user properties as needed.
7. For XT30/XT50 systems, select an authority level from **Level**. For XR systems, select profiles from **Profiles**.
8. To record detailed information about a user, open the **Custom** tab and enter information in each field as needed.
9. Select **Apply**. Repeat steps 1-8 to add more users as needed.
10. Select **OK**.

7.8 Scanning a Proximity Card

Using a 1301 Series USB Computer Proximity Reader from DMP, you can quickly scan a proximity device instead of manually entering the User Code. After properly connecting the USB to a COM port on your computer, go to **System > Configure > Remote Link** and select the **Other** tab.

To enter a User Code using the USB, select the user for which you would like to enter the user code. Press **Scan Card** at any time, then present the proximity card to the USB. The USB will automatically assign the card's code as the user's code. You can also use the USB when changing a user code.

7.9 Access Code

Access Codes prevent unauthorized persons from gaining access through a keypad and making changes to the panel programming by assigning a lockout code to the panel. Before anyone can change the panel's programming through the keypad, they must enter the designated access code.

To allow panel programming from the keypad without an access code, leave the access code blank.

To assign an access code, go to **Program > Access Code**. In **Code**, enter an access code, then select **OK**. Range for XR is 0, 100-65535. Range for XT30/XT50 is 0-65535

7.10 Send Programming to Panel

1. Close all programming and configuration windows.
2. Ensure Remote Link is connected to the panel.
3. Go to **Panel > Send**.
4. To clear codes, schedules, zone, or area programming from the panel before sending programming, select the appropriate clearing options. To clear the same programmed data from all panels, select **All Systems**.
5. To automatically request the panel's events after programming is sent, select **Request Events**.
6. To send only the programming that has changed since the last connection with the panel, select **Changes Only**.
7. To update the panel time after programming is sent, select **Update Time**.
8. To automatically disconnect from the panel after programming is sent, select **Disconnect on Completion**.
9. Select **Send**.

7.11 Program a Panel

The following topics cover how to program each section in the Program menu. The programming options available in each section depend on panel type and configuration. Refer to the appropriate panel programming guide from DMP.com/resources when programming in Remote Link.

For listed installations, refer to DMP's product Compliance Guides and Compliance Notes.

7.11.1 Retrieve Programming from Panel

> **ⓘ** **Note:** When you retrieve from a panel, any programming changes made in Remote Link that have not yet been sent to the panel are overwritten by the panel programming information that you retrieve from the panel.

1. Close all programming and configuration windows.
2. Ensure Remote Link is connected to the panel.
3. Go to **Panel > Retrieve**.
4. To automatically request the panel's events after programming is retrieved, select **Request Events**.
5. To update the panel time after programming is retrieved, select **Update Time**.
6. To automatically disconnect from the panel after programming is retrieved, select **Disconnect on Completion**.
7. To retrieve only the programming that has changed since the last connection with the panel, select **Changes Only**.
8. Select **Retrieve**.

7.11.2 Quick Programming Reference

Refer to the following tables when programming DMP accessories. For complete programming guides, refer to DMP.com/resources.

XR550

- Retrieve Programming from Panel
- Quick Programming Reference

8 Templates

8.1 Create a Template

1. Go to **File > Panel Information**.
2. Select the panel that you want to use as a template.
3. Select **Copy**.
4. Select the **Template** checkbox.
5. In **Name**, enter a name for the template.
6. Select **OK**.

8.2 Manage Templates

Go to **File > Panel Information**. Open the **Template** tab. Existing templates are displayed the list with their **Name**, **Model**, and **Version**. The **Templates** tab contains the following information:

- **Template Name:** This displays the name of the template that you select from the list. You can also change the name of the template as well.
- **Notes:** This gives you the option to makes notes about this template.
- **New:** This allows you to make a new panel template. Select the **Model**, **Version**, and any **Feature Set** (if applicable for the selected panel) for the template. Enter a name for the new template and select **OK**. The new template will display in the **Template** tab.
- **Copy Panel:** Allows you to make a new template by copying the information from an existing account.

8.3 Modify Template Programming

After a template is created, you can modify the template's programming like standard panel programming. Go to **File > Panel Information**. Open the **Templates** tab. Double-click the template that you want to edit. Modify programming as needed. For more information, refer to Program a Panel.

9 System Status

To view system status, go to **Panel > System Status**.

In **Status**, **Normal**, **Trouble**, or **Not Used** displays for each of the following items:

- **Printer**
- **Tamper**
- **Battery**
- **AC Power**
- **Line 2**
- **Line 1**
- **Wireless**

The System Status window also allows you to access the following command and inquiry functions:

- **Alarm Silence:** Silence an alarm
- **Sensor Reset:** Perform a remote sensor reset
- **Set Time/Date:** Synchronize the panel time and date with the current workstation time and date
- **Send Message:** Send a message to the panel to display on the keypad
- **Areas:** View the arm/disarm status of all panel areas
- **Zones:** View the status of all panel zones. Bypass or reset bad zones
- **Outputs:** View the status of all panel outputs and door access events. Turn outputs on or off. Lock, unlock, or grant access to doors.
- **LX-Bus Diagnostics:** Perform routine diagnostics of the panel LX-Bus
- **Forgive User:** Remotely clear a failure to exit violation when using anti-passback
- **Lockdown:** Initiate a system lockdown
- **ZWave Status:** View the status of panel Z-Wave devices

10 Request Events

Request Events allows you to download a panel event buffer into the Remote Link database.

1. Go to Panel > Request Events.
2. Configure the following options as needed:
   - **Standard:** Request all events except door access, select Standard.
   - **Door Access:** Request only door access events
   - **Disconnect on Completion:** Automatically disconnect from the panel after the event buffer is uploaded to the database
   - **All Events:** Requests all events stored in the panel event buffer based on the type of event selected. Deselect this box to select specific dates.
   - **New Events Only:** Requests all events that have occurred since the last event download.
   - **Select Date Range:** Type in the date or use the drop-down calendar.
   - **Start:** Enter the date for the oldest events you wish to retrieve. The default is the panel's internal date minus 45 days. The Start Date for events cannot be more than 45 days preceding the panel's internal date.
   - **End:** Enter the last date for the events you would like to retrieve. The end date cannot be after the panel's internal date.
   - **Panel Date:** Displays the panel's internal date.
3. Select **Request**.

> ℹ **Note:** Each time that you request events from the same panel, Remote Link stores those events in a buffer until you request events again from the same panel. You may print these events by going to **File** > **Print** > **Panel Event Buffer**.

11 Account Archive

Account Archive allows you to manage archived accounts.

To archive a panel, go to **File > System Information**. Open the panel that you want to archive, then select **Archive**.

To manage account archives, go **Panel > Account Archive**. Select one of the following options:

- **Revert:** Reverts the current account programming to the chosen archive
- **Open:** Open the selected archive version (read-only)
- **Delete:** Delete the selected archive
- **Close:** Close the **Account Archive** window

12 Diagnostics

The **Diagnostics** window is primarily used as a tool to identify and problems with the system or communication. This window allows you to view the strings of data that the panel is sending and receiving from your computer. To quickly open the **Diagnostics** window, go to **System > Diagnostics** or press Alt + F10.

13 Perform a Remote Update

Remote Link allows you to update panels remotely from your workstation. To download panel firmware, visit product software downloads.

13.1 Remote Update a Panel

1. Go to **Panel > Remote Update**.
2. In **Update File**, select **More**. Select the appropriate remote update (.ru) file.
3. Select **Update**.

13.2 Batch Remote Update Panels

1. Go to **System > Remote Update**.
2. In **Update File**, select **More**. Select the appropriate .ru file.
3. In **Devices to Update**, select any panels that you want to update. To batch update all panels, select **All**.
4. Select **Update**.
5. To resend any failed updates, select **Resend Failed**.
6. To clear completed updates from the **Progress** list, select **Clear Completed**.

14 Export and Import Account Information

The Import and Export tool allows you to import and export account information in encrypted .xml files. For information to import correctly, the provided format must be used to import accounts.

14.1 Export Account Info

1. Go to **File > Import** and **Export > Export Accounts**.
2. Select an account to export, then select **Move Right**. Repeat this step until all the accounts that you want to export are moved.
3. In **Save As**, select **More**. Select a location for the file and enter a filename for the .xml file.
4. Select **Export**.
5. Enter an encryption key for the file, then select **OK**.

14.2 Import Account Info

1. Go to **File > Import and Export > Import Accounts**.
2. In **File to Import**, select **More**. Locate and select the .xml file that you want to import.
3. To import all accounts from the file, select **Import All Accounts**.
4. Select **Load**.
5. Enter the file's encryption key, then select **OK**.
6. To overwrite all information in an existing account, select **Overwrite Existing Account**. To import a system with a different account number, select **Change Account Number**.
7. Select **Import**.

15 Print Reports

To print reports, go to **File > Print** and select a report. To configure print settings, such as selecting a printer, select **Setup**. To preview the report, select **Preview**. The following reports are available:

15.1 Account Information

Print panel settings configured in **Panel Information**. To print reports for all systems, select **All**.

15.2 Panel Programming

Print the panel programming sheet with panel information. Select fields to include as needed.

15.3 Activity

Print all panel activity, including programming changes and operator logins.

1. To print reports for all systems, go to the **Account** field and select **All**.
2. To restrict the report to a specific date range, go to the **Date** field select a start and end date. To print reports without a date range, select **All**.

15.4 Events

Print panel events or the panel events buffer.

1. In **Data Source**, select **Events** or **Panel Events Buffer**.
2. To print reports for all systems, go to the **Account** field and select **All**.
3. To restrict the report to a specific date range, go to the **Date** field select a start and end date. To print reports without a date range, select **All**.
4. In **Report Format**, select **Summary** or **Customer Mailout**. The **Summary** format includes panel summary and report information. The **Customer Mailout** format only includes events.
5. In **Messages in Report**, select the messages that you want to include.
6. To print the traffic count instead of messages, go to the **Other Reports** section and select **Traffic Count**.

15.5 Activation Status

Print SIM activation status information for cellular systems.

1. In **Include by Status**, select the statuses that you want to include in the report.
2. In **Include by Account Settings**, select the account settings that you want to include.
3. In **Sort Order**, select sorting options for the report

15.6 Recall Failure

Print a report of all the accounts that failed to report as programmed in **File > Panel Information > Extra Information > Auto Recall Frequency**.

In **Options**, select a sorting option for the report.

15.7 Compare Accounts

Create a report to compare a panel's programming to other panels, an archived version, or a template. The report is generated in .xls spreadsheet format.

1. In **Control Panel**, select the type of comparison. For **Template**, select a template from the dropdown. For **Account**, enter an account number and select **Load**.
2. In **Options**, select additional items that you want to include in the report.
3. In **Select Accounts To Compare**, select an account to compare with the template or account selected in the **Control Panel** section.
4. In **Save To**, select More. Choose a file location and name the report.
5. Select **Compare**.

15.8 1100 Update Reports

Print reports of wireless devices with obsolete hardware.

To run the report for all systems, select **All**. To run the report for a range of systems, enter the receiver number and enter the range in the **Account** fields.

To print a summary of the associated accounts, customers, and number of each device, select **Summary**. To print detailed information, including device serial numbers, select **Worksheet**.

15.9 Data Export

Export detailed panel information into separate CSV files.

1. In **C:\Link**, create a new folder for the data export files.
2. In the **Data Export Report Setup** window, select **More** next to **Location**. Double-click the new folder and select **OK**.
3. To start the filename with the account number, select **Prefix Filename with Account Number**. To start the filename with the account name, select **Prefix Filename with Account Name**.
4. Select **Export**.

15.10 Saved Reports

Print reports saved with the Advanced Reporting Module.

In **Filename**, select **More**. Find and open the saved report. In **Orientation**, select **Portrait** or **Landscape**.

16 Manage Alarms

The **Alarm List** allows you to view alarms, general information about the system in alarm, and options to acknowledge, remove, or disable alarms.

An audible alert tone sounds on your computer's internal speaker when a message is received in the Alarm List. This tone continues to sound until all messages in the Alarm List have been acknowledged. Acknowledge alarm signals by pressing F6 or select **Acknowledge**. Remote Link automatically closes the Alarm List after all messages have been acknowledged.

If an operator is not logged on when an alarm is received, Remote Link sounds the audible alert tone and displays the message "Unacknowledged Alarms: X" in red text at the bottom of the screen. "X" represents the number of unacknowledged alarms currently in the Alarm List.

To view alarms, go to **System > Alarm List**.

The **Alarm List** window contains the following sections:

An audible alert tone sounds on your computer's internal speaker when a message is received in the Alarm List. This tone continues to sound until all messages in the Alarm List have been acknowledged. Acknowledge alarm signals by pressing F6 or select **Acknowledge**. Remote Link automatically closes the Alarm List after all messages have been acknowledged.

If an operator is not logged on when an alarm is received, Remote Link sounds the audible alert tone and displays the message "Unacknowledged Alarms: X" in red text at the bottom of the screen. "X" represents the number of unacknowledged alarms currently in the Alarm List.

To view alarms, go to **System > Alarm List**.

The **Alarm List** window contains the following sections:

16.1 Visible Alarms

Control which alarms are shown in the main window.

16.2 Main Section

Lists all alarms with the account number, message, repeat count, time of alarm, and acknowledgement time/date.

16.3 General Information

Displays general information about the selected panel.

16.4 Location

Displays location information about the selected panel.

16.5 Information

Contains information from **Extra Information** configured in **Panel Information**.

16.6 Commands

The commands pane contains the following commands:

- **Ack:** Acknowledge the alarm and silence the workstation alert tone
- **Remove:** Remove the alarm from the list. The alarm must be acknowledged before it can be removed
- **Disable:** Disable the alarm and remove it from the list. The alarm must be acknowledged before it can be disabled
- **Connect:** Immediately connect to the selected account
- **Print:** Open the Events print dialog to print system alarms
- **Cancel:** Close the Alarm List

17 Advanced Tasks

The following topics cover advanced tasks like TCP trapping and configuring Remote Link for ECP passthru.

17.1 Configure TCP Traps

TCP Trapping uses the panel's connection to the monitoring center to forward communication from the panel to Remote Link.

Before creating or initiating a trap, configure TCP Trap options in **System > Configure > Remote Link > Network**. For more information, refer to Network Options.

17.1.1 Create and Send a Trap

1. Go to **Panel > Trap** and select **New**.
2. Enter the receiver and account number. For example, 1-11111.
3. Select **OK**.
4. In Options, select the following options as needed:
   - **Send File:** Send full programming to the panel from Remote Link
   - **Changes Only:** Send only programming that has changed since the last communication with the panel. To enable this option, select both Send File and Changes Only
   - **Retrieve File:** Download full programming from the panel into Remote Link
   - **Request Events:** Automatically download the panel's event buffer into the Remote Link database
   - **Remote Update:** Automatically download the selected software file to the trapped panel
   - **Change File:** Select the software update file location. The path to the update file is displayed automatically. To enable this option, select **Remote Update**.
5. To initiate the trap, go to **Panel > Set All Traps**.
6. To view the status of set traps, go to **Panel > Trap Query**.

17.1.2 Troubleshooting

Selecting Hangup forces the receiver to release the phone line and restore its on-hook status. This feature is useful when a panel drops offline, resulting in a communication error. To hangup the line, go **Panel > Hangup**.

> ⓘ **Note:** Do not use Hangup to disconnect from a panel while it is still online. Always use Disconnect to terminate the connection.

17.2 Configure ECP Passthru

Before configuring Remote Link for ECP passthru, Compass® must be configured for connected VISTA panels. For more information, refer to Com Series How-To: ECP Passthru (LT-2209) or, if using a CellComEX, the CellComEX How-To Guide: ECP Passthru (LT-2689).

1. Right-click Remote Link and select **Run as administrator**.
2. Double-click the universal communicator account.
3. Go to **Program > System Options**.
4. To enable communication, go to **Keypad input** and select **ECP**. The default of **Keypad Input** is **None**.
5. Go to **File > Panel Information**.
6. Go to **Connection Information** and enter the VISTA account number in **ECP.**
7. Go to **ECP Passthru > ECP Start/Stop Server**.

17.3 Configure DSC Passthru

For more complete information, refer to Com Series How-To: DSC Passthru (LT-2208).

1. Right-click Remote Link and select **Run as administrator**.
2. Double-click the communicator account.
3. Minimize Remote Link.
4. Open the DLS software.
5. Double-click the DSC panel.
6. Select **Upload to Panel**.

18 Add-Ons

The following topics cover registering and activating add-ons, along with details about each add-on module.

18.1 Manage Modules

To configure and manage modules, install a module, then run Remote Link as an administrator.

18.1.1 Add a Module

1. Go to **Help > Registration**.
2. Select **Add**.
3. Enter the module serial number, then select **OK**.

> ℹ️ **Note:** To ensure that the module is properly activated, do not lose the certificate or the serial number. You have a 7-day grace period between the installation and the activation of the module.

18.1.2 Activate a Module

If activating the SecureCom Wireless service module, contact SecureCom Customer Service at 877-300-8030 for activation.

1. Go to **Help > Registration**.
2. Select the module that you want to activate.
3. Select **Activate**. Remote Link will automatically generate a public key for the module. The serial number and public key will be listed in a message box.
4. Call DMP Customer Service and request an activation code.
5. Select **OK** in the message box to enter the activation code.
6. Select **Activate**.

18.1.3 Upgrade the Number of Accounts

To change the Account Level, upgrade the number of subscriber accounts allowed.

1. Go to **Help > Registration**.
2. Select the module that you want to upgrade.
3. Select **Change**. Enter the new serial number from the upgrade certificate.
4. Follow the instructions to activate the module with the new level of accounts.

18.1.4 Remove a Module

Remove a module from Remote Link

> ℹ️ **Note:** You must have administrator authority to remove modules

1. Go to **Help > Registration**.
2. Select the module that you want to remove.
3. Select **Remove**.
4. A dialog pops up to confirm your decision. To remove the module, select **Yes**.
5. A message dialog pops up to notify you when module has been successfully removed. Select **OK**.
6. Restart Remote Link.

18.2 Link Server

18.2.1 Default Link Server Log In

Username: admin

Password: LinkAdmin

18.2.2 Connect Link Server to the Database

Computer Hard Drive

Enter the path to the Remote Link database location on the computer or network hard drive. If you want to store your Remote Link database in a different location than the default folder, enter the location in the **Database Location** field. The database may also be stored on a remote network server. This option allows more than three Remote Link computers to perform extensive database operations at the same time.

Network Server

To use Remote Link with Link Server, enter the network server IP address and port number to the Remote Link database location. The default port number is 12005. Check with your Link Server administrator for the correct IP address and port number. For example, 192.168.0.1:12005.

> ℹ️ **Note:** Standard Remote Link operation supports database access for up to three computers if only one computer at a time performs extensive database access operations such as uploading or downloading information from a panel. If more simultaneous database access is required, it is recommended the Link Server software be installed on a network server.

Database Relocation

To manually move your Remote Link database, use Windows Explorer and copy the complete database folder (usually "C:\Link\Db") to the desired location. Go to the Database Location field and enter the new location of the database. If you change the location without moving the database manually, Remote Link displays a message asking, "Do you wish to create a new database?" If you select OK, Remote Link creates a new database at the location that you assigned and ignores the previous database. As a result, Remote Link does not have access to any previous account information and configurations settings from the previous database. If Remote Link does not start up correctly, the cause could be an invalid database location. Use the command line option "/dblocation" to set a local or network path to the database:

Relocate a Database Locally

1. Close Remote Link.
2. Press **Windows + R**.
3. Enter **cmd**, then press **Enter**.
4. Enter the command c:\Link\Link.exe /dblocation [PATH] where [PATH] is the file path. For example: c:\Link\Link.exe /dblocation c:\Link\newDb
5. Press **Enter**.

Relocate a Database to a Server Address

1. Close **Remote Link**.
2. Press **Windows + R**.
3. Enter **cmd**, then press **Enter**.
4. Enter the command c:\Link\Link.exe /dblocation [SERVER ADDRESS] where [SERVER ADDRESS] is the server IP and port. For example: c:\Link\Link.exe /dblocation 192.168.0.1:12005.
5. Press **Enter**.

18.3 Alarm Monitoring Module

The Alarm Monitoring module expands the capabilities of the **Alarm List** in Remote Link to include Opening and Closing Reports and other system events such as Door Access events. You can then use the module to print these reports for clients.

The Alarm Monitoring module expands the services you can offer to your clients by providing them a straightforward way to receive Opening and Closing Reports. After you print the reports using the Alarm Monitoring module, clients will be able to easily review their opening/closing events and door access events. For best results, DMP recommends that you install the software on a computer dedicated to operating the Alarm Monitoring module and Remote Link.

To view the Alarm List, press F3 or go to **System > Alarm List**. For more information, refer to Manage Alarms.

18.4 Advanced Reporting Module

The Advanced Reporting module provides you with powerful filtering capabilities to create specific reports for your needs. You can create reports using the panel event buffer or Host Log Reports. You can also generate reports received from an SCS-105 Receiver. Additionally, you can connect to the module through a direct or network connection set up in **Remote Link Configuration**.

> ℹ **Note:** If you are using the Advanced Reporting module with another module, such as Alarm Monitoring, do not enable Host Log Reports. The Advanced Reporting module will generate reports using the same messages sent to Alarm Monitoring.

Advanced Reporting provides ten Report Categories from which you can create the reports. These categories allow you to filter out the information that you do not need so the reports are concise and manageable.

Saving reports in up to seven other formats, such as a text file, provides you with added flexibility to use the reports in a method that best suits your needs. You can then export the reports to another program for archiving, storing, and integrating with other company information.

18.4.1 Printing Reports

Advanced Reports Setup allows you to print reports of the alarm message information. To open **Advanced Reports Setup**, go to **File > Print > Events**.

- **Source**: Select the source of the reports.
- **Events**: Selects the events sent from panels that have PC Log Reports enabled.
- **Panel Event Buffer**: Selects the panel event buffer as the source of the reports. Connect to the panel and then select **Panel > Request Events** to print the panel event buffer. Each time you request events from a panel, the last panel event buffer will be overwritten. If you do not want to lose the information, be sure that you have printed the buffer before you request events from the panel a second time.
- **Report Category**: Select the report you wish to run from **Report Categories**. For more information, refer to Report Category Reference.
- **Account**: Enter the account number for which you are running the report. Select **All** to create reports for all accounts.
- **Date**: Enter the date range for which you are running the report. Selecting the arrow opens a calendar as shown in the screen shot. Select the date you wish to print. You can also select **All** to print all available dates.
- **Options**: The options available change with each **Report Category** selected.

18.4.2 Report Category Reference

Zone Action

Generate zone reports.

- **Zone Action:** Select the zone action for which you will generate the report. Select All to generate a report for all zone actions.
- **Zone:** Select the zone number for which you will generate the report. Only zones that have had the action selected above will be displayed in the drop-down box. Select All to generate a report for all zones.

- **User:** Select the user for which you will generate the report. Only users that have performed the zone action selected above will be displayed in the drop-down box. Select All to generate a report for all users.

Arming/Disarming

Generate reports containing information about arming and disarming activity.

- **Action:** Select Arming or Disarming from the drop-down menu. Select All to generate a report for arming and disarming activity.
- **User:** Select the user for which you will generate the report. Only users that have performed the zone action selected above will be displayed in the drop-down box. Select All to generate a report for all users. To view arming and disarming requiring the Two Man Rule (485B only), print out the report to view the 2nd user.
- **Area:** Select the area number for which you will generate the report. Only areas that have had the action selected above will be displayed in the drop-down box. Select All to generate a report for arming / disarming activity for all areas.

Area Late to Close

- **Area:** Select the area number for which you will generate the report. Only areas that have been armed after the scheduled closing time will be displayed in the drop-down box. Select All to generate a report for all areas that have been late to close.

User Codes

- **Action:** Select Added, Changed, or Deleted from the drop-down menu. Select All to generate a report for user code additions, changes, and deletions.
- **User:** Select the user for which you will generate the report. Only users that have performed the user code change selected above will be displayed in the drop-down box. Select All to generate a report for all users who have made changes to user codes.
- **User Being Changed:** Select the user for which you will generate the report. Only users that have been changed will be displayed in the drop-down box. Select All to generate a report for all users than have been changed.

Door Access Granted

- **User:** Select the user for which you will generate the report. Only users that have been granted door access will be displayed in the drop-down box. Select All to generate a report for all users granted door access.
- **Door:** Select the door for which you will run the report. Only doors that have granted door access will be displayed. Select All to create a report for all doors that have granted a door access.

To create a report for multiple doors, choose **Select Multiple Doors** from the drop-down menu, then select the **Select Doors**. Select the box to the left of the door name and number to include that door in the report. The report can be created for any combination of doors.

Door Access Denied

- **User:** Select the user for which you will generate the report. Only users that have been denied door access will be displayed in the drop-down box. Select All to generate a report for all users denied door access. The printed report will display the reason the door access was denied.
- **Door:** Select the door for which you will run the report. Only doors that have denied door access will be displayed. Select All to create a report for all doors that have denied a door access.

To create a report for multiple doors, choose **Select Multiple Doors** from the drop-down menu, then select the **Select Doors**. Select the box to the left of the door name and number to include that door in the report. The report can be created for any combination of doors.

Schedule Change

- **Schedule Type:** Select the type of schedule for which you will run the report. Select All to create a report for all types of Opening / Closing Schedules that have been changed. To run reports for **Extended Schedules**, select **Secondary**.
- **User:** Select the user for which you will generate the report. Only users who have changed an Opening / Closing Schedule will be displayed in the drop-down box. Select **All** to generate a report for all users who have changed an Opening / Closing Schedule.
- **Area:** Select the area number for which you will generate the report. Only areas that have had the Opening / Closing Schedule changed will be displayed in the drop-down box. Select All to generate a report for all areas that have had a schedule changed.

System Monitors

- **Component:** Select the system component for which you will create the report. Select All to include all components in the report.
- **System Monitor Action:** Select the action, trouble, or restore for the report. Select All to include all System Monitor Actions in the report.

System Events

- **Event:** Select the event for which you will run the report. Select All to include all events in the report. Below is a list of all events available:
    - **Automatic Recall Test**
    - **Unauthorized Entry**
    - **System Late to Close**
    - **Exit Error**
    - **Alarm Bell Silenced**
    - **Dialer Communication Failed**
    - **Abort Message Sent**

> **Note:** System Late to Close can only be included in a System Events Report when the following factors are met. If the factors are not met, the report can be created from the Area Late to Close Report category.

- **Area Schedules** is disabled.
- **Closing Check** is enabled.

- An Opening / Closing Schedule is programmed.
- **Supervisory Reports** is enabled in **Host Log Reports**

All Events

Selecting **All Events** creates a report with all Report Categories. By default, **All** is selected.

Export Advanced Reports

While in the preview mode, you may save the reports for printing later or in another application. Select the Save icon. You may save reports in the following seven formats to allow you to export the reports to another program.

- QuickReport file (*.QRP)
- Text File (*.TXT)
- Comma Separated (*.CSV)
- HTML document (*.HTM)
- Excel spreadsheet (*.XLS)
- Rich Text Format (*.RTF)
- Windows Metafile (*.WMF)

Real-Time Events

An Advanced Reporting module is required for this feature, as well as Microsoft .NET Framework 3.5.

The **Real Time Events** window is used to display incoming events as they happen and is read-only. To open **Real Time Events**, go to **System > Real Time Events**.

- **Max Event Count:** Indicates the number of rows display. Default is **100**.
- **Auto Update:** Receive active events display on the screen. Clear the checkbox to temporarily prevent new rows from being added to the display.
- **Events:** Each event is displayed on a row with the most current event being at the top

18.5 SQL Server Module

The SQL module allows larger corporate users to take advantage of existing Microsoft SQL Server installations. This module allows administrators to connect to an existing SQL Server installation with ODBC, then export all existing panel programming data from the standard DBISAM database into a new Microsoft SQL database.

18.5.1 SQL Server Installation

Remote Link requires Microsoft SQL Server 2008 R2 or higher. Install the version that corresponds to the operating system version of the machine which the Server will operate. For example, install the 64-bit version of Microsoft SQL Server on 64-bit systems.

> ℹ **Note:** Remote Link and SQL Server do not have to be installed on the same machine. Using Remote Link on a 32-bit machine with SQL Server on a 64-bit machine (or vice-versus) is supported.

For users in mission-critical applications, such as central station monitoring, DMP recommends that an experienced SQL Server administrator performs setup and administrative duties. This includes initial setup, firewall configuration, database replication, backup, repair, and other site-specific configurations. When using Remote Link with SQL Server, all backup and repair operations must be performed by the database administrator using SQL Server management tools. Remote Link does not perform these operations. When using Remote Link with the built-in database engine or Link Server, Remote Link can perform database backup and repair operations.

A login dialog will appear the first time the user runs Remote Link with SQL Server or anytime the SQL username or password is changed by the administrator. After a successful login the user will not be prompted again unless something changes in the database. Contact your database administrator for SQL login credentials.

18.5.2 Set up the ODBC Data Source

Before configuring an ODBC data source to work with Remote Link, create a new ODBC data source on the user's workstation. Any user created to be used for SQL Server authentication must have permission to read, write, modify, and delete all tables.

> ℹ **Note:** If setting up the DSN on a Windows 7 64-bit system you need to use a 32-bit version of the ODBC configuration utility. The executable odbcad32.exe is in C:\Windows\System32\.

Add a System DSN for SQL Server

1. Go to **Control Panel > Administrative Tools > Data Sources (ODBC)**.
2. Go to **System DSN**.
3. Select **Add**.
4. In **Create New Data Source** window, give the data source a **Name** and **Description**. Make note of the name you assign.
5. Select the server from the dropdown. If you are running SQL Server Express, add \SQLEXPRESS to the end of the server name. It may also be necessary to add the port 1433 at the end of the name. For example, MY_SERVER_NAME_OR_IP_ADDRESS\SQLEXPRESS,1433
6. Select **Next**.
7. Consult with your database administrator to determine whether to use SQL Server Authentication. If using SQL Server Authentication, use the Login ID and Password provided by the administrator.
8. Select **Next**.
9. Change default database to the Remote Link database.
10. Select **Next**, then select **Finish**.
11. Test the data source.

18.5.3 Import Panel Programming

The SQL Server module allows the administrator to export all existing panel programming information from the standard DBISAM database, and then import that information into a new Microsoft SQL database.

1. Backup the database. When using the SQL Server module, Remote Link does not automatically backup the database.
2. Export database accounts. Go to **File > Import and Export > Export Accounts**.
3. Go to **System > Configure > Remote Link > Database** tab. Enter the name you gave the ODBC data source you created in the previous section "Set up an ODBC Data Source". The location must start with **dsn:**.
4. Select **OK**, then restart Remote Link.
5. After Remote Link restarts, select **Yes** to initialize database.
6. Import database accounts. Go to **File > Import and export > Import Accounts**. For more information on Importing Accounts, refer to "Export and Import Accounts".

18.6 Account Groups Module

The **Account Groups** module provides the ability to update, change, or delete profiles, schedules, output schedules, holidays, and user codes on multiple panels at the same time. This feature allows you to group panels together under one name and associate them by location, business, or other logical grouping. Additionally, you can batch remote update all panels in a group.

18.6.1 Basic Requirements

Perform batch Account Group module maintenance using the following guidelines:

- The same user number has the same profile number in all accounts
- The panels need to have account numbers established before they are listed for selection
- Remote Link is not available to perform other operations while batch updates are in process

To update, change, or remove an account group, open the Account Groups window by selecting File > Account Group Information.

The following options are available:

- **Group Name:** Lists the account groups currently defined in the database
- **New:** Enter the name of the new group to add to the database
- **Delete:** Deletes the currently selected account group
- **Accounts in Group:** Displays a list of the current account names and numbers assigned to the group selected in the Group Name list
- **Add:** Allows an account to be added to a group
- **Remove:** Allows an account to be deleted from a group
- **Open Group:** Opens the currently selected group
- **Cancel:** Exits the Account Groups window

18.6.2 Batch Account Group Maintenance

You can add, change, or remove accounts in an account group and can send that information to multiple account groups at one time, giving you a more powerful tool to manage accounts in Remote Link. To use this feature, select **Batch**. Select **Add Accounts to this Group** or **Remove Accounts**. You can also select **Edit** to display a list of all the systems in programmed Remote Link and filter your account search. Select **OK**, then select **Done**.

The Account Groups module allows group programming in the following areas:

- Holiday Dates
- Output Schedules
- Profiles
- Schedules
- User Codes

For detailed information about programming, refer to "Program a Panel".

18.6.3 Send Programming to a Group

Open the group from the **File > Account Groups** window before sending any programming information. After completing maintenance on holiday dates, schedules, output schedules, profiles, and user codes, select **Group > Send Now** to send the updated information to all the panels in the selected group. Remote Link attempts to connect to each panel in the group to send the program information.

> ℹ️ **Note:** If changes were made to Holidays, Schedules, Output Schedules, or Profiles, information sent to the account group overwrites any existing panel programming.

If Remote Link fails to contact any panel, it skips to the next panel in the list until all panels are contacted and updated. When the send process completes, the **Group Send Status** screen displays.

To view the send status of a selected group, select **Group > Send Status**.

Group Send Status

The **Group Send Status** window displays a list of the panels Remote Link attempted to connect to when the group send process was started. Any communications that fail are listed first. To resend all accounts that failed to update, select **Resend Failed**. To send a single account, select that account and select **Send Selected**. After the resend process, the **Status** column in the **Group Send Status** window updates.

18.7 Feature Upgrades

XR150/XR550 Series panels can perform a remote feature upgrade using Remote Link. This remote Feature Upgrade capability allows you to enable additional features on panels without requiring a trip to the site.

18.7.1 Purchase Feature Upgrades

If you would like to purchase a feature upgrade, the authorized purchasing agent for your company may contact DMP Customer Service at 866-266-2826. Include the upgrade features to enable and the panel serial numbers on the request. A separate feature key is issued for each panel and only enables the requested feature for that panel.

18.7.2 Available Upgrade Features

Encryption (XR550 with Network only)

Enable this feature to use 128-bit AES data encryption. This feature upgrade can only be enabled on an XR550 with Network. When using encryption, verify that a Passphrase is configured in panel programming and the Remote Link **Network Options** tab.

32 Door Add-On A / 32 Door Add-On B

XR550 Series Panels include 32 doors of access control. Door capacity can be increased to a maximum of 64 or 96 by applying the 32 Door Add-On A/32 Door Add-On B Feature Upgrade. This feature upgrade can only be enabled on an XR550 panel version 111 or higher. There are five LX-Bus ports on each XR550 panel. This feature allows an LX-Bus address (e.g. 501) to be entered at Device Setup to program a 734 attached to the bus. Once a 734 address has been programmed for the bus, the LX-Bus is automatically converted from a hardwired zone expansion bus to a hardwired Access Expansion Bus (AX-Bus).

- Each 734 module provides one door relay and four protection zones to connect switches such as door and window contacts.
- 16 doors of access can be programmed per AX-Bus to a maximum of eighty (80) 734 modules.
- Any unused AX-Bus zone numbers may be programmed as wireless zones. Hardwired zone expansion modules such as the 711, 714, 715-16 and others are incompatible with bus operation and cannot be used.
- Device Setup programming for AX-Bus address are automatically programmed as a door type. Device Type, Communication Type and Display Areas are not shown. Only 734 module programming is shown.
- An AX-Bus operation is only compatible with 734 Series Access Control modules and the Model XR550. Keypads, 734N and 734N-Wifi modules must only be use on the keypad bus.

Perform the Upgrade

To perform a remote panel feature upgrade, connect to the panel with Remote Link and go to **Panel > Feature Upgrade**. Enter the factory-supplied feature key select **Activate**.

> ⓘ **Note:** The XR550 Series Version 106 or higher only requires a six-character Feature key.

19 Update Remote Link and Link Server

Remote Link and Link Server updates are available to download from Dealer Admin.

19.1 Requirements

To download Remote Link and related software updates, you must have a Dealer Admin account. To get help with your account, contact:

SecureCom Customer Service

877-300-8030

customerservice@securecomwireless.com

No special permissions or roles are required in Dealer Admin to download Remote Link updates.

If you are using Link Server, update it before updating Remote Link on any client computer.

19.2 More Information

To learn more about using Dealer Admin, refer to Dealer Admin Help.

19.3 Update Link Server

To download and install a Link Server update, complete the steps in each of the following sections.

19.3.1 Step 1: Download Link Server

1. Sign in to Dealer Admin.
2. In the menu, expand **Dealer Resources** and go to **Downloads**.
3. Find the Link Server version that you want to download.
4. If you want to read the Technical Update for that release, select **Release Notes**.
5. To download the software, select **Download**.

19.3.2 Step 2: Update Link Server

Determine If DBISAM Needs Upgraded

With most Link releases, only **Link.exe** and associated help files need to be updated. However, if the DBISAM engine is updated you must also update **dbsrvr.exe** on Link Server.

To check the DBISAM engine version, right-click **dbsrvr.exe**, select **Properties**, then open **Details** and check **File Version**. Compare the currently-installed version of **dbsrvr** with the new version in **LinkServerUpdate.zip**. If the versions are different, an update is required. Skip to "Update Both Link Server and DBISAM".

Update Link Server Only

1. Close Link Server.
2. Find and double-click **LinkServerUpdate.zip** to run the automatic extraction utility.
3. When prompted to choose the installation location, select the directory where Link Server is currently installed. The default directory is C:\LinkServer.
4. From your PC's Start Menu, run **Link Server > Setup Link Server** and keep the existing database.
5. Enter the username and password that you use to log in to Link Server. Default username is **admin**, default password is **LinkAdmin**.

When setup is complete, the server is updated and you can update Remote Link on client computers.

Update Both Link Server and DBISAM

> ⚠️ **Caution:** This process involves overwriting application files. If you want to back up Link or Link Server, do so before completing these steps.

This procedure requires that you stop the server to apply updates, then restart it. You can either perform this from the Services app in Windows or from a Command Prompt (CMD) terminal. Do not use the System Tray icon to try to stop the service—this does not fully stop the service and does not allow you to update the server.

- To stop or start the service from **Services:** Go to **Services**, right-click the **DBISAM Database Server - DBSRVR** service and select **Stop** or **Start**
- To stop the service from Command Prompt, run net stop dbsrvr.
- To start the service from Command Prompt, run net start dbsrvr.

To update the server, complete the following steps:

1. Close Link Server.
2. Stop the DBISAM database service.
3. Find and double-click **LinkServerUpdate.zip** to run the automatic extraction utility.
4. When prompted to choose the installation location, select the directory where Link Server is currently installed. The default directory is **C:\LinkServer**.
5. When prompted to overwrite the existing files, select **Yes to All**.
6. Start the DBISAM database service.
7. Start **Link.exe** on the server. If Remote Link asks you to update the database, select **Yes**.
8. Apply **LinkUpdate.exe** to all of the workstations where Remote Link is used to access the shared server.

19.4 Update Remote Link

To download and install a Remote Link update, complete the steps in each of the following sections.

19.4.1 Step 1: Download Remote Link

1. Sign in to **Dealer Admin**.
2. In the menu, expand **Dealer Resources** and go to **Downloads**.
3. Find the Remote Link version that you want to download.
4. If you want to read the Technical Update for that release, select **Release Notes**.
5. To download the software, select **Download**.

19.4.2 Step 2: Update Remote Link

1. Close **Remote Link**.
2. Find and double-click **LinkUpdate.exe** to run the automatic extraction utility.
3. When prompted to choose the installation location, select the directory where Remote Link is currently installed. The default directory is **C:\Link**.

When setup is complete, Remote Link is updated. To check the current software version, open Remote Link and go to **Help > About**.

20 Reference

20.1 Keyboard Shortcuts

The following keys on the keyboard can be used in a window or a full screen when you are in the Remote Link program.

20.1.1 Global Shortcuts

Press	To
F1	Display Context-sensitive Help
Alt + F10	Display Diagnostics window
F11	Log On / Off
Ctrl + Tab	Switch between Remote Link windows
F3	Display Alarm List

20.1.2 Menu Keys

Press	To
Alt + (letter)	Hold down the Alt key and press the underlined letter in a menu title to open the menu. For example, Alt + F opens the File menu.
Left/Right Arrow	Move between open menus on Menu bar.
Up/Down Arrow	Move between menu options.
Enter	Choose the selected menu name or command.
Esc	Cancel the selected menu name or close the open menu.

20.1.3 Dialog Box Keys

Press	To
Tab	Move from option to option (left to right and top to bottom).
Shift + Tab	Move from option to option in reverse order.
Alt + (letter)	Move to the option or group whose underlined letter or number matches the one you type.
Alt + Down Arrow	Open a list.
Space Bar	Select an item in a list when multiple items are available.
Enter	Run a command.
Esc; or Ctrl + F4	Close a dialog box without completing the command.
F1	Open the topic of the Help File that relates to the active field or dialog box.

20.2 Frequently Asked Questions

1. **How do I make the SCS-105 receiver dial DTMF?**

In the **System > Configure > Remote Link** window, select the **Receiver** tab. In the section titled **Communications Options**, check the box labeled **Tone Dial**. This will cause the SCS-105 receiver to tone dial. The SCS-1R receiver will always pulse dial.

2. **Can I set a schedule that disarms in the evening and arms in the morning?**

Yes. For the panel to recognize a schedule as being valid, it must see an opening time before the closing time. This still applies to set a schedule that runs through midnight. Program the schedule as follows: In the Monday Opening field enter 8:00 PM. In the Monday Closing field enter 7:00 AM TUE. With this schedule, the system will disarm at 8:00 PM Monday and arm Tuesday at 7:00 AM. Repeat for each day of the week that you wish to schedule. This keeps the opening time before the closing time.

3. **What do I need to do for normal maintenance on my Remote Link computer?**

As with any computer running Windows and Windows applications, you should have a program of regular maintenance to keep the system optimized. Additionally, set a regular schedule to backup your database files.

4. **What is the Receiver Timeout Message? Why do I get an hourglass mouse cursor before I get this message.**

The receiver and computer are not communicating correctly. Check the connections between your computer and receiver.

5. **In some places I see my account number listed as 12345, while in other places it is listed as 1-12345. Which is it?**

The account number is the number that displays after the dash, while the first digit is the receiver number. In this example, 1-12345 is the receiver number (1) followed by the 5-digit account number (12345). When programming the panel, enter 12345 for the account number.

6. **I've logged on to Remote Link but several of the options are not available.**

Go to **System > Operator Configuration** to confirm the options for the operator. Make sure that the boxes are checked for each option you want assigned to the operator. Also keep in mind that not all options are available for each panel type.

7. **A new panel will not stay on-line with Remote Link. The panel will seize the line then immediately hang up.**

The account number in the file you have open while trying to connect with a panel must match the account number programmed into the panel. If you are trying to connect to a panel with the default account number

(12345) and send an existing file, this can be done. However, you must first connect to the panel with the panel's account number. Once connected, this account number can be changed to a unique account number.

20.3 Glossary

4-2 Communication definition - A hexadecimal communication format that allows the panel to send alarm and system reports to non-DMP receivers. The 4-2 format consists of a 4-digit account number, a 2-digit event code, and a 1-digit checksum.

20.3.1 A

"A" Zone (Style D) - a circuit extending from and returning to a fire alarm control device or transmitter to which normally open contacts of alarm actuating devices are connected for the initiation of alarm signals. Routinely referred to as four-wire zone supervised. See "B' zone.

abort - an authorized user of the system manually cancels an alarm after an armed zone has tripped. Used mainly when the zone trip was accidental, such as the opening of an armed door, and a police or fire response is not needed.

abort report - a report sent by the panel following an alarm report to indicate the alarm has been cancelled by an authorized user and no dispatch is required.

access - the ability or opportunity to enter an area or to obtain knowledge of certain information.

access code - a combination of ID numbers related to a defined time segment. These combinations are programmed into an access system to grant or deny access to system users. Also, programmer lockout code is a programming option that allows you to enter a special code into the panel that will then be required to gain access to the panel's internal programmer through the keypad. You can change this code at any time to any combination of numbers form one to five digits long. Once you have changed the code, it is important that you write it down somewhere and store it in a safe place. Lost lockout codes require the panel to be sent back to DMP for repair.

access control - the means of influencing and regulating the flow of people through a door.

access control card - a card containing coded information. It is placed in or near a card reader. The card is read and access is granted if the information from the card is valid for that specific time, day, and location.

access keypads - a programming option that allows door access reports to be sent to a receiver. A report is sent with each door access made from selected keypads. Keypads at addresses not selected still operate the door strike relay but do not send door access reports.

access level - access priorities.

access point - a door, gate, or other barrier through which people or vehicles can gain access to a defined area.

access privileges - controls placed on network services that limit and control user access through doors.

account number - all reporting systems have an account number that identifies them at the central station. The account number is included along with any reports the panel sends to the receiver.

acknowledge - to confirm that a message or signal has been received, such as by the pressing of a button or the selection of a software command.

action - a zone programming option that selects the action of any outputs activated by changes in the zone's condition. The four options are: steady, pulsed (one second on, one second off), momentary (one second on for one time only), and follow (on when the zone is off normal, off when the zone restores).

activity report - a record of openings, closing, alarms, and other signals received from a protected premise and maintained by the central station alarm company.

address - 1. a switch setting on a keypad, zone expander, or other device that reflects its assigned position on a data bus. Zone expanders, for example, are addressed so that the panel is able to associate its onboard zones with their programmed location and characteristics held in memory. 2. A sequence of bits used to identify devices on a network. Each network device must have a unique address. Addresses fall in two categories: physical hardware addresses and logical protocol addresses.

addressable device - an alarm system component with discrete identification that can have its status individually identified or that is used to individually control other functions.

adverse condition - any condition occurring in a communications or transmission channel that interferes with the proper transmission or interpretation, or both, of status change signals at the supervising station.

alarm - a condition in which one or more armed zones in the system have been faulted. Almost all alarms sound some form of audible device locally except in the cases of silent panic or ambush alarms.

alarm bell - a bell or siren installed on the protected premises that gives indication of an alarm condition to persons inside or nearby.

alarm control - a device that permits an alarm system to be turned on and off and provides electrical power to operate the system. Every alarm system must have an alarm control.

alarm initiating device - a device which, when actuated, initiates an alarm. Such devices, depending on their type, can be operated manually or actuated automatically in response to smoke, flame, heat, or water flow.

alarm module - an add-on device to monitor a series of sensors and initiate warning devices if required.

alarm panel - the main controlling CPU in the alarm system to which all zones, phone lines, and devices are connected.

alarm receiver - a receiver that is designed with the main purpose of receiving alarm events. Receivers are usually located and maintained at a central station company.

alarm signal - an alarm signal lets people know the alarm system has activated. The alarm signal may be a bell, siren, or visual device (local alarm), or it may be a message transmitted to a central station alarm company on leased telephone lines or the switched network. Every alarm system must have an alarm signal.

alarm silence - a keypad menu function that allows authorized users to silence alarm bells or sirens during an alarm condition on the system. Users can also enter their user code and press the command key directly from the status list. This is an exclusive function of DMP panels that allows silence of alarm bells without disarming the system.

alarm system - a combination of compatible initiating devices, control panels, and notification appliances designed and installed to produce an alarm signal in the event of emergencies.

all/perimeter - a panel mode of operation that provides for the system to be configured into just two areas: a perimeter and an interior. Exterior doors and windows are assigned to the perimeter while inside PIRs, doors, or pressure mats are assigned to the interior area.

alphanumeric - term used to describe letters and numbers together.

ambush - a silent, invisible alarm signal sent to the central station that indicates a user is being forced to disarm the system. The ambush code is sent when ambushed is programmed as YES in the panel and a code for user number one is entered at the keypad. DMP panels use a unique ambush code number to prevent false alarms.

ambush code - a special code entered into a digital keypad to indicate a duress condition that directly threatens the user. This code does not activate signaling devices at the premises.

ambush output - a panel output that is programmed to activate any time an ambush code is entered at a keypad. The output is turned off using the sensor reset option from the user menu. This output is used to lock down areas or activate strobes, etc.

American National Standards Institute (ANSI) - a federation of trade, technical, professional organizations, government agencies, and consumer groups that coordinates standards development, publishes standards, and operates a voluntary certification program.

American Standard Code for Information Interchange (ASCII) - a commonly used coding scheme that uses eight bits of data to encode alphanumeric and special control characters. Common to most computer platforms.

analog - a method of data transmission where the data is continually modulated to represent transmitted information.

annunciator - a keypad or other lighted or audible display at the protected premise that indicates the condition of the system, zones, and armed status.

anti-passback - a programming option that requires a user to properly exit (egress) an area they have previously accessed. If they fail to exit through the proper card reader location they will not be granted access on their next attempt. Also, see egress.

any bypass - a panel programming feature that allows low level users to bypass zones during the arming sequence without having to enter a higher level user code.

area - part of a protected premise that is programmed to operate separately from the other areas. Areas can have their own keypads, zones, account numbers, and arming and disarming schedules.

area arming - a panel mode of operation that provides for one or more areas to be individually armed and disarmed.

area schedules - a programming option that allows you to automatically arm and disarm areas within a system. This is done by entering schedules in the panel programming.

arm - to turn on the burglary or other non-24-hour hour protection in a protected premises.

armed - a condition in which a zone or system can be placed. When a zone is armed, a change in its normal state causes the panel to activate an alarm. Fire, panic, and other 24-hour zones are considered always armed.

armed output - a programming option that allows an output to be controlled by the arming cycle of an area.

armed rings - the number of rings the panel counts before answering the phone line when all areas of the system are armed.

arming zone - a DMP zone type that allows you to use keyswitches to arm and disarm areas within a system. This is done by entering the area number(s) to be controlled into the area section of the arming zone programming.

asynchronous communication - a technique of data transmission that sends one character at a time without waiting for an acknowledgement.

authority level - a level of access to the system and its functions that is assigned to each user code. Each area must have at least one user with a master authority in order to be able to add, change, or delete other users.

auto arm - to automatically turn on the burglary protection in one or more areas through the use of schedules. These schedules allow you to set the time of day for the arming to occur. If using the automatic arming feature along with the closing check (see closing check), the arming does not take place until the expiration of a tenminute closing check delay. If the area has been disarmed outside of any schedule, the closing check

sequence occurs one hour after the area is disarmed. At arming, bad zones are handled according to the bypass option selected. If a closing report is sent to the central station, the user number is indicated as SCH (for schedule) on the receiver.

auto disarm - to automatically turn off the burglary protection in one or more areas through the use of schedules. These schedules allow you to set the time of day for the disarming to occur. If an opening report is sent to the central station at disarming, the user number is indicated as SCH (for schedule) on the receiver.

automatic recall test - a signal generated by the panel that is sent to the central station. This signal indicates that the panel communicator is working properly and is able to send signals to the central station receiver.

automation software - central station software that receives signals from an alarm receiver and displays alarms on a display screen to allow dispatching of the proper authorities.

away - a panel arming mode in which all areas of the system are armed. This option is for when the user is leaving the premises and no person is left inside.

20.3.2 B

"B" Zone (Style A) - a circuit extending from a fire alarm control device or transmitter to which initiating or notification devices are connected. The zone is terminated with an end-of-line supervision resistor.

backup - as used in programming for receiver one and receiver two reporting, choosing YES for this option means that the receiver will be contacted by the panel in the event the primary receiver cannot be reached.

Bank, Safe, and Vault - an area operating characteristic that prevents disarming, schedule changes, and time/date changes during armed periods. This feature is typically used on bank vaults, but can also be used for restricted access storage, gun rooms, or other areas for which the user wants an extra level of protection.

bell - alarm bell - a bell or siren installed on the protected premises that gives indication of an alarm condition to persons inside or nearby.

bell action - a zone programming option that defines the action of the alarm bell output for alarms on that zone.

> **none:** no bell action for an alarm condition on the zone.

> **pulsed:** a repeating one second on, one second off bell output for the duration of the programmed bell cutoff time.

> **steady:** a steady, uninterrupted bell output for the duration of the programmed bell cutoff time.

> **temporal code**: a repeating 0.5 second on, 0.5 second off (three times) followed by 2.5 seconds off. This lasts for the duration of the programmed bell cutoff time.

bell cutoff - the length of time the alarm bell or siren is programmed to ring after an alarm. DMP panels allow a programmable length of time in one-minute increments. Entering a zero allows the bell output to run continuously. AHJ requirements for bell cutoff can vary but it is typically between five and 15 minutes.

bits per second (bps) - a unit that measures the message carrying ability of a medium. A kilobit per second (Kbps) is one thousand bits per second. A megabit per second (Mbps) is one million bits per second.

burglar alarm system - an alarm system for detecting a burglary.

burglary output - a panel output that is activated any time a specified burglary type zone is placed into alarm. The output is turned off when the user disarms the area in which the alarm occurred.

bypass - a manual shunting of a zone by a user that allows the panel to ignore any activity on the zone until it is reset back into the system. A user can bypass a zone at any time from the user menu or while arming the system if they cannot restore it to normal. Used when a user wants to keep a door or window open or when a device is in need of service. See also swinger bypass.

bypass reports - a programming option that allows zone bypasses, resets, and force arm reports to be sent to a receiver.

20.3.3 C

cancel - see abort and abort report.

cellular - a communication programming option that enables cellular transmissions with Cell-Miser™ call restrictions.

Cell-Miser™ - when Cell-Miser™ is selected in programming the panel restricts its cellular calls to zone alarms, ambush, line one trouble, abort, and recall test reports. Additionally, delayed event reports can also be sent but only if the original cellular call was made to transmit one of the previously listed reports. Line 1 trouble is sent only once during each armed period.

central station - a supervising station that is listed for central station service.

certification - a systematic program using randomly selected follow-up inspections of the certificated systems installed under the program, which allows the listing organization to verify that a fire alarm system complies with all requirements of this code. A system installed under such a program is identified by the issuance of a certificated system.

chime - a single-stroke or vibrating type audible notification appliance, which has a xylophone-type striking, bar, and/or tone.

Class A Circuit (Zone) - NFPA Style D - an arrangement of a supervised initiating or signaling line or indicating circuit that allows the operation of the circuit despite the occurrence of a single open or ground condition. A requirement of fire protection systems that requires alarm operation even when a single break or a single ground faults exists on the circuit.

Class B Circuit (Zone) - NFPA Style A - an arrangement of a supervised initiation or signaling line or indicating circuit that doesn't allow automatic circuit conditioning to operate during a single open or a single ground condition.

client - a process (program or routine) or entity (person, LAN) that employs the services of servers.

client/server - the interaction of software processes that function in a cooperative manner. Clients make requests of servers.

closed circuit system - a switch or other detector used in closed circuit alarm systems that is closed prior to alarm and opens on alarm.

closing check - this programming option enables the panel to verify that all areas in a partition that has been armed after primary/secondary or permanent/temporary schedules have expired. If the closing check finds any areas disarmed past the scheduled time, the keypad selected to display system trouble status emits a steady beep and displays CLOSING TIME! If you also select area schedules, the appropriate area name is displayed followed by - LATE. The keypad's steady beep is silenced by pressing any top row select key. If the system is not armed or a temporary schedule not extended within ten minutes, a no closing report is sent to the central station

receiver. If the area has been disarmed outside of any schedule, the closing check sequence occurs one hour after the area was disarmed.

closing code - this programming option provides for a user code to be required for system arming.

closing wait - a programming option that provides for the panel to display a message on the keypad and delay arming the system until the closing report has been acknowledged by the central station receiver.

code change reports - a programming option that allows code additions, changes, and deletions to be sent to a receiver.

coded - an audible or visible signal conveying several discrete bits or units of information. Notification signal examples are numbered strokes of an impact-type appliance and numbered flashes of a visible appliance.

collision - the condition that results when two network devices transmit at nearly the same time. The transmissions collide, making the data unusable.

command key - the command key is used to step ahead through options in the panel's programmer or user menu. Pressing the command key allows you to go forward and through each step of a menu section. As you go through the options, the keypad displays any current selections already stored in the panel's memory. The command key is also used to enter information into the panel's memory, such as phone numbers or zone names, by pressing the key after entering the information and it is being displayed correctly on the keypad.

Command Processor™ - the trademarked name for DMP control/communicator alarm panels.

common area - a unique DMP programming option that allows specification of one or more areas within a partition to arm automatically when all other areas are armed. Alternately, common areas disarm when any area in the same partition is disarmed. Common areas are ideal for lobbies, storage rooms, or other areas shared by multiple users.

communication port (COM port) - a serial port on a computer designed for communicating. DMP uses this port to connect to a receiver or direct connect to a panel.

communication type - a programming option that specifies the communication method the panel uses to report events to DMP receivers or non-DMP receivers. Note: All formats are not available for all panels. Consult a programming manual for availability.

DD - Digital Dialer communication to DMP receivers.

MPX - Multiplex communication format to DMP receivers.

M2E - Radionics Modem IIe communication format to non-DMP receivers.

CID - Ademco Contact ID communication format to non-DMP receivers.

4-2 - A hexadecimal communication format to non-DMP receivers.

HST - Asynchronous communication transmitted over a network to an SCS-1R receiver.

Contact ID (CID) - a panel-reporting format developed by Ademco that allows panels to send reports to a receiver in DTMF format. A Contact ID report is made up of 18 DTMF digits.

cross zone time - the amount of time programmed into the panel during which armed cross zoned zones must trip before an alarm report is sent to the central station. Cross zone time can be from four to 250 seconds.

cross zoning - a zone characteristic that requires the zone to trip twice, or a second cross zoned zone to trip, within a programmed amount of time before an alarm report is sent to the central station. An example of cross zoning would be two interior PIRs. One PIR might trip due to an environmental occurrence but an alarm report

would not be sent until the other PIR is also tripped or the first PIR restores and then trips again. If neither zone trips before the programmed cross zone time expires, only a zone fault report is sent to the central station. Cross zoning reduces false alarms by requiring two zone trips to send an alarm report.

cutoff output - a panel programming option that allows you to specify individual onboard outputs to turn off after a programmed time period. See cutoff time.

cutoff time - a programming option used with cutoff outputs that specifies how long a selected output remains activated. The programmable range is in one-minute increments.

20.3.4 D

data - information represented in digital form, including voice, text, facsimile, and video

day zone - a zone type that buzzes the keypad and provides a trouble report to the central station if the zone is tripped while its area is disarmed and an alarm if the zone is tripped while the area is armed. This is typically used with window foil, emergency zones, or other types of protection that needs constant supervision but not always an alarm. The keypad buzzer initiated by a day zone can be silenced by pressing any top row select key.

DD (digital dialer) - a programming option for the panel to use standard digital dialer communication to a DMP receiver. DD is a DMP proprietary format using SDLC protocol.

DDMX - a communication option in the 1912XR Command Processor panel that can allow the panel to communicate to the central station as a digital dialer during disarmed periods but then switch automatically to multiplex communication when the last area in the system is armed.

defer test time - a programming option that allows the panel to defer sending in a scheduled test report if it has already communicated with the central station receiver within the time period entered into the test frequency option. See test frequency.

delay reports - a programming option under Events Manager that provides for all non-alarm reports to be held in the panel's memory until the event buffer is nearly full or until the panel's next communication with the receiver.

delay zone - see exit zone.

detector - a unit that is installed as a satellite component in a security system designed to detect an intruder within a protected area.

device - any keypad, expander, or point addressable module that requires an address on the keypad or LX-Bus.

detector - a device used for detecting an intruder.

device fail output - this programming option provides for the specified output to turn on any time an addressed device fails to respond to polling from the panel. The output is turned off when all programmed devices respond to polling.

digital communicator - a means of transmitting alarm signals and other information to a central station using the customer's existing phone line. To transmit an alarm, the communicator seizes the customer's phone line and electronically dials the central station receiver. When the receiver answers, the communicator sends a message in the form of a sequence of tones. A mini-computer in the receiver accepts and acknowledges the message. It then prints out the information for display to the operator.

direct wire - a dedicated leased telephone line from subscriber's premises directly to a central station monitoring point. Line used for alarms only.

disarm - to turn off the burglary protection in an area using a keypad, keyswitch, or remote programmer.

disarmed rings - the number of rings the panel counts before answering the phone line when any areas of the system are disarmed.

display events - a user menu option that allows authorized users to view a record of events that occurred on the system. The panel stores in memory all alarms, troubles, and restorals as well as other options.

door access - a feature of DMP Security Command keypads or 733 Wiegand Interface modules that allow a user to enter their code number and cause an internal Form C relay to activate and release an electric door strike or magnet. A door access report containing the keypad address and user number can also be sent to the central station.

dual reporting - a method of sending the same signals to two separate receivers. An example would be to send alarms and openings/closings to receiver 1 as well as receiver 2.

DTMF (Dual-Tone Multiple-Frequency) - this feature enables touch-tone dialing.

duress - see ambush.

20.3.5 E

egress - a programming option that allows individual access doors to be assigned to detect anti-passback violations. See also anti-passback.

entry delay - the length of time programmed into the system during which the user can enter the premises through an exit zone (usually a front door) and disarm the system.

entry output - a specified output on a panel that is turned on at the start of the entry delay time. The output is turned off when the area is disarmed or the entry delay time expires.

entry zone - a zone type usually assigned to a perimeter door that allows the user a short amount of time to enter and exit while the system is armed without setting off an alarm.

Ethernet - a LAN cabling system originally developed by Xerox, Intel, and Digital. Ethernet has a bandwidth of 10 Mbps and uses the CSMA/CD access method.

events - system activity that generates messages to the reporting device

events manager - a programming option that specifies when non-alarm reports are sent to the receiver. Selecting this option does not affect zone alarm, zone trouble, zone restoral, supervisory, or serviceman reports. Closing reports are not delayed if the closing wait option is enabled.

exit alarm - an alarm that occurs when a zone is still bad at the end of the exit delay time. This usually occurs when the door through which the user exited does not close all the way before the programmed exit time expired.

exit delay time - the length of time programmed into the system during which the user can exit the premises through an exit zone (usually a front door) and disarm the system.

exit output - a specified output on a panel that is turned on any time an exit delay time starts in any area of the system. The output is turned off when the exit delay time expires or when the arming has been stopped.

exit zone - a zone type usually assigned to a perimeter door that allows users a programmable amount of time to enter and exit while the system is armed without setting off an alarm.

20.3.6 F

factory defaults - this function of the panel's programmer allows you to quickly turn programming parameters back to their factory default setting.

false alarm - an alarm signal initiated without the presence of an emergency. This term is generally used to describe an unwanted alarm condition. A false alarm report is sent by the panel due to a user error, environmental activation, or malfunction of a security device installed in the system. False alarms can be controlled by thoroughly training all users and ensuring that equipment is installed according to the manufacturer's recommendations.

fault - a report that is sent to the central station receiver whenever a fire verify or cross zoned zone is tripped once but does not trip a second time to cause an alarm.

fire alarm output - a specified output on a panel that is turned on any time a fire type zone is placed into an alarm condition. The output is turned off using the sensor reset option in the user menu while no additional fire type zones are in alarm.

fire trouble output - a specified output on a panel that is turned on any time a fire type zone is placed into a trouble condition or when a supervisory type zone is placed into an alarm or trouble condition. The output is turned off when all fire and supervisory type zones are restored to normal.

fire verification - typically used on smoke detector zones to provide a reset of the panel's switched auxiliary power or power supply (from where the smoke detectors are powered) and a delayed length of time during which the detector must trip again before an alarm is initiated.

fire verify - a zone type typically used with smoke detectors that provides a reset, after a fire alarm, of the panel's switched auxiliary power and 2-wire smoke detector zones and a delayed length of time during which the detector must trip again before an alarm is initiated.

flow control - the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

force arm - this arming option allows the panel to force arm the system and ignore all bad zones. Zones force armed in a bad condition are capable of restoring and reporting an alarm if tripped. A report of the force armed zones is sent to the central station receiver if the bypass reports option has been programmed as YES.

Form "A" Contacts - single-throw contacts that are normally open. See open circuit.

Form "B" Contacts - single-throw contacts that are normally closed. See closed circuit.

Form "C" Contacts - a dry contact, single-pole double-throw (SPDT) relay that provides one common, one normally open, and one normally closed connection. When activated, the normally open side is shorted to the common while the normally closed is opened.

4-2 Communication - a hexadecimal communication format that allows the DMP panel to send alarm and system reports to non-DMP receivers. The 4-2 format consists of a 4-digit account number, a 2-digit event code, and a 1-digit checksum.

4-Wire Bus Trouble - a keypad message indicating trouble on the keypad bus. This message is generated when one of the following conditions occur:

- Two Supervised devices on the keypad bus are set to the same address.
- No supervised devices on the keypad bus.
- Low data voltage on the yellow wire of the keypad bus.

fully armed - a condition on the system where all areas are in an armed state.

fully supervised zone - a zone in which the contact will activate an alarm in the event any disturbance occurs.

20.3.7 G

general alarm - a term usually applied to the simultaneous operation of all the audible and visible alarm notification appliances on a system to indicate the need for evacuation of a building.

glassbreak detector - a device attached to a glass surface or a window frame that senses an attack on that surface.

20.3.8 H

hardware address - the unique physical address deter'mined at the physical and data link layers. For example, each Ethernet card has a unique hardware address that is stored within the card.

holdup alarm - an alarm initiated by a mechanical panic button or software panic on a keypad in response to a robbery or assault.

home - a condition of the system where perimeter devices only are placed into an armed state allowing the user to move freely about the inside.

Home/Sleep/Away - this system option provides users with perimeter, interior, and bedroom areas that they can selectively arm from the keypad for maximum security. Selecting Away arms all areas of the system. Selecting Home arms only the perimeter protection of the system. Selecting Sleep arms the perimeter and interior areas, but leave devices near bedrooms and other nighttime areas off.

host - asynchronous communication over digital data networks.

host check-in - a programmable time period that specifies the delay, in minutes, the panel waits to send its next check-in report. Since host communication is not a polled method, the check-in time allows the SCS-1R Receiver to get a check-in report (s70) periodically to verify the communication link with the panel.

20.3.9 I

ingress (entrance) device - a device sensor configured to control access into an access-controlled area.

initialize - the initialization function of the panel's programmer allows the clearing of selected parts of the panel's program to default or blank settings. Initialization can include clear all codes, clear all schedules, clear display events memory, clear zone information, clear area information, clear communication and remote options, and a set to factory default options.

initiating device - any manually or automatically operated equipment that, when activated, initiates an alarm through an alarm signaling device.

instant alarm - see night zone.

Integrated Services Digital Network (ISDN) - a digital communications standard that integrates voice and data.

20.3.10 K

Kbps - kilobits per second. See bits per second.

keep - a programming option under Events Manager that provides for all non-alarm reports to be held in the panel's memory buffer until they're overwritten by new stored activity. You can view the contents of the memory buffer using the Remote Link software program or the display events feature in the user menu.

keypad - a device with a keyboard and display that allows users to enter codes, arm and disarm areas, view current and past events, and perform system functions such as silencing alarm bells and changing user codes. Keypads can have LED, LCD alphanumeric, or vacuum fluorescent alphanumeric displays.

keypad alarm control - a burglar alarm control that is turned on and off by entering a numeric code into a digital keypad. Signals can be sent when the control is turned on and off so that the central station alarm company can supervise openings and closings.

20.3.11 L

late to close output - a specified output on a panel that is turned on any time a programmed area remains disarmed past the scheduled closing period. The output is turned off when the area is armed, the closing schedule is extended, or the schedule is changed.

line security - the degree of protection of the signaling system that connects the subscriber's system to the central station alarm company. Two levels of line security-standard and encrypted-are recognized by UL.

line supervision - the electrical supervision of a wire run to detect tampering (a cut or shorted wire). Line supervision usually requires a terminating element at the end of the monitored wire zone.

local alarm - a visual or audible signaling device located at the premises.

Local Area Network (LAN) - a network in one area, such as a building or group of buildings.

local printer - a serial printer that can be connected to certain DMP Command Processor panels to provide a printout of system events. This feature can allow business owners to track activity of employees, check system arming and disarming times, or monitor other events of their security or fire system.

local system - an alarm system that rings a local sounding device in the event of an intrusion.

loop - see zone.

LX-Bus™ - a DMP 4-wire data bus onto which you can connect addressable zone and output expanders.

20.3.12 M

manufacturer authorization - a unique DMP panel programming option that allows you to create a one hour window during which DMP technical support technicians can contact the panel remotely for diagnostic purposes. DMP technicians can only view the system programming and cannot make any changes.

mode - a programming option that allows you to select Area, All/Perimeter, or Home/Away arming modes for the panel's areas. Area arming mode allows areas to arm independently of each other as separate systems. All/ Perimeter mode provides a perimeter and interior area as one account. Home/Sleep/Away mode provides a perimeter, interior, and, in some cases, bedrooms area as one account.

modem - a device that converts digital data from a computer into analog data, which can then be transmitted over a telephone line. This process is called modulation. It also performs the opposite process, demodulation, which converts incoming analog signals into digital data the computer can understand.

multiplex - a communication method DMP panels use that keeps the panel in contact with the SCS-1 Receiver. Alarm and system information are transmitted quickly as the panel does not need to dial a phone number or wait to be acknowledged by the receiver. Each multiplex panel is sequentially polled by the SCS-1 Receiver to maintain constant supervision.

multiplexer - a network component that combines multiple data signals onto one path.

20.3.13 N

network interface controller - a networking card, such as Ethernet, Token Ring, or FDDI, for a computer.

network server - A computer or device on a network that manages network resources. For example, a network server is a computer that manages network traffic.

night zone - a zone type that provides an instant alarm when tripped while armed and no alarm when tripped while disarmed.

non-polled address - a keypad message indicating that the device is set to an unavailable address or that the device has not been turned on in device setup.

notification zone - an area covered by notification appliances that are activated simultaneously.

20.3.14 O

open circuit - a condition in which no electrical continuity exists in a circuit of conductor. In an open circuit protective zone, the detector contacts are open when the detector is in a quiescent state and closed in alarm.

openings and closings - a prearranged schedule between the alarm subscriber and central station alarm company for turning the system on and off. The central station records this event. The central station knows when a system has been left off inadvertently.

opening report - a report sent to the central station at the time a system is disarmed showing who disarmed it, what area was entered, and the current time and date. This information is often of interest to the customer for tracking employee activity.

option - a user selectable function that can be accessed from the keypad's user menu.

output - any type of notice or action that a panel will initiate when a sensor connected to that panel is triggered.

output action - a zone programming option that defines the action of an output assigned to a zone.

> **steady:** the output is turned on and remains on until the area is disarmed, an output cutoff time expires, or the output is reset from the keypad user menu.

> **pulse:** the output alternates one second on/one second off.

> **momentary:** the output turns on only once for one second.

> **follow:** the output turns on and remains on while the zone is in an off normal, or bad condition.

output cutoff time - a programming option that allows you to specify a cutoff time for the panel's outputs. If the output is turned off by the user, or by an event restoral, the cutoff time is reset and starts over at the next occurrence.

output schedules - panel schedules that allow you to set automatic on and off times for the relay outputs on DMP panels. Output schedules can be used to turn on exterior lights, HVAC systems, CCTV cameras, or any

other contact activated devices. Outputs controlled by schedules can also be manually turned on or off by users with the proper authority level.

20.3.15 P

packet - an organized sequence of binary data that includes data and control structures.

Pager Direct™ - a reporting capability that allows a pager to receive system reports directly from the panel.

pager identification number - a programming option that allows the panel to first send a unique pager ID number prior to sending actual pager messages containing system reports.

pager reporting - a programming option that allows the panel to send alarm, trouble, opening, closing, and late to close reports to a pager.

panic - a special silent or audible alarm initiated by a user that alerts the central station to an urgent situation.

parallel - a transmission format that can send multiple bits of data at the same time. This method connects an electrical circuit whereby each element is connected across the other. The addition of all currents through each element equals the total current of the circuit.

partial arming - a condition on the system where some, but not all, areas are in an armed state.

partition - a group of one or more areas that collectively operate as a multi-area panel or partition. Each partition in a panel contains areas. An area can be an office in a building or a section of a house such as the garage. Users who operate an area in one partition cannot view areas in another partition through the same keypad. Some lesser manufacturers that do not have partition capability refer to their areas as partitions.

pass-through - the ability to gain access to one network element through another.

perimeter - the portion of a protected area or building that includes doors, windows, and other accessible openings.

perimeter arming - an arming option that allows the user to turn on only the perimeter portion of their protection. Perimeter arming allows unrestricted movements within the interior of the protected areas by leaving the interior devices disarmed.

permanent schedules - programmable schedules intended for such applications as late to close annunciation and auto arming. Permanent schedules can also be programmed to restrict codes that have certain authority levels to disarming the system only during selected times.

phone trouble output - an output that turns on any time the phone line monitor detects a voltage below 3 VDC. The output is turned off when the phone voltage rises above 3 VDC.

Port - an electrical point of entry, usually on a router, to a computer, network, or other electronic device. A router can have many ports.

Post Indicator Valve (PIV) - a cast metal post over the stem of an underground gate valve supplying water to a sprinkler system. On each side of the PIV are rectangular windows through which you can view a plate showing whether the valve is open or shut.

power fail delay - a programming option that tracks the duration of an AC power failure. When the AC power is off for the length of the programmed delay, an AC power failure report is sent to the receiver.

premises - the building or home being monitored by the security or fire system.

primary schedules - programmable schedules intended for such applications as late to close annunciation and auto arming. Primary schedules can also be programmed to restrict codes that have certain authority levels to disarming the system only during selected times.

printer - see local printer.

printer reports - a programming option that allows the definition of events that are sent to a local printer.

priority zone type - a programming option that provides for a zone to be in a normal condition before its assigned area can be armed. Priority zones cannot be bypassed or force armed.

programmer lockout code - this programming option allows you to enter an access code into the panel that will then be required to gain access to the panel's internal programmer through the keypad. You can change this code at any time to any combination of numbers form one to five digits long. Once you have changed the code, it is important that it is documented and stored in a safe place. Lost lockout codes require the panel to be sent back to DMP for repair.

programmer lockout code restrictions - you cannot set a lockout code higher than 65,535 or use the codes 6653, 2313, or any three-digit code that begins with 98. These codes are reserved by the panel for various functions.

protected premises - refers to the establishment in which an alarm system is installed

20.3.16 R

ready output - a specified output that is turned on whenever all disarmed burglary zone types are in a normal condition. The output is turned off when any disarmed burglary zone is placed into a bad condition.

receiver - a communication device that relays data from a panel to software installed on a computer.

receiver key - an eight-digit code that is programmed into Remote Link and embedded into the receiver. The panel requests this key the first time it is contacted by the receiver. The panel retains the receiver key in its memory and accepts commands only from a receiver with a matching key.

relay - an electrically activated device that provides an opening or closing across two points for the purpose of switching the control voltage of lights, annunciators, bells, or other devices.

remote key - a one to eight digit code entered into the panel's program that is used to verify the authority of the person or company, receiver or computer contacting it.

remote phone number - a phone number the panel dials after a remote programming attempt is made. Once the initial attempt has been made, the panel hangs up the phone line and dials the remote phone number.

repeater - a network device that repeats the signals on a network. Repeaters operate as the physical layer of the OSI Reference Model. Repeaters amplify weak signals from one segment and repeat them on another segment.

report - a signal or message sent by the panel to the central station receiver in response to activity within an area, a programmed occurrence (such as a timer test), or a change in the system's status.

reset - a report sent to the central station receiver in response to the resetting of a bypassed zone.

reset jumper - the two reset pins on a DMP Command Processor panel used to reset the panel prior to programming.

reset panel - a keypad display that instructs the technician to reset the panel using its onboard reset jumper before programming access can be granted.

reset swinger bypass - a programming option allowing a zone that has been swinger bypassed to reset back into the system if it has been in a normal condition for one complete hour after being bypassed.

restoral - a report sent to the central station receiver in response to the restoring to normal of an alarmed or troubled zone.

restoral report options - this programming option allows you to select whether a restoral report is sent and when.

> **no:** disables the restoral report option for the specified zone. The zone continues to operate but does not send a restoral report to the central station receiver.

> **yes:** enables a zone restoral to be sent to the receiver whenever the zone restores to normal from a bad condition.

> **disarm:** zone restorals generated during the area's armed period are held in the panel's memory until the area is disarmed. At that time, the zone restoral report is sent to the receiver.

retard delay - a programmable zone characteristic that provides for a delayed period before a short on the zone is accepted as an alarm. This feature is often used when the zone is connected to a waterflow switch to allow for fluctuations in water pressure.

RJ11 jack - a four conductor phone connector used to connect standard telephones to a phone network.

RJ31X/RJ38X jack - an eight conductor phone jack used to connect burglar and fire alarm systems to a phone network. The only difference between the two jack types is a jumper installed across terminals two and seven on the RJ38X to allow for phone cord supervision. Two phone lines are required for commercial fire systems.

RJ45 - network connection.

router - a network device that connects networks by maintaining logical protocol information for each network.

Routing Information Protocol (RIP) - a protocol used to update routing tables on TCP/IP networks.

RS-232 - a standard defining interface voltage and current levels and other signal characteristics used to couple digital equipment to a transmission link. This is the standard DMP uses for direct connecting to a computer or local printer.

20.3.17 S

schedule change reports - a programming option that allows schedule changes to be sent to a receiver.

schedules - a feature that allows you to program various panel functions to occur at predetermined times. One use of schedules is for turning relay outputs on or off at certain times of the day or week. Schedules are also used to assign times for automatic arming to occur.

second line - a programming option that allows you to use a second phone line to send reports to the central station receiver should the first phone line fail.

secondary schedules - programmable schedules in panels for use in such applications as late to close annunciation and auto arming. You can also program secondary schedules to restrict codes that have certain authority levels to disarming the system only during selected times.

security code - see user code.

Security Command® - the registered trademark name of the DMP keypad.

serial - a transmission format that sends data one bit at a time and is more widely used than parallel.

server - a network device or process that provides a service to networked clients. Two examples would be file servers or print servers.

service receiver - a receiver that is designed with the main purpose of performing service to panels from a remote location, such as changing programming or viewing events.

silent alarm - an alarm that does not sound a local bell when activated, but which signals a remote monitoring station.

Simple Network Management Protocol (SNMP) - a management protocol used to maintain and query network components. SNMP uses agents on managed nodes to maintain a database known as a Management Information Base (MIB). The data stored within the MIB can be transmitted to the management software on request.

siren - see alarm bell.

sleep - a panel arming mode that arms the perimeter and interior areas, but leaves devices near bedrooms and other night time areas disarmed.

smoke detector - a device that detects the visible or invisible particles of combustion.

split reporting - a method of sending different signals to two separate receivers. An example would be to send alarms to receiver one and openings/closings to receiver two.

status list - displays any alarm or trouble condition on a zone, and any trouble condition on an internal system monitor. If more than one alarm or trouble condition occurs at the same time, the keypad sequences this information on its display.

strike time - the length of time that a keypad relay or an access control device relay will be activated.

supervised alarm service - a central station monitored alarm system that reports opening, closing, and other activities. Supervision assures that the system is turned on and off and that only authorized personnel can gain access to protected premises.

supervised circuit - a circuit in which a break or ground in the wiring which prevents the transmission of an alarm signal, will actuate a trouble signal.

supervision - the ability to detect a fault condition in the installation wiring that would prevent normal operation of the alarm system.

supervisory signal - a signal indicating the need for action in connection with the supervision of guard tours, automatic sprinkler, or other extinguishing systems or equipment, or the maintenance features of other protective systems.

supervisory zone - a 24 hour zone type typically used for supervising fire alarm valve tamper switches on OS&Ys, butterfly valves, and PIVs.

swinger - a zone that intermittently trips while armed resulting in erroneous alarm activation. Swingers can be due to light or heat fluctuations near motion detectors or loose or partially broken wires on a zone.

swinger bypass - a programmable function that allows the panel to bypass a zone that repeatedly trips. Swingers (zones that trip often) are a serious false alarm problem but can be controlled by using the swinger bypass feature. A swinger bypassed zone may be restored to the system after it has remained stable for one hour.

swinger bypass trips - the number of times a zone can go into an alarm or trouble condition within one hour before being automatically bypassed.

Synchronous Data Link Control (SDLC) - a data link layer protocol used by IBM SNA networks and DMP Command Processor panels.

system monitor - the function that allows the panel to monitor its AC power, battery power, enclosure tamper, phone line one, and phone line two. Troubles with any of these elements can be reported to a central station or displayed on the system's keypads.

Systems Network Architecture (SNA) - a suite of communications protocols developed by IBM. It is similar to the AppleTalk protocol suite for the Macintosh.

20.3.18 T

T1 - AT&T term for a digital carrier facility used to transmit a DS-1 formatted digital signal at 1.544 Mbps.

Telco - an alternate term used for a telephone company.

temporary schedules - a programmable schedule that allows the user to give restricted, short term access to another person. Temporary schedules can be used to create a window outside of normal business hours during which a maintenance or deliveryman can enter using a special code that functions only during this window.

test frequency - a programming option that allows the selection of the how often the automatic recall test is sent to the central station receiver.

test report - see automatic recall test.

test time - the time of day the panel sends the test report to the receiver.

thickwire - a type of Ethernet cabling, also known as 10Base-5, that uses a thick (about 3/8") coaxial cable. Primarily used as a backbone to which thinwire or twisted pair hubs are connected.

transceiver - a single-ended electrical installation consisting of both transmitter and receiver. It transmits a beam that is then reflected back to the receiver in the same unit.

transient - any increase or decrease in the excursion of voltage, current, power, heat, and so forth, above or below a nominal value that is not normal to the source.

transmit delay - a feature of DMP Command Processor panels that delays the sending of burglary alarm reports to the receiver for a selectable length of time up to 60 seconds.

transmitter - in a fire or security system, a device that sends alarm signals from a protected premises to a proprietary headquarters, a central station, or a municipal headquarters.

trouble - an off normal condition on a zone during a supervised state. A normally closed zone that alarms when opened, can initiate a trouble when shorted. A fire zone that alarms when shorted can initiate a trouble when opened.

trouble signal - a signal that indicates trouble of any kind. This can be circuit break or ground occurring in an alarm system's devices or wiring.

24-hour zone - a zone that is not turned on or off by arming or disarming a system.

20.3.19 U

Underwriters Laboratories, Inc. (UL) - an agency that tests and lists various consumer products for safety and reliability. Most alarm system products are UL listed for use in various applications.

UL Certificate - a certificate issued by Underwriters Laboratories Inc. that serves as evidence that an alarm system meets UL requirements for installation, operation and maintenance.

user - a person authorized to operate all or part of the security or fire system.

user code - a one to five digit number programmed into the panel and assigned to a user that allows them to access its functions. User codes are typically assigned authority levels that restrict the user to one or more of the system's functions or to certain areas for arming and disarming or door access.

user error - the number one cause of false alarms. A user who does not know how to perform a function for which they have access, or who has not been trained properly in the operation of the system, can and will cause false alarms. It is important that all new users receive instruction on arming/disarming routines and alarm cancellation procedures to lessen the incidence of false alarms.

user menu - a keypad feature that provides a list of optional functions a user can access. These functions include sensor reset, door access, outputs on/off, system status, and user codes. Individual user menu items are displayed to persons according to the authority level of the user code they entered to get into the menu.

20.3.20 V

volt/amp (VA) rating - the products of rated input voltage multiplied by the rated current. This establishes the apparent energy available to accomplish work.

20.3.21 W

Wide Area Network (WAN) - a network that spans distances beyond the range served by LANs. WAN distances are usually measured in miles instead of feet.

wideband - a system in which multiple channels access a medium (usually coaxial cable) that has a large bandwidth, greater than that of a voice-grade channel.

wireless - the use of radio transmitters to send alarm device information through the protected premises to a wireless receiver connected to a DMP Command Processor panel.

20.3.22 Z

zone - a separate circuit or branch of a security system usually for the purpose of isolating and/or identifying alarms or trouble in a system. Multiple zones are typically assigned to an area so that all of their protection devices combined provide for the complete protection of the premises.

zone reports - the message transmitted to the central station when a zone is in an alarm or a trouble condition.

zone retard - a zone programming option that allows you to assign a retard delay time during which a shorted zone does not initiate an alarm. The retard functions only in zone short conditions and the zone must remain shorted for the full length of the retard delay before the panel recognizes its condition.

zone retard delay time - a programmable delay time that can be assigned to fire, supervisory, auxiliary one, and auxiliary two type zones. The zone retard delay can be programmed from one to 250 second increments. See also zone retard.

zoned systems - identifies the zone area or circuit in which an alarm signal originates. Most modern burglar alarm systems can signal this zone information to the central station alarm company.