REMOTE *LINK*

Table of Contents

Part 1. Getting Started with Remote Link

1. Welcome to Remote Link

Remote Link offers an interface that is simple to navigate and provides easy access to the information you need.

Help File Navigation Menu

- Select the Contents tab for the Table of Contents.
- Select the Search tab to search keywords.

Remote Link software

- Select File and then Close Panel to close the account file and all the windows you currently have open.
- Select File and then Exit to close all windows you currently have open, disconnect from connected panels, and to exit Remote Link.
- Select Window to switch between the windows you have open in Remote Link or to organize them the way you want view them. You can also switch between windows within Remote Link by holding down Ctrl and pressing Tab.
- Select Apply to apply all the changes you have made in a window when creating or editing information in Remote Link.
- Select OK to save any changes you have made in a window and to close the window.
- Press F1 on your keyboard to access contextual help specific to the field you are currently active in.

Version

This help file is current for 1.92.

2. Copyright Statement

3. Related Documentation

Before using Remote Link, you should read and be familiar with the required panel documents.

There are programming and installation guides for each DMP control panel family that fully details the various programming options and panel operation. Visit our document library at dmp.com/guides.

All discontinued product documents are located on dmp.com/discontinued_literature. There are also programming and installation guides for the hardware components you can use to connect to alarm panels and to take full advantage of optional features.You can also refer to the manuals for any other equipment that is being used as part of the system. For a complete list of manuals, or to order a manual, contact DMP Customer Service or your regional DMP Sales Representative.

You may also visit our document library at the DMP website.

4. Computer Requirements

Before installing Remote Link, make sure that your computer hardware meets these minimum specifications listed in the table below. You need to have Administrator Authority or select 'Run as Administrator' to install Remote Link software.

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

Additional Requirements

- 800 x 600 or higher resolution monitor
- CD-ROM drive
- One available COM port if connecting to an SCS-1 or SCS-1R, SCS-105, or direct connecting to a panel. Two available Com ports if using the pass-through feature.

Using a Virtual Environment

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

4.1. Installing on Windows Vista or Windows 7

This section outlines specific steps to install and use Link on Windows Vista or Windows 7.

Operating System Privileges

The two types of Operating System user accounts referenced in this section are administrator and standard user accounts. These types of accounts have different privileges that allow or restrict the functions a user can perform.

From the Windows 7 documentation: "Standard account users can use most software and change system settings that do not affect other users or the security of the computer. Administrators have complete access to the computer and can make any desired changes. Based on notification settings, administrators may be asked to provide their password or confirmation before making changes that affect other users."

Link Operator Privileges

A Link operator is an individual that interacts with Link to perform a task. Operators may use Link daily or on an as-needed basis. However, all operators must log into Link before most tasks can be performed. Link allows privileges to be granted and/or removed to operator accounts. The privileges are managed in the System >> Operator Configuration screen. The two types of Link operators are administrators and standard operators. A Link administrator has Administrator special permissions and a standard operator does not.

Roles

There are three roles discussed in this section. Note: An individual may serve more than one role for an organization.

- Workstation Administrator: Has administrator access to the workstation operating system.
- Link Administrator: Has limited operating system privileges and administrator operator privileges within the Link application. This also applies to Link Server administrators.
- Link Operator: Has limited operating system privileges and may also have limited Link operator privileges.

The remainder of this section will assume a 'typical' organizational structure and Link configuration. This is defined as:

- There are one or more Workstation Administrators who perform maintenance of the workstations. Workstation Administrators only interact with Link for installation, maintenance and decommission.

- There is at least one Link Administrator who performs operator management tasks within Link. The Link Administrator interacts with Link on an as-needed basis.
- There are one or more Link Operators who use Link on a daily basis. Link Operators cannot perform Link installation, maintenance or management tasks.

Installing

A Workstation Administrator must perform installation of Remote Link and Link Server. A Workstation Administrator must also perform any version upgrades to Remote Link and Link Server. Any Link modules (e.g. Account Groups) should be activated at the time of installation by the Workstation Administrator.

Registry Keys

Once Remote Link and all modules are installed, the Workstation Administrator should give Link Administrators Full Control access to modify the DMP key shown and its sub-keys. A Link Operator does not require any additional registry privileges.

The primary registry key that Link uses to store application data is:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Digital Monitoring Products\
```

Database

This section discusses Database setup for Remote Link. For information on configuring a Link Server database, refer to the Link Server section of this document.

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 will allow 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.

Link Server

This section discusses information specific to 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.

DBISAM Database Server

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 start automatically 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 must be able to establish a TCP/IP connection to the DBISAM Database Server address and port.

5. Safeguarding Your Remote Link Database

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

Location

You can find the location of the Remote Link database by selecting System >> Configure >> Remote Link to open the Remote Link Configuration window. Select the Database tab near the top of the window. The Database Location field will display the path to your database.

If you would like to store your Remote Link database in a different location than the default folder, enter the location that you prefer for your Remote Link database in the Database Location field before setting up any accounts.

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, you will receive 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 just assigned and ignores the previous database. This means you will not have access to any previous account information and configurations settings from the previously existing Remote Link database.

Note: If you are using Remote Link on a computer connected to a network, run Remote Link from your local hard drive, not from a network drive. Remote Link accesses the database more quickly if the database is located on the local computer rather than a network drive. Only one computer at a time may use a Remote Link database.

6. Log ON/OFF

Before using Remote Link, you must log into the program with a user name and password. When you open Remote Link, the Remote Link Login window automatically displays. You may log off and then log in as another user any time the program is open.

Default Log In

User Name: `new`

Password: `new`

7.1 Quick Connect

7.1. Connecting to a Panel through Cell

Follow the steps below to configure Remote Link to connect to a panel through a cellular communication.

1. Select File and select Panel Information.
2. Select a panel.
3. In the Connection Information box, select Cellular from the drop-down menu in the Type field.
4. Enter the phone number or SIM/MEID number for the cellular communication.
5. Select OK to apply these changes.

Retrieve the Phone number or SIM/MEID number

SecureCom Wireless users

1. Select System and then select SecureCom Wireless Activations. This shows a list of all SecureCom activations.
2. Copy the phone number or SIM/MEID number and paste it into the phone number box of the Connection Information box.

Non-SecureCom Wireless users

Enter the SIM phone number into the phone number box of the Connection Information box.

7.2. Connecting to a Panel through Dial-up

Follow the steps below to configure Remote Link to connect to a panel through an SCS-1, SCS-1R, SCS-VR or SCS-105 Receiver using a dial-up connection.

1. Select File and select Panel Information.
2. Select a panel.
3. In the Connection Information box, select SCS-1 / SCS-105 from the drop-down menu in the Type field.
4. Enter the Remote Key.
5. Enter the phone number of the panel.
6. Select Yes from the drop-down menu in the Dial field.

Note:You only need to complete the prior steps one time. On further connections simply select the panel and then Connect as explained below.

7. After you have entered all the Connection Information, select OK to open the panel.
8. Select Panel and select Connect.
9. Select Connect to connect to the panel.

7.3. Connecting Directly to a Panel

Connect directly to a panel with a 462N Interface Card or XR500 Series Serial Port. Follow the steps below.

1. Select File and select Panel Information.
2. Select a panel.
3. In the Connection Information box, select Direct from the drop-down menu in the Type field.
4. Enter the COM Port to which the panel is connected.
5. Enter the Baud Rate of the COM Port.

Note: You only need to complete the prior steps one time. On further connections, simply select the panel and then Connect as explained below.

6. After you have entered all the Connection Information, select OK to open the panel.
7. Select Panel and select Connect.
8. Select Connect to connect to the panel.

Part 1. Registering and Activating Modules

1. Entering a Module Serial Number

Enter the module serial number in Remote Link to begin the activation process. Each module comes with a manual and certificate containing the serial number needed for activation.

Modules

Alarm Monitoring, Command Center, and Advanced Reporting modules

Enter a Module Serial Number

1. Run Remote Link as administrator.
2. Navigate to Help >> Registration.
3. Select Add.
4. Type the module's serial number as it appears on the certificate.
5. Select OK. A message box will appear reminding you to activate the module within 7 days.

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.

If you have purchased additional modules to add on to Remote Link, you can enter and view their serial numbers under Help >> Registration. The serial numbers must be kept for proper activation of the modules. If you have installed additional modules, enter the serial numbers immediately to ensure a quick activation.

2. Activating a Module

Within the 7-day grace period, contact DMP Customer Service to activate the module.

If activating the SecureCom Wireless service module, contact SecureCom Customer Service for activation.

Modules

Alarm Monitoring, Command Center, Advanced Reporting, Account Groups, and SecureCom Wireless modules

Activate the Module

1. Navigate to Help >> Registration. If your module is not listed, the serial number has not been entered and the module has not been registered.
2. Select the module you wish to activate from the list of modules.
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. With the serial number and the public key available to you, call DMP Customer Service to have them generate an activation code.
5. Select OK in the message box to enter the activation code from DMP Customer Service.
6. Select Activate. Now your module is registered, activated, and ready to use.

Change the Account Level

To change the Account Level, upgrade the number of subscriber accounts allowed. Select the module from the list and select Change. You will then be prompted to follow the same steps as registering and activating a new module.

3. Upgrading an Account Level

Modules

Alarm Monitoring, Command Center, or Advanced Reporting module

Upgrade the Account Level (the maximum number of allowable subscriber accounts)

1. Ensure you have the new CD-ROM and Certificate.
2. Navigate to Help >> Registration.
3. Select the module that you are upgrading.
4. Select Change. Enter the new serial number for the module from the upgrade certificate.
5. Follow the instructions to activate the module with the new level of accounts.

4. Removing a Module

Remove a module from Remote Link.

Note: You must have Administrator Authority to remove modules.

Modules

Alarm Monitoring, Command Center, and Advanced Reporting modules

Remove a Module

1. Navigate to Help >> Registration.
2. Select the module that you wish to remove from the list in the Registration window.
3. Select Remove.
4. A pop-up window displays asking if you are sure you want to remove the module. Select Yes to remove the module.
5. A window says, "Module Successfully Removed." Select OK.
6. Restart the program for the changes to take effect.

5. SecureCom Wireless Activations

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

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.

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 is required for each installation of Remote Link. Contact SecureCom Customer Service for activation of additional installations of Remote Link.

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 Register.
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. If you wish to continue registering and activating the module, follow the steps described in How to Activate the Module.

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.

1. Select System and then select Securecom Wireless Activations.
2. Select 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 and then selecting Communication.
3. Select the path programmed for cell communication and select Activate.
4. When the Activate SIM/MEID screen displays, enter all of the 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 either 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 MEID 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. Plans available include:

Using Model 380-200 SIM/MEID	SIM/ MEID	Data Included
Plan 203: Back-up alarm signal only	Level 200	0 KB
Plan 205: Back-up or primary alarm signal only, provides for weekly test	Level 200	50 KB

Using Model 380-400 or 380-400T SIM/MEID	SIM/ MEID	Data Included
Backup: Backup communication for use with panels with network, dialer, or Wi-Fi primary. Systems using the Backup rate plan that are programmed with cell primary will be automatically changed to the panel rate plan. The backup rate plan is date constrained, the XR150/XR350/XR550 Series plan is not. The modem must have been activated for the first time on or after January 15, 2016. The XR150/XR350/XR550 Series rate plan is hardware constrained to XR150/XR350/XR550 Series panels.	Level 400	50 KB
Plan 406: Primary path with a daily test	Level 400	50 KB
Plan 408: Primary path with hourly check-in and O/C reports for up to 4 areas.	Level 400	200 KB
Plan 410: Primary path with an hourly test and O/C reports for up to 8 areas.	Level 400	300 KB
Plan 416: UL Primary Fire path with a 5 minute check-in and O/C reports for up to 8 areas (NFPA 2010).	Level 400	1000 KB
Plan 425: Primary path provides for 3 minute check-in OR 4 minute check-in with O/C reports for up to 16 areas.	Level 400	2000 KB
XT30/XT50 Series, XTLplus/XTLtouch Series: Flat rate, no overages, includes daily test, O/C reports	Level 400	N/A
XR150/XR350/XR550 Series: Flat rate, no overages, includes daily test, O/C reports	Level 400	N/A
CellComSL/DualCom: Flat rate, no overages, includes daily test, O/C reports	Level 400	N/A

- Status: This displays the current status of the SIM/MEID. To update the status of the current SIM/MEID, select 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. Plans available include:

Text Plans Available	SIM/MEID	Available Panels
None: Messaging is not included	Level 400	• XT30/XT50 Series • XTLplus/XTLtouch Series • XR150/XR350/XR550 Series • XTLC Series • XR100/XR500 Series • CellComSL Series • DualCom Series
SMS100: 100 Messages per month	Level 400	• XT30/XT50 Series • XTLplus/XTLtouch Series • XR150/XR350/XR550 Series • XTLC Series • XR100/XR500 Series • CellComSL Series • DualCom Series
SMS200: 200 Messages per month	Level 400	• XT30/XT50 Series • XTLplus/XTLtouch Series • XR150/XR350/XR550 Series • XTLC Series • XR100/XR500 Series • CellComSL Series • DualCom Series
MyAccess: Unlimited messages	Level 400	• XT30/XT50 Series • XTLplus/XTLtouch Series • XR150/XR350/XR550 Series • XTLC Series • XR100/XR500 Series • CellComSL Series • DualCom Series

Deactivate the SIM/MEID

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

Transfer the SIM/MEID

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.

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 will notify you. Select Next when you've made your selections.

Remote Link displays the Transfer Summary window. If the current and new information looks correct, select Finish. When the transfer completes, the Success window displays. Select Done to close the Transfer SIM or MEID window.

Part 1. Remote Link Management

1.1 Configuring Remote Link

1.1. Receiver Tab

The programming options in the Remote Link Configuration window are available on the following tabs: Receiver, Modem, Database, Other, Network, Modules, and Custom Fields.

Access Receiver Programming Options

1. Navigate to System >> Configure >> Remote Link.
2. Select the Receiver tab.

1.1.1. Current Receiver

You can view receiver models and select one to configure by selecting the Model drop-down box.

1.1.2. Communication Options

COM Port

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. Be careful to 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.

Baud Rate

Set your baud rate to the same setting as your receiver. The default setting is 9600 baud. If you are using an SCS-1 Receiver Version 812 or SCS-1R to access your alarm panels, you may set your baud rate to 19200. The baud rate set here must also be set in the SCS-1 Receiver. See LT-0065 for more information about configuring

the SCS-1 Receiver or LT-0717 for the SCS-1R Receiver. If you are using an SCS-105 or SCS-1R/SCS-150 Receiver to access your alarm panels, set your baud rate to 9600.

Dial Out Line

This number refers to which line card that your current receiver will use to dial out.

- SCS-1 or SCS-1R (using SCS-1062): Select 1-5
- SCS-1R/150 (using SCS-150): Select 1-8
- SCS-105: Set this value to 1

Tone Dial

Check this box if you wish to tone dial. Leave this box empty for pulse dial.

Note: The SCS-1 or SCS-1R will always pulse dial, regardless of this setting.

1.1.3. Receiver General Options

Areas

Select which reporting format Remote Link will use to communicate with panels. Bin: 2-character hexadecimal mode. Use this mode with SCS-105 Receivers. Dec: 2-character decimal mode. Select this mode if the SCS-1 or SCS-1R Receiver has been programmed to require Dec mode.

Start Character

When the SCS-1 or SCS-1R Receiver has a line configured to attach to a data network, set the Start Character to the same as the character programmed in the SCS-1 LSU Host Configuration. The default setting is STX. Refer to your SCS-1 Receiver Installation and User's Guide (LT-0065) or SCS-1R Receiver Installation Guide (LT-0717).

None

Use this option when the SCS-1 or SCS-1R Receiver is not connected to a data network.

STX

Use this option when the SCS-1 or SCS-1R Receiver is configured to use STX.

Other

If the SCS-1 or SCS-1R Receiver is set to a different Start Character than the available options, select Other and enter that Start Character in the field immediately to the right of the Start Character menu.

CRC

Check this box if the SCS-1 or SCS-1R Receiver CRC option in the LSU Host Options is set to YES.

Sequence Numbers

Check this box if the Sequence Numbers option in the SCS-1 or SCS-1R Receiver LSU Host Setup is set to YES.

1.1.4. Receiver Lengths

Line

This field designates how many digits the receiver will use for the line number used by the panel to communicate a message.

- SCS-1 or SCS-1R Receivers: Select 1 to allow single-digit numbers or 2 to allow two-digit line numbers. Select 0 to allow no line numbers.
- SCS-105 Receivers: Always select 0 for SCS-105 Single Line Receivers.

Zone

This field determines how many digits may be assigned to report a zone number. This number should correlate with the number of digits of the zones that report to the panel. For example, the XR200 panel has zones 1 through 299. So you would want to set this to 3 to allow all 299 zones to report.

- SCS-1 or SCS-1R Receivers: This number must match the zone number programmed in the Host setup programming on the receiver.
- SCS-105 Receivers: Use 3 for SCS-105 Single Line Receivers.

User

Select the number of digits used to report a user number. Select 3 to allow 999 users.

- SCS-1 or SCS-1R Receivers: This number must match the User number programmed in the Host setup programming on the receiver.
- SCS-105 Receivers: Use 3 for SCS-105 Single Line Receivers.

1.1.5. Default Receiver Number

The Default Receiver field allows you to assign a receiver number for Host/Net Monitoring. Enter a number from 1 to 9 that represents Host/Net Monitoring. This is to help you distinguish between alarms received in the Host mode and those received from another type of receiver, such as an SCS-1 or SCS-1R Receiver. You must have an additional module to use. If you do not enter a number in this field, the receiver number for host monitored accounts will default to 1 (one).

1.2. Modem Tab

Use the Modem tab to configure Remote Link when connecting to an XR550 Series for programming the panel at 2400 baud through the panel dialer. This allows you to connect to the panel using a standard computer modem.

1.2.1. Communication Options

COM Port

Select the COM Port that is connected to your modem. Use the Modem tab to configure Remote Link to connect to a panel that has a DMP Fast Modem installed or when connecting to an XR150/XR550 Series panel for programming at 2400 baud through the panel dialer. This allows you to connect to the panel with a standard computer modem.

Note: These are for the local computer modem.

Baud Rate

Set the baud rate for Remote Link to communicate with the computer modem. Default setting is 9600.

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 ON/OFF, also known as software flow control. If neither setting operates correctly, select None. For more information see your modem documentation.

Tone Dial

Check this box if you wish to tone dial. Leave this box empty for pulse dial.

1.2.2. General Options

Dial Time Out

Enter the length of time Remote Link will wait for the XR150/XR550 Series panel to pick up. Enter a range from 1 to 255 seconds. The default is 60 seconds.

Modem Initialization String

If an initialization string is required for the modem communicating to the panel, enter the setup string here. The string can be up to 32 characters long.

Special Initialization String

The special initialization string required to ensure the modem communicates consistently at a slower baud rate is entered here. The string can be up to 32 characters long.

Note: Only one initialization string can be used. Select the correct one for your operation. See Panel Information.

1.3. Database Tab

The settings in the Database tab allow 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 Remote Link database, as well as merge another Remote Link database into the existing or import your Remote Access database into Remote Link. You may move your Remote Link 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 the possible loss of valuable data.

1.3.1. General Options

Computer Hard Drive

Enter the path to the Remote Link database location on the computer or network hard drive. If you would like to

store your Remote Link database in a different location than the default folder, type 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. Refer to the Link Server Installation Sheet (LT-0837).

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 and enter the information using the following format:

- server: `xxx.xxx.xxx.xxx:ppppp`
- `x` = IP Address
- `p` = Port Number

Note: Standard Remote Link operation supports database access for up to three computers as long as only one computer at a time performs extensive database access operations such as uploading or downloading information from a panel. If more computers or more extensive 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 type the new location of the database into the field. If you change the location listed in the Database Location field without first 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 just assigned and ignores the previous database. This means that Remote Link does not have access to any previous account information and configurations settings from the previously existing Remote Access database.

Note: If you are using Windows 2000 or XP, only users with administrative privileges in Windows can relocate the database. If a user without administrative privileges attempts to move the database, Remote Link does not save the attempted relocation.

If Remote Link does not start up correctly, one cause could be an invalid database location. Use the command line option "/dblocation" to set the path to the database. Go to Start >> Run and type `c:\Link\Link.exe /dblocation LOCATION`.

In place of LOCATION, type:

- "`c:\database path\`" for a local or shared file server database
- server:`192.168.0.111.12005` for a server based database
- where `192.168.0.111` is the IP Address where the server database is located

1.3.2. Backup your Database

As a safety measure, it is always wise to create a backup of your database. Remote Link provides you with the option to backup your database on a regular basis. A reminder will appear to remind you to backup your database.

Note: 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.

Backup Location

1. Select the Database tab.

2. Select Options to display the Backup Options window.
3. Enter the backup location where you want the backup database to reside. For example, C:\Backup tells Remote Link to place the backup database in the backup folder on the C drive of your computer.
4. If the database resides on a network server, check with your System Administrator. The backup function cannot be performed for a database that resides on a server. You may choose to have Remote Link remind you when it is time to backup your database by selecting the "Remind me to backup after" checkbox.
5. Enter the number of days you would like between backup reminders.
6. Select OK when you are finished.

You may also select Backup to run the backup immediately or at any time to run a non-scheduled backup. When it is time for a scheduled backup, a pop-up window will appear. If you select Yes, the pop-up window closes and opens the Backup Options dialog box. Select Backup to perform the scheduled backup. If you select No, another pop-up window will appear the next time you log into Remote Link.

Note: Only the System Administrator can backup the Remote Link Database. If an operator with a authority level lower is logged on when a backup reminder message is displayed, the operator is prompted to contact the System Administrator.

1.3.3. Merge Database

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

Note: The Merge option is not available if using Remote Link with the SQL Server module.

How to Merge Database

1. Select Merge in the Merge Database section.
2. In the Merge Database window, enter the path to another Remote Link database to merge with the existing database. All of the accounts from the chosen database are copied and merged into the 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.

Caution: 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. After following the instructions above, select Merge to complete the merge operation.

1.3.4. Purge Options

Purge allows you to remove Remote Link activity from the database. When the database resides on a remote network server, check with your System Administrator. The Purge operation cannot be performed for a database that resides on a remote network server.

Start Date

Enter the first date that you would like to purge events.

End Date

Enter the last date that you would like to purge events.

Activity

Select Activity to remove the Remote Link activity.

Acknowledged Messages

Select Acknowledged Messages to remove all acknowledged Alarm List messages. You can still print these messages after you have purged them.

Events

(Must have an additional module to use) Selecting Events purges events such as all alarms, troubles, opening/closing events, and door access events. After these events are purged, you cannot print these reports.

Note: You may purge Activity, Acknowledged Messages, and Events by selecting all three checkboxes. If no checkbox is selected, Remote Link will not remove anything from its database.

If needed for reference, print the Activity, Acknowledged Messages, or Events lists prior to performing the purge process. If the related window is open with Activity, Acknowledged Messages, or Events displaying prior to starting the purge process, the list of Activity, Acknowledged Messages, or Events continue to display. Close and then reopen the specific List window to remove the purged items from the display.

Select Purge to remove all activity and/or events from the Remote Link database for the selected dates.

1.3.5. Restoring from Backup

The Restore from Backup window automatically appears if your database is corrupt and you need to restore it. To restore from a backup, you must have a backup file already made. Be sure to backup your Remote Link database frequently. When using 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.

Restore from File

Enter the file from which you wish to restore. Press the button to the right of the field to browse for the most recent backup file.

Restore Location

Enter the location in which you want the backup to be restored.

The Restore Location will typically be where your Remote Link database currently resides. Press the Restore button to restore your database from the selected backup file. If the Restore from Backup window does not automatically open, close Remote Link and follow the directions below.

1. Go to Start >> Programs >> Remote Link.

2. Select Restore Database.

1.3.6. Repairing Your Database

It is possible your Remote Link account database 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. If you believe your Remote Link database is damaged or corrupt, close Remote Link and follow the directions below.

1. Go to Start >> Programs >> Remote Link.

2. Select Repair Database.

You will then see an information window listing off the database files that are being repaired. When the database is repaired, the Log On / Off window will open.

Note: When using 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.

1.4.1 Other Tab

1.4.1. General Options

Time Zone

Under the Other tab, select the appropriate time zone where your Remote Link computer is located from the drop-down menu. If your time zone is not listed, enter a time zone value according to the table of time zones.

Enable Debug Logging

Select the Enable Debug Logging to allow all communication between the panel, receiver, and Remote Link to be saved in the debug table for diagnostic purposes. Deselect the box to disable this function. When the box is deselected, you will not be able to view communication in the diagnostics screen. By default, Enable Debug Logging is selected.

Enable Alarm/Event Monitoring

Select Enable Alarm/Event Monitoring to allow Remote Link to display panel alarms and system event messages in the Alarm List. Deselect this option when Remote Link is used for programming purposes with a shared database without displaying panel messages. By default, Enable Alarm/Event Monitoring is checked and should be checked when using the Alarm/Event Monitoring mode.

Logging Threshold

Select the type of issue to log into the Remote Link error log file. By default, Logging Threshold is set to Warning. All messages with a severity equal to or greater than the threshold setting will be logged.

Inactive User Application Timeout Feature

By default the Inactivity feature is disabled. Select the checkbox to 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 or No to extend their Remote Link Session.

Debug

Detailed information that does not indicate an error, similar to communication strings. This setting greatly increases the size of the log file.

Information

General information detail about program operations.

Warning

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

An error that requires operator action to recover or restore normal operation such as an invalid COM Port selection for the receiver.

Critical

An error that caused Remote Link to stop responding such as an Access Violation or database corruption.

1.4.2. Archive

Enable Auto Account Archive

Select this option to allow panel account programming to be automatically archived (saved separately) when connecting to a panel with programming different than the programming currently on file. Default is deselected. To archive panel account programming manually, select File >> Panel Information.

Max Per Account

Select the maximum number of panel programming archive versions allowed to be stored per account. Allowed range is 1 to 20 archives. Default is 5.

1.4.3. Pass Through Options

Mode

When Remote Link is in the Pass Through mode, standard panel reports will be sent to and acknowledged from a host computer. Select the appropriate setting.

None

Select this option if you are not using Pass Through mode to relay signals to automation software.

Pass Through

Select this option to pass reports through the Remote Link computer to a host automation computer.

Outgoing COM Port

Select the COM port that Remote Link will use to communicate with your host automation computer.

Baud Rate

Set the baud rate to 9600 unless your automation software requires a different setting.

1.4.4. Admin Reader

When using a 1301 Series proximity reader to enter User Codes from proximity credentials, configure the COM Port and Baud Rate here. Refer to the 1301 Series Installation Sheet (LT-0619) as needed.

Note: The proximity reader USB connects to a standard USB port on a PC and operates as a virtual COM port requiring a special driver from the following web site.

http://www.ftdichip.com/Drivers/VCP.htm

When using non-DMP proximity credentials, download and adjust the Configuration Utility values as needed.

http://www.rfideas.com/Software/

COM Port

Select the virtual COM Port to which the proximity reader is connected.

Baud Rate

Select the baud rate at which the Remote Link communicates with the proximity reader. The default Baud Rate is 9600.

Reader Model

Select the connection used for the proximity reader.

Serial

Select this option when using a Reader connected to a serial port.

USB 6081

Select this option when using a Reader connected to the USB port.

Max Code Length

Select the number of characters, 5-10, for the user code.

Wiegand Length

When using a custom card, enter the total number of bits to be received in Wiegand code including parity bits. Enter a number between 0-255 to equal the number of bits. Default is 26 bits.

User Code Position

Enter the user code start bit position. Enter a number between 0-255. Default is 9.

User Code Length

Enter the number of user code bits. Enter a number between 16-32. The default is the DMP value of 17 which is

pre-programmed.

Set Card Defaults

Select to set the proximity reader fields based on the current value of the Max Code Length.

Test

Select the Test button to ensure that you have entered the proper COM Port and Baud Rate.

1.5.1 Network Tab

1.5.1. Network Options

TCP Trap

The options available are used to configure the TCP communication connection to the SCS-101 version 103 or higher or SCS-104 installed in the SCS-1 or SCS-1R receiver. This allows network panels with a dynamic IP address to be trapped for Remote Link upload/download.

TCP Trap Enabled

Check this box to enable TCP Trapping.

Programming App. Address

Enter the IP address of the Remote Link computer used to program panels. If the Remote Link computer 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.

Programming App. Port

This is the port used by the Remote Link computer to make the connection to the network panel using TCP protocol. The default value is 2002.

Trap Server Address

Enter the IP address of the SCS-101 or SCS-104 installed in the SCS-1 or SCS-1R receiver. This address is used by Remote Link to send trap messages.

Trap Server Port

This is the port used by Remote Link to communicate with the SCS-101 or SCS-104 installed in the SCS-1 or SCS-1R.

Auto Send Traps

This enables Remote Link to resend the trap command continuously to the SCS-1R receive. This prevents the receiver from discarding the trap after a four-hour period. The trap is resent based on the number of seconds programmed into the Auto Send Delay. Default is disabled.

Auto Send Delay

If Auto Send Traps is enabled, enter the number of seconds that Remote Link waits between resetting traps. Default is 180 seconds. Minimum is 30 seconds.

Customer

Choose a customer from the drop-down list. Traps will be sent only to the accounts of the customer selected.

SOCKS Proxy

A SOCKS proxy server is a server-based computer application used to transfer data between client computers using a set of filtering rules for enhanced security. SOCKS is an abbreviation for "sockets," which are connection points on the Internet. The SOCKS Internet protocol serves to keep client machines safe and anonymous for security purposes and to help speed up the access of routinely accessed data, especially when used in conjunction with a firewall.

How SOCKS works

SOCKS works as a client/server. A users' workstation must have a SOCKS client 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 will initiate a connection to a SOCKS server. The SOCKS protocol allows authentication and logging of the connection requests. The SOCKS server then acts as the IP Client for the connection request. This means that the external server is only aware of the SOCKS Server (the proxy).

SOCKS has the following key features:

- provides authentication for protocols that cannot be authenticated
- by passes default routing in the internal network

SOCKS requirements:

- the client program must have a SOCKS client capability
- the client operating system must have SOCKS client capability
- you must run and maintain a SOCKS server
- Version: Select the SOCKS Proxy version from the pull down menu.
- Host: Enter the IP address of the SCS-101 or SCS-104 installed in the SCS-1 or SCS-1R receiver.
- Port: Enter the port through which you will connect to the panel. number 1 to 65535.

Cellular Network

This enables a cellular backup connection for Remote Link.

Direct Cell: Select the checkbox to enable. Remote Link communicates with the panel through a cellular connection using a SIM/MEID card.

Note: See Backup Connection Information for additional setup information.

1.6.1 Modules Tab

1.6.1. Monitoring Options

Host Monitoring (Must have an additional module to use)

- Host Monitoring: Select Host Monitoring Enabled to allow the module to receive signals from network enabled panels.
- 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 (Must have an additional module to use)

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

Command Center (Must have an additional module to use)

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

Note: The Arm/Disarm status of the panel can be tracked with XR150/XR350/XR550 Series, XR150INT/ XR550INT Series, XT30/XT50 Series, XT30INT/XT50INT Series, XTLplus/XTLtouch Series, CellCom Series, and DualCom Series.

1.7.1 Custom Fields Tab

1.7.1. Custom Fields

Custom Fields

The Custom Fields tab is used to rename field titles and maintain selections in drop down lists located on the Panel Information screen and the User Codes screen.

Edit List

The Edit List button allows the list of acceptable selections to be maintained by an Administrator. Select the field to change and select Edit List.

Table and Field

These indicate the database location. These are preloaded and cannot be edited.

Caption

This is the field title that is displayed on the Panel Information and User Codes screens. Double-click in the Caption column to change the title.

Limit To List and Admin Add

These two settings work together to determine how entries, that use a drop down list of items, will be handled.

The following table describes the effect of the possible combinations:

Limit To List	Admin Add	Description
unselected	unselected	All operators can enter text. Entries are not added to the drop down list, but the values entered for the panel are stored in the database.
unselected	selected	All operators can add to the list. A prompt appears to confirm addition of the item to the drop down list.
selected	unselected	Selections are strictly limited to items in the drop down list. Additions can only be made from the Remote Link Configuration screen.
selected	selected	Entries for non-Administrative operators are limited to items in the drop down list. Administrators can enter text not in the drop down list.

2. Operator Configuration

The programming options in the Remote Link Operator Configuration window are available on three tabs, Operator Information, Panel Programming, and User and Status Programming. To give users authority to log in to Remote Link, select System and select Operator Configuration.

2.1. Operator Information Tab

Classic Log In

Log In Information

To authorize a new operator to log in to Remote Link, select New at the bottom left corner of the window. In the Login Information fields, enter a Login and Password for the new user. At Re-enter Password retype the same password to verify. Each login ID and password may have up to 32 characters.

Personal Information

Enter the operator's last and first name.

Account Access

To authorize the operator to access all accounts, select All. To restrict the operator to certain accounts, select Restrict and select the . . . button. In the Select Accounts window, place a checkmark next to the accounts the operator is authorized to access.

Note: The Account Access restrict option does not prevent an operator from using the trap function to send and/or retrieve changes made by other operators. When the Account Groups module is enabled, the Account Access restrict option does not prevent an operator from adding users and the display only lists accounts the operator is authorized to access.

User Restrictions

To limit the operator to view only access. This operator will not have the ability to program, change or add panel information. Select the View Only option.

Administrator

Check the Administrator box to provide complete authority to perform administrative functions within Remote Link, such as adding new operators and configuring Remote Link.

Note: At least one operator must always have Administrator level authority. Only users with Administrator level authority may add or modify authorities.

Remote Update

Check the Remote Update box to authorize the operator to perform remote updates from the System >> Remote Update, Panel >> Remote Update, or Trap >> Options >> Remote Update windows. When Remote Update is not checked, the windows are grayed out and the operator cannot perform the remote update operation.

Import and Export

Check the Allow Import and/or Export box to authorize the operator to import and/or export panel account information and programming. See File >> Import and Export >> Import Accounts or File >> Import and Export >> Export Accounts.

Cellular Activations

Check the box to authorize the operator to activate, deactivate, update or assign SecureCom Wireless cellular SIM cards to active control panel accounts.

Advanced Filtering

Check the box to authorize the operator to use the advanced filtering option.

Allow Trap

Check the box to authorize the operator to create, set, send, and retrieve traps. This must be enabled for the trap options in the Remote Link Panel menu to be accessible to the user.

Single Sign-On Authentication/Windows Credentials Authentication

Single Sign-On and Windows Credentials Authentications allows a Remote Link operator to be associated with their Windows user account. When launched, Remote Link matches the Windows user currently logged in to an operator in the Remote Link database. The Single Sign-On feature eliminates the need to log into Remote Link--the operating system has already authenticated the user. However Windows Credentials Authentication feature is more secure than the Single Sign-On where users leave their computers "unlocked" when they step away. The Windows Credential feature prompts the user for their (Windows) password when they launch the application. If a Windows user account fails to match a Remote Link operator an Application Access Denied dialog box displays and the user is denied access to Remote Link.

Remote Link will default to using Classic Login when upgrading software from previous versions that did not support Single Sign-On or when creating new databases.

Note: Administrator level authority is required to add Single Sign-On users or modify authorities.

To Enable Single Sign-On or Windows Credentials:

1. From the main Remote Link screen, select System >> Operator Information to display the Operator Configuration window.
2. Select Authentication… at the bottom center of the screen. The Operator Authentication Method dialog displays detailing the three types of operator authentication.
3. Select Next to continue.
4. The Select Authentication Method dialog box displays with Classic Login, Single Sign-On and Windows Credentials checkboxes. Select Single Sign-On or Windows Credentials and select Next to continue.
5. The Single Sign-On or Windows Credentials dialog box displays with the Remote Link administrator account and the Windows user account to be mapped. Select Finish to complete authorization.

Once enabled, the Login, Password, and Re-enter Password controls on the Operator Configuration screen in Remote Link are replaced with Single Sign-On Information containing:

- Windows User Account
- Operator's Name (User Name)

Select Edit to display the Windows Select User window. From the Select User window you may select:

- Object Types
- Locations
- Check Names

Note: You will need to associate a Windows user account to each of the existing Remote Link operators. Until all operators listed in Operator Configuration are set up to use the Single Sign-On or Windows Credential options, those operators will effectively be disabled.

Object Types

The Windows User Object Type is automatically displayed.

Locations

Select Locations to select the location of the Windows user account. You may select the local computer or a Windows directory of users on the network. When the local computer is selected, access is limited to the

selected computer. If the same operator logs in to a different computer, access will be denied.

Check Names

Enter a user name in the field and select Check Names to search the directories for matching user names.

Advanced

Select Advanced to display the expanded search feature.

To add or remove available search criteria, select Columns.

Once the desired search columns have been selected, you may enter key words and other information in the Common Queries fields.

Additional Information

Personal Information

Enter the operator's last and first name.

Account Access

To authorize the operator to access all accounts, select All. To restrict the operator to certain accounts, select Restrict and select the . . . button. In the Select Accounts window, place a checkmark next to the accounts the operator is authorized to access.

User Restrictions

To limit the operator to view only access. This operator will not have the ability to program, change or add panel information. Select the View Only option.

Note: The Account Access restrict option does not prevent an operator from using the trap function to send and/or retrieve changes made by other operators. When the Account Groups module is enabled, the Account Access restrict option does not prevent an operator from adding users and the display only lists accounts the operator is authorized to access.

Special Permissions

Administrator

Check the Administrator box to provide complete authority to perform administrative functions within Remote Link, such as adding new operators and configuring Remote Link.

Note: Be sure at least one operator always has Administrator level authority. Only users with Administrator level authority may add or modify authorities.

Remote Update

Check the Remote Update box to authorize the operator to perform remote updates from the System >> Remote Update, Panel >> Remote Update, or Trap >> Options >> Remote Update windows. When Remote Update is not checked, the windows are grayed out and the operator cannot perform the remote update operation.

Import and Export

Check the Allow Import and/or Export box to authorize the operator to import and/or export panel account information and programming. See File >> Import and Export >> Import Accounts or File >> Import and Export >> Export Accounts.

Cellular Activations

Check the box to authorize the operator to activate, deactivate, update or assign SecureCom Wireless cellular SIM cards to active control panel accounts.

Advanced Filtering

Check the box to authorize the operator to use the advanced filtering option.

Allow Trap

Check the box to authorize the operator to create, set, send, and retrieve traps. This must be enabled for the trap options in the Remote Link Panel menu to be accessible to the user.

2.2. Panel Programming Tab

You may select the All button to select all options on the Panel Programming Tab. Select Clear to remove all options. Check each box to assign the operator authority to perform panel programming options. Each option refers to a menu option under Programming.

2.3. User and Status Programming Tab

You may select the All button to select all options on the User and Status Programming Tab. Select Clear to remove all options.

User Programming

Check each box to assign the operator authority to perform user programming options. Each option refers to a button in the System Status window accessed by selecting Program >> User Codes.

Panel Status

Check each box to assign the operator authority to perform system status commands. Each option refers to a button in the System Status window accessed by selecting Panel >> System Status.

Alarm List

Check the appropriate boxes for operators to have authority to acknowledge, remove, or disable alarms from the Alarm List Window. When upgrading from previous Remote Link versions the alarm authority options are automatically enabled.

2.4. Receiver Programming Tab

Each option refers to an SCS-150 programming window. Check each box to assign the operator authority to perform receiver programming options. You may select the All button to select all options on the Receiver

Programming Tab. Select Clear to remove all options.

3. Configuring 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 will only be displayed when the panel is open or when you are connected to a panel. For example, the Arm/Disarm button will not be displayed and enabled until you are connected to a panel. Also, toolbar buttons are not displayed if the panel does not support that feature.

Placing Buttons on the Toolbar

To customize your toolbar, open System >> Toolbar Configuration. The Toolbar Configuration window will then open. From the Available Menus box, select the menu option you would like to place on the toolbar. Then press the Add button.

Using the Arm/Disarm example, select the plus sign next to Command in the Available Menus box. Then select Arm/Disarm and press the Add button.

Arranging the Toolbar

The Toolbar box displays the menu options you have placed on the toolbar. To arrange the menu options on the toolbar, use the Move Up and Move Down buttons. You can also use the Separator button to add a separator to group common menu options, such as Panel Information and Connect.

If you would like to remove a menu option from the toolbar, select the option from the Toolbar list and press the Remove button.

Displaying the Toolbar

After you have placed the menu options in the Toolbar list, you may customize how you would like the toolbar to display. Check the Show Toolbar box to display the toolbar. You may show an image of the menu option by checking the Show Images box.

Select Show Caption to display the menu option name. If you show the images and the caption, you can select where you want the caption to display. To display the caption below the images, check the Show Caption Below Image box. If you do not check the Show Caption Below Image box, the caption will display to the right of the image.

4. Performing a Remote Batch Update

Performing a remote software update (flash update) allows you to quickly and conveniently update the software without making a trip to the site.

The following products can accept software updates from a remote location using Remote Link:

- SCS-101 version 102 or higher
- SCS-104
- XR150/XR350/XR550 Series
- XR150INT/XR550INT Series

- XT30/XT50 Series version 123 or higher firmware and Level M hardware with Network
- XT30INT/XT50INT Series
- XTLplus/XTLtouch Series
- XR500N/XR100N

Software updates are posted to DMP.com/Dealer_Direct. Follow the online directions to download the update.

Note: Save the update in a location on your computer hard drive you will remember.

Creating an Account for the Device to be Updated

To perform a remote update, you must first create an account for that device if one does not already exist. For example, to update an XR550 panel, create an account in the Panel Information window by selecting New. Select XR550 from the Model drop-down list in the New Panel window. Then enter the XR550 IP Address and IP Port in the Connection Information window.

The IP Port must be the same as the Upgrade Port programmed in the XR550. When performing a Remote Update on an SCS-101/SCS-104, the IP Port must be the same as the Telnet Port programmed in the SCS-101/ SCS-104. When programming an SCS-104, the IP Port must be the same as the Programming Port programmed in the SCS-104.

Note: If the network device being updated is behind a router, you must open a port for the remote update. Refer above for the default values for the port. Be sure that the proper port is opened in the router that corresponds with the port programmed in Remote Link.

Performing the Update

To perform a remote update, select System >> Remote Update from the drop-down menu. In the Remote Update window, use the browse button to find the software update file on your computer's hard drive. Remote Link will automatically search the database for the devices for which the software update applies and will display those devices in the Panels to Update portion of the window.

In the Devices to Update portion of the window, check the box next to the devices you wish to update. You may select All to select all devices and Clear to clear all devices.

After you have selected all of the devices you wish to update, select Update in the bottom left corner of the screen. As the update occurs, the Current and Overall Progress bars will inform of the progress of the update.

If any problems occur during the update, Remote Link will display this information in the Log box, and you must complete the update again.

Note: The Remote Update can also be performed as part of the Trapping operation.

5. Performing a Remote Update

Performing a remote software update (flash update) allows you to quickly and conveniently update the software without making a trip to the site.

The following products can accept software updates from a remote location using Remote Link:

- SCS-104
- XR150/XR350/XR550 Series
- XR150INT/XR550INT Series
- XT30/XT50 Series version 123 or higher firmware and Level M hardware with Network
- XT30INT/XT50INT Series
- XTLplus/XTLtouch Series

- XR500N/XR100N

Software updates are posted to DMP.com/Dealer_Direct. Follow the online directions to download the update.

Note: Save the update in a location on your computer hard drive you will remember.

Performing the Remote Update

(XR150INT/XR550INT Series, XR150/XR550 Series, XR100N/XR500N Series, and XT50 Series Version 123 or higher firmware and Level M hardware with Network Panels)

1. To perform a remote panel update, connect to the panel to be updated through network or cellular connection.
2. After successfully connecting, select Panel >> Remote Update from the drop-down menu.
3. In the Remote Update window, use the browse button to locate the firmware update RU file on your computer hard drive and select Update.

Direct Connect using DMP Model 399 Cable

Performing a Panel Update Using 399 Cable (XR150INT/XR550INT Series and XR150/XR550 Series)

1. Place a jumper across the Reset header.
2. Remove any attached bus from the LX500 header, if necessary.
3. Connect a DMP 399 cable from the LX500 header to the serial COM port of the PC operating Remote Link version 1.43 or higher and containing the XRx50RU file.
4. Start Remote Link and create or open the panel account that matches the panel to be updated.
5. Set the Connection Information Type to Direct with a baud rate of 38400 and choose the appropriate COM port. Select OK.
6. Remove the jumper from the Reset header.
7. From the keypad, enter the Diagnostics Menu (2313) and press CMD (Command) until PC Programming displays.
8. Press a top row select key and PROGRAMMING will display at the keypad for the duration of the Remote Update session. After the session has ended or no Remote Link Connection made in 1 minute, the keypad will display RECONNECT LX BUS.
9. Select Panel >> Connect, then select Connect.
10. Once connected, select Panel >> Remote Update, then select the correct RU file for the XRx50 panel model.
11. Select <Update> in Remote Link.
12. After the software version is updated, place a jumper across Reset header then remove the DMP 399 cable.
13. Reattach the bus removed from Step 2 to the LX500 header.
14. Remove the Reset jumper to resume normal panel operation.

Performing a Panel Update Using 399 Cable (XR500/XR100 Series)

1. Move the jumper to R, the top two pins of J23.
2. Place a jumper across the Reset.
3. Connect a DMP 399 cable to the 4-pin header below the RS232 port on panel.
4. Remove the jumper from the Reset header.
5. Start Remote Link and create or open the panel account that matches the panel to be updated.

6. Set the Connection Information Type to Direct with a baud rate of 9600 and choose the appropriate COM port.
7. Select Panel >> Remote Update, then select the correct RU file for the XR panel model.
8. After the software version is updated, place the jumper across the Reset, move the jumper from R to L for LX Bus or X for Wireless and remove the 399 cable.
9. Remove Reset jumper to resume normal panel operation.

Performing a Panel Update Using 399 Cable (XT30INT/XT50INT Series or XT30/XT50 Series)

The XT30/XT50 Series panel software can be updated via the panel's programming (PROG) header. To update the panel with a new software version, complete the following steps:

1. Place a jumper across the Reset header and then remove the yellow and green wires from keypad bus terminals 8 and 9.
2. Connect a DMP 399 Cable from the Programming Header to the serial COM port of the PC operating Remote Link and containing the XT RU file. Requires Remote Link 1.43 or higher.
3. Start Remote Link and create or open the panel account that matches the panel to be updated.
4. Set the Connection Information Type to Direct with a baud rate of 38400 and choose the appropriate COM port.
5. Select Panel >> Remote Update, then select the correct RU file for the XT panel model.
6. While placing a short across the LOAD header, remove the jumper from the Reset header. Then remove the short from the LOAD header and select <Update> in Remote Link.
7. After the software version is updated, place the jumper across Reset then remove the 399 cable.
8. Replace the yellow and green wires to terminals 8 and 9.
9. Remove Reset jumper to resume normal panel operation.

Performing a Panel Update Using 399 Cable (XTLC, XTLN, XTLN-WiFi)

The XTLC/XTLN/XTLN-WiFi Series panel software can be updated via the panel's programming (PROG) header. To update the panel with a new software version, complete the following steps:

1. If using a wired keypad, unplug the keypad from the panel.
2. Connect a DMP 399 Cable from the Programming Header to the serial COM port of the PC operating Remote Link and containing the XTLC/XTLN/XTLN-WiFi RU file.
3. Start Remote Link and create or open the panel account that matches the panel to be updated.
4. Set the Connection Information Type to Direct with a baud rate of 38400 and choose the appropriate COM port. Select OK to apply changes.
5. Select Panel >> Remote Update, then select the correct RU file for the XTLC/XTLN/XTLN-WiFi panel model.
6. Press and hold down both of the Reset and Load buttons on the XTLC/XTLN/XTLN-WiFi panel. Release the Reset button first, followed by the Load button. If the TX and RX LEDs are solid lights, then select <Update> in Remote Link. If not, repeat this step.
7. After the software version is updated, press and release the Reset button and remove the 399 cable.
8. If using a wired keypad, plug the keypad back into the panel.
9. Set the Connection Information Type back to Cellular or Network and select OK to apply changes.

Performing the Update (SCS-104 Receiver Line Cards)

Use the following steps to perform the SCS-104 update:

1. Remove the SCS-104 Line Card from the SCS-1R Receiver.
2. Connect a Model 399 Programming Cable to the PROG header on the line card and to a computer with Remote Link.
3. Place a shorting clip across the 2 pins of the LOAD header.
4. Reinstall the SCS-104 Line Card into the SCS-1R Receiver to power up line card.
5. Open Remote Link (version 1.61 or higher) and select System >> Remote Update from the drop-down menu.
6. In the Remote Update window, use the browse button to find the SCS104.RU software update file on your computer's hard drive. Remote Link automatically recognizes the update for the SCS-104 and allows you to select the COM port where the line card is connected.
7. Select Update. After the update is complete, remove the SCS-104 from the receiver and disconnect the 399 cable and remove the shorting clip from the LOAD header. Reinstall the Line Card to begin normal operation.

6. Feature Upgrade

The XR500 Series and XR150/XR550 Series panels have the ability to 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.

Purchasing Feature Upgrades

If you would like to purchase a feature upgrade, the authorized purchasing agent for your company may contact DMP Customer Service. Include the upgrade feature(s) to enable and the panel serial number(s) on the request. A separate feature key is issued for each panel. The feature key only enables the requested feature on the specified panel.

The panel serial number can be located in several different ways:

- Printed on a label located on the right side of the XR500 or XR150/XR350/XR550 PCB.
- Using panel diagnostics. See the Appendix in the XR500 Series Programming Guide (LT-0679) or XR150/ XR350/XR550 Series Programming Guide (LT-1232).
- Using Remote Link (version 1.18 or higher)
  a. Initial panel connection screen displays panel serial number when you connect.
  b. System Information screen displays all enabled panel features.
  c. The Panel >> Feature Upgrade window displays panel model, enabled panel features, and panel serial number.

Available Upgrade Features

Encryption (XR500N, XR550 with Network only)

Enable this feature to provide AES data encryption. This feature upgrade can only be enabled on an XR500N panel version 105 or higher or XR550 with Network installed. Encrypted communication cannot be enabled on a standard XR500 or XR550 panel.

All No Yes Option

When this feature is enabled on an XR500 Series version 106, the ALL NO YES option does not display at any

keypad during arming or disarming. Each area assigned to the user profile is chosen to be armed or disarmed individually.

Service Code Authentication

Enable this feature on an XR500 Series version 108 panel to authenticate service personnel before allowing access to panel programming or the User Menu. The Service Code is programmed into the SCS-1R receiver. The Service User code is user number zero (0) in the panel and can only be created in the panel remotely. Once a valid Service Code is entered at the panel, the panel validates the code with the SCS-1R, and access is granted to panel programming or User Menu. The service person then has 30 minutes to complete programming before authenticating again. If the Service Code entered is not validated, access to programming or the User Menu using the Service User code is denied.

32 Door Add On A / 32 Door Add On B

XR550 Series Panels operating with Version 111 (1/11/16) firmware now includes 32 doors of access control for the XR550. At no extra charge, this firmware update provides the ability to program an additional 16 doors of access to the system using 734 Wiegand Interface modules connected to any of the XR550's LXBus headers. Combined with the 16 doors of access available from the keypad bus totals 32 doors.

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. allows an LXBus 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 LXBus is automatically converted from a hardwire zone expansion bus to a hardwire Access Expansion Bus (AXBus) and the bus begins to operate as shown below.

- 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 AXBus to a maximum of eighty (80) 734 modules. Please see the table below for available addresses.
- Any unused AXBus 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 AXBus 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 AXBus operation is only compatible with 734 modules and the Model XR550. Keypads, 734N and 734N-Wifi modules must only be use on the keypad bus. AXBus operation is incompatible with the Model XR150 and XR350 control panels.

Performing the Upgrade

To perform a remote panel feature upgrade, connect to the panel to be upgraded. After successfully connecting, select Panel >> Feature Upgrade from the drop-down menu. The Feature Upgrade window displays the panel model number and serial number, a list of available features, and the currently enabled features.

In the Feature Upgrade window, enter the factory-supplied feature key in the field and press the Activate button. The Feature Upgrade window automatically updates to show the new feature as enabled on the panel.

Note: The XR550 Series and XR500 Series Version 106 or higher only require a six (6) character Feature key. XR500 Series Version 105 panels require a 16 character feature key.

Note: If the State Enabled does not display next to the feature, double check and re-enter the (6) character Feature key, and select Activate.

Note: The AES encryption feature upgrade can only be enabled on an XR550N or XR500N Panel. Encrypted

communication cannot be enabled on a standard XR550 or XR500 panel.

Note: Verify a Passphrase is entered in the Network Options Tab to ensure data transmissions are sent using encryption.

7. Real Time Events

(Must have Advanced Reporting module and Microsoft.NET Framework 3.5)

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. You may open the Real Time Events window by selecting System >> Real Time Events.

Max Event Count: This indicates how many rows display at one time. Default is 100.

Auto Update: Check this box in order to receive active events display on the screen. Un-check 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. Each event is color coded according to the event type:

EVENT	COLOR OF ROW
Fire	Red
Emergency	Lime
Burglary	Yellow
Auxiliary	Gray
Supervisory	Orange-Yellow
Panic	Light Green
Default (all others)	Pale Yellow

8. Diagnostics Window

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, press Alt and F10.

9. Managing Account Archives

Account Archive can be accessed by selecting Panel >> Account Archive. The Account Archive feature allows panel account programming to be stored for comparison or the archived version may be used to revert current panel programming to an archived version. Remote Link can be programmed to store up to 20 archived programming records per account. To program the number of account archive versions stored per account, select System >> Configure >> Remote Link >> Other Tab.

Revert

This option reverts the current panel account programming to a previous programming version. Select the archive version and select Revert. Remote Link automatically creates an archive version of the current programming before reverting to the selected panel programming. Once the panel account has been reverted, the programming is stored as the Current version and CAN be sent to the panel.

Open

This option opens the account archive version for viewing purposes. This is a read only option.

Delete

This option permanently removes the selected account archive version.

Part 1. Panel Management

1. Panel Information

If you wish to add, delete, or change accounts in Remote Link, select File >> Panel Information. This opens the Panel Information window.

- The Name column provides you with a simple name to associate with each account number.
- The City column helps you keep track of the location of each account.
- The Receiver column shows which receiver you are using to connect to that panel.
- The Account column shows the account number that you assign to each alarm account.
- The Model column lists the model of the panel account.
- The Version column lists the firmware version of the panel account.
- The Date column lists the date of the firmware version of the panel account.
- The Panel Phone column lists the telephone number of the panel account.

Note: You must scroll to the right to view the account's Model, Version, Date, and Panel Phone.

System Info Button

For XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series panels, select the account name in the Panel Information window and press the System Info button to view the account name, model number, panel software version, serial number, MAC address, and enabled features list. For all other panels the System Info button displays only the account name, model number, and firmware version number.

1.1. General Information

Enter a name for the account in the Name field in the General Information section. The receiver number and account number appear in this section of the Panel Information window as well. You may change the account number in the Account # field if necessary. Refer to Account Number Conventions for information about assigning account numbers.

1.2. Connection Information

Connection Information is used to set up connection to the panel from the Remote Link computer. See Connection to a Panel for more information.

Primary Communication Information

A Primary Communication type is available and may be programmed as one of the following:

Type

From the Type menu select which type of connection you will use to communicate with the panel:

SCS-1 / SCS-105: Select this option to communicate with the panel through an SCS-1, SCS-1R or SCS-105 Receiver using a dial-up connection.

Network: Select this option to communicate with the panel through a data network connection. Depending on the panel, connect to the network through:

- The XR500N/XR500E panel onboard Ethernet.
- The XR100N panel onboard Ethernet.
- The XR150INT/XR550INT and XR150/XR350/XR550 with Network panel onboard Ethernet.
- An XT30/XT50 Series or XTLplus/XTLtouch Series panel onboard Ethernet.

Direct

Select this option to communicate with the panel through a direct cable connection.

Modem

Select this option to communicate using a standard computer modem to a panel that has a DMP Fast Modem installed or to the 2400 baud programming dialer of an XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panel. First configure your computer's modem in the Modem Tab. Then configure the modem as described below.

Modem Special

For XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series (Version 112 or higher) and XR100 Series panel communication requirements, when a slower baud rate that does not fluctuate is needed to ensure data integrity. Modem Special allows this type of control when using a computer modem to dial out.

Note: Only one modem can be used. Select the correct one for your operation.

Cellular

Remote Link communicates with the panel through a cellular connection using a SIM/MEID card.

Remote Key

(Only operators with authority for Remote Options can view the Remote Key) Enter a numerical code up to 8 digits long that the panel should use as a password to verify its identity to the Remote Link computer. The panel must give the correct key to Remote Link before any programming may take place. All panels are shipped from the factory with the key preset as blank.

For security reasons, the Remote Key cannot be viewed from a keypad connected to the panel.

Note: The programming options listed below will vary according to the type of connection you select in the Type

field discussed above.

Phone

Enter the panel phone number. This field will only appear when you select SCS-1 / SCS-105 or Modem in the Type field.

Note: If you need to dial a number to access an outside line, enter that number before the panel's phone number. Also 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.

Note: Modems from some manufacturers require a comma (,) for a pause rather than the letter P. Check your Modem documentation before entering the panel phone number.

Dial

Select how you want the receiver to handle the phone line connection with the panel. This field will only appear when you select SCS-1 / SCS-105 or Modem in the Type field.

No: Do not dial the panel phone number to make contact with the panel. This is used mainly for multiplex and asynchronous accounts.

Yes: Use the panel phone number entered in the Account Information file to dial the subscriber's panel.

Pickup Only

Select this option to have Remote Link pickup when the panel calls in to the receiver. This allows Remote Link to seize the panel when the panel calls in. The following example illustrates how to perform a Pickup Only using Remote Link.

A Central Station Operator calls the Installing Technician using the same phone line as the SCS-105. The Installing Technician answers the phone using the same phone line as the panel. Using Remote Link, the Central Station Operator selects Pickup Only from the Dial drop-down menu and SCS-1/SCS-105 from the Type drop-down menu. Then the Operator will select Panel >> Connect and press the Connect button to connect with the Technician's panel.

When the SCS-105 goes on-line (the amber OL LED will light) the Central Station Operator tells the Technician to enter 984 Command at the keypad. The Technician then selects NBR and enters any number other than zero (0). Remote Link will then seize the phone line and the Operator and Technician hang up their phones.

IP Address

Enter the IP address of the panel. This field will appear only when you select Network in the Type field. Do not enter leading zeros when entering the IP address.

IP Port

Enter the port through which you will connect to the panel. 2001 is the default port. This field will appear only when you select Network in the Type field.

COM Port

Select the computer's communication port that is connected to your panel. This field will only appear when you select Direct in the Type field.

Baud Rate

Set the Baud Rate to 9600. The only time you may want to select a slower baud rate is if you are using a direct cable connection and you are having communication problems. The setting on the 462N card must match this entry. This field will appear only when you select Direct in the Type field.

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

1.2.1. Connecting to a Panel

Connecting to a Panel (Off-site)

1. Connect to the panel through network connection.
2. After successfully connecting, select Panel >> Remote Update from the drop-down menu.
3. In the Remote Update window, use the browse button to locate the firmware update RU file on your computer hard drive and select Update.

Direct Connect using DMP Model 399 Cable (On-site)

XR150INT/XR550INT Series and XR150/XR350/XR550 Series

1. Place a jumper across the Reset header.
2. Connect a DMP 399 Cable from the LX500 Bus Header to the serial COM port of the PC operating Remote Link and containing the XRx50 RU file. Requires Remote Link 1.43 or higher.
3. Start Remote Link and create or open the panel account that matches the panel to be updated.
4. Set the Connection Information Type to Direct with a baud rate of 38400 and choose the appropriate COM port. Select OK.
5. Remove the jumper from the Reset header. Enter Diagnostics Menu (2313) and press Command until PC Programming displays.
6. Press a top row key and PROGRAMMING will display at the keypad for the duration of the Direct Connect session. After the session has ended or no Remote Link connection made in 1 minute, the keypad will display RECONNECT LX BUS.
7. Select Panel >> Connect in the Remote Link. A Connection Status window will open. Select Connect to connect to the panel.
8. After the Direct Connection is completed, select Panel >> Disconnect and disconnect. Place the jumper across Reset then remove the 399 cable.
9. Remove Reset jumper to resume normal panel operation.

XR500 Series and XR100 Series

1. Place a jumper across the Reset header and then remove the yellow and green wires from the keypad bus terminals 8 and 9.
2. Move the jumper to R, the top two pins of J23.
3. Connect a DMP 399 cable to the 4 pin header below the RS232 port on panel.
4. Remove the jumper from the Reset header.
5. Start Remote Link and create or open the panel account that matches the panel.

6. Set the Connection Information Type to Direct with a baud rate of 9600 and choose the appropriate COM port. Select OK.
7. Select Panel >> Connect, then select Connect.
8. After programming is complete, select Panel >> Disconnect, then select Disconnect. Place the jumper across the Reset, move the jumper from R to L for LX Bus or X for Wireless and remove the 399 cable.
9. Replace the yellow and green wires to terminal 8 and 9.
10. Remove Reset jumper to resume normal panel operation.

XT30 Series, XT50 Series, XTLplus Series, XTLtouch Series, XTLC/XTLN/XTLN-WiFi Series panels

Direct connect is for Remote Updates only. See Performing a Remote Update for more information.

1.3. Backup Connection Information

Backup Communication Information

A Backup Communication type is available and may be programmed as one of the following:

Type: From the Type menu select which type of Backup Connection will be used to communicate with the panel:

None: Select this option if no backup communication is desired.

SCS-1 / SCS-105: Select this option to communicate with the panel through an SCS-1, SCS-1R or SCS-105 Receiver using a dial-up connection.

Phone: Enter the panel phone number. This field will only appear when you select SCS-1 / SCS-105 or Modem in the Type field.

Note: If you need to dial a number to access an outside line, enter that number before the panel's phone number. Also 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.

Note: Modems from some manufacturers require a comma (,) for a pause rather than the letter P. Check your Modem documentation before entering the panel phone number.

Dial: Select how you want the receiver to handle the phone line connection with the panel. This field will only appear when you select SCS-1 / SCS-105 or Modem in the Type field.

No: Do not dial the panel phone number to make contact with the panel. This is used mainly for multiplex and asynchronous accounts.

Yes: Use the panel phone number entered in the Account Information file to dial the subscriber's panel.

Pickup Only: Select this option to have Remote Link pickup when the panel calls in to the receiver. This allows Remote Link to seize the panel when the panel calls in. The following example illustrates how to perform a Pickup Only using Remote Link.

A Central Station Operator calls the Installing Technician using the same phone line as the SCS-105. The Installing Technician answers the phone using the same phone line as the panel. Using Remote Link, the Central Station Operator selects Pickup Only from the Dial drop-down menu and SCS-1/SCS-105 from the Type drop-down menu. Then the Operator will select Panel >> Connect and press the Connect button to connect with the Technician's panel.

When the SCS-105 goes on-line (the amber OL LED will light) the Central Station Operator tells the Technician to enter 984 Command at the keypad. The Technician then selects NBR and enters any number other than zero (0). Remote Link will then seize the phone line and the Operator and Technician hang up their phones.

Modem: Select this option to communicate using a standard computer modem to a panel that has a DMP Fast Modem installed or to the 2400 baud programming dialer of an XR150INT/XR550INT Series, XR150/XR350/ XR550 Series or XR100/XR500 Series panel. First configure your computer's modem in the Modem Tab. Then configure the modem as described below.

Modem Special: For XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series (Version 112 or higher) and XR100 Series panel communication requirements, when a slower baud rate that does not fluctuate is needed to ensure data integrity. Modem Special allows this type of control when using a computer modem to dial out.

Note: Only one modem can be used. Select the correct one for your operation.

Cellular: Remote Link communicates with the panel through a cellular connection using a SIM/MEID card.

Note: Cellular can not be the Backup Communication type if Cellular is selected as the Primary.

Failed Communication

The Primary Communication type will be attempted two times. Remote Link will display "Connecting to panel on Primary Connection" while attempting to establish a connection.

If communication through the Primary Connection type is unsuccessful, Remote Link will attempt to establish communication through the Backup Communication type two times. Remote Link will display "Connecting to panel on Secondary Connection" while attempting a connection.

In the event communication is unsuccessful through the Primary and Backup Communication type, Remote Link will display "Unable to connect to panel".

1.4. Location

In the Location section of the Panel Information window, enter the address where the panel is located. Also enter a voice phone number for the panel location, and a night phone number where you may speak to someone about the panel after business hours.

Extra Information: You may record additional notes about the panel account by selecting Extra Information. Selecting Extra Information opens the Extended Panel Information window.

1.5. Extended Panel Information

Select Extra Information if the Panel Information window to open the Extended Panel Information window.

There are several fields in the Extended Panel Information window:

Response: Enter any information for the operator on what type of response to send in case of an alarm on this panel.

Notes: Enter any 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 the name, address, and phone number for the individuals to contact in case of an alarm on this panel account.

Auto Recall Frequency: Enter the number of days (0 to 60) during which the panel is expected to send at least one Automatic Recall Test. By default this field is blank. When the field is blank or 0 (zero)is entered, Remote Link will not look for an Automatic Recall Test for the account.

If Remote Link does not receive an Automatic Recall Test within that period, the account is placed in the Recall Failure List. You may print the list of accounts that failed to send an Automatic Recall Test by going to File >> Print >> Recall Failure List.

After an Automatic Recall Test is received, Remote Link begins counting down to look for the next Automatic

Recall Test from the account. The countdown adds two hours onto the entered number of days. For example, if 2 is entered in the Auto Recall Frequency field, Remote Link will look for the next test in 50 hours-48 hours plus two.

Allow Test Deferrals: Check this box to allow Remote Link to accept any incoming message from the account as the Automatic Recall Test. For example, if 2 is entered in the Auto Recall Frequency field and the account sends an opening signal within the 2 days, Remote Link will accept the opening signal as the Automatic Recall test. Remote Link will then restart the timer after the opening signal is received.

Note: These two fields, 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 tab.

Hyperlink: (Must have the Alarm Monitoring module or Command Center to Use) Enter the file or URL address you wish to open. See Creating a Hyperlink for more information.

1.6. Creating a Hyperlink

Open File >> Panel Information. Select the account to which to will assign the hyperlink. Select Extra Information near the bottom of the screen. One hyperlink is available for each account.

In the Hyperlink field, enter the URL (Internet) address or enter the desired file and file path. A browse button, indicated by three small dots, is located to the right of the Hyperlink field. Press this button if you would like to search for the desired file.

Note: Specify the path to the desired file: For example, `D:\My Documents\sitemap.jpeg`.

Also, you must have the application program needed to open the file loaded on the computer. For example, if you entered `D:\My Documents\sitemap.doc`, you must have Microsoft Word installed on the computer.

After you have entered the desired file or Internet address, press the Test button to verify that the Hyperlink button located in the Alarm List window will open the proper file or Internet address.

1.7. Sorting and Searching Accounts

The Name, City, Account and Panel Phone tabs at the top of the Panel Information window sort your accounts by account name, account number, the city where the account is located or panel phone number.

When you select the Name tab, the accounts are sorted alphabetically by the name of the account.

When you select the City tab, the accounts are sorted alphabetically by the city that the account is located.

When you select the Account tab, the accounts are sorted by the account numbers and are listed in ascending order.

When you select the Panel Phone tab, the accounts are sorted by the panel phone numbers and are listed in ascending order.

When you select the Customer tab, the accounts are sorted by the customer name and are listed in ascending order.

When you select the Region tab, the accounts are sorted alphabetically by the region that the account is located.

1.8. Receiver Information Tab

The Receiver Tab section allows you to add, copy and delete an SCS-1R Receiver using an SCS-150 processor card.

To add a new receiver, select New, and enter the Version number, Receiver number, and Account number for the receiver and select OK. The account number is needed to maintain database integrity and is not used by the system. Any number that is not used by a panel is fine.

Receiver Name: Enter a name for the receiver. The receiver name can be 32-characters long.

COM Port: Select the COM port used for connecting to the receiver. Be sure to select a setting that does not interfere with a mouse, modem, or any other device on the computer. The programmed COM port cannot be used for any other purpose while Remote Link is running.

If a COM Port is programmed for a receiver, Remote Link verifies that a good connection exists before opening the receiver for editing. If no receiver is connected, an error message is displayed. To edit a receiver without testing the connection, set COM Port to None.

To copy an existing receiver, select the receiver from the list and select Copy. A new window appears, allowing changes to be made to the information. Once the new information has been added, select OK.

To delete a receiver, select the corresponding receiver from the list and select Delete.

To program a receiver, select the corresponding receiver from the list and select OK.

To filter accounts, select the Panel Filter button. This allows filtering of panel or user information. This option is not available if using the SQL Server module.

1.8.1.1 Receiver Programming

1.8.1.1. Receiver Sys Options

Note: Before continuing, select Retrieve to import the current receiver information.

Company Name: Enter your company name using up to 40 characters.

Receiver Number: Used to distinguish between multiple SCS-1R systems. There can be from 0 to 9 systems programmed. Default is 1.

Receiver Key: An eight-character alphanumeric code requested when using remote programming. Default is blank.

Service Code: A 5-digit service authorization code used to authenticate service personnel before allowing access to panel programming or performing any user operations. 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. Default is 00000.

Hours From GMT: Number of hours (0 to 23) from the Greenwich Time zone (GMT) where the SCS-1R is located. Please see the table of time zones in the Appendix to help locate the appropriate time zone. Default is 6 (Central Time).

Dialer Line Monitor: Enable monitoring of all digital dialer line cards for any failed communications with panels. Default is disabled.

Send: Select Send to send the Receiver System Options programming to the SCS-1R.

1.8.1.2. Print Operation

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

Note: Before continuing, select Retrieve to import the current receiver information.

Print: Defines when to use the printer: Never, Always, or Primary (Host output) Fail. Never will suppress all printing, Always will print all messages from the receiver, and Primary (Host output) Fail will print only when the communication to the primary host fails. Default is Always.

Port Type: Serial is the communication type.

Send: Select Send to send the Print Operation programming to the SCS-1R.

1.8.1.3. Receiver Line Cards

Note: Before continuing, select Retrieve to import the current receiver information.

New: Select the NEW button near the bottom of the window to add a new line card.

Card Number: Enter the card number, 1 through 8.

Note: Lines 6-8 can only be used with SCS-104 Line Cards using SCS-150 Version 101 and updated SCS-RACK hardware.

Card Model: Select None, SCS-104, SCS-101, or SCS-100 from the drop-down menu.

Send Time to Panels: Select this option to allow the receiver to update the panel's internal clock as the panel communicates with the SCS-150. Select NO to prevent the receiver from updating the communicating panel's internal clock.

SCS-104 Dialer

Dialer Line Enable: Select to enable Dialer Lines 1-4 on each card number.

Send ANI/DNIS Information: Select to enable the Automatic Number Identification (ANI) and Dialed Number Identification Service (DNIS) information to be sent. 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: Select to enable the Caller ID information to be sent to host automation.

Echo Cancel Disable: Echo Cancellation is technology used by telephone companies to eliminate echo from voice telephone transmissions. In some cases this technology can interfere with alarm signals. If you have problems with Echo Cancellation interfering with your signals, select to turn off the echo cancellers. If you are not having problems with the telephone company echo cancellation, do not select to leave the echo cancelers on.

SCS-104 Network

Network Line Enable: Select to enable the network for the selected line card. Default is selected.

Local IP Address: Enter the SCS-104 IP address. This address must be unique and cannot be duplicated. The default value is 192.168.000.250.

Local Port: This identifies the port used to communicate messages to and from the panel. If a setting change is required, enter the new number. 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 SCS-104. The default value is 255.255.255.000.

Passphrase: In order to communicate using encryption, XR550INT, XR550 Series, and XR500 Series panels reporting in to the SCS-104 at the receiver must have a Passphrase. This Passphrase must be programmed into every panel reporting in to the SCS-104 at the receiver. The SCS-104 installed in the receiver must also be programmed with the same Passphrase.

To enable encryption enter an 8 to 16-character Passphrase using alphanumeric characters. If you leave the Passphrase blank, the SCS-104 communicates with XR550 Series and XR500 Series panels, but the data is not encrypted. The Passphrase is blank by default.

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 & S17 Always: When disabled, the S16 Panel Not Responding message is sent to the automation computer for each supervised account that has stopped sending check-in messages unless 50 S16 messages have been generated for different accounts within one minute. This could occur because the network has failed. Once this occurs, S72 Network Trouble is sent and the receiver stops sending S16 messages to the automation computer. The receiver sends S73 Network Restored and will begin sending S16 messages after the receiver starts receiving check-in messages again.

When enabled, the S16 Panel Not Responding message is 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.

When enabled, the S17 Panel Response Restored message is 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. Default is disabled.

Acknowledge Panel Substitution Message: When selected, the SCS-104 replies with an acknowledgment to messages sent by substituted panels. See the Substitution Code section of the panel programming guide for the definition of a substituted panel. 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.

When not selected, substituted panels are not sent acknowledgments for their messages. For each message received from a substituted panel, an S58 Alarm: Panel Substitution message is sent to the host automation computer and receiver printer.

Note: Select this option for all receiver installations except for Canadian receiver installations where the security requirement is ULC Level 5 and then this option should not be selected.

SCS-104 Check-in Table

Check-in Table IP Address: 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. Additionally, the list of supervised network accounts used by an SCS-104 or SCS-101 on a primary receiver can be mirrored by the SCS-CTM for use by an SCS-104 or SCS-101 card on a second receiver. Refer to the SCS-CTM User's Guide (LT-0940).

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

Enter the IP address for the computer where the SCS-CTM Check-in Table Manager software is installed. When no SCS-CTM software is installed, leave the IP address set to 000.000.000.000.

Check-in Table Port: Enter the IP port used to communicate Check-In Table messages to the SCS-CTM Check-in Table Manager program. Valid range is 1 to 65,535. Default is 2005.

Check-in Table ID: Enter the table ID number to be used by the SCS-CTM Check-in Table Manager to identify the check-in table. Valid range is 1 to 255. Default is 1.

Send: Select Send to send the Receiver Line Card programming to the SCS-1R.

1.8.1.4. 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.

Note: Before continuing, select Retrieve to import the current receiver information.

Host Number: 1

Host Name: Select a name for the Receiver Host. Name can be 16-characters.

Host Type: Primary.

Port Type: Serial.

Start Character: Select a start character to precede all host messages. Default is None.

Use CRC: Select to enable CRC error checking on each message sent to the host. Default is disabled.

Use Sequence: Select to enable 1-99 numbering of all messages sent to the host. Default is disabled.

Test Interval (minutes): Enter number of minutes between message tests. The test interval can be between 1-60 minutes. Default is 1.

Acknowledge Timeout (seconds): Enter the number of seconds (1-15) that the receiver should wait for an acknowledgment from the host before re-sending the message. Default is 3.

Retries to Failure: Enter the number of retries allowed without receiving an acknowledgment from the host before entering a failed state. This retry number includes the initial message sent to host. The retry range may be from 1-15. Default is 3.

Line Number Length: Enter the number of digits, 0 (zero) through 2, used to report the SCS-1R Receiver signal line number. Default is 0.

Send: Select Send to send the Receiver Host Programming to the SCS-1R.

1.8.1.5. Receiver Status

Select to see the Receiver Model, Version Number, and Firmware Date.

1.8.1.6. Serial Ports

Select to open the Receiver Serial Port Programming window.

Note: Before continuing, select Retrieve to import the current receiver information.

Auxiliary

Baud Rate: 9600.

Usage: Auxiliary.

Host Output

Baud Rate: Select the baud rate for the Host port. Default is 9600.

Usage: Host

Activity Log/Printer

Baud Rate: Select the baud rate for the Printer port. Default is 1200.

Usage: Printer.

Send: Select Send to send the Receiver Serial Port Programming to the SCS-1R/SCS-150.

1.8.1.7. Receiver Diagnostics

Select to display the MAC Address, Serial Number, Version Number, Firmware Date, Bank Number, Key value, Write Count and DB Version.

1.8.2. Filtering Accounts

The Panel Information screen has a "right click" popup menu that allows quick filtering of the records in the grid. Select what data to filter and right click the mouse button. These options will appear:

Add to Filter: Adds the value of the field as an additional condition for the filter.

Clear Filter: Removes all filtering.

Filter by Selection: Makes the value of the field the only condition for filtering records. For example, if you right click on the XR40 and select Filter by Selection, then the filtered list shows all of the XR40 panels in the database.

Note: To export the filtered list of records, enable Advanced Filtering privileges in Operator Configuration and

access the Panel Filter window for export options.

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

1.8.2.1. Panel Information Filter Window

On the Panel Information Window, select Panel Filter. This allows filtering of panel or user information.

Note: To access the Panel Information Filter Window, enable Advanced Filtering privileges in Operator Configuration.

Once the Panel Information Filter window opens, there are two options, Panel Filter and User Filter.

1.8.2.2. Panel Filter Option

Select the Panel Filter button field to filter the information in the panels.

Fields: Select the field to be filtered. You can select any of the 10 listed fields to perform a filter.

By Range: If Account or Model is selected for the Field, enter the Starting and Ending Range. Select OK to view the results.

By Value: If the City, Customer, Name, Region, State, Version, Panel IP, or Panel Phone Fields are selected for a filter, enter a Field Value and select a Search Type.

Field Order: Select how the filtered information is displayed. Select either Alphabetical or Logical. Default is Logical.

View Summary: This button shows a summary of the items and values selected for the filter.

Searched: This tab displays the items and values of the last filter performed.

1.8.2.3. User Filter Option

On the Panel Information Filter Window, select the User Filter button field to filter the information in the user profiles. To limit the filter to a selected panel, check the Limit Users to Selected Panel box to the right of the User Filter button and highlight the panel from the list.

Fields: Select the field to be filtered. You can select any of the seven listed fields to perform a filter.

By Range: If ID Number or User Number is selected for the Field, enter the Starting and Ending Range. Select OK to view the results.

By Value: If the Name, Department, or any of the User Fields are selected for a filter, enter a Field Value and select a Search Type.

Field Order: Select how the filtered information is displayed. Select either Alphabetical or Logical. Default is Logical.

View Summary: This displays a summary of the items and values selected for the filter.

Searched: This tab displays the items and values of the last filter performed.

1.8.2.4. Filter Results

The results of the filter appear in the Panel Information Filter window.

File Name: To export the filtered information, type in a valid file name and location where the exported information is to be stored. Select the small button to the right of the File Name to browse the computer directory and select a location.

Export: Once a valid File Name and location is entered, select Export to export the information. If you want to export only certain users, select the users from the filtered information, select the Export Selected Users box, and select Export.

1.9. Setting up New Alarm Accounts

To add a new account, select New near the bottom left corner of the Panel Information window. The New Panel window appears on your screen.

A checkbox labeled Programming On File allows you to specify whether or not the panel's programming is kept on file. If you wish to maintain the panel's programming in Remote Link, leave the box checked. If you wish to assign the new panel to a main account and use the main account's programming as the new panel's programming, deselect the box by selecting the box. Programming On File is checked as default.

When you select the drop-down arrow in the Model field, Remote Link displays a list of the panel models. Select the appropriate panel model number. For XR550 with Encryption or XR500E panels, select the XR550 with Network or XR500N panel and check the appropriate panel type under Feature Set.

In the Version field just below Model, enter the firmware version of your panel.

Feature Set: When you select a panel, the Feature Set displays the available features and panel types. Check the enabled features of the panel for the account you are creating.

Select Encryption when an XR550 with Encryption or XR500E panel is installed. The encryption feature allows the panel to send and receive data using AES encryption. To complete encryption programming, enter a Passphrase in Network Options.

Select SVC USER AUTH to enable the option to authenticate service personnel before allowing access to panel programming or the User Menu.

Leave the Receiver field set to 1 unless you have multiple receivers.

In the Account field, enter the account number you wish to assign to this subscriber account. Only numbers may be used for account numbers: Do not use letters when assigning account numbers. When assigning account numbers, follow the conventions described in Account Number Conventions.

1.9.1. Account Number Conventions

When assigning account numbers, keep the following conventions in mind.

When using Digital Dialer (DD), Host or Net (HST or NET) mode or Cellular (CELL) communication, the range of available account numbers is 1 through 65535. Do not use a leading 0 (zero) if you are assigning an account number of four digits or less. The panel automatically right justifies the account number if it does not fill the display.

When using Modem IIe (M2E), Contact ID (CID), or 4-2 communication, select an account number between 1 and 9999.

When using Multiplex (MPX) communication, you must select a 5-digit account number as described below.

The first number is the receiver line number, which is usually 1, and the second number is always 0.

Assign three digits between 000 and 127 as the main panel account number. The full account number will read between 10000 and 10127.

If you wish to assign separate account numbers to individual areas, then assign an area account number between 128 and 999. The final account number for areas will read between 10128 and 10999.

1.10. Modifying Account Information

To edit information on existing accounts, open the Panel Information window by selecting File >> Panel Information.

To modify the information on an account, select the account on the left side of the Panel Information window, then change or add the information on the right half of the window. You may also add additional information to each account by selecting Extra Information to open the Extended Panel Information window.

1.11. Copy Existing Account File or Create Templates

If you want to create a new account by using an existing account file as a template, open the Panel Information window by selecting File >> Panel Information. Select the account file that you wish to use as a template by selecting that account in the list. Then select Copy at the bottom of the window to open the Copy Panel window.

Source: This field shows the account name and number that you are using as a template.

Model: Select the model number of the panel from the drop-down menu.

Version: Enter the firmware version of the panel.

Receiver: Leave the Receiver field set to 1 unless you have multiple receivers.

Account: Enter the account number that you wish to assign to the new account. Take note of the account number guidelines discussed in Account Number Conventions.

Template: Select this to create a template to be added into the Template tab. Enter a name for the template. The template can then be used to compare panel programming against existing panels.

When you have filled in all of the fields in the Copy Panel window, select OK to go back to the Panel Information window. Fill in the fields of the Panel Information window according to the directions in Setting Up New Alarm Accounts.

1.12. Managing Templates

The Template tab under Panel Information can be used to create and manage templates of panel programming and to use for comparison against existing programming of panel accounts.

Search: This field allows you to search for a particular panel within the existing templates.

General Information

Any existing templates appear in the list with the Name, Model and Version.

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. Type in a name for the newly created template and select OK. The new template will display in the Template Tab.

Copy Panel: This allows you to make a new template by copying the information from an existing account. Follow the instructions above in "Copy Existing Account File or Create Templates".

1.13. Account Archive

Account Archive allows panel account programming to be automatically or manually archived for comparison or the archived version may be used to revert current panel programming to an archived version. Remote Link can be programmed to allow up to 20 archived programming records per account. To program the maximum number of account archives allowed, select System >> Configure >> Remote Link >> Other Tab.

To manually archive the current panel account information and programming, select Archive on the Panel Information window. The panel account programming is stored with the current date and time.

To enable Remote Link to archive panel account programming automatically, select System >> Configure >> Remote Link >> Other Tab.

1.14. Export Account Information

On the left half of this window, is the list of available accounts under the heading Select Accounts to Export. On the right half of this window, under the heading Accounts to Export, is a list of the accounts that have been chosen. To add an account to the Export window, highlight the account name on the left side of the screen and press the > button. To remove an account from the Export window, highlight the account name on the right side of the screen and press the < button.

When installing multiple panels in different locations, a technician can program each panel and then export the panel account information and programming as an individual file for each panel installed or as one file with all installed panels together.

When the technician returns to the Central Station, all the panel files can be imported into to the Central Station Remote Link computer. See Import Account Information.

Save As: To create or replace a file, enter the location and name of the exported file by typing in the Save As field or browse for the file location by selecting the button to the right of the Save As field and make sure the file name ends with .xml extension. Press the Export button to export one or multiple files to the location and name specified.

Enter Encryption Key: Enter a 4 to 64 character encryption key and press OK. The same encryption key is needed when importing the file. For security purposes, the exported data file is encrypted to ensure panel programming is not compromised. Each time a file is exported, a new encryption key needs to be entered.

1.15. Import Account Information

Accounts selected for import will display on the left section of this window. On the right section of this window are two available options regarding an account that already exists in the Remote Link data base.

File to Import: Enter the location and name of the import file in the File to Import field or browse for the file location and name by selecting the button to the right of the File to Import field. When the file name displays, press the Load button to display the account in the Select Accounts to Import list.

Enter Encryption Key: Enter the 4 to 64 character encryption key that was used when the file was exported. For security purposes, the exported data was encrypted to ensure panel programming was not compromised.

Select Accounts to Import: The receiver number, account number and panel name display. A * next to the checkbox indicates that the panel currently exists in the Remote Link data base. Highlight the name and select the import process to use, overwrite or change, shown on the right of the screen. A checkmark then displays in the box next to the receiver number to confirm the selection.

- Overwrite Existing Account: the panel and account number currently exist and importing replaces the existing account.
- Change Account Number: allows the receiver number and/or account number to be changed for the file(s) you are importing.

Press the Import button to import the selected accounts.

Note: When a panel is included in an Account Group, selecting Overwrite Existing Account deletes the existing panel account and replaces it with the imported panel account.

1.16. Printing with Remote Link

The Print command allows you to print account and panel programming information, panel event buffers, and activity reports. You may print to an attached printer or preview the reports on your computer screen.

Select File >> Print, then chose which type of report you wish to print.

1.16.1. Printing Account Information Reports

To print an account information report, select File >> Print >> Account Information to open the Account Report Setup window.

All: Check this box to print the account reports for all panel accounts. If the All checkbox is not selected, the account information for the panel that is opened in Remote Link will be printed.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to File >> Print >> Saved Report.

Print: Select this button to print the account reports to an attached printer.

1.16.2. Printing Panel Programming Reports

Prints panel programming for the account open in Remote Link.

Reports to Include

Check the box for each type of report that you wish to print. Select All to select all programming and Clear to remove all selections. Checking Include Lockout Code will print the panel Access Code.

Note: Printing User Codes prints a list of the users, along with the information about each user. Check Include Passcodes to include the actual passcodes numbers for each user. Check Sort by Name to print a sorted list of users sorted alphabetically by the users' names.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to File >> Print >> Saved Report.

Print: Select this button to print the account reports to an attached printer.

1.16.3. Printing Activity Reports

Prints a report of Remote Link system activity. You can select print options from the choices listed below.

Account: Enter the range of account numbers for which you wish to print the Activity Report Log. Enter the receiver number followed by a dash and the account number, such as 1-12345.

All: Check this box to print the Activity Report Log for all accounts.

Date: Enter the range of dates for which you would like to print the report. Select the arrow to the right of the field to open the drop-down calendar, as shown above. Select the date to select the desired date. You may also type in the appropriate date.

All: Print the Activity Log Report for all dates.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to File >> Print >> Saved Report.

Print: Select this button to print the account reports to an attached printer.

1.16.4. Printing Events

Print a report of events, such as signals and messages received by the Alarm List or events stored in the event buffer. To print event reports, select File >> Print >> Events. You can select print options from the choices listed below.

Data Source

Events: Select to print a report of events received by the Alarm List for the selected panels and dates.

Panel Events Buffer: Select to print the stored events downloaded from a subscriber panel.

Account: Enter the range of account numbers to print the Events Report selected above. Enter the receiver number followed by a dash and the account number: 1-12345, for example.

All: Check this box to print event reports for all accounts.

Date: Enter the range of dates for which you would like to print a report. Select the arrow to the right of the field to open the drop-down calendar. Select the date to select the desired date. You may also type in the appropriate date.

All: Select to print event reports for all dates. If Panel Events Buffer is selected above, then the report would include all dates that have events stores in the Remote Link event buffer for the selected panel.

Report Format

Choose which format to print the reports.

Summary: Prints the Events Report sorted by account number.

Customer Mailout: Customer Mailout allows the reports to be printed in a customer-friendly layout by sorting the Events by account and automatically breaking the pages when a new account is detected.

Messages in Report

Select the individual messages to appear in the report or select All to have all of the messages appear in the report.

Other Reports

Select to have Traffic Count appear in the report.

1.16.5. Printing Activation Status Reports

Print activation status reports for all SIM cards associated with an account. To print activation status reports, select File >> Print >> Activations Status. You can select print options from the choices listed below.

Sort by Account: Select to print a report sorted by account number.

Sort by Name: Select to print a report sorted by account name.

Sort by SIM #: Select to print a report sorted by SIM number.

Sort by Status: Select to print a report sorted by the status of the SIM card.

Include by Status: Select to print only the selected status. Options include All, Unassigned, Missing Path, Date Range, Activated, Deactivated, Pending, and Other.

1.16.6. Messages in Alarm List Report

Check the box next to the event type that you would like to print. You may select any combination of the following event types.

- Alarm
- Trouble
- Restoral
- System
- All: Selecting All will check all boxes.

- Clear: Selecting Clear will clear all boxes.
- Setup: Select this button to enter the printer setup window to configure your print options.
- Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to File >> Print >> Saved Report.
- Print: Select this button to print the account reports to an attached printer.

Note: If you have a module, such as Alarm Monitoring, Command Center, or Advanced Reports, installed you have additional printing options. See the module's section of the help file for more information.

1.16.7. Printing Recall Failure Reports

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

You may sort by the Account Name or Account Number by selecting the appropriate radio button.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to File >> Print >> Saved Report.

Print: Select this button to print the account reports to an attached printer.

If a panel misses a programmed test in Auto Recall Frequency, the date is listed in the last column, labeled Expected. If a Host panel misses a check-in, "No Check In" will be listed in the Expected column.

1.16.8. Printing Advanced Reports

Prints Advanced Reports using the Advanced Reporting module. This screen allows you to sort and filter the panel's events.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, go to File >> Print >> Saved Report.

You may also export files using one of seven file formats. You can then use the reports in other applications, such as Microsoft Excel. See Exporting Reports for more information.

Print: Select this button to print the account reports to an attached printer.

Select here for a complete discussion of the Advanced Reporting module.

1.16.9. Compare Accounts Report

This option allows comparison of a variety of panels to each other, to an archived version and/or to a template and a report is generated in .xls spreadsheet format. Access this option in File >> Print >> Compare Accounts.

Control Panel

Template: Select this option to choose a panel template to compare to existing accounts. If selected, the existing templates display in the drop-down menu that is below. Select the template to compare. Once a template is selected, the panel model information appears to the right.

Account: Select this option to use an existing panel account to compare to another existing account(s). If selected, enter the Receiver number and Account number of the account to compare. Once a panel is selected, select Load and the selected panel model information appears to the right.

Show Like Models Only: If selected, any accounts with the same model number display below under Select

Accounts To Compare. If not selected, all accounts display regardless of model.

Show Like Versions Only: If selected, any panels with the same model number and same version display below under Select Accounts To Compare. If not selected, all panels with the same model display regardless of version.

Show Archive: This option displays for Account comparisons. If selected, archived panel programming versions are displayed under Select Accounts To Compare.

Options

Sort by Account: Select this option to have the spreadsheet report created where each account is compared to the template side-by-side in two columns and other accounts are compared below the first. If not selected, all accounts are compared to the template side-by-side in multiple columns.

Include Text Names: Select this option to have the spreadsheet report list differences in text names for the panel's zones, outputs, devices, etc.

Include Users: Select this option to have the spreadsheet report list differences in users for the accounts being compared.

Include Schedules: Select this option to have the spreadsheet report list differences in Schedules for the accounts being compared.

Include Profiles: Select this option to have the spreadsheet report list differences in User Profiles for the accounts being compared.

Saved Comparisons

Saved Comparisons option allows the selected compared accounts to be saved for future comparisons.

After selecting the accounts to compare, save the selected comparisons by typing a name directly into the drop-down menu box and selecting the Save button. The new comparison name displays in the drop-down menu.

To compare accounts with the same information as a saved comparison, select the comparison name from the drop-down menu and select Load. The information from the selected comparison displays in the Accounts To Compare fields.

To delete a saved comparison from Remote Link, select the comparison name from the drop-down menu and select Delete.

Select Accounts to Compare: All accounts to be selected for comparison display here. Select the accounts that you want to compare to the template or account selected above in the Control Panel. Select the account and press the arrow key to place the account in the right column for comparison. You may select as many as you would like to compare.

Accounts to Compare: This column displays all accounts that have been selected for comparison. If you need to remove an account from this column, select and select the arrow button to place the account back into the other column.

Save to: Select the name and location where you want the spreadsheet report saved.

Compare: Select this to create the spreadsheet report.

1.16.10. Exporting Data Reports

To export data reports as CSV (Comma Separated Value) files that can be opened in Microsoft® Excel, select File >> Print >> Data Export. The account open in Remote Link will be exported to a file that you have designated. It is recommended that you create a folder to save the programming because several files will be created when Data Export is selected. All files will have a .csv extension, which can be opened in Excel.

Location: Press the button to the right of the Location field to browse for the folder in which you will save the programming.

Prefix Filename with Account Number: Select this checkbox if you want all of the files to contain the account number in the file name. For example, a file name with the account number would read "1-12345 Area Information.csv."

Prefix Filename with Account Name: Select this checkbox if you want all of the files to contain the account name in the file name. For example, a file name with the account name included would read "John Doe Area Information.csv."

When the files have been exported, the Data Export Report Setup window will automatically close.

1.16.11. Printing a Saved Report

If you have saved a report and you now wish to print it, go to File >> Print >> Saved Report. Enter the filename of the saved report. Press the button to the right of the Filename field to browse for the saved report you wish to print.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen.

Print: Select this button to print the account reports to an attached printer.

Note: If you have the Advanced Reporting module, you can save reports in seven different formats.

1.17. Panel Menu

Use the Panel menu option to contact a panel for programming or downloading. The Panel menu also allows you to trap a panel to send and retrieve programming files and view details about the system status.

1.17.1. Connect

To connect to a panel, select File >> Panel Information to open the Panel Information window. Select the panel you wish to connect to by selecting the line for that account, then selecting OK.

You may also search for a specific account by typing the name or account number into the Search field. After selecting the desired panel account, select OK to open the account.

Now select Panel >> Connect to open the Connection Status window and select Connect. The Connection Status window will close after Remote Link has connected to the panel.

This option allows you to connect the Remote Link program to a subscriber's panel for programming, problem diagnosing, or downloading stored information.

Note: You may update the default panel account number from Remote Link by connecting to the panel with its default account number. The new file will overwrite the account number along with the remainder of the panel programming.

For example, a new panel has been installed with the factory default account number of 12345. First create the file with the appropriate account number, such as 33333. Open the file for account number 33333, then open the Connect window. In the Account field of the Connect window, remove 33333 and enter 12345. This will allow you to connect to the default panel. Select Connect. When the panel is connected, go to Panel >> Send. This will send the file for account number 33333. The panel account number is now 33333.

Inactivity Timeout

A timeout occurs if no activity (upload/download) is detected within 4 minutes and 30 seconds. At timeout, a message box appears and allows an operator to extend the connection. If an extension is not performed, Remote Link will disconnect with the panel 1 minute later. Remote Link must be communicating with the panel

using one of the following methods:

- The computer network card (NIC)
- The computers serial port to direct connect to a 462N Network Interface Card

For information on some error messages that may appear if your connection is not properly configured, see Connection Error Messages.

1.17.1.1. Connection Error Messages

Errors While Connecting

The following messages indicate an error has occurred while Remote Link is attempting to connect to a panel, but the connection cannot be established. You may also get an error message after the actual physical connection is established but you still cannot connect to the panel. See Errors after Connected for more information about these errors.

Error connecting, please make sure TCP/IP is installed: The computer is not properly configured for network communication. Consult the Windows help file for assistance.

Error connecting, invalid connection information: Possibly there is no COM port selected in File >> Panel Information. In the Panel Information window, select an unused COM Port from the drop-down list.

Error connecting, invalid connection information: Port (possibly in use). Another field in Remote Link Configuration or another application is using COM port. Verify that the COM Port selected in the Panel Information window is not the same as the COM Port selected in System >> Configure >> Remote Link (Remote Link Configuration window). Also verify that another application on the computer is not using a COM Port that is used by Remote Link.

Panel Connection Error: Timeout trying to call panel. No reply from panel. Check that receiver is getting dial tone and the Phone Number is correct in Panel Information.

Panel Connection Error: Timeout trying to initiate connection with receiver. Remote Link cannot get a reply from the receiver. Check the following settings and items:

- In System >> Configure >> Remote Link check the COM port in the Receiver Tab.
- Check the connection between receiver and computer.
- Verify that the proper cables are being used with the proper connector pinout.
- Verify that the receiver is getting power.

Panel Connection Error: Invalid connect response while calling panel. Remote Link did not receive proper reply from panel. Try again.

Errors after Connected

The following messages may occur after the connection has been made with the panel, yet the panel and Remote Link cannot communicate. The letters in parentheses, such as (-VA), after some error messages represents the actual message you would see when viewing the Diagnostics window (Alt + F10).

Panel Connection Error: Timeout. Remote Link did not receive a reply from panel.

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

Panel Connection Error: Receiver not authorized to connect. (-VA) This error message only applies to 1512,1812, 1912, and XR200 Command Processor™ Panels.

For 1512, 1812, and 1912 panels, the user must enter a valid User Code at the Remote Authorize menu. Disable this by 'turning off' Remote Authorize in panel's Menu Display, which can only be programmed using a keypad.

For XR200 panels, program Service Receiver to Yes. Go to Program >> Remote Options and select Yes from the drop-down menu next to Service Receiver. If Service Receiver is No, this message will appear when attempting to connect to the panel.

Panel Connection Error: Invalid receiver number. (-VR) The receiver key in the receiver that you are using does not match the previously stored key in the panel's Alarm Receiver or Service Receiver location of Remote Options. Use the correct receiver key (programmed through System >> Configure >> SCS-1 System) or program Service Receiver as Yes in Remote Options of the panel's programming.

Panel Connection Error: Invalid connect sequence. (-VD)

Panel Connection Error: Invalid remote key. (-VC). Panel's Remote Key does not match the Remote Key in the Panel Information window. Be sure that the Remote Key in the Panel Information window is the same as that programmed in the panel.

Panel Connection Error: Panel busy with other communication. (-VB)

Panel Connection Error: Panel not connected. (-VN)

Error requesting max partitions: Remote Link could not get the max partitions from the panel.

Connection cancelled: Action aborted by user.

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

1.17.2. Disconnect

To disconnect from a panel, select Panel >> Disconnect to open the Connection Status window. Select Disconnect.

1.17.3. Send

The Send function allows you to send a new or revised program file to a subscriber's panel.

Note: Close all Remote Link programming windows before sending the file to the panel.

To send a program file to a panel, select Panel >> Connect and connect to the panel. After selecting Panel >> Send, the Send to Panel window appears allowing you to send the data to the panel. As the file is being loaded, Remote Link tracks the status of the data transfer.

Before sending the file, you can also select to clear the codes, schedules, zone, and area information from the panel. Select Changes Only to send only the programming that has changed to the panel.

Select Update Time to send a time update to the panel.

Select Disconnect on Completion to automatically disconnect from the panel after the programming has been sent to the panel.

The Currently Sending section of the Send To Panel window tracks the status of the data transfer. The top bar indicates that communication is occurring between Remote Link and the panel. The bottom bar tracks the status of the entire file.

1.17.4. Retrieve

The Retrieve function allows you to retrieve a copy of a subscriber panel's programming, schedules, and user codes.

Note: Close all Remote Link programming windows before retrieving the file from the panel.

After selecting Retrieve, the Retrieve From Panel window appears allowing you to initiate the retrieval of data from the panel.

Select Request Events to automatically request the panel's events upon completion of the file retrieval.

Select Update Time to send a time update to the panel after Remote Link has retrieved the data from the panel.

Select Disconnect on Completion to automatically disconnect from the panel after the programming has been retrieved from the panel.

For XR150INT/XR350INT Series, XR150/XR350/XR550 Series and XR100/XR500 panels Version 204 or higher, select Changes Only to retrieve only the programming that has changed since the last connection with the panel.

XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series panels Version 117 or higher have additional retrieve options available. Refer to Requesting Events.

The Currently Receiving section of the Retrieve From Panel window tracks the status of the data transfer. The top bar indicates that communication is occurring between Remote Link and the panel. The bottom bar tracks the status of the entire file.

After the information has been retrieved, Remote Link displays a window with the message "Panel Retrieved."

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.

1.17.5. System Status

Select Panel >> System Status to open the System Status window. This window allows you to view the status of several system items from one convenient window.

The System Status window displays the status of the following.

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

The status for each item displays one of the following messages.

- Normal
- Trouble
- Not Used

The System Status window also allows you to access command and inquiry functions. Select the desired button from the bottom of the window.

1.17.5.1. Alarm Silence

The Alarm Silence option allows you to turn off the alarms connected to a panel.

To silence an alarm, select Command >> Alarm Silence. A pop-up window will appear with the message "Alarm silenced successfully."

If the alarm can not been silenced you will receive the message, "Unable to silence alarm."

1.17.5.2. Sensor Reset

The Sensor Reset option allows you to turn off the power on the panel's switched auxiliary power terminal for 5 seconds. This causes devices such as smoke and glassbreak detectors to power down and reset when the power is restored.

To execute a sensor reset, select Command >> Sensor Reset. A pop-up window will appear with the message "Sensors Reset Successfully" to notify you that the reset command completed successfully.

If the sensor reset command failed, a window will appear on your screen with the message "Unable to reset sensors."

1.17.5.3. Set Time and Date

This option allows you to synchronize the time and date in the panel with the time and date on your Remote Link computer.

When you select Set Time and Date in the System Status window, a pop-up window will appear with the message "Time and Date set successfully"

If Remote Link cannot set the time on the panel, you will see the message "Unable to set Remote Time and Date."

Note: The XR6 and XR10 panels do not have an internal clock.

1.17.5.4. Send Message

Send Message to a Keypad

The Send Message feature allows you to send a message to a panel that will display on the keypad or on a printer connected to the panel.

Select Send Message from the System Status window. Enter the message up to 16 characters long in the Message to Send field.

If you want to send the message to one or more keypads, select the Keypad option, then check the box beside each keypad that you wish to display the message. Select the Send button.

When the Send Message command is successful, you will see "Message Sent Successfully" in a pop-up window.

This message will cycle on the keypad display until it is turned off. To remove the message, you will need to send a blank message. In the Message to Send field, press the space bar once, then select Send.

To remove the message on-site, perform a panel reset.

Send Message to a Printer

If you wish to send the message to a printer connected to the panel, select the Printer option and select Send.

Note: If you send a message to a printer, there must be a printer connected to the panel that is turned on and ready to print. If the printer is not ready to print, your message will be lost. Remote Link will confirm that your message was sent to the panel successfully, but Remote Link cannot confirm that the message actually printed.

When the Send Message command is successful, you will see "Message Sent Successfully" in a pop-up window.

If no options are checked in Program >> Printer Reports, you will receive a "Printer not enabled" message.

Send a Service man Message

On model 1512, 1812, and 1912 panels, you may also use the Send Message feature to send a Service man message to the panel. Enter the message in the Message to Send field, select Service man, and select Send. When the technician on-site accesses programming at the panel, the Service man message will display on keypad address number one.

When the Send Message command is successful, you will see "Message Sent Successfully" in a pop-up window.

1.17.5.5. Area Status

Remote Link will display the arm/disarm status of all areas assigned to the panel in the Area Status window. You may arm or disarm each area individually. To open the Area Status window, select Panel >> System Status, and select Areas.

The Area Status window displays the following information.

- Area: The number of the area.

- Name: The name assigned to the area.
- Current Status: The current arm/disarm status of the area.
- Desired Action: Select Arm or Disarm from the drop-down menu to change the status of the area.
- Bad Zone Action: During remote arming, some zones in the selected areas may not be in a normal condition. Using the Bypass or Force option allows you to arm the normal zones within the area while bypassing or force arming the zones that are not in a normal state.
- Instant Arm: Checking this box allows the selected area to be instantly armed.
  Note: You cannot instantly arm all areas on All/Perimeter or Home/Sleep/Away systems.

How to Arm and Disarm

- To arm or disarm an active area, select that area from the Area Status list and select the arrow to open the drop-down menu, as shown in the picture above. Select Arm or Disarm form the drop-down list. Select the Arm/Disarm button near the bottom of the window to send that information to the panel.
- When you arm or disarm an area, a pop-up window appears to notify you of successful arming or disarming.

1.17.5.6. Zone Status

The Zone Status window allows you to view the status of all zones assigned to a panel. Select Panel >> System Status and select the Zones button to open the Zone Status window. This window displays any zone that is bypassed, force armed, open, shorted, or normal. The Zone Status window also allows you to bypass and reset selected zones.

To view the status of a zone, fill in the Start at Zone, Partition, and Area fields at the top of the window and select Request. Selecting the 24-hour box will display all 24-hour zones, such as Fire, Fire Verify, Supervisory, Emergency, and Panic zones.

1.17.5.7. Output Status

The Output Status window allows you to view the status of the relay outputs connected to a panel and grant Door Access events.

To view the status of outputs on a panel, enter an output number in the Start at Output Number field at the top of the window and select Request. The Status column below the Request button displays the current status of each output; Steady, Pulse, or Off.

1.17.5.8. Forgive User

The Forgive User option allows you to clear a failure to exit violation when using the anti-passback feature. When a user does not exit the premises with a valid code, the user must be forgiven before they are allowed to re-enter.

Partition: Enter the partition number that the user or users are assigned.

Note: This option does not appear on the XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panels.

User: Enter the user number that you wish to forgive an anti-passback violation.

All: Check this box to forgive all anti-passback violations.

1.17.5.9. LX-Bus Diagnostics

The LX Bus Diagnostics window allows you to perform remote diagnostic routines on LX-Bus zones. To open the LX Bus Diagnostics window, select Panel >> System Status and select LX Bus Diagnostics.

The LX Bus Diagnostics window displays the status of zones connected to the panel's LX-Bus that are not in a normal state.

XR550INT Series, XR550 Series, and XR500 Series panels	Zones 500 through 999
XR350 Series panels	Zones 500 through 799
XR150INT Series, XR150 Series, and XR100N Series panels	Zones 500 through 599
XR200, XR200-485(B) panels	Zones 100 through 199 for LX-Bus 1 and Zones 200 through 299 for LX-Bus 2

If an LX-Bus zone is not in a normal state, you will receive one of three messages.

Missing: The zone expander is not responding to polling from the panel.

Overlap: Two or more zones are sharing the same bus address.

Extra: Zones are detected that have not been programmed.

If an LX-Bus zone is in a normal state, it will not appear in this window. The purpose of the LX Bus Diagnostics window is to track problems with zones that are not in a normal state.

The LX Bus Diagnostics window will only display information about zones connected to the panel's LX-Bus, and will not display information on zones connected directly to the panel or connected to the keypad bus.

1.17.5.10. ZWave Devices Status

Each tab displays a list of Z-Wave devices that are currently programmed in the panel. Select each tab to see a list of that device Number, Name, State, and Settings.

Request: Select the Request button to retrieve the list of Z-Wave devices currently programmed into the panel.

1.17.5.11. Bad Zone Action

During remote arming, some zones in the selected areas may not be in a normal condition. Use the Bypass or Force option to arm the normal zones within the area while bypassing or force arming the zones that are not in a normal state.

Note: If a priority zone is in a bad state, you will not be able to arm the area until the priority zone is restored to normal.

1.17.5.12. Area Status Messages

When you arm or disarm an area using the Area Status window, you will see one of the following pop-up messages indicating the action performed.

- Armed successfully.
- Armed successfully. Some zones have been bypassed.
- Armed successfully. Some zones have been Force Armed.
- Disarmed successfully.
- Unable to disarm. Command disabled in panel. The remote disarm option has been disabled. To enable remote disarming, check the Remote Disarm box in Program >> Remote Options.
- Unable to arm. # bad zones. The area(s) cannot arm because there are non-bypassable zones faulted.

1.17.5.13. Zone Bypass / Reset

To bypass a zone, select the zone from the list in the Zone Status window and select Bypass. The zone remains bypassed until reset from Remote Link, reset from the keypad User Menu, or when the area is disarmed.

Note: Use caution when bypassing. Be certain of the zone type and the implications of bypassing before attempting to bypass a zone.

To reset a zone, select the appropriate bypassed zone from the list in the Zone Status window and select Reset. This removes the bypass from that zone.

1.17.5.14. Outputs On/Off

The Outputs Status window allows you to remotely turn on or off any of the output relays on a panel. You may specify Steady, Pulse, Momentary, or Off for any of the outputs.

To control the output relays, select the Output tab near the bottom of the window. Then type the number of the output in the Output field at the bottom left corner of the Output Status window. You may also select an output from the list by selecting once on that line.

After selecting an output, chose which action you wish to apply to that output by selecting one of the four buttons at the bottom of the window.

Steady: To activate the output continuously.

Pulse: To activate the output to pulse at 1-second intervals.

Momentary: To activate the output one time for 1 second.

Off: To turn off the output.

1.17.5.15. Door Access Control

The Output Status window allows you to lock and unlock doors and grant door access. Select the Door tab near the bottom of the Output Status window.

The Door feature allows you to remotely activate the door access relay on Security Command keypads, Easy Entry keypads, and 733 or 734/734N/734N-WiFi Wiegand Interface modules. You must know the address number of the keypad or 733 or 734/734N/734N-WiFi module to which the door strike is connected.

There are three commands available under the Door tab:

Lock: Lock the specified door.

Unlock: Unlock the specified door.

Access: Unlock the specified door for 5 seconds.

1.17.5.16. Lockdown

Select the Lockdown button to remotely lock all doors programmed as Public Doors in Device Setup. This feature can be used in emergency situations where it is necessary to restrict the site's access to authorized users only.

When the Lockdown button is pushed, Remote Link sends a message to the panel to turn off the output door relays for the Public Doors programmed in Device Setup. The relays then stay off until the next scheduled on time.

During a Lockdown, access cards can still be used to access or egress the area.

Note: The Lockdown feature is available for XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series panels only.

1.17.6. Request Events

To open the Request Events window, select Panel >> Request Events.

This option allows you to download a subscriber panel event buffer into the Remote Link database.

All Panels

Select Disconnect on Completion to automatically disconnect from the panel after the panel event buffer is

downloaded into the Remote Link database.

Note: Press the Alt key and F10 key to view the messages in the Diagnostics Window as the panel is receiving events. Open the Diagnostics Window before selecting Request.

To continue, select Request. While Remote Link retrieves the events, a status bar appears on your screen that tracks Remote Link status while downloading events.

Each time you request events from a panel, Remote Link stores those events in a buffer until you request events again from the same panel.

XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series panels

The Request Events window provides two options to identify the types of events to request from the panel. Check the boxes in the Request Events window to download Standard or Door Access events separately

Standard: Requests all events except door access events.

Door Access: Requests only Door Access events.

XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series

The Request Events window allows you to choose all events stored in the panel event buffer, new events that have occurred since the last download, or only those events that occurred during the time period selected in the Start and End dates.

Dates to Include

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 previous to 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.

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.

1.17.7. Trapping A Panel

This option allows you to initiate a trap so that when a subscriber's panel contacts the SCS-1 or SCS-1R Receiver or SCS-105 Single Line Receiver, it is held on-line and will be connected to with Remote Link.

Note: In order for the user to initiate a trap, the user must have permission to do so. Permission to Allow Trap can be given in the Operator Configuration screen of Remote Link. Permission must be given before the user can initiate a trap.

To create a trap, go to Panel >> Trap. Select New and enter the account number of the panel that you wish to trap with the receiver number as a prefix (for example, . 1-12345). After you enter the account number in the New Trap window, select OK to return to the Trap window. Select the options for the trap.

If you program a new Trap and do not select any options in the Trap window, Remote Link will hold the panel on-line and notify the operator that the panel is holding.

Options

Send File: Select this option to send the entire panel programming to the panel from Remote Link.

Changes Only: Select this option to send only programming that has changed since the last communication with the panel. To send changes only, select both the Send File and the Changes Only boxes.

Retrieve File: Select this option to retrieve the full panel programming from the panel to Remote Link.

Request Events: Select this option to automatically download the panel's event buffer into the Remote Link database.

Note: The Remote Update and Change File options are only available on XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100N/XR500N Series, XTLtouch/XTLplus Series, and XT30/XT50 Series Version 123 firmware and Level M hardware panels using TCP trap.

Remote Update: Automatically download the selected software file to the trapped panel. Check this box to enable the Change File option.

Change File: Select to browse and select the software update file location. When selected, the path to the update file automatically displays.

If you decide to cancel a trap before it occurs, select the appropriate panel in the Trap window and select Delete.

1.17.7.1. Set All Traps

Selecting Set All Traps from the Panel Menu sends all of the traps you have created in the Trap window. This allows you to easily send traps after the SCS-105 has been reset while you have Remote Link open.

Note: In order for the user to initiate a trap, the user must have permission to do so. Permission to Allow Trap can be given in the Operator Configuration screen of Remote Link. Permission must be given before the user can initiate a trap.

1.17.7.2. Trap Query

Note: In order for the user to initiate a trap, the user must have permission to do so. Permission to Allow Trap can be given in the Operator Configuration screen of Remote Link. Permission must be given before the user can initiate a trap.

This option is used to view the status of panel trap messages stored in the receiver SCS-101 or SCS-104. The Trap Query window remains empty until the Request button is selected. Remote Link then queries the SCS-101 or SCS-104 configured in the TCP Trap tab in Remote Link Configuration. A new window displays the status of stored panel trap messages. The status displays as Waiting, Sent, Failed, or Expired. The SCS-101 or SCS-104 can store up to 50 panel trap messages at a time.

Note: Remote Link only supports the use of one SCS-101 or SCS-104 for network panel trapping. If you wish to send panel trap messages to a second SCS-101 or SCS-104, the Trap Server Address configured in Remote Link Configuration >> TCP Trap tab must to be changed to the second SCS-101 or SCS-104 IP address.

1.17.7.3. Hangup

This option is for use after a subscriber's panel has dropped off line. An attempt to send data to the panel results in a communication error box.

Selecting Hangup forces the receiver to release the phone line and restore its on-hook status.

Note: Do not use Hangup to disconnect from a panel while still on-line. Always use Disconnect to terminate the connection.

Part 1. Panel Programming

1. Programming Menu

Use the Programming menu to change programming options in a panel or database file.

Panel programming options can also be changed by a service technician at the premises. Changes made to a panel from a keypad in the field may not match an account file saved in the Remote Link database. You may wish to verify whether any changes have been made to the panel programming from the keypad by retrieving the account information from the panel. To do this, select Panel >> Retrieve and select Retrieve. Depending upon the panel model and configuration, it may take several minutes or more to download this information from the panel.

There are two buttons at the bottom of each window in the Programming menu, one pointing left and one pointing right. These arrows lead to the previous or next item in the Programming menu, making it easier to move through the programming windows.

Each panel from DMP offers different features. Remote Link displays only the features in the Program menu that are available on the panel with which you are connected. For more complete descriptions of the various Program menu options, refer to the appropriate programming guide for the panel model that you are programming.

2. Communications

The Communications window is used to configure the panel's communication options. The Communications window automatically configures itself to show only the features available to the panel to which you are connected.

The Communications window uses index tabs to divide the program items into four groups.

Method: The features under the Method Tab allow you to set Communication Type, Second Line type, Second Line Test, Events Manager, DTMF, Transmit Delay, and Host/Net Setup.

Test Timer: The Test Timer Tab lets you schedule the automatic recall test of the panel's main and backup communication lines.

Receiver 1: Use the Receiver 1 Tab to instruct the panel to send Alarm, Supervisory/Trouble, Opening / Closing and User, Test Timer, and Door Access reports to Receiver 1.

Receiver 2: The Receiver 2 Tab allows you to send Alarm, Supervisory/Trouble, Opening / Closing and User, Test Timer, and Door Access reports to Receiver 2.

Host/Net: The Host/Net Tab provides additional options when Host/Net is selected as the communication type.

Note: XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series panels version 200 or higher uses Communication Paths instead of Method Tab.

2.1. Method Tab

The Method Tab allows you to program the method of which the panel will communicate with the receiver.

Connection: Select the Communication Type for the panel.

Other: Select the panel's Main Account Number, the Transmission Delay, and Events Manager.

Second Line: Select the backup communication type for the panel.

2.1.1. Connection

Communication Type: Select the communication format you want the panel to use when contacting a receiver. The panel uses the format you select for sending alarm, trouble, and supervisory reports to the receivers

programmed under the Receiver 1 and Receiver 2 tabs.

Note: Refer to Account Number Conventions for information about account numbers and communication types.

The options available for Communication Type are listed below.

None: Select None when you are programming local systems. Selecting None ends communications programming. When Main Communication is set to None and there is an unrestored system trouble, the keypad sounds every day at 10:00 am.

WiFi: Network communication to SCS-1R or SCS-VR Recievers.

Contact ID: Select Contact ID for communication to SCS-1R receivers using the Ademco Contact ID format.

Host or Net: Allows the panel to communicate using asynchronous communication through a Network Interface Card or an onboard network connection. The panel transmits the DMP Network/Output reporting format over a data network to the SCS-1 or SCS-1R Receiver. When Net or Host is selected as the communication type, the Net or Host Tab is enabled allowing you to configure the network communication options. After selecting Host or Net for the Main communication type, the Host or Net tab is enabled allowing you to configure the network communication options.

Note: When Network or Host is selected, Backup Type allows you to select D2 for two-line supervision when using a Model 893 or 893A Dual Phone Line module or RS-232 for radio backup communications using the RS-232 connector on the XR500N or XR500E panel v121 or earlier.

When NET or NET with NET BACKUP is selected, 2ND LINE is None, and a message fails to transmit to the primary receiver or secondary receiver (if programmed), only the first buffered message is attempted until communication is restored. After communication is restored, all buffered messages are sent.

Digital Dialer: Select Digital Dialer when you are using DMP's proprietary (SDLC) format for communication over standard telephone lines to an SCS-1, SCS-1R or SCS-105 receiver.

All zone alarms and restorals transmitted by the panel on the host channel are also duplicated on the communication line selected under Backup Type.

Cellular Network: Allows the panel to communicate to using the 263C or 263H Cellular Communicators. When Cellular Network is selected, Backup Dialer and Backup Cell is not available for backups on the XT30/XT50.

On XR100/XR500 Series panels version 118-121, Cellular Network displays on the Backup Type menu if CID or DD is selected under Communication Type. When you select Cellular, the panel sends signals on the second (backup) communication line with Cell-Miser restrictions.

Cellular is only allowed as Second Line for XR200 Series and XR2400F Series control panels.

Modem IIe (M2E): Select Modem IIe for communication to non-DMP receivers using the Radionics Modem IIe format. This communication option is not available on the XR150/XR350/XR550 Series, XR100/XR500 Series, XT30/XT50 Series, XT30INT/XT50INT, XTLC, XTLN, or XTLN-WiFi panels.

4-2: Select 4-2 for communication to non-DMP receivers that can only process data in the 4-2 format. This communication option is not available on the XR150/XR350/XR550 Series, XR100/XR500 Series v121 or earlier, XT30/XT50 Series, XTLC, XTLN, or XTLN-WiFi panels.

Multiplex (MPX): On XR200, XR200-485, and XR2400F panels, Multiplex allows the panel to communicate using multiplex communication to a SCS-1 Receiver using a polled communication line. Alarm and system information transmit 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/SCS-1R Receiver to maintain constant supervision.

DTMF: When DTMF is checked, the panel dials using Dual-Tone Multiple Frequency (touch-tone) dialing. When this box is empty, the panel uses pulse dialing.

2.1.2. Second Line

XR500/XR100 Series Version 121 or earlier has a Second Line section.

Backup Type: In the Backup Type drop-down menu, select the mode of communication for the backup communication line. The options available in the Backup Type menu are:

Note: XR100/XR500 Series panels Version 200 or higher uses Communication Paths instead of Communications >> Method.

Cellular (Cell): On XR100/XR500 Series panels Version 118 - 121, Cellular displays on the Backup Type menu if CID or DD is selected under Communication Type. When you select Cellular, the panel sends signals on the second (backup) communication line with Cell-Miser restrictions. Select this if your backup communication method is through a cellular communicator.

Host or Net (HST or NET): On XR100/XR500 Series panels Version 118 - 121, Network displays on the Backup Type menu if CID or DD is selected under Communication Type. Allows the panel to communicate using asynchronous communication through a Network Interface Card or the onboard network connection port. The panel transmits the DMP Network/Output reporting format over a data network to the SCS-1 or SCS-1R Receiver. When Net or Host is selected as the communication type, the Net or Host Tab is enabled allowing you to configure the network communication options. If Host/Net is selected under Communication Type, you cannot select Host or Net as the second (backup) line.

D2: D2 displays on the Backup Type menu if Host or Net is selected under Communication Type. Select D2 to supervise a second telephone line using an optional Model 893 or 893A Dual Phone Line module.

RS-232: On XR500 Series version 118 - 121, RS-232 displays on Backup Type menu if Network is selected under Communication Type.

Messages are sent using RS-232 after they have failed to communicate with the programmed Primary NET IP and Backup IP. Select RS-232 when using DB-9 backup communications by directly connecting to the RS-232 port on the panel. Set the panel jumper to R and briefly reset the panel using the reset jumper to activate RS-232 operation. Refer to the XR500 Series Installation Guide (LT-0679).

When Net Backup is YES and a Modem String is programmed, an Automatic Recall Test is sent using the RS-232 line based on the normal programming selections in Test Frequency, Net Fail Time, Defer Test Time, and Test Time options just as they do for DD. When the RS-232 Automatic Recall Test fails to communicate, a Warning: Panel Backup Communications Fail (S12) report is sent using the Primary NET IP. The next time the panel successfully sends a report over the 2ND LINE, a Backup Communication Line Restore (S04) report is sent.

None: When you select None, the panel does not send signals on the second (backup) communication line.

Digital Dialer (DD): Select Digital Dialer when you are using DMP SDLC format for communication over standard telephone lines to an SCS-1, SCS-1R or SCS-105 receiver.

2.1.3. Backup

XT30/XT50 Series has only two choices for a backup to the primary connection.

Backup Dialer: Backup Dialer option is available if Communication is set for Network. The Backup Dialer tries to send the message after the main communication fails on Network. If the backup dialer fails then the message is discarded.

Backup Cell: Backup Cellular option is available if Communication is set for Network, Contact ID or Direct Dialer. The Backup Cellular tries to send the message after the main communication fails for 60 seconds on Network and 10 dial attempts using Direct Dialer or Contact ID. If the backup dialer fails then the message is discarded.

Note: When Cellular Network is selected as Connection >> Communication Type, no backup is available.

2.1.4. Other

Main Account Number: This is the account number that the panel uses to report all system troubles, fire alarms, supervisory alarms, and automatic recall tests.

Note: Refer to Account Number Conventions for information about account numbers and communication types.

Transmission Delay: Enter the length of time that you want the panel to wait before sending burglary reports to the central station. Select a time from 1 to 60 seconds. Alarm bells and relay outputs are not delayed during this period. Enter 0 (zero) to disable transmission delay.

Events MGR (XR100/XR500 Series panel Version 121 or earlier): The Events Manager menu specifies when the panel will send non-alarm reports.

Events Manager does not affect zone alarm, zone trouble, zone restoral, supervisory, or serviceman messages. Also, this feature will not delay closing reports if Closing Wait is checked in Program >> System Options.

Note: The Events Manager menu is not available on XT30/XT50 Series, XT30INT/XT50INT Series, XTLplus/ XTLtouch, XTLC, XTLN, or XTLN-WiFi panels.

The following three items are the options in the Events Manager menu.

- Send Events Immediately - All reports are sent to the receiver as they occur.
- Delay Events - All non-alarm reports are held until the panel memory buffer contains 12,000 events on the XR100/XR500 for the past 45 days. Any event older than 45 days automatically clears from the system memory. Also, once the full 12,000 events are stored, any new event causes the oldest event to be cleared.

Note: Network communication does not delay reports but send them as they occur.

- Keep Events - All non-alarm reports are held in the panel memory buffer until they are overwritten by new activity.

Note: Contact ID and Modem IIe (M2E) do not delay or keep events, but send them as they occur.

2.2. Test Timer Tab

Second Line Test (XR100/XR500 Series v121 or earlier): Allows you to test your backup communication line.

The options in the Second Line Test menu are the following four items:

None: When you select None, the panel does not send a test signal on the second (backup) communication line.

Regular: When you select Regular, the second line will test each time that your main communications line is programmed for a test.

Weekly: When you select Weekly, the second line sends a test once per week. When Second Line Test is set to Weekly, the panel disregards test time deferrals (see Defer Test below).

Monthly (30 days): When you select Monthly, a test of the second line will be sent every 30 days. When you select this option the panel disregards test time deferrals (see Defer Test below).

Note: On XT30/XT50 Series panels, the backup communication is tested at the same frequency as the main communication.

Test Time: Enter the time of day that the panel transmits an automatic recall test for the main communication line. This test signal will verify that communication is working properly between the panel and the central station. Enter entries between 12:00 AM to 11:59 PM.

Test Days (XT30/XT50, XTLplus/XTLtouch, XT30INT/XT50INT Series, XR100/XR500 Series V121 or earlier): Select how often the panel sends a test signal using the main and backup communication paths to the central station. Only the communication paths that are programmed are available.

Net Test Days (XTLN, XTLN-WiFi, XT30/XT50, XTLplus/XTLtouch): Select how often the panel sends a test signal using network communication to the central station.

Cell Test Day (XTLplus/XTLtouch, XTLC): Select how often the panel sends a test signal using cellular communication to the central station.

Defer Test: Select Yes to allow the panel to defer the programmed automatic recall test. Select No to send the test report as programmed, regardless of the previous panel communication. Test Frequency must also be programmed when Defer Test is set to Yes. Not Available on XT30INT/XT50INT Series, XT30/XT50 Series, XTLplus/XTLtouch, or XTL Series panels.

Test Frequency: This allows you to specify, from 1 to 60 days, the maximum length of time between automatic recall tests. Not Available on XT30INT/XT50INT Series, XT30/XT50 Series, or XTLplus/XTLtouch Series panels.

Example: Two panels, A and B, are programmed the same: Defer Test is set to Yes and Test Frequency is set to 7.

Panel A: Panel A sends no signals to the receiver during the seven day Test Frequency cycle. On the seventh day Panel A sends the automatic recall test to the receiver.

Panel B: On the third day of the seven day Test Frequency cycle, Panel B sends a signal to the receiver. The automatic recall test is not sent to the receiver because Panel B has communicated with the receiver during the programmed Test Frequency cycle. The seven day cycle is restarted at the time the signal is received.

Note: These two fields, Defer Test and Test Frequency, should have the same value as the Auto Recall Frequency and Allow Test Deferrals fields in File >> Panel Information >> Extended Panel Information.

2.3. Receiver 1 Tab

Alarms: Sends Abort, Alarm, Alarm Restoral, Ambush, Exit Error, and System Recently Armed reports to Receiver 1.

Supervisory Troubles: Sends Supervisory, Trouble, Trouble Restoral, Force Armed, Zone Fault reports, and Serviceman Messages to receiver 1.

Opening / Closing and User: Sends Opening, Closing, Door Access, Late to Close, Unauthorized Entry, Schedule and Code changes, Zone Reset, and Zone Bypass reports by user to Receiver 1.

Test Report: Enables the panel to send the automatic recall test report to Receiver 1. The panel sends the automatic recall test reports as determined by the programming in the Test Timer tab.

Backup: Enables Receiver 1 to serve as a backup for Receiver 2 if Receiver 2 does not respond to communication attempts by the panel. Not Available on XT30INT/XT50INT Series, XT30/XT50 Series, or XTLplus/XTLtouch Series panels.

1st Phone No.: Enter the primary phone number for communications with Receiver 1.

2nd Phone No.: Enter the secondary phone number for communications with Receiver 2.

Note: You may program a 3-second pause in the dialing sequence by entering the letter P. You may also program a dial-tone detect by entering the letter D.

The following features are available for XR100/XR500 Series panels only.

XR100/XR500 Series Characters: For the 1st and 2nd phone numbers, entering the letter P programs a 2-second delay in the dialing sequence. Panels do not require a dial tone detect D. Dial tone detect is an automatic XR500 Series panel function.

Note: You can place the "* 7 0 P" (Star, Seven, Zero, Pause) in the telephone number first position to cancel Call Waiting. For example, program NET with second line DD and phone number *70P555-1212, and you have NET with Call Waiting canceled on the second line.

Caution: A call waiting cancel programmed on a non-call waiting telephone line, would prevent communication to the central station.

XR500 Series/XR100 Series Area Code Selection for Cellular Communication: You can also enter a letter C in the

first or second telephone number. When entered, the characters before the C are only used with a 2nd LINE Cellular call is being made. All other calls made on the main phone line only use the characters entered after the letter C. The letter C is never dialed and is recognized by the panel as a marker only. The C character counts as part of the 32 allowable characters.

XR500 Series/XR100 Series Automatic CID Communication: You can place a letter T in the telephone number first position to allow a message to be sent to the receiver using CID communications. Once the CID message is sent, subsequent messages are sent using the communications method selected under Communication Type until another telephone number with a T in the first position is encountered. This option allows capture by AES radio or CID backup communication to a CID receiver using a specific telephone number.

The automatic backup CID communication feature allows for the following communication options:

DD with CID second number

NET with DD second line

NET with CID second line

NET with DD/CID second line

For example, program NET with second line DD and phone number T555-1212, and you have NET with CID second line.

XT30/XT50 Series (Version 103 or higher), XT30INT/XT50INT, XTLplus/XTLtouch, XTLC, XTLN, and XTLN-WiFi panels

1st IP Address: Enter the first (primary) IP address where the panel sends network or cell messages. The IP address must be unique and cannot be duplicated on the network. Enter all 12 digits and leave out the periods. For example, enter IP address 192.168.0.250 as 192168000250. The periods display automatically.

Note: For Network: The first and second IP addresses are alternately used for 8-second intervals until successful communication or 1 minute elapses.

1st IP Port: Enter the first IP port number to be used in conjunction with the First IP Address. The IP port identifies the port used to communicate messages to and from the panel. The default IP Port setting is 2001. The default IP Port setting for XT30INT/XT50INT is 3001.

2nd IP Address: Enter the second IP address where the panel sends network messages. The IP Address must be unique and cannot be duplicated on the network.

2nd IP Port: Enter the second IP port number to be used in conjunction with the Second IP Address. The IP port identifies the port used to communicate messages to and from the panel. The default IP Port setting is 2001. The default IP Port setting for XT30INT/XT50INT is 3001.

Door Access (XR500 Series, XR100 Series, and XR200-485 only): Sends door access granted reports to Receiver 1.

Note: The door access granted report is only sent if the device number has also been selected in Access Keypad Enable in the System Reports window.

2.4. Receiver 2 Tab

Alarms: Sends Abort, Alarm, Alarm Restoral, Ambush, Exit Error, and System Recently Armed reports to Receiver 2.

Supervisory Troubles: Sends Supervisory, Trouble, Trouble Restoral, Force Armed, Zone Fault reports, and Serviceman Messages to receiver 2.

Opening / Closing and User: Sends Opening, Closing, Door Access, Late to Close, Unauthorized Entry, Schedule and Code changes, Zone Reset, and Zone Bypass reports by user to Receiver 2.

Test Report: Enables the panel to send the automatic recall test report to Receiver 2. The panel sends the

automatic recall test reports as determined by the programming in the Test Timer tab.

Backup: Enables Receiver 1 to serve as a backup for Receiver 2 if Receiver 2 does not respond to communication attempts by the panel. Not Available on XT30INT/XT50INT Series or XT30/XT50 Series panels.

Pager Direct

This option allows the panel to send Alarm, Trouble, Opening and Closing, and Late to Close reports to a customer's alphnumeric or numeric pager (numberic only with XRSuper6). The panel uses DTMF or modem tones to generate the account and report information sent over the pager terminal equipment.

Pager Type

None - Select NONE allow you to use the Receiver 2 programming to send panel reports to a second central station receiver.

Alpha - Reports are sent to the customer's alphanumeric pager.

Num - Reports are sent to the customer's numeric pager.

1st Phone No.: Enter the primary phone number for communications with Receiver 1.

2nd Phone No.: Enter the secondary phone number for communications with Receiver 2.

Note: You may program a 3-second pause in the dialing sequence by entering the letter P. You may also program a dial-tone detect by entering the letter D.

The following features are available for XR100/XR500 Series panels only.

XR100/XR500 Series Characters: For the 1st and 2nd phone numbers, entering the letter P programs a 2-second delay in the dialing sequence. Panels do not require a dial tone detect D. Dial tone detect is an automatic XR500 Series panel function.

Note: You can place the "* 7 0 P" (Star, Seven, Zero, Pause) in the telephone number first position to cancel Call Waiting. For example, program NET with second line DD and phone number *70P555-1212, and you have NET with Call Waiting canceled on the second line.

Caution: A call waiting cancel programmed on a non-call waiting telephone line, would prevent communication to the central station.

XR500 Series/XR100 Series Area Code Selection for Cellular Communication: You can also enter a letter C in the first or second telephone number. When entered, the characters before the C are only used with a 2nd LINE Cellular call is being made. All other calls made on the main phone line only use the characters entered after the letter C. The letter C is never dialed and is recognized by the panel as a marker only. The C character counts as part of the 32 allowable characters.

XR500 Series/XR100 Series Automatic CID Communication: You can place a letter T in the telephone number first position to allow a message to be sent to the receiver using CID communications. Once the CID message is sent, subsequent messages are sent using the communications method selected under Communication Type until another telephone number with a T in the first position is encountered. This option allows capture by AES radio or CID backup communication to a CID receiver using a specific telephone number.

The automatic backup CID communication feature allows for the following communication options:

DD with CID second number

NET with DD second line

NET with CID second line

NET with DD/CID second line

For example, program NET with second line DD and phone number T555-1212, and you have NET with CID second line.

1st IP Address: Enter the first (primary) IP address where the panel sends network or cell messages. The IP address must be unique and cannot be duplicated on the network. Enter all 12 digits and leave out the periods. For example, enter IP address 192.168.0.250 as 192168000250. The periods display automatically.

Note: For Network: The first and second IP addresses are alternately used for 8-second intervals until successful communication or 1 minute elapses.

1st IP Port: Enter the first IP port number to be used in conjunction with the First IP Address. The IP port identifies the port used to communicate messages to and from the panel. The default IP Port setting is 2001

2nd IP Address: Enter the second IP address where the panel sends network messages. The IP Address must be unique and cannot be duplicated on the network.

2nd IP Port: Enter the second IP port number to be used in conjunction with the Second IP Address. The IP port identifies the port used to communicate messages to and from the panel. The default IP Port setting is 2001.

Door Access (XR500 Series, XR100 Series, and XR200-485 only): Sends door access granted reports to Receiver 2.

Note: The door access granted report is only sent if the device number has also been selected in Access Keypad Enable in the System Reports window

2.5. Host or Net Tab

The Host or Net Tab is available only if the communication type is set to Host or Net. Host communication requires your SCS-1 Receiver to have firmware version 805 or higher.

2.5.1. XR500N/ XR100N Series Panels v121 or earlier NET Tab

XR100N/XR500N Series Control panels Version 121 and earlier

Receiver IP: Enter the IP address of the receiver programmed in the Receiver 1 Tab. This address is used to communicate messages over the network.

Receiver Port: Enter the port of the receiver. The default port is 2001.

Net Setup String: Enter a dial string up to 32 characters long for the panel to send to the onboard Ethernet connector or a network device connected to a 462N Network Interface Card. You may also enter an IP Address with a setup string. If you are using a non-DMP network device such as a CDPD Modem, refer to the device literature for the setup string. The default port number is 2001.

If Net Backup is not enabled and the device connected to the 462N card is a DMP network device, do not enter the Net Setup String in this field. If the device is not a DMP network device, enter the device Net Setup String in this field.

If Net Backup is enabled and you are using the onboard Ethernet connector and one 462N Card, enter the Net Setup String for the second network device. The Net Setup String is sent to the second network device, such as a cellular modem, which sends the messages to the receiver.

Note: If NET Backup and UL AA are enabled, the panel only sends the S72 (WARNING: NETWORK TROUBLE) message after the first series of network message attempts fails.

Retry Time: Enter the number of seconds (3 to 15 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. For example, if Retry Time is set to 15, the panel retries four times. The default Retry Time is 5 seconds.

Net Backup Enable: Check the Net Backup Enable checkbox to enable Net Backup and require panel messages to be sent to a backup IP Address if the messages fail to communicate to the remote (primary) IP address. Leave the box empty to disable Net Backup. For more information about the Net Backup feature, refer to Host/Net

Backup Examples in the help file.

When Net Backup is enabled and the J23 jumper on the XR500 panel is set to R, panel messages are sent through the RS-232 serial port.

Note: Second line programming is available for dialer communication types such as CELL or DD to backup network communications.

Supervised Backup Enable: Check the Supervise Backup Enable checkbox to enable supervised communication and send checkins to the network Central Station receiver for the Network Backup. Leave the box empty to disable supervised communication.

Programming options for supervision of Network Backup is provided by the same options used by the Communications Type programming for UL AA, Check In Time, and Fail Time. If Substitution Code is enabled, then it is automatically enabled for Network Backup. When Supervise Backup is enabled, Net Trouble only displays on the keypad if both primary and backup IP address communications fail.

UL AA Enable: Select the box to enable UL AA Mode. UL AA involves check-in reports. Check-in reports are a method of supervising the panel communication with the receiver. To be UL AA compliant, panels must check-in with the receiver every 6 minutes when armed. By default, UL AA is not enabled.

The SCS-1 or SCS-1R Receiver verifies that the next Check-in report is received at the appropriate time. SCS-1 version 805 or higher firmware is required in the SCS-1 Receiver. When UL AA is enabled and the check-in fails after one minute, the panel sends a WARNING: NETWORK TROUBLE (S72) report on the 2ND LINE. The next time the NET report is successfully sent, the panel sends a NETWORK RESTORED (S73) report over the 2ND LINE.

Note: Network Trouble, Network Fail Notification, is automatically enabled when UL AA is enabled. Network Trouble allows the panel to detect a failure of the primary network and send an S72, Network Trouble message, through the DD if it is programmed as the second line. When the primary network restores the panel sends an S73, Network Restored, message.

Disarm Check-in: If you enable UL AA, this field displays. Enter the number of minutes, from 1 to 6 or R, between disarmed check-in reports. If any area is armed, the report is automatically sent every 6 minutes.

Enter R in the Disarm Check-in field to program the panel to send the check-in report at random times, but always between 5 to 60 minutes.

Substitution Code Enable: If UL AA is disabled, the Substitution Code Enable field is enabled. Check the box if the panel sends a Panel Substitution Code when communicating with the receiver. The Panel 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. By default, the Substitution Code is not enabled. When UL AA is enabled, the substitution code is always sent.

Check-in Time: If you disable UL AA, enter the number of minutes, from 0 to 240, between check-in reports. This occurs when the panel is armed or disarmed. Check-in reports are a method of supervising the panel for communication with the receiver. When 0 (Zero) is entered, the check-in feature is disabled. By default, the Check-in Time is 6 minute.

Fail Time: Allows the receiver to miss multiple check-ins before logging that the panel is missing. For example, if Check-in Time is set to 10 and Fail Time is set to 30, the receiver only indicates a Panel Not Responding after 30 minutes. The panel attempts to send the message every 10 minutes.

The Fail Time must be equal to or greater than the Check-in Time. For example, if the Check-in Time is 10 minutes, the Fail Time should be 10 minutes or more. The maximum Fail Time is 240 minutes. By default, the Fail Time is 6 minute.

Notify Network Trouble: Sends a notification when there is trouble with the network. When UL AA is enabled, this feature is automatically enabled. When Notify Network Trouble is enabled and the panel detects a failure of

the primary network, the panel sends an S72, Network Trouble message, through the digital dialer (DD) if it is programmed as the second line. Also, the trouble keypads sound a continuous tone and display "NETWORK - TRBL." Press any key to silence the tone.

When the primary network restores the panel sends an S73, Network Restored message, through the digital dialer (DD) if it is programmed as the second line. The "NETWORK -TRBL" display is removed from the keypad and the tone automatically silences.

Net Test Enable: Check this box to send an S97 network communication test message to the Central Station receiver over the network based on the Test Time and frequency programmed in Communications.

Note: The S97 test message is specific to network operation. The S88 and S07 messages are specific to and only sent using the digital dialer. Having separate test messages for network and digital dialer operation allows the Central Station to identify the communication path used to send the message.

Net Fail Test: The time programmed in Net Fail Test increases the dialer test frequency programmed in Test Time during a network failure. Select a 2, 4, or 8-hour interval between digital dialer contact attempts. The digital dialer sends an S88, Automatic Recall Unrestored System message or an S07, Automatic Recall Test message at the programmed minutes indicated in the Automatic Recall Test Time. Select 0 (zero) to disable more frequent digital dialer testing when NET communications fail. Default is 0 (zero).

2.6. Advanced Communication Tab

XT30/XT50 Series Panels (Version 102 or earlier)

1st IP Address: Enter the first (primary) IP address where the panel sends network or cell messages. The IP address must be unique and cannot be duplicated on the network. Enter all 12 digits and leave out the periods. For example, enter IP address 192.168.0.250 as 192168000250. The periods display automatically.

Note: For Network: The first and second IP addresses are alternately used for 8-second intervals until successful communication or 1 minute elapses.

For Cellular: The message is sent using First GPRS APN and the First IP Address. If no acknowledgment is received, First GPRS APN and the Second IP address are used, followed, if needed, by Second GPRS APN and first and second IP addresses, respectively.

1st IP Port: Enter the first IP port number to be used in conjunction with the First IP Address. The IP port identifies the port used to communicate messages to and from the panel. The default IP Port setting is 2001.

2nd IP Address: Enter the second IP address where the panel sends network messages. The IP Address must be unique and cannot be duplicated on the network.

2nd IP Port: Enter the second IP port number to be used in conjunction with the Second IP Address. The IP port identifies the port used to communicate messages to and from the panel. The default IP Port setting is 2001.

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 server. The APN may contain up to 32 characters. Default is set to SECURECOM200 when a version 100 or 101 XT30/XT50 panel is used and the default is set to SECURECOM400 when a version 102 or higher XT30/XT50 panel is used. If using a SecureCom T-Mobile SIM card, enter GRID.T-MOBILE.COM for the APN.

Second GPRS APN: Enter the second APN (Access Point Name). This works as a backup in case the first APN fails. The APN may contain up to 32 characters. Default is set to SECURECOM200 when a version 100 or 101 XT30/XT50 panel is used and the default is set to SECURECOM400 when a version 102 or higher XT30/XT50 panel is used. If using a SecureCom T-Mobile SIM card, enter GRID.T-MOBILE.COM for the APN.

Check-in Minutes: Enter the number of minutes (15 to 240) between check-in reports. Check-in reports are a method of supervising the panel for communication with the receiver for Net communication. Enter 0 (zero) to

disable this feature. The default Check-In Minutes is 200 minutes.

Note: XT30/XT50 Series Version 102 and higher do not send check-in reports using cellular communication.

Fail Time Minutes: Fail Time Minutes allows the receiver to miss a defined number of check-ins before logging that the panel is missing. For example, if Check-In Minutes is 20 minutes and Fail Time is 30 minutes, the receiver only indicates a Panel Not Responding after 30 minutes. The Fail Time must be equal to or greater than the Check-in Minutes: If the Check-in is 20 minutes, the Fail Time must be 20 minutes or more. The maximum Fail Time is 240 minutes. The default Fail Time is 240 minutes for Net and 0 minutes for Cell.

XT30INT/XT50INT Series, XT30/XT50 Series (Version 103 or higher), XTLplus, XTLC, XTLN, and XTLN-WiFi panels

First GPRS APN (XT30INT/XT50INT, XT30/XT50, and XTL): Enter the first APN (Access Point Name). This allows an access point for cellular communication and is used to connect to a DNS server. The APN may contain up to 32 characters. Default is set to SECURECOM200 when a version 100 or 101 XT30/XT50 panel is used and the default is set to SECURECOM400 when a version 102 or higher XT30/XT50 panel is used. If using a SecureCom T-Mobile SIM card, enter GRID.T-MOBILE.COM for the APN. The default for XT30INT/XT50INT panel is NUMEREX.CXN.

Second GPRS APN (XT30INT/XT50INT, XT30/XT50, and XTL): Enter the second APN (Access Point Name). This works as a backup in case the first APN fails. The APN may contain up to 32 characters. Default is set to SECURECOM200 when a version 100 or 101 XT30/XT50 panel is used and the default is set to SECURECOM400 when a version 102 or higher XT30/XT50 panel is used. If using a SecureCom T-Mobile SIM card, enter GRID.T-MOBILE.COM for the APN. The default for XT30INT/XT50INT panel is NUMEREX.CXN.

Note: For Cellular: The message is sent using First GPRS APN and the First IP Address. If no acknowledgment is received, First GPRS APN and the Second IP address are used, followed, if needed, by Second GPRS APN and first and second IP addresses, respectively.

Check-in Minutes: Enter the number of minutes (0, or 3 to 240) between check-in reports. Check-in reports are a method of supervising the panel for communication with the receiver. Enter 0 (zero) to disable this feature. The default Check-In Minutes is 0 (zero) minutes.

Fail Time Minutes: Fail Time Minutes allows the receiver to miss a defined number of check-ins before logging that the panel is missing. For example, if Check-in is 20 minutes and Fail Time is 30 minutes, the receiver only indicates a Panel Not Responding after 30 minutes. The Fail Time must be equal to or greater than the Check-in Minutes: If the Check-in is 20 minutes, the Fail Time must be 20 minutes or more. The maximum Fail Time is 240 minutes. The default Fail Time is 240 minutes.

CellComSL, DualCom Series

Check-in Minutes: Enter the number of minutes (0, or 3 to 240) between check-in reports. Check-in reports are a method of supervising the panel for communication with the receiver. Enter 0 (zero) to disable this feature. The default Check-In Minutes is 0 (zero) minutes.

Fail Time Minutes: Fail Time Minutes allows the receiver to miss a defined number of check-ins before logging that the panel is missing. For example, if Check-in is 20 minutes and Fail Time is 30 minutes, the receiver only indicates a Panel Not Responding after 30 minutes. The Fail Time must be equal to or greater than the Check-in Minutes: If the Check-in is 20 minutes, the Fail Time must be 20 minutes or more. The maximum Fail Time is 240 minutes. The default Fail Time is 240 minutes.

3.1 Communication Paths

3.1. Communication Path Tab

Configure the communication options for the panel. The information you program varies with the Communication Type you select.

Compatibility

XR100/XR500 Series v200 or higher

XR150/XR550 Series

XR150INT/XR550INT Series

Account Number

The Account Number is a 1 to 5 digit number used to identify which panel is sending a message. Enter the account number sent to the SCS-1R or SCS-VR Receiver. Messages may be sent to a central station or via PC Log Reports to a PC. The default is 12345.

NET, CELL, and DD: The range of valid account numbers for a panel is 100-65535. A range of valid account numbers for a CID path is 1-9999. For accounts of four digits or less, do not enter leading zeros.

Transmit Delay

Enter the number of seconds (15 to 45) the panel waits before sending burglary zones (Night, Day, or Exit) reports to the receiver. Other zone type reports are sent immediately. Alarm bells and relay outputs are not delayed during this period. Program Burglary Outputs for pulsed or steady, and set Abort Reports to YES if Opening and Closing reports are not being sent. Enter 0 (zero) to disable this function. The default is 30.If the area where the alarm occurred is disarmed during the Transmit Delay time, only an Abort Report (S45) message is sent to the receiver.

If the area where the alarm occurred is disarmed after the alarm message is sent to the receiver but before the Bell Cutoff time expires even if the alarm was silenced, an Alarm Cancelled (S49) message is sent. Otherwise the alarm is sent at the end of the delay. The Alarm Cancelled report cannot be disabled

Communication Path

Up to eight communication paths may be programmed. Each path is designated as a primary or backup communication route. Path 1 is always Primary but other paths may be programmed as additional primary or backup.

Each primary path establishes a new path group. A path group is made up of the primary path and its subsequent backup paths. Typical communication takes place on the primary path with backup paths being used only when the primary path fails or when the backup path is programmed to duplicate messages. There is no option to backup path 8.

Communication Type

Specifies the communication method the panel uses on this path to report system events to SCS-1R, SCS-VR Receivers, or non-DMP receivers. Default is NONE for Path 1, and NONE for Path 2-8.

- None: For local systems. Selecting NONE ends communication programming.
- Digital Dialer: Digital Dialer communications to an SCS-1R Receiver.
- Network: Network communication using the panel onboard network connection. The DMP Network/Output reporting format is transmitted over a data network to the SCS-1R or SCS-VR Receiver.
- Contact ID: This option allows the panel to communicate to DMP receivers using the Contact ID format.
- Cellular Network: This option allows communication over the cellular network using the 263LTE or 263H Cellular Communicators.
- Wi-Fi: Network communication to SCS-1R or SCS-VR Receiver
- RS232: This option can be used for radio backup communications or other communication options and used the onboard serial port.

Path Type

The Path Type defines if the path is Primary or Backup. Because Path 1 is Primary, this option only displays for paths 2-8. Default is Backup.

Note: If the Primary Communication Type is CELL, then the backup Communication Type can only be NET or 232.

Test Report

Test Report determines if test reports are sent on this path. Reports are sent according to the programming in Test Frequency and Test Time. Default is Yes.

- Select YES to allow the programmed test report to be sent on the path currently being programmed.
- Select DEFER to not send a test report if the panel communicates any message to the receiver within the time set in Test Frequency.
- Select NO to not send test reports on this path.

Test Frequency

Test Frequency determines the frequency of the test report. Enter a number from 1 to 60 and select DY (Day) or HR (Hour) by pressing the far right select key or area. Default is 1 Day.

Frequency Unit

Select Day or Hour. Default is Day.

Test Day

Use this option to set the day of the Test Report. This option appears only when Test Report is Yes, Test Frequency is Day and a multiple of seven. Press CMD to display the first four days of the week. Press CMD to display the last three days. Select the day of the week to send the test report. Default is SUNDAY.

Test Time

Use this option to select the time of day for Test Reports. Select the hour, minute and AM/PM. Enter 0:00 AM to disable this feature. Default is 0:00 AM

Check In

This option displays if the COMM TYPE is NET or CELL. Check-in reports are a method of supervising the panel for communication with the receiver. For NET the default is YES. For CELL the default is YES.

- Select RND (Random) for the panel to check-in at random times from 6 to 60 minutes when all areas are disarmed. If any area is armed a check-in is sent every 6 minutes.
- Select ADPT (Adaptive) for a backup path to adapt to the check-in programming from this groups primary path if the primary path becomes unavailable. Check-in programming includes Check-in and Fail Time.
- Select ADP3 (Adaptive 3) for a backup path to adapt using a 3 minute Check-in and Fail Time if the primary path becomes unavailable. This option also indicates a Communication Trouble (S10) if the cell tower is unavailable for 3 minutes.

When YES is selected, enter the number of minutes between check-in reports, from 2 to 240 for NET or 3 to 240 for CELL, when the panel is armed or disarmed. For CELL the default is 0. For NET the default is 200

Fail Time

This option displays if CHECKIN is set to YES. Entering a FAIL TIME allows the receiver to miss multiple check-ins before logging that the panel is missing. The maximum fail time is 240 minutes. For example, if CHECKIN is 10 and FAIL TIME is 30, the receiver only indicates a Panel Not Responding after 30 minutes. The FAIL TIME must be equal to or greater than the CHECKIN time. Default is equal to CHECKIN for CELL. Default is 240 for NET

Encryption (XR550 with Encryption only)

This option displays only if the Communication Type is NET or CELL. Select 128 or 256 to enable the encryption level for the path currently being programmed. Default is NO.

Note: 256-bit encrypted messages to the SCS-1R receiver only communicate when using SCS-104 Receiver Line Cards with Version 102 or higher software.

Receiver IP

This option displays only if the Communication Type is NET or CELL. Enter the Receiver IP address where the panel sends network messages. The Receiver IP Address must be unique and cannot be duplicated on the network. Enter all 12 digits and leave out the periods. For example, enter IP address 192.168.0.250 as 192168000250. The periods display automatically.

Receiver Port

Enter the receiver port number. Valid range is 1 to 65,535. Default is 2001.

First Telephone Number

This option displays only if the Communication Type is DD or CID.This is the first number the panel dials when sending reports to the receiver. Phone numbers can have two lines of 16 characters each to equal up to 32 characters.Enter P to program a three-second pause in the dialing sequence. The P character counts as part of

the 32 allowable characters.Enter R as the first character for rotary (pulse) phone function. The R character counts as part of the 32 allowable characters.Call Waiting: You can place the “* 7 0 P” (Star, Seven, Zero, Pause) in the telephone number first position to cancel Call Waiting. For example, program NET with second line DD and phone number *70P555-1212, and you have NET with Call Waiting cancelled on the second line.

Caution: A call waiting cancel programmed on a non-call waiting telephone line would prevent communication to the central station.

Second Telephone Number

The panel dials the second number when two successive tries using the first number fail. If the panel cannot reach the receiver after two attempts using the second number, it returns to the first number and makes two additional attempts. A total of ten dialing attempts are made using the first and second phone numbers.Each number can be up to 32 characters in length including any P or R characters entered for pause or rotary connections or call waiting cancel option.Should all ten attempts fail, the panel continues to attempt sending the message using the next programmed path. If all programmed communication paths fail, the panel clears the communication buffer and makes one communication attempt each hour to send a TRANSMIT FAILED (S87) report to the receiver. Access the User Menu Display Events feature to view the report information not sent to the receiver or download the report with Remote Link.

3.2. Advanced Tab

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 set to SECURECOM400.

Note: This option is not used when LTE modems are used for communication.

Second GPRS APN

Enter the second APN (Access Point Name). This works as a backup in case the first APN fails. The APN may contain two lines of 16 characters to equal 32 character. Default is set to SECURECOM400.

Note: This option is not used when LTE modems are used for communication.

Fail Test Hours

This option sets the frequency for a Backup or Adaptive path to send a test report when the closest previous path fails within its path group. For example, if a backup path is programmed to send a weekly test report and the Fail Test Frequency is set to 2 hours, when the previous path fails within its group, the backup path starts sending a test every 2 hours until the previous path restores. If Fail Test Frequency is set to 0, test reports are sent only according to Test Report programming. Range is 0 to 24 hours. Default is 0.

Protocol

This option displays only when Communication Type is NET. Select TCP to communicate over the network using

TCP protocol. Select UDP to communicate using UDP protocol. Default is TCP.

Retry Seconds

This option displays for NET Communication. Enter the number of seconds (between 6 and 15) 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. For example, if retry time is set to 15, the panel retries four times.The default Retry Time is 6 seconds.

Substitution Code

This option displays when the Communication Type is NET or CELL. The Panel 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. The default is NO.Select YES to send a substitution code with every message.Select SHARED (SHR) to use the same substitution code as operating in the previous path

232 Port

This option displays for Communication Type RS232 and sets the physical RS-232 port to the XR500 onboard connector or one of the DMP Model 461 Interface Adaptor Card slots labeled A, B, C, D, or E. Use slot A if using a 462N Network Interface Card with or without the 461 card.

Select ONBOARD to use the onboard connector. Set the XR500 Series panel J23 jumper to R and briefly reset the panel using the reset jumper to activate RS-232 operation. Default is Onboard.

232 Setup String

This option displays when the Communication Type is 232. Enter up to two lines of 16 characters to equal up to 32 characters for the destination address that may include an IP address. Example: AT#UCXXX.XXX.XXX.XXX#PPPPP where X is the IP address and P is the port number.

893A

This option displays when the Communication Type is DD or CID.

The 893A option allows reports to be sent to the receiver on a second DD line using the 893A module. Default is NO. When using this option, Test Report messages (S07 Automatic Recall Test or S88. Unrestored System Recall Test) are sent to the receiver at the frequency programmed in Test Frequency, alternating between the first and second phone line. For example, a DD path with an 893A module set for daily test report frequency sends a test report through phone line 1 one day and phone line 2 the next day. If the 893A option is set to YES, enter up to 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

Second Line Prefix

This option displays if the 893A option is selected. 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 Switch

This option displays for DD or CID Communication Types.Enter the number of attempts to send an alarm message before switching to the next path. Range is from 1 to 10. 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. Default is 1.

Duplicate Alarms

This option displays for BACKUP paths. If Yes is selected, the current backup path duplicates all alarms occurring on its group primary path. Default is NO.

Alarm Reports

This option displays when the Path Type is Primary. All backup paths within the group follow the same programming for Alarm Reports. Default is YES.

When YES is selected, the following reports are sent to the receiver 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

Supervisory/Trouble Reports

This option displays when the Path Type is Primary. All backup paths within the group follow the same programming for Supervisory/Trouble Reports. Default is YES.

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

Serviceman reports are sent regardless of the selection made for Supervisory/Trouble reports.

Opening/Closing and User Reports

This option displays when the Path Type is Primary. All backup paths within the group follow the same programming for Opening/Closing and User Reports. Default is YES.

When YES is selected, the following reports by user are sent to this receiver.

- Opening
- Code changes (including adding, deleting, changing)
- Closing
- Schedule changes (temporary, permanent, shift)
- Bypass
- Holiday date changes
- Reset

Door Access Report

This option displays when the Path Type is Primary. All backup paths within the group follow the same programming for Door Access Reports. Default is DENY.

Select YES to enable Door Access Granted and Denied reports to this receiver whenever a door access is granted to a user. The Door Access Granted report is only sent if the keypad number has also been selected in Access Keypads under the SYSTEM REPORTS programming.

Select DENY to enable Door Access Denied reports only to this receiver when a door access is denied to a user

Panic Test (Network only)

YES allows the panic zone test verification and failure results to be sent to the central station receiver. NO disables the panic test report. The default setting is NO. The system test start, stop, panic zone verification, and panic zone failure messages sent to the central station and the trips count operation are the same as used under the Walk Test. See Using the Walk Test section in the Appendix.

Send Communication Trouble

This option displays for each path and determines if and how 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

This option displays for each path and if YES, each panel message includes path information such as path number, communication type, and path type. Default is NO.

4. Network Options

Network Options are provided to define the network configuration for the panel. This information will be used during communication of messages through the network.

Note: IP addresses and port numbers may need to be assigned by the network administrator. When entering an IP, Gateway, or Subnet Mask address, be sure to enter all 12 digits and leave out the periods. For example, IP address 192.168.000.250 is entered as 192168000250.

DHCP Enabled

If the panel uses a dynamic IP address, select the checkbox. If the panel has a static IP address, do not select the checkbox. To determine if you have a dynamic or static IP address, contact your company IT Administrator.

Local IP Address

Enter the local IP address. The Local IP Address must be unique and cannot be duplicated. The default local IP address is 192.168.0.250.

Gateway Address

Enter the local gateway address. The Gateway IP Address is needed to exit your local network. The default gateway address is 192.168.0.1.

Subnet Mask

Enter the local subnet mask assigned to the panel. The default subnet mask address is 255.255.255.000.

DNS Server

Enter the IP address of the DNS (Domain Name System) used by the panel to resolve domain names into IP addresses. The default address is 192.168.0.1.

Programming Port

Enter the network port to be used for programming the panel. The default value is 2001.

Note: The Local IP and Programming Port need to match the IP Address and IP Port entered in the Panel Information window. If a router is connected to the panel, the ports must be opened in the router.

TCP Enabled

When this option is enabled, the panel communicates over the network using standard TCP protocol. When this option is not enabled, the panel communicates using UDP protocol. The TCP communications default value is Not Enabled.

Passphrase

To enable encryption, type an 8 to 16-character Passphrase using alphanumeric characters. If you leave the Passphrase blank, the panel communicates with the SCS-1R or SCS-VR Receiver, but the data is not encrypted. The Passphrase is blank by default.

An XR550 panel with encryption is capable of communicating 128-bit or 256-bit encrypted data to an SCS-104

line card installed at the receiver. The XR550 panel with encryption and the receiver SCS-104 line card must have the same password called a Passphrase.

Caution: Do not lose the passphrase. A lost or forgotten Passphrase requires that the XR550 panel and every SCS-104 line card at the receiver be individually reprogrammed with a new passphrase.

Note: An XR550 panel with encryption communicates using AES encryption. If you currently have an XR550 panel with network installed, you may purchase a separate feature key to activate encrypted communications using the Feature Upgrade process described in the Feature Upgrade Section. Encrypted communication cannot be enabled on a standard XR550 panel. 256-bit encrypted messages to the SCS-1R receiver only communicate when using SCS-104 Receiver Line Cards with Version 102 or higher software

734N Listen Port

Enter the port number that the 734N/734N-POE will use to send communication to the panel. This must be the same port that is programmed in Panel IP Port within the 734N/734N-POE Communication programming menu.

Note: The 734N Listen Port cannot be the same as the panel network programming port.

734N Passphrase

Enter an 8 to 16-character Passphrase to encrypt communication with the734N/734N-POE module. The 734N Passphrase must match the 734N Passphrase entered in Communication programming of the 734N. The Passphrase is blank by default.

Note: A passphrase is required for operation

5. Messaging Setup

Use Messaging Setup to enter the information needed to receive messages directly from the panel via MyAccess™ SMS Text using Cellular communication. All of the name and password options below allow up to 32 lowercase characters to be entered. The Destination addresses allow up to 48 characters to be entered.

Enable Messaging

Select the checkbox to allow the panel to send messages to three programmed destinations. The checkbox is unselected by default.

System Name

Enter a unique name for the panel. The panel name is used as the sender of the message. The text entered is displayed with initial caps. If this field is left blank, the panel account number is sen

Destination 1

Enter the first cell phone number where messages will be sent. The message can be sent to any device (computer, cell phone, PDA) as long as a valid cell phone number is entered.

Destination 1 User Number

Enter a valid user number from this account. This option is used when sending commands such as arming or disarming back to the panel using MyAccess SMS Text from the same cell phone or PDA. The user number must

have the authority to perform the commands as if it occurred at the keypad. MyAccess SMS Entering 0 (zero) disables this option. Default is 0.

Destination 2

Enter the second destination cell phone number.

Destination 2 User Number

Enter a valid User Number for arming/disarming authorization.

Destination 3

Enter the third destination cell phone number.

Destination 3 User Number

Enter a valid User Number for arming/disarming authorization.

Email Communication Type

This option is only available if an email address has been entered in the Destination Section. Choose NET to send email messages over the network. Choose CELL to send email messages using cellular communication. Default is NET.

O/C SMS

Select YES to allow the panel to send Opening and Closing messages to a cell phone via SMS protocol. Default is NO. This option displays if any destination is a cell phone number.

Monthly Limit

This option displays if any programmed destination is a cell phone number using CELL communication. This number limits the monthly incoming and outgoing SMS messages allowed to be sent or received by the panel.

A panel event that causes messages to be sent to destination cell phone numbers is counted towards the panel's monthly limit. For example, if an alarm message is sent to a cell phone number, a total of 2 messages are counted towards the monthly limit for the panel. SMS messages sent from a cell phone to the panel, including status requests and MyAccess SMS Text messaging commands, also count toward the monthly limit. The limit is reset at midnight on the 14th of every month. Range is from 0 to 999. When 0 is entered, there is no limit on the number of messages able to be sent or received by the panel. Default is 0.

Note: The SecureCom Wireless text plan selected for the panel should match or exceed the programmed Monthly Limit

SMTP Configuration

The remaining options will only appear if email messaging has been selected to be sent via network. The options allow the email server to be selected by the installing dealer. Typically this will be the email service

provided by the installing dealer. This allows opportunity for additional services to be provided to the end user.

SMTP Server

Enter the SMTP (Simple Mail Transfer Protocol) Server name. The SMTP email server is responsible for sending the email to its destination. An example SMTP email server name is: mail.somedomain.com. The domain should be the email server that will provide email support for your alarm customers.

SMTP Server Port

The SMTP server port number is the port that the panel uses to initiate a TCP connection with the email server. The default port is 25.

SMTP Username

Most SMTP servers require a user name to send email. This will be sent to the SMTP server in conjunction with the SMTP Password to provide email authentication to the server.

SMTP Password

Most SMTP servers require a password to send email. This will be sent to the SMTP server in conjunction with the SMTP User name to provide email authentication to the server.

From Email Address

Enter the email address on file with the email service. This will show up in the email messages as the sender's address.

6. Device Setup

Define the panel's physical configuration. You can install and address up to sixteen supervised devices on the keypad data bus or AX-Bus on the panel. You may change the types of connected devices and the areas or partitions where those devices are assigned. The Device Setup screen varies by panel model.

Compatibility

- XR150/XR350/XR550 Series
- XR150INT/XR550INT
- XR100/XR500

Card Formats

Select the slot number (1-7) that you would like to program a custom non-DMP card format into. Select 8 if you would like to program a DMP card format. For a chart of commonly used card formats and their defaults, refer to the 734 Installation Guide (LT-0737).

Wiegand Code Length

When using a custom credential, enter the total number of bits to be received in Wiegand code including parity bits. Press any select key or area to enter a number between 1-255 to equal the number of bits. Default is 26

bits. Typically, an access card contains data bits for a site code, a user code, and start/stop/parity bits. The starting position location and code length must be determined and programmed into the 734/734N/734N-POE module.

Site Code Position

Enter the site code start position in the data string. Enter a number between 0-255. Default is 1.

Site Code Length

Enter the number of characters the site code contains. Enter a number between 1-16. Default is 8.

User Code Position

Define the User Code start bit position. Enter a number between 0-255. Default is 9.

User Code Length

Define the number of User Code bits. Enter a custom number. On a 734 module, custom numbers can only be between 16-40.On a 734N/734N-WiFi module, custom numbers can be between 1-255. The default is 16.

Require Site Code

Press the select key or area under YES to use a site code. In addition to User Code verification, door access is only granted when any one site code programmed at the SITE CODE ENTRY option matches the site code received in the Wiegand string

Site Code Display

Program up to 8 eight-digit site codes. Site code range is 0-16,777,214. Site Code 1 defaults to 127. Site Codes 2-8 default to blank.

Number of User Code Digits

734 Series Wiegand Interface modules recognize user codes from 4-12 digits in length. Enter a user code in Remote Link. This number must match the user code number length being used by the panel.

For an Area System, use 4 to 12 digits (typically 5).For all other systems and panels, use 4 digits. Any selection above 5 digits require entry of the custom card definitions with custom site and user code positions for the Wiegand string. When searching the bit string for the user code, the digits are identified and read from left to right.

Device Number

Enter the address of the device you are programming. If using a wireless keypad, program the device number in the Status List Auxiliary 1 Zones programming option to display wireless keypad troubles. After you program each option for the first keypad, repeat these programming steps for each additional keypad. The valid range for KEYPAD, FIRE, and EXPANDER type devices is 1 -16. The valid range for DOOR type devices is 1 - 16 and 501 - 961. See the AX Bus Addresses and 734 Zone Numbers chart. Wireless keypads and network door controllers

are not able to occupy address 1.

DOOR Device Type

The XR550 provides the ability to program an additional 16 doors of access to the system using 734 Series Wiegand Interface modules connected to any of the XR550's LX-Bus headers. This can be combined with the 16 doors of access available from the keypad bus for a total of 32 doors.Door capacity can be increased to a maximum of 64 or 96 by applying purchased feature keys. Feature keys are purchased through DMP Customer Service and entered into the panel using a keypad or Remote Link.

Programming and Operation

Once a 734 address has been programmed for the bus, the LX-Bus is automatically converted from a hardwire zone expansion bus to a hardwire Access Expansion Bus (AX-Bus) and the bus begins to operate as shown below.

- Each 734 Series 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 Series module programming is shown.

Note: An AX-Bus operation is compatible with 734, 734N, and 734N-POE modules and the Model XR550. Keypads must only be used on the keypad bus. AX-Bus operation is incompatible with the Model XR150 and XR350 control panels

AXBus Available Addresses and 734 Zone Numbers

734 Address	LX500		LX600		LX700		LX800		LX900	
	Door	*Zones*	*Door*	*Zones*	*Door*	*Zones*	*Door*	*Zones*	*Door*	*Zones*
1	501	501-504	601	601-604	701	701-704	801	801-804	901	901-904
2	505	505-508	605	605-608	705	705-708	805	805-808	905	905-908
3	509	509-512	609	609-612	709	709-712	809	809-812	909	909-912
4	513	513-516	613	613-616	713	713-716	813	813-816	913	913-916

5	517	517-520	617	617-620	717	717-720	817	817-820	917	917-920
6	521	521-524	621	621-624	721	721-724	821	821-824	921	921-924
7	525	525-528	625	625-628	725	725-728	825	825-828	925	925-928
8	529	529-532	629	629-632	729	729-732	829	829-832	929	929-932
9	533	533-536	633	633-636	733	733-736	833	833-836	933	933-936
10	537	537-540	637	637-640	737	737-740	837	837-840	937	937-940
11	541	541-544	641	641-644	741	741-744	841	841-844	941	941-944
12	545	545-548	645	645-648	745	745-748	845	845-848	945	945-948
13	549	549-552	649	649-652	749	749-752	849	849-852	949	949-952
14	553	553-556	653	653-656	753	753-756	853	853-856	953	953-956
15	557	557-560	657	657-660	757	757-760	857	857-860	957	957-960
16	561	561-564	661	661-664	761	761-764	861	861-864	961	961-964

Note: If a 734 module is programmed as a Device on any LX-Bus, all other zones programmed as a wired zone module will stop communicating with the panel on that same LX-Bus. Purchase Feature Keys for an additional 32 to 64 more doors

Note: 734N/734N-WIFI cannot be programmed through Device Setup on an AX-Bus. Wireless zones can be programmed on any remaining open addresses on the AX-Bus, such as on the LX500 bus, zones 500, 565 - 599 are open for any wireless module programming if sixteen 734 modules are connected to the LX500 bus.

Device Name

A device name must be given to each device in the system. Enter the name you wish to assign to a device. The

name may be up to 32 characters.

Device Type

This allows you to specify the type of device installed at a particular address on the keypad bus.

None

No device is connected to this address.

Keypad

The device type is a non-fire, non-access keypad.

Door

The device is an access control device and is either a keypad using door strike functions or a Wiegand Interface module. Devices with an address higher than 16 are automatically assigned as a DOOR device type.

Fire

The device is a 630F Remote Annunciator.

Expander

The device is a Zone Expansion module.

Device Communication Type

For a Device Type of Door, select Keypad Bus to communicate with a device on the keypad bus or select Network to communicate with a device using a network connection. Default is Keypad Bus.

Keypad

Select KPD-BUS for wired keypads or select WLS for wireless keypads. Default is KPD-BUS.

Door

For wired devices, select KPD BUS for addresses 1-16 or select AX BUS for addresses 501-964. For network devices, select NETWORK. You also have an option for wireless doors. For Wireless devices, select WLS

Serial Number

Enter the eight-digit serial number found on the wireless keypad. You can install and address up to four wireless keypads.

Note: This option only displays if Device Type is KEYPAD and Device Comm Type is WIRELESS.

Supervision Time

Select the supervision time required for the wireless device. The device must check-in at least once during this

time or a missing condition is indicated. Zero (0) indicates an unsupervised wireless keypad. Default is 240 minutes. When the panel is reset or a receiver is installed or powered down and powered up, or Remote Link disconnects, the supervision timer restarts for all wireless zones.

Note: This option only displays if Device Type is KEYPAD and Device Comm Type is WIRELESS.

Access Areas

Enter the area numbers that you wish to grant door access for this device. Users must have matching access area numbers assigned to their code to receive a door access at this device.If you do not enter any area numbers, all users with Door Access authority receives a door access without regard to schedules. If the user code is programmed for Anti-Pass YES, then the user is logged into all matching areas. This user is not allowed to access these areas again until they have egressed the area. When all areas accessed by a door are armed, the door is locked by the panel.

Note: For an All/Perimeter, Home/Sleep/Away, or Home/Sleep/Away with Guest system, Access Areas should be left at factory default setting

Panels

- Areas 1 to 32 for XR500INT Series, XR550 Series, or XR500 Series panels
- Areas 1 to 16 for XR350 Series panels
- Areas 1 to 8 for XR150INT Series, XR150 Series, or XR100 Series panels

Note: Enter the sequence of addresses separated by commas to enable egress areas devices. For example, enter addresses 1 through 4, 6, and 10 through 16 as 1-4, 6, 10-16.

Egress Areas

Use this option to detect Anti-passback violations. Anti-passback requires a user to properly exit (egress) an area they have previously accessed. If users fail to exit through the proper card reader location they are not granted access on their next attempt. Users must have matching access area numbers assigned to their profile, to receive a door access at this device. If the user is programmed for Anti-Pass YES, then the user islogged out of all matching areas. This allows the user to again access the area. See Access Areas section.If you do not enter any area numbers, all users with Door Access authority receives a door access without regard to schedules. If you are not using the Anti-Pass feature leave Egress Areas blank.

Note: For an All/Perimeter, Home/Sleep/Away, or Home/Sleep/Away with Guest system, Egress Areas should be left at factory default settings. If an area is programmed as an access area, it cannot be programmed as an egress area and therefore does not display during Egress Areas programming.

Panels

- Areas 1 to 32 for XR550INT Series, XR550 Series, or XR500 Series panels
- Areas 1 to 16 for XR350 Series panels
- Areas 1 to 8 for XR100 Series, XR150 Series, or XR150INT Series panels

Note: Enter the sequence of addresses separated by commas to enable egress areas devices: i.e.., enter addresses 1 through 4, 6, and 10 through 16 as 1-4, 6, 10-16.

Display Areas

Display Areas allows the panel burglary activities to be segmented so that only specific area(s) and their associated operation appear at a particular keypad. Area number(s) selected in this field affect the way users interact with the system from this particular device. For example: Program Device 1 to show only the zone activities and armed status of Area 1.

Enter the area number(s) that this keypad is to display. This allows specific area control from specific devices, as well as annunciation of zones (by type) assigned to those area(s). Display Areas default selects all area numbers. When Display Areas is left defaulted (all areas selected), Menu Display and Status List items determine whether zone alarms and troubles display at this device, regardless of area assignment. Also, all system areas may be armed and disarmed from this device.

Note: For an XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series system set to All/Perimeter or Home/Sleep/Away operation, Display Areas should be left at factory default settings.

For Home/Sleep/Away with Guest arming systems, the Display Areas selection determines which system the keypad arms and disarms. With areas 1, 2 or 3 selected, the keypad is assigned to the Main system. With area 4, 5 or 6 being the first areas selected, the keypad is assigned to the Guest 1 system. With area 7, 8 or 9 being the first areas selected, the keypad is assigned to the Guest 2 system. Keypads can have additional areas assigned for event display.

User Action Allowed

When an area(s) is selected, the following user actions are allowed.

- Arming/Disarming of the area(s) selected from the ARM or DISARM menu
- Zone Bypass of zones assigned to the area(s) selected
- Zone Monitor of zone assigned to the area(s) selected
- Shift schedule changes allowed for the area(s) selected
- Closing Check Schedule Extend is allowed for the area(s) selected
- Door Schedules changes are allowed for devices that have a matching area(s) as defined in Device Access Areas
- Door On/Off Menu operation is allowed for devices that have a matching area(s) as defined in Device Access Areas

Note: The previous user actions also require the matching area(s) be programmed in User Profile: Arm/Disarm area(s).

Status Display Allowed

When an area(s) is chosen, the following displays are allowed.

- Armed Status of the selected area(s)
- Zone Alarms and troubles for burglary (NT, DY, EX, A1, A2) type zones assigned to the selected area(s)
- Late to Close status of the selected area(s)
- Zone Status (normal/fault) of zones that are assigned to the selected area(s)

Options and Actions Not Affected

The following options are not affected by the Display Areas operation. The User Code authority level controls access to these items.

- Sensor Reset Menu
- Outputs On/Off Menu
- System Status Menu
- System Test/Panic Test
- User Profiles
- Forgive Anti-Passback
- Service Request
- Set System Time and Date
- Fire Drill
- Display Events
- 24-hour zones display at keypads based on Status List programming only

Note: A common area and its operations cannot be assigned to a specific keypad

Display Areas example

When Device 1 has Area Display set to 20, 21, and 22, it annunciates troubles and alarms only for zones assigned to those areas. When arming/disarming from Device 1, only areas 20, 21, and 22 may be armed/disarmed, even when the User Profile has authority to arm/disarm other system areas.

Exception: Disarming of other areas not selected in Display Areas can be accomplished by presenting a card that has disarming authority and matching profile areas with areas assigned in Device Access Areas.

Strike Time: This option displays if DOOR is selected as Device Type.

Enter the length of time that a keypad or access control device relay will be activated. Magnetic locks or electric door strikes can be connected to the relay and released for the length of time specified here. Enter a time between 1 and 250 seconds. The default is 5 seconds.

You can enter 0 to activate the device relay with a toggle action. This allows the user to activate or deactivate the device relay each time a valid user code is entered. The device relay is activated or deactivated until a user code is entered again.

Note: The Request to Exit door access time of a keypad or 734/734N Wiegand Interface module is not affected by this selection. The Request to Exit time will remain at 5 seconds.

Strike Delay: This option displays if DOOR is selected as Device Type.

Enter the number of minutes, 0 to 9, to delay a door strike after a valid code is entered or a card read occurs. When a valid card read or code is received, the activation of the door strike is delayed for the number of minutes programmed. The standard door strike message is sent to the Central Station receiver and logged in the Display events at the time of card read or code entry and is not delayed. During this delay, all subsequent codes entered or cards presented to the reader for a door strike are ignored and no record of the attempt is stored. Enter zero to disable. Default is 0 (zero).

Fire Exit: This option allows the door access relay at this address to be released whenever fire panic keys are pressed or a Fire or Fire Verify zone alarm is in the keypad Status List. The relay resets whenever a Sensor Reset is performed to remove all Fire and Fire Verify zone alarms from the Status List. Leave this field empty to prevent the door access relay at this address from releasing during a fire alarm.

Output Group: This option allows the output group (relays) assigned to the user profile to turn ON when the device relay is activated for the programmed strike time. This could be used to operate an elevator control. See the User Profiles section of the XR500/XR100 User Guide (LT-0683), the XR150/XR350/XR550 User Guide (LT-1278), or the XR150INT/XR550INT User Guide (LT-1278INT) for more information.

Override: Select this option to allow door On/Off schedules to be overridden by the armed condition of the system.

Checking the Override box causes the panel to ignore the ON time for a door schedule when all areas assigned to Access Areas for this device are armed. If any area disarms after the door schedule on time, the panel will turn on the device output. A door output that is on during a disarmed period will automatically turn off when all access areas assigned to the device arm, even if the scheduled off time has not been reached.

You may use the Override feature to keep doors locked when a business opens late, or is forced to close early, due to a snowstorm or other cause. Leave the Override field blank to allow door schedules to operate independent of system armed status.

Auto Force Arm: Enable to have all Display Areas assigned to this keypad automatically arm and to force arm faulted zones at arming. If Closing Code is programmed as YES, only the matching areas between the Display Areas and the User Code's authorized areas arm. Also, when enabled, the user is not prompted to select areas to disarm after entering a code at Entry Delay or after choosing Disarm at the keypad. All matching areas assigned to the User Code and to this keypad are automatically disarmed. When not enabled, the user is prompted to select areas (ALL NO YES) and choose to force arm or bypass at arming and disarming. See the Device Setup section of the XR500 Series Programming Guide (LT-0679),the XR100 Series Programming Guide (LT-0896), XR150/XR350/XR550 Series Programming Guide (LT-1232) or the XR150INT/XR550INT Series Programming Guide (LT-1232INT).

Door Real-Time Status: Enable to have real-time door status messages sent to PC Log reporting and Entré reporting for this device. Messages are sent anytime the panel turns the door relay on or off. Default is disabled.

Send Door Forced Message: Enable to have the panel send a real-time door status message of Forced Open (FO) to PC Log reporting and Entré reporting when the door relay is off, but the door zone has transitioned from its normal state. Default is disabled.

Public Door: Enable to program the device as a public door. Any door programmed as a public door will remotely lock when the Lockdown button is activated in Panel >> System Status. The Lockdown feature can be used in emergency situations where it is necessary to restrict the site's access to authorized users only. See Lockdown for more information.

XTL/XTLN/XTLN-WiFi Panels

The Device Setup window allows you to define the XTL/XTLN/XTLN-WiFi panel configuration. You can install and address up to four wireless keypads.

Device Number: Enter the address number of the wireless keypad you are programming. The valid range is 2-5.

Device Name: Enter the name you wish to assign to the wireless keypad. The name may be up to 16 characters long. If no name is entered, *UNUSED* is displayed.

To remove a keypad from the system, delete the device name by leaving this option blank.

Note:> Do not remove the keypad if it is currently in use.

Serial Number: This option only displays when a device number is entered above. Enter the eight-digit serial number found on the wireless keypad.

Supervision Time: Select the supervision time required for the wireless keypad. The wireless keypad must

check-in at least once during this time or a missing condition is indicated for that device. Select 60 or 240 minutes. Select None for unsupervised operation. Default is 240 minutes.

XT30INT/XT50INT Series, XT30/XT50 Series Panels (Version 106 or higher)

The Device Setup window allows you to define the XT30/XT50 panel configuration.

Device Number: Enter the address number of the devices you are adding to the system. The valid range is 1-8.

Device Name: Enter the name you wish to assign to the device. The name may be up to 16 characters long.

Wireless: Enable to use a wireless keypad for this device number. Deselect to use a wired keypad for this device number. Default is disabled. You may install and address up to four wireless keypads.

Serial Number: This option only displays when Wireless is selected for this device number. Enter the eight-digit serial number found on the wireless keypad.

Supervision Time: This option only displays when Wireless is selected for this device number. Select the supervision time required for the wireless keypad. The wireless keypad must check-in at least once during this time or a missing condition is indicated for that device. Select 60 or 240 minutes. Select None for unsupervised operation. Default is 240 minutes.

6.1. 734/734N/734N-WiFi Options

Program 734 Options: Select 734 Options tab to program the 734 Wiegand Interface module.

Note: Device type on the General Tab must be set to DOOR and Device Communication Type must be set to Keypad Bus for 734 operation.

Program 734N/734N-WiFi Options: Select 734 Options tab to program the 734N/734N-WiFi Wiegand Interface module.

Note: Device type on the General Tab must be set to DOOR and Device Communication Type must be set to NETWORK for 734N/734N-WiFi operation.

Zone 2 Options

Activate Zone 2 Bypass: Select to enable the Bypass option. Unselect allows standard zone operation on Zone 2. Default setting is deselected.

If the door being released by the 734/734N/734N-WiFi module is protected (contact installed), you can provide a programmable Bypass entry/exit timer by connecting its contact wiring to the 734/734N/734N-WiFi module Zone 2. When the onboard Form C relay activates and the user opens the door connected to Zone 2, the zone is bypassed for the number of seconds programmed in Zone 2 Bypass Time allowing the user to enter/exit.

If Zone 2 does not restore (door closed) within the programmed bypass time, the 734 piezo pulses during the last ten seconds. If Zone 2 restores prior to the end of the programmed time, the piezo silences. If the zone does not restore before the programmed time, the 734/734N/734N-WiFi ends the bypass and indicates the open or short zone condition to the panel.

Relock on Zone 2 Change: Select to turn the 734 door relay off and relock the door when Zone 2 changes state. Disabling this option leaves the relay on for the door access time when Zone 2 restores. The default is disabled.

Zone 2 Bypass Time: Enter the number of Bypass seconds to elapse before the Bypass timer expires. Range is from 20 to 250 seconds. If the door remains open when the timer expires a zone open/short is sent to the panel for Zone 2. The default is 40 seconds.

Zone 3 Options

Activate Zone 3 Request to Exit: Selecting enables the Zone 3 Request to Exit (REX) option.

Disabling allows standard zone operation on Zone 3. Default setting is disabled.

Optionally connect a PIR (or other motion sensing device) or a mechanical switch to Zone 3 to provide REX capability to the system. When Zone 3 shorts, the onboard Form C relay activates for the programmed number of seconds. During this time, the user can open the protected door to start the programmed Bypass entry/exit timer. After the programmed number of seconds, the relay restores the door to its locked state.

The 734/734N/734N-WiFi module provides a bypass-only option for REX on Zone 3. When Zone 3 opens from a normal state, only a bypass occurs: the onboard relay does not activate. This bypass-only option uses two methods of REX. The first REX device provides the programmed Bypass entry/exit timer. The second REX device, or manual device such as a door knob, unlocks the door.

An example of the shunt-only configuration is a door to an office that is locked 24 hours a day. Users pass a REX motion detector positioned by the door to begin the programmed exit timer. Within the programmed number of seconds the user must then manually activate a second device, such as a REX device or manual door knob, to unlock the door. If the door is opened after the programmed number of seconds, the zone goes into alarm.

Zone 3 Request to Exit Strike Time: Enter the number of Request to Exit seconds to elapse. Range is from 5 to 250 seconds. The default is 5 seconds.

Activate Onboard Speaker: Select to enable the onboard piezo speaker for local annunciation. Disable to turn the piezo off for all operations. This does not affect remote annunciator open collector (RA) operation. The default is disabled.

Card Options

Card Options: Select DMP to indicate the reader sends a 26-bit DMP data string. Select CUSTOM if using a non-DMP credential or user code length of 6 to 12 digits. Select ANY to activate the door relay for the programmed Zone 3 Rex Strike Time when any Wiegand string is received. Default is DMP.

Note: When set to DMP, the 734/734N/734N-WiFi converts 17 bits of the 26-bit data string into a 5-digit number.

Wiegand Code Length: When using a custom product, enter the total number of bits to be received in Wiegand code including parity bits. Select a number between 1-255 to equal the number of bits. Default is 26 bits.

Typically, an access card contains data bits for a site code, a user code, and start/stop/parity bits. The starting position location and code length must be determined and programmed into the 734/734N/734N-WiFi module.

Site Code Position: Enter the site code start position in the data string. Enter a number between 0-255. Default is 1.

Site Code Length: Enter the number of characters the site code contains. Enter a number between 1-16. Default is 8.

User Code Position: Enter the User Code start bit position. Enter a number between 0-255. Default is 9.

User Code Length: Enter the number of User Code bits. For 734, when used with a XR150/XR350/XR550 Series, version 103 or higher, a custom user code can be a number between 16-40. For all other panels they can then be a number between 16-32. For 734N/734N-WiFi, custom user codes can only be a number between 1-255. The default is 16.

Require Site Code: Select to enable the use of a site code. In addition to User Code verification, door access is only granted when any one site code programmed below matches the site code received in the Wiegand string.

Site Codes: You can program up to eight site codes. Site code range is 0-999 for the 734 and the range is 0-255 for the 734N/734N-WiFi. Any previously programmed site codes display. Enter a three or five digit site code number followed by the tab key to advance to the next Site Code.

Note: A card with a site code greater than three digits cannot be used. Use only cards with three-digit site codes.

Number of User Code Digits: The 734 module recognizes user codes from 4-12 digits in length. The 734N/734N-WiFi module recognizes user codes from 1-12 digits in length. This number must match the user code number length being used by the panel. Default is 5. For a XR150/XR350/XR550 Series Area System version 102 use 4 to 12 digits (typically 5). For XR100/XR500 Series Area System, use 4 to 10 digits (typically 5). For all other systems and panels, use 4 digits.

Any selection above 5 digits require entry of the custom card definitions with custom site and user code positions for the Wiegand string. When searching the bit string for the user code, the digits are identified and read from left to right.

No Communication with Panel: This option defines the relay action when communication with the panel has not occurred for five seconds. Choose the action required. Default is Off.

Off (Relay Always Off) — The relay does not turn on when any Wiegand string is received. Off does not affect any REX operation.

Site (Accept Site Code) — Door access is granted when the Wiegand site code string received matches any programmed site code. For details refer back to the Require Site Code option.

Any (Any Wiegand Read) — Door access is granted when any Wiegand string is received.

ON (Relay Always On) — The relay is always on.

Last (Preserve Last) — The relay remains in the same state and does not change when communication is lost.

7. 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 from this window. To edit a device, select the device to be edited from the upper left hand window list or select the device type tab on the dialog box (All, Lights, Locks, Thermostats, Controllers or Other). Select the device Name in the dialog box, make the desired edits, and 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 one is damaged. You can back up Z-Wave settings by selecting Backup on the Z-Wave Setup window. If a previous backup exists, the Restore button is available and Last Backup Date: displays. If no backup exists, the Last Backup Date: displays Never. This feature is available for XT30/XT50 and XTLplus Series panels.

8. Z-Wave Favorites

The Favorites window allows you to create and edit Z-Wave Favorites by adding, deleting or changing existing Z-Wave devices from Favorites. If your panel has existing Favorites programmed, they will be displayed after the panel has been retrieved. You may create a new Favorite by selecting New at the bottom of the window, entering the new Favorite number in the Number field, entering the Favorite name in the Name field, and selecting Apply.

To remove a Favorite, select it from the Favorites list in the upper left corner of the window and select Delete. A dialog box will display confirming you want to delete the selected Favorite, select Yes to delete or No to cancel. Each Favorite can contain up to 25 devices.

Note: New devices must be added to the panel and then retrieved using Remote Link before they can be added to a Favorite.

To edit a Favorite, select the Favorite to be edited and a device type (Lights, Locks, Thermostats, or

Unknown). The following options are available for each device type:

Add: Select the Add button and select the device to add from the Device pull-down menu. Select Apply to save the Favorite.

Remove: Select the device to remove from the Favorites programmed device field and select Remove. A dialog box will display confirming you want to remove the selected device from the Favorite, select Yes to remove or No to cancel.

Apply: After adding or removing a device in a Favorite, selecting Apply saves the changes to the Favorite.

Cancel: This cancels the current change being made to the selected Favorite.

Device Tabs

Lights: There are two types of lights: binary and multilevel. Binary type lights utilize a simple on/off switch and multilevel lights utilize a dimmer switch. The light type cannot be changed.

Device: A list of all Light type devices displays.

Light Level: If the selected light is a simple on/off switch a set of 'On' and 'Off' radio buttons display. The default is 'On.' Lights with a dimmer switch display a 'Dim' option. Select the light level by sliding the bar from 0-99. If set to 0, the 'Off' button is selected and if set to 99, the 'On' button is selected. The default is 49.

Locks

Device: A list of all Lock or Garage Door type devices displays.

State: Each lock has a dropdown to select 'Locked' or 'Unlocked.' The default is 'Locked.'

Thermostats

Device: A list of all Thermostat type devices displays

Heat Set Point: Enter the default heat temperature for a Thermostat. The range is 55 to 95 degrees Fahrenheit.

Cool Set Point: Enter the default cool temperature for a Thermostat. The range is 55 to 95 degrees Fahrenheit.

Thermo Mode: Enter the mode for a Thermostat. The available options are 'Heat,' 'Cool,' 'Auto,' and 'Off.' The default is 'Heat.'

Fan Setting: Enter the fan setting of the healing and cooling system. The available options are 'Auto' and 'Off.' The default is 'Auto.'

Unknown: This tab is for devices that do not exist in the Remote Link database or those that are not Lock, Light or Thermostat type devices. If a device did not properly initialize with the panel it is given the device type 'Other' and displays here. Unknown devices cannot be edited or added to a Favorite, but they may be removed from a Favorite.

9. Remote Options

The Remote Options window allows you to enter the information needed for connecting to the panel using Remote Link software.

General Options

Remote Key: Enter an alphanumeric code up to 16 characters long that the panel will use as a password to verify its identity with Remote Link. The panel must give the correct key to Remote Link before any programming may take place. All panels are shipped from the factory with the remote key preset as blank.

For security reasons, the Remote Key cannot be viewed from a keypad connected to the panel.

Remote Disarm: Checking the Remote Disarm box allows the panel to be disarmed remotely (keyfob, Android/iOS App, Virtual Keypad™ app, or by MyAccess text messaging). Default is disabled for XR100/XR500 panels. Default is enabled for XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XT30/XT50 Series and XT30INT/XT50INT Series panels.

Dialer Options

XR500/XR100 Version 206

Allow Dialer Remote (XR500/XR100 Version 206 only): Enable to allow remote programming over the phone line. Default is enabled.

Armed Answer Rings: Enter the number of times you wish for the panel to allow the phone line to ring before it answers while all areas of the system are armed. Any number from 0 to 15 can be entered. If 0 (zero) is entered, the panel does not answer the phone when all system areas are armed. The default is 8 (eight).

Disarmed Answer Rings: Enter the number of times you wish for the panel to allow the phone line to ring before it answers while any area of the system is disarmed. Any number from 0 to 15 can be entered. If 0 (zero) is entered, the panel does not answer the phone when all system areas are armed. The default is 8 (eight).

PC Modem: Allows connection to an XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series, or XR100 Series panel for remote programming at 2400 baud through the panel dialer. Leave this box checked to allow communication through an SCS-105.

Receiver Key Operation

When enabled, the panel requests the receiver's key during its first message to the SCS-1R Receiver and this becomes the alarm receiver key. A receiver key is an alphanumeric code programmed into the receiver and identifies it to alarm panels. The panel retains this alarm receiver key in memory and allows remote commands to be accepted over the dialer from the alarm receiver. If an alarm occurs during a remote connect, the alarm report is immediately sent to the alarm receiver and does not appear at the remote programming software.

Enabling this option also enables remote commands and programming to be accepted from a secondary receiver other than the alarm SCS-1R Receiver. The panel requests the service receiver key the first time it is contacted by another receiver and this becomes the service receiver key. The panel retains this service receiver key in memory and accepts remote commands from the service receiver. If an alarm occurs during a remote connect, the panel disconnects from the service receiver and calls the alarm receiver. Alarm reports are only sent to the alarm receiver.

It is important that the alarm receiver key and the service receiver key programmed into the receiver at the central station are NOT the same so the panel can determine the difference between receivers.

When disabled, remote commands and programming are not accepted from the SCS-1R Receiver using digital dialer and all memory of receiver keys is cleared.

Alarm Receiver (XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Version 205 or earlier, and Version 207 or higher): 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 (XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Version 205 or earlier, and Version 207 or higher): 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. If you select No and then attempt to connect to the panel using Remote Link, you will see an error message and will not be allowed to connect.

Network Options

Allow Network Remote: This option displays only if the panel has network capability. Enable to allow remote programming over the network.

Encrypt Network Remote: Enable to encrypt data sent over the network. Default is disabled.

Network Programming Port (XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100N/XR500N Version 206 or higher): Enter the programming port number. The programming port identifies the port used to communicate messages from the panel. The default Programming Port setting is 2001.

Cellular Options

Allow Cell Remote: Enable to allow remote programming over a cellular connection. Default is enabled.

Encrypt Cell Remote: Enable to encrypt data sent over a cellular connection. Default is disabled.

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 set to SECURECOM400.

Second GPRS APN: Enter the second APN (Access Point Name). This works as a backup in case the first APN fails. The APN may contain two lines of 16 characters to equal 32 character Default is set to SECURECOM400.

RS-232 Options

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

Entré Options

(XR100N/XR500N Version 206 or higher, XR150/XR350/XR550 Series, or XR150INT/XR550INT Series panels)

Entré Connection: This option displays only if the panel has network capability. Select NET to allow a dedicated network connection with Entré. Options are NONE or NET. Default is NONE.

Entré Incoming TCP Port: This option displays only if NET is chosen for the Entré connection. Enter the port number for the incoming Entré connection. The port identifies the port used to communicate with the Entré software. This port cannot be the same port as programmed in Network Programming Port. The default Entré Incoming TCP Port setting is 2011.

Entré IP Address: This option displays only if NET is chosen for the Entré connection. Enter the Entré IP address where the panel sends network messages. The Entré IP Address must be unique and cannot be duplicated on the network. Default is 0.0.0.0

Note: When entering an IP address be sure to enter the periods and do not enter leading zeros. For example, IP address 192.168.000.125 is entered as 192.168.0.125.

Entré Outbound TCP Port: This option displays only if NET is chosen for the Entré connection. 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 IP Address: This option displays only if NET is chosen for the Entré connection. Enter the IP backup address where the panel sends network messages if the first Entré IP Address fails. The Entré IP Address must be unique and cannot be duplicated on the network.

Note: When entering an IP address be sure to enter the periods and do not enter leading zeros. For example, IP address 192.168.000.125 is entered as 192.168.0.125.

Entré Backup TCP Port: This option displays only if NET is chosen for the Entré connection. Enter the backup port number for the outbound Entré connection in case the connection to the primary IP fails. Default is 2001.

Entré Checkin: 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 an 8 to 16-character Passphrase using alphanumeric characters. If you leave the Passphrase blank, the panel communicates with Entré, but the data is not encrypted. The Passphrase is blank by default.

Entré Reports (XR150/XR550 only): In the Remote Options window, select from the following reports. All Entré reports default to enabled.

- Arm/Disarm - 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 - 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 Commands - Sends user code changes, schedule changes, and door access denied events.
- Door Access - Sends door access activity: door number, user number and name, and time and date the event occurred.
- Supervisory - 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.

Program Sync Options

Send Local Changes (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series Version 204 or higher): This option allows the panel to automatically update a remote programming computer at the central station with any changes made to the panel. Select NET or DD to send local programming changes or User Menu changes to user codes, user profiles, schedules, or holiday dates to Remote Link after exiting the programming or User Menu. If NET is selected, changes are sent using Network. If DD is selected, changes are sent using Dialer. Select None to disable this feature. Default is None.

Remote Change IP (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series Version 204 or higher): This option displays when NET is selected for Send Local Changes. The Remote Change IP Address must be unique and cannot be duplicated on the network. Default is 000.000.000.000

Note: When entering an IP address do not enter leading zeros.

Remote Change Port (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series Version 204 or higher): This option displays when NET is selected for Send Local Changes. Enter the Port number. Valid numbers are from 1 to 65535. Default is 2002.

Remote Phone Number (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series Version 204 or higher): This option displays when DD is selected for Send Local Changes. Enter the phone number the panel dials when sending programming changes. After entering a phone number, the panel sends any panel changes to the Remote Link programming computer.

The phone number can have two lines of 16 characters each to equal 32. Enter a P to program a two second pause in the dialing sequence. The P character counts as part of the 32 allowable characters. Enter *70P as the string first characters to cancel call waiting. No dial tone detect "D" is required. Dial tone detect is an automatic

panel function.

App Key (XR150INT/XR550INT Series or XR150/XR350/XR550 Series): Enter the 8-digit App Key obtained in your Dealer Settings tab at DMPDealerAdmin.com. This option is a security feature of the Virtual Keypad iPhone/ Android App used only when your Dealer Settings at DMPDealerAdmin.com have EASYconnect set as the Communication Type. This communication option is only available for panels with onboard network and is used to eliminate the need for a static IP address programmed in Network Options. To enter a new App Key, delete the old key and enter any combination of 8 digits provided by DMPDealerAdmin.com. Press COMMAND. The default for this option is blank.

XT30/XT50/XTL/XTLN/XTLN-WiFi Panel

Remote Key: Enter a numerical code up to eight digits long for the panel to use as a password to verify its identity to the Remote Link computer. The panel must give the correct key to Remote Link before any programming may take place. All panels ship from the factory with the key preset as blank.

The Remote Key must match the number entered in the Remote Key field in the Panel Information window. For security reasons, the Remote Key cannot be viewed from a keypad connected to the panel.

Remote Disarm: Check the Remote Disarm box to allow the panel to be disarmed remotely. Default is enabled.

Armed Answer Rings: Enter the number of times you wish for the panel to allow the phone line to ring before it answers while all areas of the system are armed. Any number from 0 to 15 can be entered. If 0 (zero) is entered, the panel does not answer the phone when all system areas are armed. The default is 8 (eight).

Disarmed Answer Rings: Enter the number of times you wish for the panel to allow the phone line to ring before it answers while any area of the system is disarmed. Any number from 0 to 15 can be entered. If 0 (zero) is entered, the panel does not answer the phone when all system areas are armed. The default is 8 (eight).

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. If you select No and then attempt to connect to the panel using Remote Link, you will see an error message and will not be allowed to connect.

App Key (XT30/XT50 Series Version 112 or higher): Enter the 8-digit App Key obtained in your Dealer Settings tab at DMPDealerAdmin.com.

This option is a security feature of the Virtual Keypad app used only when your Dealer Settings at DMPDealerAdmin.com have “EASYconnect” set as the Communication Type.

This communication option is only available for panels with onboard network and is used to eliminate the need for a static IP address programmed in Network Options. The default for this option is blank.

CellComSL, DualCom Panel

CellComSL Version 123

Remote Key: Enter a numerical code up to eight digits long for the panel to use as a password to verify its identity to the Remote Link computer. The panel must give the correct key to Remote Link before any programming may take place. All panels ship from the factory with the key preset as blank.

The Remote Key must match the number entered in the Remote Key field in the Panel Information window. For security reasons, the Remote Key cannot be viewed from a keypad connected to the panel.

Remote Disarm: Check the Remote Disarm box to allow the panel to be disarmed remotely. Default is enabled.

10. 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.

Zone Restorals: This option allows you to control when and if a zone restoral report is sent to the central station receiver. There are three options for how the panel will send zone restoral messages.

Yes: Enables the zone restoral report option. Zone restorals are sent each time a zone restores from a trouble or alarm condition.

No: Disables the zone restoral report option. Zones continue to operate normally but do not send restoral reports to the receiver.

Disarm: Enables the panel to send non-24-hour zone restoral reports whenever a zone that has restored from a trouble or alarm condition is disarmed. All 24-hour zones send restoral reports as they restore.

Access Keypad Enable: Enter the keypad addresses, 1 through 16 for XR350/XR550 Series, and XR500 Series panels and 1 through 8 for XR150 Series and XR100 Series panels, that you wish to send door access reports to the receiver. A report is sent with each door access made from the selected keypads. The report includes the user name and number, and the address of the keypad accessed by the user.

Keypads at addresses not selected still operate the door strike, but do not send door access reports to the central station.

Enter the sequence of addresses separated by commas to enable door access reports; i.e. addresses 1 through 4, 6 and 10 through 16 would be entered as 1-4,6,10-16 in the Access Keypad Enable field.

Opening/Closing Reports: This option allows the selection of Opening/Closing Reports and the number of reports sent to the receiver.

No (XT50/XT30 Series, CellComSL, and DualCom panels) : No opening and closing reports are sent.

Yes (XT50/XT30 Series, CellComSL, and DualCom panels) : Sends opening and closing reports for each programmed area.

Abort Reports: Programs the panel to send an Abort Signal Received (S45) message to the receiver. This abort report is sent any time an area is disarmed after an alarm report has been sent and the bell cutoff time has not expired.

For XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR500 Series panels Version 110 or higher, if the area where the alarm occurred is disarmed after the alarm message has been sent to the receiver but before the bell cutoff time expires even if the alarm was silenced, an Cancel Signal Received (S49) message is sent. The Cancel Signal Received report cannot be disabled.

Note: The panel sends a "Warning: Alarm Bell Silenced" report to the central station if a user silences the alarm bell from a keypad.

Abort reports are also sent when the system is disarmed during transmit delay while the bell output timer is active.

Note: For XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series, and XR100 Series, if the area where the alarm occurred is disarmed before the alarm message has been sent to the receiver during transmit delay and before the bell cutoff time expires even if the alarm was silenced, an Abort Signal (S45) message is sent.

If the area where the alarm occurred is disarmed after the alarm message was sent and before the bell cutoff time expired, a Cancel Signal (S49) message is sent. The Cancel Signal message cannot be disabled.

Bypass Reports: Checking the Bypass Reports box sends all zone bypasses, resets, and force arm reports to the receiver. The bypass report includes the zone number, zone name, and the user name and number of the

individual operating the system.

Schedule Change Reports: Checking the Schedule Change Reports box sends all schedule changes to the receiver. The report includes the day, opening time, and closing time. In addition, the Schedule Change feature will send the user name and number of the individual making these changes. Schedule changes made through Remote Link are not sent to the printer or the event buffer.

Code Change Reports: Checking the Code Change Reports box sends all code additions, changes, and deletions to the receiver. The code change report includes the user name and number added or deleted and the user name and number of the individual making the change. Code changes made through Remote Link are not sent to the printer or the event buffer.

Ambush: Checking this box sends an ambush report to the central station whenever user code number one is entered at a keypad. If you leave this box empty, the panel does not send ambush reports, and user number one becomes a standard user code instead of an ambush code.

Late To Open (XT30/XT50, XTL, XTLN, and XTLN-WiFi only): Enter 1-240 as the number of minutes to elapse that the system may remain armed after the opening time of a schedule without sending a Late To Open message. If the system continues to be armed after the Late to Open minutes expire, a Late To Open message is sent to the central station. Default is 0, which disables the Late To Open option.

Early To Close (XT30/XT50, XTL, XTLN, and XTLN-WiFi only): Enter 1-240 as the number of minutes that the system can be armed prior to the scheduled closing time. If the system is armed prior to the Early to Close minutes, an Early To Close message is sent to the central station. Default is 0, which disables the Early To Close option.

11. System Options

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

11.1. XR Series Panels

XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series, and XR100 Series Panels

System: Configures the system operation for the panel. Choose the operation from the drop-down menu:

Note: Program Arming Mode in Area Information for XR200 Series and 2400F Series panels.

Area: Assigns the panel as an area system. Each area needs to be named in Program >> Area Information.

- XR500 Series, XR550 Series and XR550INT Series panels support Areas 1-32
- XR350 Series panels support areas 1-16
- XR100 Series, XR150 Series and XR150INT Series panels support Areas 1-8
- XR20/XR40 Series panels support Areas 1-4.

All/Perimeter: Assigns the panel as an All/Perimeter (perimeter and interior) system.

- Area 1 = Perimeter and Area 2 = Interior

Home/Sleep/Away: Assigns the panel as a Home/Sleep/Away (perimeter, interior, and bedrooms) system.

- Area 1 = Perimeter, Area 2 = Interior, and Area 3 = Bedrooms

Home/Sleep/Away with Guest (XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series panels): This allows the alarm system to be divided into a main house HOME/SLEEP/AWAY system and up to two other guest houses that also are set up as HOME/SLEEP/AWAY systems.

Areas 1, 2, and 3 are the Perimeter, Interior, and Bedrooms for the Main house system. Areas 4, 5, and 6 are the Perimeter, Interior, and Bedrooms for the Guest 1 house system. Areas 7, 8, and 9 are the Perimeter, Interior, and Bedrooms for the Guest 2 house system. These areas are automatically assigned per system and cannot be changed. See Display Areas in Device Setup to assign keypads to a system. Zones are assigned to a

system by assigning the system's area numbers to the zone in Zone Information programming.

When either All/Perimeter, Home/Sleep/Away, or Home/Sleep/Away with Guest is selected, the area names are automatically assigned and cannot be modified.

Note: Areas 3 and higher in All/Perimeter operation, Areas 4 and higher in Home/Sleep/Away operation, and Areas 10 and higher in Home/Sleep/Away with Guest systems are not available for use and are initialized.

Instant Arm (XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series panels): When selected, the arming keypad displays INSTANT for selection during the exit countdown delay when arming fewer than all areas of the system. At the time instant arming is selected, any entry and exit delays programmed for the areas being armed are ignored. The entry delay for previously armed areas is not affected by instant arming. Default is unselected for an Area System, and selected for an All/Perimeter, Home/Sleep/Away system, or a Home/Sleep/Away with Guest system.

Video (XR200 Series panels): Select YES forces the panel to wait for 60 seconds after a successful communication with a central station receiver before making any additional communication attempts. This 60-second period can be used to allow video transmission or alarm verification (such as 2-way voice) equipment to use the phone line. After the 60-second timer. the panel can once again seize the phone line and send any reports being buffered.

C100/FA100 Wireless Arming (XR200 Series and XR500 Series panels): Allow the use of Inovonics remote arming transmitters.

Closing Wait: When this option is selected, the keypad displays "ONE MOMENT" when an area is armed. The system waits for an acknowledge signal from the central station before arming the selected area(s) and performing a bell test, if that option is selected under Program >> Output Options.

The panel must receive the acknowledge signal from the central station within 90 seconds. If the panel does not receive the acknowledge signal from the central station within 90 seconds, the keypad will display "LOCAL SYSTEM ONLY." Exit delays begin after this 90-second period. The Opening / Closing and User box in Program >> Communications under the Receiver 1 or Receiver 2 tab must be checked to enable Closing Wait.

Reset Swinger Bypass: When Reset Swinger Bypass is selected, an automatically bypassed zone is reset if it remains in a normal condition for one complete hour after being bypassed. The panel sends a report of the automatic reset to the central station if Bypass Reports is checked in Program >> System Reports.

Primary Programming Language: Enables keypads connected to the panel to always display panel programming in the selected language. Available languages are English, Spanish and French. Default is English.

Secondary Programming Language: Allows the installer the choice to view programming in English, Spanish or French. When the programming menu is accessed, the installer is prompted to choose the programming language. When the Secondary Programming Language is set to None, the option to choose a language does not display. Default is None.

Primary User Language: Enables the keypads connected to the panel to always display User Menu and Status List in the selected language. Default is English.

Secondary User Language: Allows the user the choice to view User Menu and Status List in English, Spanish, or French. When the User Menu is accessed, the user is prompted to choose the language. Status list continues to display in the last language selected until another language is selected. When the Secondary Programming Language is set to None, the option to choose a language does not display. Default is None.

For example, selecting Spanish at a keypad displays the User Menu and Status List in Spanish at that keypad. When the user later accesses the keypad, pressing Command once displays the multi-lingual option. If English is selected at that keypad, the User Menu and Status List change to English until another language is selected.

Wireless House Code (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series Version 113 and higher and XR100 Series): When using 1100 Series Wireless, enter a House Code between 1 and 50 for the

wireless system to use. The 1100X Wireless Receiver automatically programs the house code into the wireless transmitters when the unique transmitter serial number is programmed into the panel.

Default is 0 indicating no wireless is being used.

The house code identifies the panel, receiver, and transmitters to each other. When operating, the receiver listens for transmissions that have the programmed house code and transmitter serial number.

Note: The flexibility of DMP two-way wireless operation allows an existing house code to be changed in the panel at any time. The transmitters may take up to two minutes to learn the new house code and continue operation.

Note: When any wireless zone programming is changed in the panel, wireless receiver zone programming is updated. At that point, all wireless zones display as normal for approximately one minute, regardless of the actual state of the zone.

When using FA Series Wireless on XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR500 Series enter 99 for the house code.

Detect Wireless Jamming (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series Version 114 and higher and XR100 Series): This option displays when using 1100 Series wireless devices and the programmed House Code is between 1 and 50. When selected and the wireless receiver detects jamming, a trouble or alarm message is sent to the central station receiver.

Wireless Audible Annunciation: This option displays when the House Code entered is for an 1100 Series Wireless system (1-50). Select the keypad buzzer annunciation method for wireless troubles. Select ANY to enable annunciation anytime. Select DAY to enable annunciation except during sleeping hours (9 PM to 9 AM). Select MIN (minimum) to annunciate only Fire and Fire Verify zones during daytime hours (9 AM to 9 PM). Default is DAY.

Keypad Panics Enabled (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series Version 114 and higher, and XR100 Series): When selected, the two-button panic key operation programmed at the keypad sends Panic, Emergency, or Fire messages to the central station receiver. When not selected the two-button panic operation is disabled.

Enhanced Zone Test: Select this option to enable Enhanced Zone Test operations. The default is deselected.

Enhanced operation allows:

- Panic Test and Walk Test functions can be restricted to operate only during an Area 32, Shift 4 schedule if programmed.
- A Verify message is sent each time a zone is tested. If a zone is tripped multiple times, a Verify message is sent for each trip. This allows the Central Station to record the number of devices per zone.
- The Verify message for each zone test is sent at the time the trip occurs instead of at the end of Walk Test. The System Test Begin and System Test End Central Station messages indicate the type of zone being tested. The System Test Begin message also includes the user name and number.

Send 16 Char Names: This option allows the central stations to select being sent either the first 16 characters of the name field or the entire programmed name, up to 32 characters, for user name, user profile, zone name, area name, output name, and group name.

When selected, the first 16 characters of the name field are sent to the central station. If not selected, all characters entered in the name field up to the maximum of 32 characters are sent. The default is checked.

Note: Using 32 character names increases the length of the DMP Serial 3 message from the panel to the receiver. The SCS-1R receiver does not require an update to pass these messages to the Host Automation System of the Central Station. Before using names longer than 16 characters, determine whether the Host Automation System of your Central Station can accept 17 to 32 character names. If not, only use 16 character names.

Keypad Armed LED

This option is available only when using an Area system. Select ALL to require all keypad display areas to be armed before the keypad Armed LED turns on. Select ANY to turn on the keypad Armed LED when any keypad display area is armed. Default is ALL.

Use False Alarm Question (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series Version 208 and higher)

This option allows an alternate display at the keypad when a burglar alarm occurs.

When selected, the keypad displays “IS THIS A FALSE ALARM? NO YES” rather than “CANCEL VERIFY” for Home/Away or All/Perimeter systems.

Default is disabled.

Allow Own User Code Change (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR500 V210 or higher)

This option allows users without user code authority to change their own user code. When selected, the User Code menu displays USER CODE: ***** at the keypad to allow that user to change their own code. If disabled, the user cannot change their personal user code. Default is disabled.

Panic Supervision (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR500 V210 or higher)

Select to enable a 30 day supervision of the Model 1145-1-B-PSV Wireless Key Fob. Default is disabled.

This option allows an 1145-1-B-PSV key fob that is lost or has a dead battery to be identified at the Central Station host automation system as a missing transmitter, without the need to apply a supervision time in zone information programming. SCS-VR Version 1.3.5 or higher is required to receive 1145-1-B-PSV supervision messages through the XR500 panel.

The 1145-1-B-PSV key fob supervision message is communicated to SCS-VR using all XR500 communication paths where Panic Test is YES within Advanced Communication programming. A supervision message is automatically sent from the key fob to SVS-VR every four hours, resetting the 30 day countdown timer for that key fob serial number. If the 30 day timer expires for a key fob serial number, SCS-VR will generate a zone missing message to the host automation system. For the application where an 1145-1-B-PSV key fob is programmed into several XR500 Version 210 or higher panels, a supervision message sent through any XR500 into which the key fob is programmed will satisfy the 30 day timer. The SCS-VR zone missing message to host automation will be for the last panel account number where the key fob successfully communicated a supervision message to SCS-VR. The 1145-1-B-PSV key fob MISSING is not displayed or recorded at the XR500 control panel.

In addition, this option allows for manual testing of 1145-1-B-PSV key fobs during Walk Test (8144) or Panic Test from the user menu. A key fob that is successfully activated during these test modes will cause an increment to the keypad display TRIPS counter and a Verify message is sent to SCS-VR for that zone. For those 1145-1-B-PSV key fobs that are programmed into the panel but not manually tested, a Fail message is NOT displayed at the keypad and is not sent to SCS-VR.

Time Change:

Hours from GMT: Enter the Greenwich Mean Time (GMT) zone where the panel is located. For example, Central Standard Time would be entered as 6. Please see the table of time zones to help locate the appropriate time zone.

Time Change: When this box is checked, the panel requests time updates from the receiver.

Delays

Zone Activity Hours (XR150/XR350/XR550 Series V107 or higher, XR150INT/XR550INT Series): Allows you to select the number of hours a countdown timer is set to monitor for non-activity. The range for the countdown timer is 0 to 9 hours. The countdown timer starts when the panel is disarmed.

Note: This feature is used to monitor a person for non-activity. This could be used for a person living alone to detect when they have not tripped a disarmed zone within a programmed period of time.

Entry Delay 1: Enter the Entry Delay time for all Exit type zones programmed to use Entry Delay 1. When an armed Exit type zone is faulted, the keypad prewarn tone begins sounding. All keypads programmed to prewarn for that zone display ENTER CODE:- and the name of the zone causing the entry delay. When the first digit of a code is entered, the prewarn tone stops at that keypad. If an invalid code is entered, the prewarn tone begins sounding again. The area must be disarmed before the delay expires or an alarm report is sent to the receiver and an alarm sounds. All zones in that area are delayed along with the Exit zone. Entry Delay times can be from 20 to 250 seconds.

Program Entry Delay 2, 3, and 4 following Entry Delay 1 instructions.

Note: XR150INT/XR550INT Series panels Entry Delay times can be from 5 to 250 seconds.

Note: Specific Exit Error operation is based on the Entry Delay used (1-4) with an EX type zone.

Note: For XR100/XR500 Version 200 or lower, when the SIA CP-01 option is not enabled, the first digit entered at the keypad does not stop the prewarn tone.

Cross Zone Time: Enter the time allowed between zone faults. When zones are cross zoned, the same zone or a second cross zoned zone must fault within this time in order for an alarm report for both zones to be sent to the receiver. If the cross zone time expires without the second zone faulting, only a zone fault from the first zone is reported. Cross-zone time can be from 4 to 250 seconds. Entering 0 (zero) disables this function.

Zone Retard Delay: Enter the retard time assigned to Fire, Supervisory, Auxiliary 1, Auxiliary 2, and Panic type zones. The retard delay only functions when the zone is shorted. The zone must remain shorted for the entire length of the Retard Delay before being recognized by the panel. The Zone Retard Delay can be from 1 to 250 seconds. Entering a zero disables this feature.

Power Fail Delay: Tracks the duration of an AC power failure. When the AC power is off for the length of the programmed delay time, an AC power failure report is sent to the receiver. The delay time can be from 1 to 15 hours. If you enter a 0 (zero), the panel sends the AC power failure report after a 15-second delay.

Miscellaneous Options

Swinger Bypass Trips: Enter the number of times a zone can go into an alarm or trouble condition within one hour before being automatically bypassed. Bypassed zones are automatically reset whenever the area they are assigned to is disarmed. All 24-hour zones are reset when any area of the system is disarmed. Entering 0 (zero) disables this function.

XR500 Series/XR100 Series Version 206 or lower - select 1 to 2 trips

XR500 Series/XR100 Series Version 207 or higher - select 1 to 6 trips

XR150/XR350/XR550 Series - select 1 to 6 trips

XR150INT/XR550INT Series - select 1 to 6 trips

XR200, XR200-485(B), XR2400F - select 1 to 7 trips

Note: The panel hour timer starts at 59 minutes past the hour. If the hour timer expires before the trip counter is exceeded, the trip counter returns to zero. If the trip counter is exceeded before the hour expires, the panel

automatically bypasses the zone. A report of the automatic bypass is sent to the receiver if Bypass Reports is checked in Program >> System Reports.

Bypass Limit (XR150INT/XR550INT Series, XR150/XR350/XR550 Series/XR500 Series/XR100 Series): Enter the maximum number of zones (0 to 8) that can be bypassed in an area when that area is being armed. This limit is only in effect when arming from the keypad. Entering 0 (zero) disables this function allowing an unlimited number of zones to be bypassed. Default is 0.

Inactive User Code Audit (XR150INT/XR550INT Series, XR350 Series, and XR500 V210 or higher)

This option allows users to choose the number of days a user code can remain unused before the panel sends an Inactive User Code message to the receiver. The range is 0-365 days. For XR150/XR550 Series panels, this option is found in the Profiles section.

Occupied Premise (XT30/XT50, XR150/XR350/XR550/XR150INT/XR550INT/XR500 Series/XR100 Series Version 201 or higher): For All/Perimeter or Home/Sleep/Away systems, select this option to allow the panel to automatically disarm the interior area(s) when arming all areas and a perimeter exit zone is not tripped during the exit delay. This False Alarm Reduction feature will keep a user from arming the entire system when they do not exit and remain in the premise. Select NO to disable this feature. Default is checked. Deselect to disable this feature.

Note: With a Home/Sleep/Away with Guest arming system, this feature only applies to the main system.

Inactive User Code Audit (XR150/XR350/XR550 Series and XR500 V210 or higher)

This option allows users to choose the number of days a user code can remain unused before the panel sends an Inactive User Code message to the receiver. The range is 0-365 days.

Weather Zip Code (XR100/XR500 V212 or higher, and XR150/XR350/XR550 Series)

This option allows local U.S.A. weather updates to display on the keypad. Enter the zip code of the user at this prompt. When no number is entered, weather conditions are not displayed. Default is blank.

Weather Zip Code (XR150INT/XR550INT Series)

This option allows International weather updates to display on the keypad. Enter the zip code of the user at this prompt. When no number is entered weather conditions are not displayed. Default is blank.

ISO2 Country Code (XR150INT/XR550INT Series)

Enter the 2-letter country code. Default is US.

Card Plus PIN (XR500E): When checked, all existing user codes will need a PIN number assigned. Program the PIN number in Program >> User Codes. For door access, arm/disarm, or User Menu access, the first code must be entered from a proximity patch, credential card, fob, etc., on a reader from a DMP Keypad (Models 7063, 7163, 7073, 7173, 7872, 7873,) or an external reader. The second code is a PIN number keyed in at the keypad or can be a second credential.

Note: The Card Plus PIN option is only available on Area Systems.

SIA CP-01 (XR500 Series Version 200 or earlier): When selected, the panel operates according to SIA CP-01 standards for the following operations:

Power Up and Stop Routine: the 60 second zone startup delay is turned on.

Keypress Alarm Silence: during an alarm, the keypad alarm and bell output turn off when the first key is pressed at a keypad.

Entry Delay: entering the first digit of a code at the keypad stops the keypad prewarn tone.

Exit Delay: the keypad displays the Exit Delay time countdown and annunciates a tone at 8 second intervals until

the last 10 seconds when annunciation is at 3 second intervals.

Exit Error Operation for Entry Delay 1

When the exit zone is faulted (door still open) at the end of the exit delay:

- the bell sounds for the length of time set in Bell Cutoff programming
- the Entry Delay operation starts, requiring code entry to disarm
- if not disarmed, a zone alarm and an Exit Error are sent to the receiver

Automatic Disarming Operation: The Interior automatically disarms if an exit zone is not tripped during the Exit Delay time when arming All or Away.

Advanced Options

Latched Supervisory Zones (XR100, XR500 Series, XR150/XR350/XR550 Series Panels): Selecting YES latches supervisory zone alarms on the keypad display until the sensor reset operation is performed.

Selecting NO automatically clears the alarm from the keypad display when the supervisory zone restores to a normal condition. Default is YES.

11.2. XT Series Panels

System Options for XT30INT/XT50INT, XT30, XT50, XTLC, XTLN, XTLN-WiFi Panels

System (Arming Mode): This option configures the area arming styles for the panel. Choose the arming mode from the drop-down menu:

Area (Not Available on XRSuper6): Assigns the panel as an area system. Each area needs to be named in Program >> Area Information.

- XT30INT/XT50INT, XT30, XT50, XTL, XTLN, and XTLN-WiFi panels support Areas 1-6

- XR20 and XR40 panels support Areas 1-4

All/Perimeter: Assigns the panel as an All/Perimeter (perimeter and interior) system.

- Area 1 = Perimeter and Area 2 = Interior

Home/Sleep/Away: Assigns the panel as a Home/Sleep/Away (perimeter, interior, and bedrooms) system.

- Area 1 = Perimeter, Area 2 = Interior, and Area 3 = Bedrooms

Note: When any wireless zone programming is changed in the panel, wireless receiver zone programming is updated. At that point, all wireless zones display as normal for approximately one minute, regardless of the actual state of the zone.

Closing Code: When this box is selected, a code is required for system arming. If this box is not selected, a code is not required for system arming.

Closing Check: Select this box to have the panel verify that all areas have been armed after a schedule expires. If the Closing Check finds any areas disarmed past the scheduled time, all keypads emit a steady beep and display CLOSING TIME!. The user must extend the schedule or arm the system within 10 minutes or a Late to Close message will be sent to the central station.

Reset Swinger Bypass: When this box is selected, an automatically bypassed zone is reset if it remains in a normal condition for one complete hour after being bypassed.

The panel sends a report of the automatic reset to the central station if Bypass Reports is checked in Program >> System Reports.

Time Display: Checking this box allows the keypads to display the time and day in the keypad's status list. Leave this box empty if you wish not to display the time and day.

Telephone Access: When this box is selected, the panel allows the use of standard DTMF telephones to arm,

disarm, and check status of the panel.

Wireless House Code (XT30INT/XT50INT/XT30/XT50/XTLC/XTLN/XTLN-WiFi only): When using 1100 Series Wireless, enter a House Code between 1 and 50 for the wireless system to use. The 1100D/1100DINT Series Wireless Receiver automatically programs the house code into the wireless transmitters when the unique transmitter serial number is programmed into the panel. Default is 0 indicating the DMP wireless is not being used.

Note: The XTL/XTLC/XTLN/XTLN-WiFi have a random House Code default.

The house code identifies the panel, receiver, and transmitters to each other. When operating, the receiver listens for transmissions that have the programmed house code and transmitter serial number.

Note: The flexibility of DMP two-way wireless operation allows an existing house code to be changed in the panel at any time. The transmitters may take up to two minutes to learn the new house code and continue operation.

Note: When any wireless zone programming is changed in the panel, wireless receiver zone programming is updated. At that point, all wireless zones display as normal for approximately one minute, regardless of the actual state of the zone.

Detect Wireless Jamming: This option displays when using 1100 Series wireless devices and the programmed House Code is between 1 and 50. When selected and the wireless receiver detects jamming, a trouble or alarm message is sent to the central station receiver.

Wireless Audible Annunciation: This option displays when the House Code entered is for an 1100 Series Wireless system. Select the keypad buzzer annunciation method for wireless troubles. Select ANY to enable annunciation anytime. Select DAY to enable annunciation except during sleeping hours (9 PM to 9 AM). Select MIN (minimum) to annunciate only Fire and Fire Verify zones during daytime hours (9 AM to 9 PM). Default is DAY.

Use Built-In 1100 (XT50 Only): Select this option if using the built-in wireless on the XT50. If selected, zones 80 and 85-99 are available to be programmed as wireless zones. If this option is not checked, then zones 80 and 85-99 are not available. Default is enabled. See XT30/XT50 Series Programming Guide (LT-0981) for more detailed information.

Keypad Panics Enabled: When selected, the two-button panic key operation programmed at the keypad sends Panic, Emergency, or Fire messages to the central station receiver. When not selected the two-button panic operation is disabled.

Use False Alarm Question (XT30INT/XT50INT/XT30/XT50/XTLC Version 108 and higher/XTLN/XTLN-WiFi)

This option allows an alternate display at the keypad when a burglar alarm occurs.

When selected, the keypad displays “IS THIS A FALSE ALARM? NO YES” rather than “CANCEL VERIFY”. Default is enabled.

Delays

Zone Activity Hours: Allows you to select the number of hours a countdown timer is set to monitor for non-activity. The range for the countdown timer is 0 to 9 hours. The countdown timer starts when the panel is disarmed.

Note: This feature is used to monitor a person for non-activity. This could be used for a person living alone to detect when they have not tripped a disarmed zone within a programmed period of time.

Arm/Disarm Activity Days: Select the number of days a countdown timer is set for area arming and disarming activity. The range for the countdown timer is 00 to 99 days. Each time an area is armed or disarmed, the timer is restarted. When the timer counts down to zero because of no arming or disarming activity, the panel sends a "XX Days No Arming/Disarming" message to the receiver. After the message is sent, the timer does not

restart until a panel reset occurs or an area is armed or disarmed.

Note: For the message to be sent to the receiver, Supervisory/Troubles must be selected in Panel >> Communications >> Receiver 1 or Receiver 2.

Entry Delay 1: Enter the Entry Delay time for all exit-type zones programmed to use Entry Delay 1. When an armed Exit type zone is faulted, the keypad prewarn tone begins sounding. "ENTER CODE: -" and the name of the zone causing the Entry Delay displays on all keypads.

When the first digit of a code is entered, the prewarn tone stops at the keypad. If, within five seconds, a valid user code is not entered or an invalid user code is entered, the prewarn tone begins sounding again. Fifteen seconds must elapse before entering a digit silences the prewarn tone again.

The area must be disarmed before the entry delay expires or an Alarm Message is sent to the receiver and an alarm sounds. All Burglary type zones in all areas are delayed along with the Exit zone.

Entry delay times can be from 30 to 250 seconds. Repeat the above for Entry Delay 2 if it is being used. Default is 30 seconds for Entry Delay 1.

Note: Specific Exit Error operation is based on the Entry Delay used (1 or 2) with an EX type zone. See Exit Delay.

Exit Delay: Enter the exit delay time for all Exit type zones. When the exit delay time begins all activity on exit and burglary zones is ignored until the exit delay expires. The keypad displays the Exit Delay time countdown and annunciates the Exit Delay tone at 8 second intervals until the last 10 seconds when annunciation is at 3 second intervals. The exit delay can be from 45 to 250 seconds. Default is 60 seconds.

During Exit Delay, if an exit zone trips, then restores, and trips again, the Exit Delay timer restarts. This restart can occur only once.

Note: When Communication Type is NET, the Exit Delay restart does not occur.

Exit Error Operation: At arming, when an entry/exit zone (EX) is faulted at the end of the exit delay then one of two sequences occur:

For Entry Delay 1 EX type zones:

- the bell sounds for the length of time set in Bell Cutoff programming
- the Entry Delay operation starts, requiring code entry to disarm
- if not disarmed, a zone alarm and an Exit Error are sent to the receiver

For Entry Delay 2 EX type zones:

- the zone is force armed and a zone force arm message is sent to the receiver
- an Exit Error is sent to the receiver
- the bell sounds for the length of time set in Bell Cutoff programming

Cross Zone Time: Enter the time allowed between zone faults. When zones are cross zoned, the same zone or a second cross zoned zone must fault within this time in order for an alarm report for both zones to be sent to the receiver. If the cross zone time expires without the second zone faulting, only a zone fault from the first zone is reported. Cross-zone time can be from 4 to 250 seconds. Entering 0 (zero) disables this function.

Power Fail Delay: Tracks the duration of an AC power failure. When the AC power is off for the length of the programmed delay time, an AC power failure report is sent to the receiver. The delay time can be from 1 to 15 hours. If you enter a 0 (zero), the panel sends the AC power failure report after a 15-second delay.

Miscellaneous Options

Swinger Bypass Trips: Enter the number of times (1-6) a zone can go into an alarm or trouble condition within one hour before being automatically bypassed. Bypassed zones are automatically reset whenever the area they

are assigned to is disarmed. All 24-hour zones are reset when any area of the system is disarmed. Entering 0 (zero) disables this function.

Note: The panel hour timer starts at 59 minutes past the hour. If the hour timer expires before the trip counter is exceeded, the trip counter returns to zero. If the trip counter is exceeded before the hour expires, the panel automatically bypasses the zone. A report of the automatic bypass is sent to the receiver if Bypass Reports is checked in Program >> System Reports.

Weather Zip Code (XT30 Series, XT50 Series, XTLC, XTLN/XTLN-WiFi Series panels)

This option allows local U.S.A. weather updates to display on the keypad. Enter the zip code of the user at this prompt. When no number is entered, weather conditions are not displayed. Default is blank.

Weather Zip Code (XT30INT/XT50INT Series)

This option allows International weather updates to display on the keypad. Enter the zip code of the user at this prompt. When no number is entered weather conditions are not displayed. Default is blank.

ISO2 Country Code (XT30INT/XT50INT Series)

Enter the 2-letter country code. Default is US.

Occupied Premise : When selected, this allows the panel to automatically disarm the interior area(s) when arming all areas and a perimeter zone is not tripped during the exit delay. This False Alarm Reduction feature will keep a user from arming the entire system when they do not exit and remain in the premise. Select NO to not automatically disarm interior area(s). Default is checked.

11.3. CellCom Series Panels

System Options for CellComSL and DualCom

Reset Swinger Bypass: When selected, an automatically bypassed zone is reset if it remains in a normal condition for one complete hour after being bypassed.

Time Change

Hours from GMT: Enter the Greenwich Mean Time (GMT) zone where the panel is located. For example, Central Standard Time would be entered as 6. Please see the table of time zones to help locate the appropriate time zone.

Time Change: When this box is checked, the panel requests time updates from the receiver.

Delays

Entry Delay 1: Enter the Entry Delay time for all exit type zones programmed. When an armed Exit type zone is faulted, the area must be disarmed before the entry delay expires or a fault will be detected. All burglary type zones are delayed along with the Exit zone. Entry delay times can be from 30 to 250 seconds. Default is 30 seconds.

Exit Delay: Enter the exit delay time for all Exit type zones. When the exit delay time starts, all activity on exit and burglary zones is ignored until the exit delay expires. During Exit Delay, if an exit zone trips, then restores, and trips again the Exit Delay timer restarts. This restart can occur only once. Exit delay times can be from 30 to 250 seconds. Default is 60 seconds.

Exit Error Operation: At arming, when any entry/exit zone (EX) is faulted at the end of the exit delay then a zone alarm and an Exit Error are sent to the receiver.

Cross Zone Time: Enter the time allowed between zone faults. When a zone programmed for cross zoning faults, the communicator begins counting down the Cross-Zone Time entered here. If the same zone or another

cross-zoned zone faults within this time, an alarm report is sent to the receiver.

If the Cross-Zone Time expires without the second zone fault, only a zone fault report from the first zone is sent to the receiver. The Cross-Zone Time can be from 4 to 250 seconds in one second increments. Enter 0 (zero) to disable the Cross-Zone Time feature.

Power Fail Delay: Tracks the duration of an AC power failure. When the AC power is off for the length of the programmed delay time, an AC power failure report is sent to the receiver. The delay time can be from 1 to 9 hours. Entering a 0 (zero) sends the AC power failure report after a 15-second delay.

For example, if the power failure delay is set for two hours, then the power failure report will be sent between 2-3 hours.

Miscellaneous Options

Swinger Bypass Trips: Enter the number of times (1-6) a zone can go into an alarm or trouble condition within one hour before being automatically bypassed. Bypassed zones are automatically reset whenever the area they are assigned to is disarmed. All 24-hour zones are reset when any area of the system is disarmed. Entering 0 (zero) disables this function.

Note: The panel hour timer starts at 59 minutes past the hour. If the hour timer expires before the trip counter is exceeded, the trip counter returns to zero. If the trip counter is exceeded before the hour expires, the panel automatically bypasses the zone.

Keypad Input

This option allows the CellComSL or DualCom to communicate with Ademco/Honeywell panels over the Ademco/ Honeywell ECP bus using the zone 4 + and zone 4- terminals.

This allows the communicator to add/delete/change user codes, arm/disarm the Ademco/Honeywell panel, and forward alarm messages from the Ademco/Honeywell to the central station.

Select ECP to enable communication. When NONE is selected, Zone 4 functions as a Bell input. Default is NONE.

See Programming Guide for CellComSL Series for information on programming an Ademco/Honeywell ECP Connection.

11.4. 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 Cadelonia
14	Guam*, Sydney
15	Tokyo, Seoul
16	Hong Kong, Singapore
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
	* Arizona, Hawaii, American Samoa, Guam, Puerto Rico, and the Virgin Islands do not observe Daylight Savings Time.

12. Bell Options

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

Options

There are three types of alarm output available Steady, Pulse, and Temporal (Code 3). Selecting None for an alarm event will cause no alarm to sound for the specified type of alarm.

Action Zone Type

Fire Bell Action Fire Type zones

Burglary Bell Action Burglary Type zones and Exit Error output

Supervisory Bell Action Supervisory Type zones

Panic Bell Action Panic Type zones

Emergency Bell Action Emergency Type zones

Aux 1 Bell Action Auxiliary 1 Type zones

Aux 2 Bell Action Auxiliary 2 Type zones

Miscellaneous Options

Bell Cutoff Time: Enter the maximum time for the bell output to remain on. If the bell output is manually silenced or the area is disarmed, the cutoff time is reset. Enter 0 (zero) to provide continuous bell output. Default is 15 minutes unless otherwise noted.

XT30, XT50, XTL, XTLN, XTLN-WiFi - select 1 to 15 minutes (Default is 5)

Note: The XTL/XTLN/XTLN-WiFi does not allow 0 (zero) to be entered in Bell Cutoff Time.

XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series - select from 1 to 99 minutes

Automatic Bell Test: When this box is selected, the bell output is turned on for two seconds each time an area is completely armed from a keypad.

The automatic bell test is delayed until the Closing Wait acknowledgment is received (if selected). If the Closing Wait acknowledgment is not received within 90 seconds, the bell test will not occur. If Closing Wait is not selected in the System Options window, the automatic bell test occurs when the last area arms.

A bell test only occurs when the areas are armed from a keypad. Arming performed from an arming zone or remotely from Remote Link does not activate a bell test.

Bell Output (XR500 Series, and XR100 Series panels): Enter the output number when needed to follow the panel bell output operation for all actions and off conditions on XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panels. Enter 0 (zero) to disable the output.

Note: When BELL ACTION is set to T for Temporal Code 3, the Bell Output action for an LX-Bus output is pulse.

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

Bell Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XT30/XT50 Series, or XTL/XTLN/XTLN-WiFi Series panels): Enter the output/Favorite number to follow the panel bell (terminal 5) operation for all action and off conditions. Enter 0 (zero) to disable the output.

Note: When BELL ACTION is set to T for Temporal Code 3, the output action is Pulse when connected to:

-an LX-Bus output on an XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panel.

-an output on an XT30, XT50, XRSuper6, XR20, or XR40 panel.

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

13. Output Options

The Output Options window allows you to assign individual outputs to activate for various events. The Output Options window also enables you to set the Cutoff Outputs, Output Cutoff Time, and the Heat and Cool Saver

Temperatures.

Options Section

Cutoff Outputs: Enter the output to turn off after the time specified in Cutoff Time.

To enter an output, click in the field and type the number key for the desired output. The number appears in the field. To turn off an output number, highlight the number that appears in the Cutoff Outputs field and press the delete key.

XT30INT/XT50INT, XT30/XT50, XTL, XTLN, XTLN-WiFi - 1 to 4

XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series - 1 to 6

Cutoff Time: If you assign a Cutoff Output, you may enter a Cutoff Time in one minute increments for the output to remain on. Enter 0 (zero) for continuous output.

XT30INT/XT50INT, XT30/XT50, XTL, XTLN, XTLN-WiFi, - 1 to 15 minutes

XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series - select from 1 to 99 minutes

Energy Saving Section

(XR150INT/XR550INT Series, XR150/XR350/XR550 Series, CellcomSL, DualCom Seies, XT30INT/XT50INT Series, XT30/XT50 Series, XTL/XTLN/XTLN-WiFi Series Version 112 or higher panels)

Heat Saver Temperature: Enter the desired temperature setting for all Z-Wave thermostats when the system is armed ALL or AWAY. When the system is disarmed the thermostats return to their previous settings. The range is 55 to 95 degrees. Default is 0.

Cool Saver Temperature: Enter the desired temperature setting for all Z-Wave thermostats when the system is armed ALL or AWAY. When the system is disarmed the thermostats return to their previous settings. The range is 55 to 95 degrees. Default is 0.

Outputs Section

Program individual outputs to activate for various events. Enter 0 (zero) to disable any output. Select from the following output numbers:

XT30INT/XT50INT, CellComSL, DualCom, XT30, XT50, XTL, XTLN, and XTLN-WiFi Series

1 to 4

31 to 34 - Slow response time wireless outputs (activates within 15 seconds)

41 to 44 - Fast response time wireless outputs (activates within 1 second

F1 to F20 - Activate Z-Wave Favorites

XR100 Series

1 to 6

450 to 474 - Slow response time wireless outputs (activates within 15 seconds)

480 to 499 - Fast response time wireless outputs (activates within 1 second)

500 to 599 - LX-Bus output

D1 to D8 - Keypad door strike relay for addresses 1-16

G1 to G20 - Output group

XR500 Series

1 to 6

450 to 474 - Slow response time wireless outputs (activates within 15 seconds)

480 to 499 - Fast response time wireless outputs (activates within 1 second)

500 to 999 - LX-Bus output

D1 to D16 - Keypad door strike relay for addresses 1-16

G1 to G20 - Output group

XR150INT/XR550INT Series, XR150/XR350/XR550 Series

1 to 6

450 to 474 - Slow response time wireless outputs (activates within 15 seconds)

480 to 499 - Fast response time wireless outputs (activates within 1 second)

500 to 999 - LX-Bus output (XR550)

500 to 799 - LX-Bus output (XR350)

500 to 599 - LX Bus output (XR150)

D1 to D16 - Keypad door strike relay for addresses 1-16 (XR350/XR550)

D1 to D8 - Keypad door strike relay for addresses 1-8 (XR150)

F1 to F20 - Activate Z-Wave Favorites

G1 to G20 - Output group

Communication Fail Output: Enter the output/Favorite to turn on when a Digital Dialer (DD) system fails to communicate on three successive dial attempts or if the backup connection line transmits a report. The Communication Trouble Output also turns on when NET is selected as the primary communication method and NET communication fails after one minute. When NET communication is restored the Communication Trouble Output automatically turns off.

To reset a Communications Fail Output, disarm any area. Enter 0 (zero) to disable the output.

Fire Alarm Output (Not available for CellComSL): Enter the output/Favorite number to turn on when a fire type zone is placed in alarm. The output turns off when a Sensor Reset is performed while no additional fire type zones are in alarm. Enter 0 (zero) to disable the output.

Fire Alarm Output is not compatible with Cutoff Outputs.

FIRE TROUBLE OUTPUT (Not available for CellComSL)

Enter the output number to turn on when a fire type zone is placed in trouble, when a supervisory type zone is placed in trouble, or when any system monitor (AC, Battery, Phone Line 1 or Phone Line 2) is placed in trouble. The output turns off when all fire and supervisory type zones, or system monitors are restored to normal. Enter 0 (zero) to disable this output. This output is not compatible with Cutoff Outputs. This output can be connected to a lamp, LED, or buzzer using the Model 716 Output Expansion module.

An output assigned as a Fire Trouble Output cannot be assigned as a Cutoff Output.

Panic Alarm Output (XR150INT/XR550INT Series): Enter the output/Favorite number to turn on for 3 seconds when any Panic type zone is placed in an alarm condition. The output will turned on again for 3 seconds for each additional Panic zones in alarm. Enter 0 (zero) to disable.

Panic Alarm Output (Not available for CellComSL): Enter the output/Favorite number to turn on when any Panic type zone is placed in an alarm condition. The output is turned off after all Panic zones are restored from an alarm condition and a Sensor Reset is performed. Enter 0 (zero) to disable.

Wireless Outputs (XT30, XT50, XTL, XTLN, or XTLN-WiFi)

If a wireless output is programmed, the panel sends the Panic Test Cadence or the Panic Alarm Cadence to the output when a Panic Test is performed or a Panic Zone is placed in alarm.

Wireless Outputs (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series)

The Panic Alarm is compatible with the Model 1118 Wireless Remote Indicator Light and the Model 1116 Wireless Relay Output connected to a Model 572 Indicator LED.

- When a Panic Alarm occurs, the LED turns on steady for five minutes and then turns off.
- When a Panic Test is initiated from the keypad, the LED flashes quickly for five minutes.
- For a Panic Alarm, a fast response wireless output number is recommended.

Ambush Output (Not available for CellComSL): Enter the output/Favorite number to turn on when an Ambush code is entered at a keypad. The output turns off when a Sensor Reset is performed.

Entry Output (Not available for CellComSL): Enter the output/Favorite number to turn on at the start of the entry delay time. The output turns off when the area disarms or the entry delay time expires.

Exit Output (XR500/XR100 Series): Enter the output number to turn on when an exit delay time starts in any area of the system. The output turns off when the area arms or when the arming has been stopped.

Begin Exit Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XT30INT/XT50INT Series, XT30/XT50 Series, XTL Series Version 110 or higher only, and XTLN/XTLN-WiFi Series): Enter the output/Favorite number to turn on when an exit delay time starts in any area of the system. The output turns off when the area arms or when the arming stops.

End Exit Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XT30INT/XT50INT Series, XT30/XT50 Series, XTL Series Version 110 or higher only, and XTLN/XTLN-WiFi Series): Enter the output/Favorite number to turn on when an exit delay time ends in any area of the system. The output turns off when the system disarms.

Ready Output (Not available for CellComSL): Enter the output/Favorite number to turn on when all disarmed burglary zone types are in a normal state. The output turns off when any disarmed burglary type zone is in a bad state. This output is not compatible with Cutoff Outputs.

Phone Trouble Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series,): Enter the output number to turn on when the phone line monitor in the DMP 893A detects a voltage below 3 VDC on the phone block. The output is turned off when phone voltage rises above 3 Vdc.

Late to Close Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series,): Enter the output/Favorite number to turn on at the expiration of a closing schedule. The output activates simultaneously with the "CLOSING TIME!" keypad display. The output turns off when the late area is armed, the closing is extended, or the schedule is changed.

Device Fail Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series): Enter output number to turn on when an addressed device fails to respond to polling from the panel. The panel also sends a missing device report to the receiver. The output is turned off when the device reported as missing responds to polling or is removed from the system.

Enter 0 (zero) to disable this output and the LX-Bus device fail reporting to the central station.

The Device Fail Output option should not be used if the system has any unsupervised devices.

Note: Remote Link displays the first Device Missing message. Subsequent Device Missing messages are incremented on the repeat counter and do not display individually.

Sensor Reset Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series):

Closing Wait Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series):

Armed Output (XT30INT/XT50INT Series, XT30/XT50 Series, XTL Series Version 110 or higher only, and XTLN/XTLN-WiFi Series): Enter the output/Favorite number to turn on any time an area of the system arms. The output turns off when the system completely disarms. Enter 0 (zero) to disable this output.

Favorites

For a Home/Away system

When the system is armed AWAY, the programmed Favorite activates.

When the system is armed SLEEP, the programmed Favorite plus 1 is activated. For example, If the Armed Output is F05, F06 activates when Sleep is armed.

When the system is armed HOME, the programmed Favorite plus 2 is activated. For example, If the Armed Output is F05, F07 activates when Home is armed.

For an All/Perimeter system

When the system is armed ALL, the programmed Favorite activates.

When the system is armed PERIMETER, the programmed Favorite plus 1 is activated.

For example, If the Armed Output is F05, F06 activates when Perimeter is armed.

For an Area system:

When any area of the system is armed, the programmed Favorite activates.

Disarmed Output (Not available for CellComSL and XR500/XR100 Series panels): Enter the output/Favorite number to turn on when all areas of the panel are disarmed. The output turns off when the an area is armed. Enter 0 (zero) to disable this output.

Burglary Output (Not available for CellComSL and XR500/XR100 Series panels): Enter the output/Favorite to turn on any time a burglary zone goes into alarm. The output turns off when the area in which the alarm occurred disarms and no other burglary zones are in alarm. Enter 0 (zero) to disable this output.

Arm-Alarm Output (Not available for CellComSL): Enter the output/Favorite number to turn on steady when any area of the system is armed. If an alarm occurs causing the keypads to turn Red, this output pulses and continues to pulse for approximately three (3) minutes after the panel is disarmed.

Wireless Outputs

The Arm-Alarm Output is compatible with the Model 1117 Wireless LED Annunciator and the Model 1116 Wireless Relay Output connect to a Model 572 Indicator LED.

- When the Model 1117 is battery operated the LED is off when the system is armed to conserve battery life. If an alarm occurs, the output flashes quickly.
- When the Model 1116 is connected to a Model 572 LED annunciator, the LED is on when the system is armed. If an alarm occurs, the output pulses.

Note: The Arm-Alarm Output option is available on XR150/XR350/XR550 Series, XR100/XR500 Series, XT30, XT50, XRSuper6, XR20, and XR40 panels.

Supervisory Alarm Output (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series): Enter the output number to turn on when a supervisory zone type is placed into an alarm. The output turns off when all supervisory type zones are restored to normal. Enter 0 (zero) to disable. Default is 0.

Home/Perimeter Output, All/Away Output, Sleep Output (XT30/XT50, XTLplus, and XR150/XR550 Series): Enter the output/Favorite number to you would like to have associated with the selected arming type.

14. Output Information

This section allows you to assign an output number and name to relay outputs. In addition you can program wireless outputs into the panel when using an 1100 Series Wireless Receiver.

To program a new output, select New, and enter each field described below. When you are done, select OK.

To delete an output name, select the corresponding line from the list and select Delete.

Note: Serial Number and Supervision Time options are available on XR150INT/XR550INT Series, XR150/XR350/ XR550 Series, XR100/XR500 Series, XT30INT/XT50INT, XT50, and XR30.er6, XR20, and XR40 panels.

Output Number: Enter the number of the output you are programming. Select from the following output numbers:

Note: In order for wireless output troubles to display at a keypad, the keypad address must be specified at the Auxiliary 1 Zones prompt in Status List programming.

XT30INT/XT50INT, XT30/XT50

1 to 4

31 to 34 - Slow response time wireless outputs (activates within 15 seconds)

41 to 44 - Fast response time wireless outputs (activates within 1 second)

F1 to F20 - Activate Z-Wave Favorites

XTL, XTLN, XTLN-WiFi

31 to 34 - Slow response time wireless outputs (activates within 15 seconds)

41 to 44 - Fast response time wireless outputs (activates within 1 second)

F1 to F20 - Activate Z-Wave Favorites

XR150INT, XR150 Series, XR100 Series,

1 to 6

450 to 474 - Slow response time wireless outputs (activates within 15 seconds)

480 to 499 - Fast response time wireless outputs (activates within 1 second)

500 to 599 - LX-Bus output

D01 to D08 - Keypad door strike relay for addresses 1-16

G01 to G20 - Output group

XR350

1 to 6

450 to 474 - Slow response time wireless outputs (activates within 15 seconds)

480 to 499 - Fast response time wireless outputs (activates within 1 second)

500 to 799 - LX-Bus output (XR350)

D01 to D16 - Keypad door strike relay for addresses 1-16 (XR350/XR550)

F1 to F20 - Activate Z-Wave Favorites

G01 to G20 - Output group

XR550INT Series, XR550, XR500 Series

1 to 6

450 to 474 - Slow response time wireless outputs (activates within 15 seconds)

480 to 499 - Fast response time wireless outputs (activates within 1 second)

500 to 999 - LX-Bus output

D01 to D16 - Keypad door strike relay for addresses 1-16

G01 to G20 - Output group

Output Name: Enter the name you wish to assign to a specific output. An output name may be up to 16 characters long.

Note: XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series Version 205 or higher accept names up to 32 character.

Real-time Status (XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series Version 203 or higher): If selected, this allows Real-Time Status reports, such as Output ON, OFF, PULSE, or TEMPORAL to be sent to the PC Log computer to monitor zones, doors, and outputs by reporting status changes.

Serial Number: Enter the eight-digit serial number found on the wireless output. The serial number must be between 15000000 and 15999999 and cannot contain any non-numeric characters. A panel cannot have two wireless outputs with the same serial number. Each wireless output programmed for a specific panel must have a unique serial number.

Supervision Time: Select the supervision time required for the wireless output. The wireless output must check in at least once during this time or a missing condition is indicated for that output. 1100 Series transmitters automatically check in based on the supervision time selected for the wireless output, no additional programming is needed. Select 3, 60, or 240 minutes.

On XTLN, XTLN-WiFi, XTL Version 105, XT30/XT50 Version 106, XR100/XR500 Series Version 207, XR150/XR350/XR550 Series and XR150INT/XR550INT Series panels, the 3 minute supervision time is only available if using an 1135/1135DB Wireless Siren. Select None for unsupervised operation. Default is 240 minutes.

Note: When the panel is reset, a receiver is installed or powered up, or Remote Link disconnects, the supervision timer restarts for all wireless outputs.

Trip with Panel Bell (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series Version 207 or higher, XT30INT/XT50INT Series XT30/XT50 Series Version 106 or higher, XTL, XTLN, and XTLN-WiFi): Select this option to have the 1135/1135DB wireless siren follow the panel's bell output cadence for the zone type and bell cutoff time up to 15 minutes. Default is YES.

Description: A description or note can be assigned to each Output Name in the field on the right side of the Output Information window. To enter a note or description, press the Description button to open the Edit Rich Text window. After typing the note, go to File >> Save and Exit to save the work and close the Edit Rich Text window. The note appears in the field above the Description button.

15. 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.

Output Group Number: Enter a group number from 1 to 20 in the Group Number field.

Output Group Name: Enter a name for the Output Group selected. You may enter up to 32 characters for a group name.

Note: XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series Version 205 or higher accept names up to 32 character.

Output Number: Enter the number of the output you wish to assign to a group. You may assign up to eight outputs per group. Entry range:

XR150INT Series, XR150 Series, or XR100 Series Series

- select 1 to 6, 500 to 599, D1 to D8 (doors), or G1 to G20 (groups)

XR350 Series

- select 1 to 6, 500 to 799, D1 to D16 (doors), F1 to F20 (Favorites), or G1 to G20 (groups)

XR550INT Series, XR550 Series, XR500 Series

- select 1 to 6, 500 to 999, D1 to D16 (doors), or G1 to G20 (groups)

Note: Output Groups 1 through 10 can be assigned to a user profile for applications such as elevator control. See the Output Group section of the XR150INT/XR550INT Series User Guide (LT-1278INT), XR150/XR350/XR550 Users Guide (LT-1278), or XR500/XR100 Users Guide (LT-0683) for additional information.

Note: Output groups 11 through 20 can be assigned to a profile using Remote Link.

Assign a description or note about each output group in the field at the bottom right corner of the Output Groups window. To enter a note or description, press the Description button to open the Edit Rich Text window. After you type your note, go to File >> Save and Exit to save your work and close the Edit Rich Text window. Your note appears in the field above the Description button.

16. Menu Display

XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series panels

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

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.

Time Display: Enter the keypad addresses that can display the time and day of the week.

Arm Disarm Display: Enter the keypad addresses from which users can arm and disarm the system.

Note: Enter the sequence of addresses separated by commas to enable door access reports; i.e. addresses 1 through 4, 6 and 10 through 16 would be entered as 1-4, 6, 10-16.

17. Status List

XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series panels

This option allows you to program alarm, trouble, and status keypad displays. Each option that you program will automatically cycle on the keypad display when the keypad is not performing any other function.

The options in the Status List window define which keypad addresses display the various status information. Any combination of addresses can be entered to display the status items that follow. If you do not want a particular status item to display, do not enter any addresses in these fields.

Note: Enter the sequence of addresses separated by commas to enable door access reports; i.e. addresses 1 through 4, 6 and 10 through 16 would be entered as 1-4,6,10-16.

System Troubles Status Monitors: Specifies the addresses where System Troubles are displayed. If you select this option for a keypad address, the following will display at the selected keypad:

- AC Power
- Battery Power
- Closing Check
- Panel Box Tamper
- Phone Line 1
- Phone Line 2
- Wireless Receiver Trouble
- Wireless Jamming Trouble or Alarm

Fire Zone Keypads: Specifies the keypad addresses to display all fire zone alarms and troubles. The zone name is displayed on the keypad and if it is a trouble condition, a steady trouble buzzer will sound at the keypad.

Burglary Zone Keypads: Specifies the addresses where all burglary zone alarms and troubles are displayed. Burglary zones include Night, Day, and Exit type zones. Burglary zone troubles remain in the list until the zone restores.

Supervisory Zone Keypads: Specifies the addresses where all supervisory zone alarms and troubles are displayed. When the keypad displays a supervisory zone, the keypad buzzer will sound. To silence the keypad buzzer, enter a valid user code at the keypad.

Panic Zone Keypads: Specifies the addresses where all panic zone alarms and troubles are displayed. The name of the zone remains in the list until the zone restores. The keypad buzzer does not sound for panic alarms or troubles.

Emergency Zone Keypads: Specifies the addresses where all emergency zone alarms and troubles are displayed. The name of the zone remains in the list until the zone restores. The keypad buzzer does not sound for emergency alarms or troubles.

Auxiliary 1 Zone Keypads: Specifies the addresses where all Auxiliary 1 zone alarms and troubles are displayed. The name of the zone remains in the list until the zone restores. The keypad buzzer does not sound for Auxiliary 1 alarms or troubles.

Auxiliary 2 Zone Keypads: Specifies the addresses where all Auxiliary 2 zone alarms and troubles are displayed. The name of the zone remains in the list until the zone restores. The keypad buzzer does not sound for Auxiliary 2 alarms or troubles.

Communication Path Trouble: Specifies the way communication path troubles are displayed on keypads programmed to display system troubles.

Select NO to not display communication path troubles on any keypad.

Select YES to display COMM -TRBL when any communication path fails.

Select ALL to display COMM -TRBL only when all communication paths have failed.

18. Printer Reports

XR100/XR500 Series panels

This section allows you to program the types of reports the panel will print using the optional Printer Interface Card. The Printer Interface Card allows you to connect a compatible 40 or 80 character serial printer to the alarm panel.

The options you may select in the Printer Reports window are:

Arm / Disarm Reports: Prints arming, disarming, and Late to Close reports. Reports include the area number, name, and action (armed, disarmed, or late), the user number, user name, and time and date.

Zone Reports: Prints changes in the status of active zones. Reports include the zone number, name, and type as well as the action (alarm, trouble, bypass, etc.) user number (if applicable) and area name.

User Command Reports: Prints user code changes, outputs turned on or off, schedule changes, and User Menu functions.

Door Access Reports: Prints door access activity. Reports include the door number, user number and name, and the time and date of the door access.

Supervisory Reports: Prints system monitor troubles and system events.

Customer Name: (1812 panel only.) Enter the name of account in the Customer Name field.

19. PC Log Reports

PC Log Reports menu is available on all XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series Version 106 or higher

Host Log Reports menu is available on Version 105 and lower: XR500 Series

This section allows you to program the types of PC log reports the panel sends through the onboard Ethernet port, 462N Network Interface Card, or the J21 Serial Connector. The reports include information such as the type of activity, time and date of the activity, and user name and number. These data reports can be accessed using the Advanced Reporting module. See the Advanced Reporting module section for more detailed information. See the XR150/XR350/XR550 Series Installation Guide (LT-1233), XR500 Series Installation Guide (LT-0681) for detailed J21 or J1 setup information or the XR100 Series Installation Guide (LT-0899) for detailed J1 setup information.

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

Note: The network connection that the PC/Host Log Reports are sent through is not monitored for network trouble. PC/Host Log Reports is intended as an auxiliary log of panel activities and is not intended nor designed for Central Station Monitoring.

If there is trouble with the network connection, the panel will continue to attempt to send the PC/Host Log Reports until the connection is reestablished. The panel will then send the reports. Also, a Network Trouble message will not be sent if the connection is lost. The PC/Host Log Reports have the lowest priority of panel reports sent.

PC/Host Log Reports CANNOT be sent to an SCS-1 or SCS-1R Central Station Receiver.

Comm Type (XR500/XR100 Series Version 106 or higher): Select the Communication Type for the panel to send the PC Log Reports. Default is None.

Options Section

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.

Zone Reports: Sends changes in the status of active zones. Includes the zone number, name, and type as well as the action (alarm, trouble, bypass, etc.) user number (if applicable) and area name. When the Walk Test or Panic Zone Test (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500N/XR500E/XR100N panels only) is performed, Verify and Fail messages are also sent for each zone.

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

Door Access Reports: Sends door access activity. Includes the door number, first and second (485B only) user number, first and second (485B only) user name, and the time and date.

Supervisory Reports: Sends system monitor reports, such as AC and battery, and system event reports. Supervisory Reports also sends the following reports:

- Abort
- Alarm Bell Silenced
- System Recently Armed
- Ambush
- Exit Error
- Unauthorized Entry
- Late to Close (only sent as a Supervisory Report if Area Schedules is not enabled, Closing Check is enabled, and an opening/closing schedule has been programmed.)

Note: To send these reports through the PC/Host Log, you must enable Supervisory Reports.

Real-time Status (XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series Version 203 or higher): Select to send Real-Time Status reports for selected zones, doors, and outputs. The specific reports must also be selected by individual zone or output. The Real-Time Status messages are sent to a PC running a graphic display software. The messages that can be sent are:

- Door Open with zone number
- Door Closed with zone number
- Door Open with door number
- Door Closed with door number
- Output On
- Output Off
- Output Pulse
- Output Temporal

Net Options

Net IP Address: This option displays when the Communication Type is Net. Enter the IP address containing up to 16 characters.

Net Port: This option displays when the Communication Type is Net. Enter the port number. Valid port numbers are from 0 to 65535. Default is 2001.

232 Port: This option displays when Communication Type is 232. To enable PC Log Reports, select either the onboard connector (O) or select A, B, C, D or E for the corresponding slot in use on the Model 462N Network Interface card. The slots are labeled from left to right, beginning with A. Default is 0.

232 Setup String: This option displays when the Communication Type is RS-232. Enter up to a 32 character modem string.

For XR500 Series Version 121 or earlier

PC Log Address: Enter up to two lines of 16 characters to equal 32 characters for the IP address string that is sent to the network device to allow PC Log messages to be sent to a PC through an IP Network.

Do not enter a PC Log Address string:

- If you are using a direct connection through the 462N card to a Remote Link computer or if you are using J21 Serial Connector on an XR500N/XR500E/XR100N panel for PC Log Reporting.

When using an XR500N/XR500E/XR100N, enter the following address string: AT#UCXXX.XXX.XXX.XXX#PPPPP to direct PC Log reports to a new address using the Ethernet connection. The Xs represent the target IP Address, and the Ps represent the port number. The default port number is 2001. An example of a PC Log Address string is: AT#UC192.168.001.099#2001.

Note: The PC Log Address CANNOT be the same as that entered in Communication remote IP address.

20. Area Information

To program a new area, press the New button and enter the settings for the new area into the fields in the Area Information window.

To delete a programmed area, select the area in the list on the left side of the window and press the Delete key.

To modify the programming for an area, select the area by selecting the line in the list, and then make any desired changes to the fields in the Area Information window. Select OK when you finish making changes to the area.

XR150INT/XR550INT Series and XR150/XR550 Series panels

Global Settings

Exit Delay: Enter the exit delay time for all Exit type zones in this area. When the exit delay time starts, all activity on that zone and other non-24-hour zone types in the area is ignored until the exit delay expires. The keypad displays the Exit Delay time countdown and annunciates the Exit Delay tone at 8 second intervals until the last 10 seconds when annunciation is at 3 second intervals.

The exit delay can be from 30 to 250 seconds. Default is 60 seconds.

During Exit Delay, if an exit zone trips, then restores, and trips again, the Exit Delay timer restart. This restart can occur only one.

Exit Error Operation: At arming, when an entry/exit zone (EX) is faulted at the end of the exit delay then one of two sequences occur:

For Entry Delay 1 EX type zones:

- the bell sounds for the length of time set in Bell Cutoff programming.
- the Entry Delay operation starts requiring code entry to disarm.
- if not disarmed, a zone alarm and an exit error are sent to the receiver.

For Entry Delay 2-4 EX type zones:

- the zone is force armed and a zone forced and a zone force arm message is sent to the receiver.
- an Exit Error is sent to the receiver.
- the bell sounds for the length of time set in Bell Cutoff programming.

Early Morning Ambush (Network panels only): Enter the number of minutes (1 to 15) before a silent alarm (Early Morning Ambush S33) is sent to the central station using the area 1 account number. Enter 0 (zero) to disable this option.

When a user code is entered to disarm area 1 at a keypad or reader with Access Areas assigned to area 1, the same or different user code must be entered within the programmed number of minutes to prevent an ambush message from being sent to the receiver. The second user code also must have authority to disarm area 1.

In addition, a zone activation with Alarm Action Message C also cancels the Early Morning Ambush timer and stops an Ambush message from being sent to the receiver. See Report to Transmit section in Zone Information.

The keypad does not display any indication that the ambush timer is running.

Indications can be provided by assigning an output number to Entry Output and Ambush Output in Output Options. Entry Output turns on one minute before the timer expires and turns off at expiration. Ambush Output turns on at the times' expiration and turns off when Sensor rest is performed.

Closing Check: Select to enable the panel to verify that all areas in the system are armed after permanent or extended schedules expire. If the Closing Check finds any areas disarmed past the scheduled time, the keypads selected to display System Trouble Status displays CLOSING TIME! and emits a steady beep. When Area Schedules is set to YES in Area Information, the specific area and name display followed by - LATE.

When Auto Arm is NO, if within ten minutes the system is not armed or if the schedule is not extended, a Late to Close report is sent to the SCS-1R Receiver. When Auto Arm is YES, the area arms. See Automatic Arming section.

If the area becomes disarmed outside of any schedule, the Closing Check sequence occurs after the Late Arm Delay time. See Late Arm Delay.

When Closing Check is NO and Auto Arm is YES, the system immediately arms when the schedules expires. No

warning tone occurs.

In addition, when Closing Check is NO, the option to extend a schedule does not display when the schedule expires.

Closing Code: When selected, a code number is required for system arming. If not selected, a code number is not required for system arming.

Any Bypass: 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.

Area Schedules (XR100/XR500 Series): Select the Area Schedules box to allow each area to set its own shift schedules 1 to 4. Deselected will provide one set of schedules for the system.

Area Schedules (XR100/XR500 Series): Select the Area Schedules box to follow individual sets of area schedules programmed in the User Menu. Deselected for all areas to follow only one set of schedules in the User Menu. See Schedules for information.

Configuring Area Information

Area: Assign a number to the area you are programming.

- XR550INT, XR550, and XR500 Series panels = 1 - 32 areas
- XR350 Series = 1 - 16 areas
- XR150INT and XR150 Series panels = 1 - 8 areas
- XT50/XT30, XTLC/XTLN/XTLN-WiFi = 1 - 6 areas

Area Name: Assign a name up to 32 characters long for the area you are programming. Only Area systems allow the Area Name to be changed. An All/Perimeter or Home/Sleep/Away System have preassigned names and cannot be changed.

- Area 1 = Perimeter
- Area 2 = Interior
- Area 3 = Bedrooms

Areas 1, 2, and 3 are the Perimeter, Interior, and Bedrooms for the Main house system. Areas 4, 5, and 6 are the Perimeter, Interior, and Bedrooms for the Guest 1 house system. Areas 7, 8, and 9 are the Perimeter, Interior, and Bedrooms for the Guest 2 house system (XR550INT, XR550, XR350, XR500 only).

Note: XR100/XR500 Series Version 204 and earlier accept 16 character names.

Account Number: Enter the account number to be sent to the receiver for this area. Choose an account number compatible with the Main Communication Type selected in Communications. The default Account Number is the one previously entered in Communications.

For XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series panels Version 203 or higher, this account number is used when sending area messages and events to the central station. XR100 and XR500 alarm systems send an area account number instead of the system account number with the following panel messages/events based in the area assigned to the zone that initiated the alarm:

- WARNING: Alarm Bell Silenced (S34)
- Abort Signal Received (S45)
- Cancel Signal Received (S49)
- ALERT: System Recently Armed (S78)
- ALERT: Exit Error (S80)
- ALARM: Verify Signal Received (S96) (not currently sent on area systems)

The XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series has always sent the area account number for the following messages:

Zone event messages for all non-24 hour zones assigned to an area

- Arming
- Disarming

The XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series sends the following messages using the area account number based on the lowest area number in Display Areas programming from the keypad being used:

- User Code Add/Change/Delete
- Door Access/Denied
- User 1 Ambush and Early Morning Ambush
- System Test Begin/End
- Unauthorized Entry
- Service Code and Service Request

The XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series sends the following messages using the area account number based on the area number:

- Late to Arm for area schedules

Opening/Closing Reports: With this option, you can select which area can send Opening/Closing Reports to the central station when an area is armed and disarmed.

Bad Zones: Some zones may not be in a normal condition at the time that they are to automatically arm. This option allows you to program the panel response to these bad zones.

Bypass: This option will bypass all bad zones upon arming. A report of the bypass is sent to the receiver if you select Bypass in the System Reports window.

Force Arm: This option will force arm all bad zones upon arming. Zones that are force armed are capable of restoring and reporting an alarm if tripped. A report of the force arm is sent to the receiver if Bypass is selected in the System Reports window.

Refuse Arm: This option will refuse automatic arming in the event of a bad zone at arming. The panel sends a "No Closing" report to the receiver regardless of whether Closing Check is selected in the Partition Information or System Area Information window.

Armed Output: Enter the output number to turn on when this area is armed. If an exit delay is used for this area, the Armed Output turns on at the start of the exit delay. The output is turned off when this area is disarmed. The output cannot be turned on from the User Menu Outputs On/Off option or from the System Status window.

Burglary Bell Output: Enter the output number (0 to 6, 500 to 999, G1 to G20, D1 to D16, or F1 to F20) that is turned on any time a Burglary type zone is placed in alarm. The output is turned off when you disarm any area and no other Burglary type zones are in alarm. The output can also be turned off using the Alarm Silence option in the User Menu or by entering a user code with the authority to silence alarms. The duration of this bell output follows the time entered section. If Bell Test is selected YES, the Burglary Bell Output entered here is turned on for two seconds each time the system is armed.

Late Output: Enter the output number to turn on at the expiration of a closing schedule. The output will activate simultaneously with the "CLOSING TIME!" keypad display. This output turns off when the late area is armed, the closing is extended, or the schedule is changed.

Late/Arm Delay : Enter 4 to 250 minutes to delay before automatic re-arming occurs after the area becomes disarmed outside of schedules. Default is 60 minutes.

Note: The late Arm Delay can be superseded by the Re Arm Delay setting of the User Profile assigned to the user who disarmed the area.

Auto Arming: Selecting this box will allow this area to arm automatically as scheduled. If no schedules are programmed and this option is selected, the area will auto arm every hour. Leaving the Auto Arm box empty will disable automatic arming for this area.

If Closing Check is enabled, the automatic arming function does not take place until the expiration of the a ten minute Closing Check delay. See Closing Check. 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 option selected in Bad Zones. If a closing report is sent, the user number is indicated as SCH on the SCS-1R receiver.

On XR500 Series panels, if within ten minutes after the schedule expires, the system is not armed or a temporary schedule is not entered to extend the closing time, a Late to Close report is sent. When Auto Arm is YES, the area arms. If the area becomes disarmed outside of any schedule, the Closing Check sequence occurs after the Late/Arm Delay time.

When Closing Check is NO and Automatic Arming is YES, the system immediately arms when the schedule ends. No warning tone occurs. When NO is selected at the Closing Check prompt, the Extend Time option does not display when a schedule expires.

Auto Disarm: When this option is selected, the area automatically disarms according to schedule. Not selecting this box will disable automatic disarming by schedule for the area.

Note: For XR100/XR500 Version 200 or lower, when the SIA CP-01 option in System Options is set to NO, the Interior area auto disarm does not occur if an exit zone is not tripped during the exit delay time.

Bank Safe & Vault: When this option is selected, the area can only be disarmed during scheduled times. Not selecting this box will disable Bank Safe & Vault mode for this area.

Note: Do not assign Bank Safe & Vault areas to an Arming zone. Arming zones can disarm Bank Safe & Vault areas outside of a schedule.

Common Area: Selecting this box will enable the area to operate as a common area. This area is armed when the last area in the partition is armed and is disarmed when the first area in the partition is disarmed. You can have multiple common areas in each partition.

Two Man Rule: Checking this box will require two user code entries to disarm or allow door access in this area. When a user presents a code to a keypad or reader requesting door access or disarm, the keypad will display "2ND CODE". A second user code with at least the same authority must be entered to allow entry or to disarm.

Arm First: Enables the area to operate as an Arm First area. This area automatically arms when any non-Arm First area assigned to the same keypad is armed but does not disarm when other areas become disarmed. If an Arm First area has faulted zones that cannot be bypassed, arming stops. Default value is NO.

Description: Enter a note about the area that you are programming. To enter a note or description, press the Description button to open the Edit Rich Text window. After you type your note, go to File >> Save and Exit to save your work and close the Edit Rich Text window. Your note appears in the field above the Description button.

Program >> Area Information

- To program a new area, press the New button and enter the settings for the new area into the fields in the Area Information window.
- To delete a programmed area, select the area in the list on the left side of the window and press the Delete key.
- To modify the programming for an area, select the area by selecting the line in the list, and then make any desired changes to the fields in the Area Information window. Select OK when you finish making changes to

the area.

XT30INT/XT50INT Series, XT50/XT30 Series, XTL/XTLN/XTLN-WiFi Series panels

Area: Assign a number to the area you are programming.

- XT50/XT30, XTLC/XTLN/XTLN-WiFi = 1 - 6 areas

Area Name: Assign a name up to 32 characters long for the area you are programming. Only Area systems allow the Area Name to be changed. An All/Perimeter or Home/Sleep/Away System have preassigned names and cannot be changed.

- Area 1 = Perimeter
- Area 2 = Interior
- Area 3 = Bedrooms

Bad Zones: Some zones may not be in a normal condition at the time that they are to automatically arm. This option allows you to program the panel response to these bad zones.

Bypass: This option will bypass all bad zones upon arming. A report of the bypass is sent to the receiver if you select Bypass in the System Reports window.

Force Arm: This option will force arm all bad zones upon arming. Zones that are force armed are capable of restoring and reporting an alarm if tripped. A report of the force arm is sent to the receiver if Bypass is selected in the System Reports window.

Refuse Arm: This option will refuse automatic arming in the event of a bad zone at arming. The panel sends a "No Closing" report to the receiver regardless of whether Closing Check is selected in the Partition Information or System Area Information window.

Auto Arming: Select to enable this area to arm automatically according to the opening and closing schedule.

If Closing Check is selected, the automatic arming does not take place until the expiration of a 10-minute Closing Check delay. If the area has been disarmed outside a schedule, the Closing Check delay occurs one hour after the area is disarmed.

At arming, faulted zones are handled according to the option selected in Bad Zones. If a Closing Report is sent, the user number is indicated as SCH on the SCS-1R Receiver.

Auto Disarm: Select to allow this area to automatically disarm according to a schedule. If an Opening report is sent to the receiver, the user number is indicated as SCH.

Description: Enter a note about the area that you are programming. To enter a note or description, press the Description button to open the Edit Rich Text window. After you type your note, go to File >> Save and Exit to save your work and close the Edit Rich Text window. Your note appears in the field above the Description button.

21. Zone Information

The Zone Information window allows you to define the operation of each protection zone programmed in the panel. Use the Zone Information window to program all protection zones, whether located on panel, keypad, zone expanders, or a wireless interface.

To create a new zone, select New and enter the information for the new zone as described below. To delete an existing zone, select that zone in the list and select Delete. To enter a description or a note about a zone, select Description.

Zone Templates

Zone Templates allow zone programming to be saved as a template.

After entering the zone, save the selected zone programming as a zone template by typing a name directly into

the drop-down menu box and selecting Save. The new template name displays in the drop-down menu.

If a user wishes to set up a zone with the same information as a template, select the template name from the drop-down menu and select Load. The information from the selected template displays in the Zone Information fields. The Zone Number and Wireless Serial Number are not populated as part of the template process. These should be manually entered for each zone.

To delete a saved template from Remote Link, select the template name from the drop-down menu and select Delete.

21.1. Standard Tab

Zone Number: Enter the number of the zone you are programming.

Zone Name: Assign a name to each zone in the system. Zone names may have up to 32 alphanumeric characters. The name can display at the keypads during arming and disarming so the user does not have to memorize zone numbers. A name must be given to each zone in the system. Users can associate a zone name with a particular protection point.

To add a one name to the system, select New and then enter up to 32 characters for the new zone name.

Type: The zone type defines the panel response to the zone being opened or shorted. This is called the Alarm Action. There are up to 13 possible alarm action responses depending on the zone type and any restrictions it may have. When you assign a Type to a zone, automatic zone responses are made.

The panel contains 12 default zone types for use in configuring the system. These zone types provide the most commonly selected functions for their applications. All zone types except the Arming zone type can be customized by changing the options listed in the Action tab.

Area: Enter the area number where you are assigning the zone. In an Area system or a Home/Sleep/Away with Guest system, enter the area number where this zone is being assigned. Area numbers can be assigned for Night, Day, Exit, Auxiliary 1 and Auxiliary 2 zones.

Note: On an XR150INT/XR550INT Series, XR150/XR350/XR550 Series or XR100/XR500 Series panel configured for All/Perimeter or Home/Sleep/Away operation, only the pre-configured Area Names display.

- Area 1 = Perimeter
- Area 2 = Interior
- Area 3 = Bedrooms

Follow Area: Allows Night, Day, Aux 1, or Aux 2 burglary zones to be delayed by following any exit or entry delay that is currently running in the area that is specified.

Armed Areas (XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500/XR100 Series): When Arming is selected as the Zone Type, select the area numbers to be armed when this zone is faulted.

Each panel model contains multiple default zone types for use in configuring the system. These zone types provide the most commonly selected functions for their applications. See Zone Types for a list and description of the different zone types.

21.2. Action Tab

DO Message: The DO (disarmed open) message is the message that the panel transmits to the central station when the zone is opened while in a disarmed state. Not available for 24-hour zone types. See Action Tab Message Options for All Panels below.

DO Output: Enter the output or Favorite number (F1-F20) that you want to activate when this zone opens in a disarmed state. The panel can activate the output regardless of DO Message. Not available for 24-hour zone types.

DO Output Action: This option assigns an action to the output programmed in DO Output. Not available for 24-

hour zone types. See Action Tab Output Options for All Panels below.

DS Message: The DS (disarmed short) message is the message that the panel transmits to the central station when the zone is shorted while in a disarmed state. Not available for 24-hour zone types. See Action Tab Message Options for All Panels below.

DS Output: Enter the output or Favorite number (F1-F20) that you want to activate when this zone shorts in a disarmed state. The panel can activate this output regardless of DS Message. Not available for 24-hour zone types.

DS Output Action: This option assigns an action to the output programmed in DS Output. Not available for 24-hour zone types. See Action Tab Output Options for All Panels below.

AO Message: The AO (armed open) message is the message that the panel transmits to the central station when the zone opens while in an armed state. See Action Tab Message Options for All Panels below.

AO Output: Enter the output or Favorite number (F1-F20) that you want to activate when this zone opens in an armed state. The panel can activate an output regardless of the AO Message.

AO Output Action: This option assigns an action to the output programmed in AO Output. See Action Tab Output Options for All Panels below.

AS Message: The AS (armed short) message is the message that the panel transmits to the central station when the zone is shorted while in an armed state. See Action Tab Message Options for All Panels below.

AS Output: Enter the output or Favorite number (F1-F20) that you want to activate when this zone shorts in an armed state. The panel can activate the output regardless of the AS Message.

AS Output Action: This option assigns an action to the output programmed in AO Output. See Action Tab Output Options for All Panels below.

Action Tab Message Options for All Panels

These options apply to DO, DS, AO, and AS drop-down message menus.

- None: Reports are NOT sent to the receiver. The bell output does not activate and there is no display in the panel alarmed zones or status list. Only the selected relay output operates.
- Alarm: The panel sends alarm reports to the central station. The bell output activates according to zone type.
- Trouble: The panel sends trouble reports to the central station.
- Local: The panel does not send reports to the central station. The bell output still activates according to the zone type.
- Door Propped Open: Allows keypads to warn users that a door has been left open past a specified amount of time. When a door opens, the panel begins to count the time programmed in Entry Delay 4 in the System Options window. The bell output does not activate for Door Propped Open events. If the time expires and the zone has not returned to normal, the keypad buzzer sounds and "CLOSE THE DOOR" displays on the keypad. Any keypads selected in the Prewarn field in Program >> Zone Information notify users of a door prop condition. If the zone has not returned to normal, the time programmed into Entry Delay 4 counts down again. If the time expires a second time and the zone has not returned to normal the following occurs:
  - the panel sends a fault to the central station
  - the output (if programmed in Zone Information) triggers
  - "ZONE NAME - OPEN" displays on the keypad until a user code is entered

Action Tab Output Options for All Panels

These options apply to DO, DS, AO, and AS drop-down output action menus.

- None: No action to the selected output.
- Pulse: The output alternates one second on and one second off until the area is disarmed, the cutoff time expires, or the output is reset from the User Menu.
- Steady: The output is turned on and remains on until the area is disarmed, the output cutoff time expires, or the output is reset from the keypad User Menu.
- Momentary: The output is turned on only once for one second.
- Follow: The output is turned on, and remains on while the zone is either open or shorted. When the zone restores, the output turns off.

21.3. Zone Information--Wireless Tab

Wireless: Select this option if the zone you are programming is DMP wireless.

- XR150INT/XR550INT Series, XR150/XR350/XR550 Series or XR100/XR500 Series panels Version 113 and higher, connect to the 1100X, 1100XI, or 1100XH Wireless Receiver.
- XT30 or XT50 panels connect to the 1100D, 1100DI, or 1100DH Wireless Receiver.
- XT50 with onboard 1100 Series Receiver.
- XTL with onboard 1100 Series Receiver.
- XTLN, XTLN-WiFi with onboard 1100 Series Receiver.

Serial Number: Enter the eight-digit serial number found on the wireless device. When the panel zone stores the serial number, the panel House Code is transmitted to that specific transmitter. This transmission is performed by the wireless receiver when Remote Link disconnects.

All DMP wireless programming is stored in the panel. The wireless receiver obtains the necessary programming information from the panel.

- Each time the receiver is powered down and powered up
- When a new receiver is installed
- When the programmer STOP routine is selected
- When the panel is reset
- When Remote Link disconnects

The receiver memory refresh takes up to 45 seconds to complete depending on the number of DMP wireless zones programmed. Normal receiver operation is inhibited during the memory refresh period.

Contact

Universal Transmitters: Choose Internal to use the internal reed switch contacts or choose External to connect an external contact to the 1101, 1103, or 1106 terminal block. Default is Internal.

Note: The 1101, 1103, or 1106 Universal Transmitter serial number may be programmed for two zones provided the Contact type (Internal or External) is programmed differently for each zone.

For example, program transmitter serial number 01345678 on an XT30INT/XT50INT, XT30/XT50, XTL, XTLN, or XTLN-WiFi Series panel as Zone 31 with an Internal contact type and Zone 32 with an External contact type. The same serial number is used for both zones.

Note: When using both contacts, you must use consecutive zone numbers. The following list shows acceptable consecutive zone number examples:

- XT30INT/XT50INT, XT30/XT50, XTL, XTLN, or XTLN-WiFi Series - zones 31 and 32 or zones 34 and 41
- XR550INT Series, XR550 Series or XR500 Series - zones 543 and 544 or zones 976 and 977
- XR350 Series - zones 543 and 544 or zones 741 and 742

- XR150INT Series, XR150 Series or XR100 Series - zones 522 and 523, or zones 596 and 597

Contact N/O: Select this option to indicate an external device connected to the 1101 terminal block is programmed to use a normally open (N/O) contact. Leave this box not checked to use a normally closed (N/C) contact.

1114 Wireless Four-Zone Expander

The same Serial Number is used for all four contacts. Choose Contact 1, 2, 3, or 4.

Note: When using the contacts, you must use consecutive zone numbers. For example, use serial number 08345678 on an XR100 or XR500 Series panel to program Contact 1 for Zone 561, Contact 2 for Zone 562, Contact 3 for zone 563, and Contact 4 for zone 564.

The following list shows acceptable consecutive zone number examples:

- XT30INT/XT50INT, XT30/XT50, XTL, XTLN, or XTLN-WiFi Series - zones 31, 32, 33, and 34 or zones 41, 42, 43, and 44
- XR550INT, XR550, or XR500 Series - zones 543, 544, 545, and 546 or zones 976, 977, 978, and 979
- XR350 Series - zones 543, 544, 545, and 546 or zones 741, 742, 743, and 744
- XR150INT, XR150, or XR100 Series - zones 522, 523, 524, and 525 or zones 596, 597, 598, and 599

Note: A tamper on the 1114 is transmitted as the zone number assigned to Contact 1.

Supervision Time: Select the supervision time required for the wireless zone. The wireless transmitter must check-in at least once during this time or a missing condition is indicated for that zone. 1100 Series transmitters automatically check-in based on the supervision time selected for the wireless zone, no additional programming is needed. If two zones share the same transmitter, the last programmed supervision time is stored as the supervision time for both zones. Select 3, 60, or 240 minutes. On XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR100/XR500 Series Version 207 or higher, XT30INT/XT50INT Series, XT30/XT50 Series Version 106 or higher, XTL, XTLN, and XTLN-WiFi Series panels, the 3 minute Supervision Time can only be selected if the zone type is fire, fire verify, or supervisory. Select None for unsupervised operation. Default is 240 minutes.

Note: When the panel is reset or a receiver is installed or powered down and powered up, or Remote Link disconnects, the supervision timer restarts for all wireless zones.

LED Enabled: Select this option to turn on a panic, pendant, or hold-up transmitter LED during Panic or Emergency operation. The LED always operates when the transmitter case is open and the tamper is faulted.

Note: When any wireless input zone for a particular address is programmed (Ex: 11-14 = Addr 1 on the Keypad Bus or 586 on an XR500 Series or XR100 Series LX-Bus), the receiver responds to the panel for this address. Other devices, such as keypads or hardwired zone expanders, cannot use this address. Zones connected directly to the panel cannot be wireless.

Disarm/Disable

This option displays for 1103 Universal Transmitters, and 1122, 1126, 1127 Wireless PIRs. Select this option to disable the zone tripped message (short) to the 1100X Series Receiver from the PIR transmitter during the disarmed period. When disabled, the PIR only sends supervision, tamper and low battery messages during the disarmed period to extend the transmitter battery life. Select NO to always send zone tripped messages in addition to supervision, tamper and low battery. Default is NO.

Wireless PIR Pulse Count

This option displays for 1122, 1126, and 1127 Wireless PIRs. Select the number of infrared pulse counts (2 or 4) the PIR will use before sending a short message to the 1100X Series Receiver. The first infrared pulse starts a timer and count. If no additional infrared pulses occur in 25 seconds, the timer and count are reset. Default is 4.

Wireless PIR Sensitivity

This option displays for 1122, 1126, and 1127 Wireless PIRs. Select the sensitivity setting for the PIR. Selecting LOW sets the PIR to operate at 75% sensitivity for installations in harsh environments. Selecting HIGH sets the PIR to maximum sensitivity. Default is LOW.

Wireless PIR Pet Immunity

This option is for the 1122 Wireless PIR Motion Detector. Selecting On from the drop-down menu enables pet immunity for animals up to 55 pounds. Default is Off.

21.3.1. 1100 Series Wireless Options

Wireless: Select this option if the zone you are programming is DMP wireless.

- XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panels Version 113 and higher, connect to the 1100X, 1100XI, or 1100XH Wireless Receiver.
- XT30, XRSuper6, XR20, or XR40 panels connect to the 1100D, 1100DI, or 1100DH Wireless Receiver.
- XT50 with onboard 1100 Series Receiver.

Serial Number: Enter the eight-digit serial number found on the wireless device. When the panel zone stores the serial number, the panel House Code is transmitted to that specific transmitter. This transmission is performed by the wireless receiver when Remote Link disconnects.

All wireless programming is stored in the panel. The receiver obtains the necessary programming information from the panel.

- Each time the receiver is powered down and powered up
- When a new receiver is installed
- When the programmer STOP routine is selected
- When the panel is reset
- When Remote Link disconnects

The receiver memory refresh takes up to 45 seconds to complete depending on the number of DMP wireless zones programmed. Normal receiver operation is inhibited during the memory refresh period.

Contact

1101 Universal Transmitters: Choose Internal to use the internal reed switch contacts or choose External to connect an external contact to the 1101 terminal block. Default is Internal.

Note: The 1101 Universal Transmitter serial number may be programmed for two zones provided the Contact type (Internal or External) is programmed differently for each zone.

For example, program transmitter serial number 01345678 on an XT30, XT50, XRSuper6, XR20, or XR40 panel as Zone 31 with an Internal contact type and Zone 32 with an External contact type. The same serial number is used for both zones.

Note: When using both contacts, you must use consecutive zone numbers. The following list shows acceptable consecutive zone number examples:

- XT30, XT50, XRSuper6, XR20, or XR40 - zones 31 and 32 or zones 34 and 41
- XR550INT Series, XR550 Series, or XR500 Series - zones 543 and 544 or zones 876 and 877
- XR350 Series - zones 543 and 544 or zones 745 and 746
- XR150INT Series, XR150 Series, or XR100 Series - zones 522 and 523, or zones 596 and 597

Contact N/O: Select this option to indicate an external device connected to the 1101 terminal block is programmed to use a normally open (N/O) contact. Leave this box not checked to use a normally closed (N/C) contact.

1114 Wireless Four-Zone Expander

The same Serial Number is used for all four contacts. Choose Contact 1, 2, 3, or 4.

Note: When using the contacts, you must use consecutive zone numbers. For example, use serial number 08345678 on an XR100 or XR500 Series panel to program Contact 1 for Zone 561, Contact 2 for Zone 562, Contact 3 for zone 563, and Contact 4 for zone 564.

The following list shows acceptable consecutive zone number examples:

- XT30, XT50, XRSuper6, XR20, or XR40 - zones 31, 32, 33, and 34 or zones 41, 42, 43, and 44
- XR550INT Series, XR550 Series, or XR500 Series - zones 543, 544, 545, and 546 or zones 876, 877, 878, and 879
- XR350 Series - zones 543, 544, 545, and 546 or zones 775, 776, 777, and 778
- XR150INT Series, XR150 Series, or XR100 Series - zones 522, 523, 524, and 525 or zones 596, 597, 598, and 599

Note: A tamper on the 1114 is transmitted as the zone number assigned to Contact 1.

Supervision Time: Select the supervision time required for the wireless zone. The wireless transmitter must check-in at least once during this time or a missing condition is indicated for that zone. 1100 Series transmitters automatically check-in based on the supervision time selected for the wireless zone, no additional programming is needed. If two zones share the same transmitter, the last programmed supervision time is stored as the supervision time for both zones. Select 3, 60, or 240 minutes. Select None for unsupervised operation. Default is 240 minutes.

Note: When the panel is reset or a receiver is installed or powered down and powered up, or Remote Link disconnects, the supervision timer restarts for all wireless zones.

LED Enabled: Select this option to turn on a panic, pendant, or hold-up transmitter LED during Panic or Emergency operation. The LED always operates when the transmitter case is open and the tamper is faulted.

Note: When any wireless input zone for a particular address is programmed (Ex: 11-14 = Addr 1 on the Keypad Bus or 586 on an XR500 Series or XR100 Series LX-Bus), the receiver responds to the panel for this address. Other devices, such as keypads or hardwired zone expanders, cannot use this address. Zones connected directly to the panel cannot be wireless.

Disarm/Disable

Select this option to disable the zone tripped message (short) to the 1100X Series Receiver from the 1126 PIR transmitter during the disarmed period. When disabled, the 1126 only sends supervision, tamper and low battery messages during the disarmed period to extend the transmitter battery life. Select NO to always send zone tripped messages in addition to supervision, tamper and low battery. Default is checked.

Wireless PIR Pulse Count

Select the number of infrared pulse counts (2 or 4) the 1126 PIR will use before sending a short message to the 1100X Series Receiver. The first infrared pulse starts a timer and count. If no additional infrared pulses occur in 25 seconds, the timer and count are reset. Default is 4.

Wireless PIR Sensitivity

Select the sensitivity setting for the 1126 PIR. Selecting LOW sets the 1126 to operate at 75% sensitivity for installations in harsh environments. Selecting HIGH sets the PIR to maximum sensitivity. Default is LOW.

21.3.2. 1100 Series Key Fob Wireless Options

The 1100 Series offer a Four-Button, Two-Button, or One-Button Key Fob transmitter. As needed, refer to the 1100 Series Key Fob Programming Sheet (LT-0706).

The 1100 Series Key Fobs are compatible with:

- 1100X, 1100XI, and 1100XH Wireless Receivers with XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series, Version 114 and higher, or XR100 Series panels
- XT50 Series panels with onboard 1100 Series Wireless Receiver
- XTL, XTLN, or XTLN-WiFi panels

Key Fob Information

Zone Number: Enter the number of the zone being programmed for the key fob.

- XT30INT/XT50INT, XT30/XT50, XTL, XTLN, XTLN-WiFi Series - zones 31-34 or 41-44
- XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series - zones 400-449

User Number: Enter the user number for the key fob.

- XT30INT/XT50INT, XT30, XTL, XTLN, or XTLN-WiFi - 1-30
- XT50 - 1-99
- XR150INT/XR550INT, XR150/XR350/XR550, or XR100/XR500 Series - 1 to 9999

Note: To operate arming and disarming properly on XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panels, the Key Fob should be assigned to a User Number with appropriate area assignments, however, the User Number does not have to exist at the time the Key Fob is programmed. The Key Fob User Number can be added later by the User.

Serial Number: Enter the eight-digit serial number found on the key fob.

Supervision Time: Select the supervision time required for the key fob zone. The wireless transmitter must check in at least once during this time or a missing condition is indicated for that zone. Select 3, 60, or 240 minutes. Select None for unsupervised operation. Default is None.

Number of Buttons: Select the number of buttons (1, 2, or 4) on the key fob being programmed.

Button Action: When programming a key fob button, select from the following action options:

- Arming: When selected, pressing this button arms selected areas and force arms bad zones.
- Disarming: When selected, pressing this button disarms selected areas.
- Toggle Arm/Disarm: When selected, pressing this button changes the armed state of selected areas. If arming, bad zones are force armed. When pressed again, the opposite action occurs.
- Status: When selected, pressing this button causes the key fob LED to indicate the system arm/disarm status.
- Panic: When selected, pressing this button sends a Panic type alarm with no restoral.
- Panic 2 Btn: To operate as a panic type alarm, program two buttons using PANIC 2 BTN. When both buttons

are pressed at the same time a Panic type alarm is sent with no restoral. If only one button is pressed, no action takes place.

- Emergency: When selected, pressing this button sends an Emergency zone type alarm with no restoral.
- Emergency 2 Btn: To operate as an emergency type alarm, program two buttons using EMERGENCY 2 BTN. When both buttons are pressed at the same time an emergency zone type alarm is sent with no restoral. If only one button is pressed, no action takes place.
- Output: When selected, pressing this button causes an output to turn on steady, pulse, momentary, toggle or off as programmed.
- Sensor Reset: When this button is pressed the panel performs a standard Sensor Reset.
- Unused: When this button is pressed, no operation or action takes place.

Button Press Time: Select the amount of time for the user to press the button before the action initiates a message to the wireless receiver. The Button Press Time can be SHORT (1/2 second) or LONG (2 seconds). Select Button Press Time for Arm, Disarm, Toggle, Status, Output, or Sensor Reset buttons.

Note: The Button Press Time is not programmable for Panic (PN or PN2), Emergency (EM or EM2) or Unused (UN) zones. For these zones the button time is always set to LONG (2 seconds).

Arm/Disarm Areas: On an Area system or Home/Sleep/Away with Guest system, enter the area numbers to be armed/disarmed by the Key Fob button being programmed.

- XT30INT/XT50INT, XT30/XT50, XTL, XTLN, or XTLN-WiFi - Areas 1-6
- XR150INT, XR150, or XR100 Series - Areas 1-8
- XR350 Series - Areas 1-16
- XR550INT, XR550, or XR500 - Areas 1-32

On XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panels, list all areas that apply. In order to arm or disarm these areas, the Profile assigned to the User Number needs to have the same area numbers selected. Any area may be selected at Arm/Disarm Areas but only matching area numbers are armed or disarmed when the specific button is pressed. For example, in Areas selection, areas 1, 3, and 7 are selected. In the User Profile Arm and Disarm Areas, areas 1, 2, 4, and 7 are selected. When the user presses the button to Arm or Disarm area(s), only matching areas 1 and 7 Arm/Disarm.

Note: When more areas are selected at Arm/Disarm Areas than are authorized in the User Profile, in the future the user can be given access authority to additional areas through the User Profile without requiring additional panel programming to select Arm/Disarm Areas.

When the XT30INT/XT50INT Series, XT30/XT50 Series, XTL/XTLN/XTLN-WiFi, XR150INT/XR550INT Series, XR150/XR350/XR550 Series, or XR100/XR500 Series panel is configured for All/Perimeter or Home/Sleep/Away system operation, specify the area to be armed by the Key Fob button being programmed. For All/Perimeter systems, choose PERIM or ALL, for Home/Sleep/Away or Home/Away systems, choose HOME, SLEEP, or AWAY.

Note: On XR150INT/XR550INT, XR150/XR350/XR550, or XR100/XR500 Series panels, Areas 3 and higher in an All/Perimeter system, and areas 4 and higher in a Home/Sleep/Away system are not available for use.

Output Number: Specify the output number the key fob button press activates for OUT, PN, PN2, EM, EM2 programmed buttons. A different output number can be assigned to each key fob button.

- 1 to 4, 31-34 or 41-44 on XT30INT/XT50INT Series, XT30 Series/XT50 Series, or XTL/XTLN/XTLN-WiFi panels.
- 1 to 6, 500 to 999, D1 to D16, or G1 to G20 on XR5550INT Series, XR550 Series, or XR500 Series panels.
- 1 to 6, 500 to 599, D1 to D8, or G1 to G20 on XR150INT Series XR150 Series, or XR100 Series panels.
- 1 to 6, 500-799, D1 to D16, F1 to F20, or G1 to G20 on XR350 Series panels.

Output Action: When programming the relay output action taken by the panel when a valid Output Number is

entered, select from the following action options:

- Steady: The output is turned on and remains on continuously.
- Pulse: The output alternates one second on and one second off. The pulsing rate for a Model 716 relay attached to the LX-Bus is 1.6 seconds.

Note: Pulse is not available for key fob button outputs programmed D1 to D16 or G1 to G20.

- Momentary: The output is turned on only once for one second.
- Toggle: The output alternates between the on state and off state.

Note: Toggle is not available for key fob button outputs programmed G1 to G20.

- Off: The output is turned off. If programmed, the output was turned on by some other means such as another button press, a zone action, or a schedule.

Notes: When the output is assigned to PN/PN2 or EM/EM2 button action and is turned on, the output turns off when any area is disarmed.

When the output action is steady, pulse or toggle and the output is turned on, the output remains on until:

- the output cutoff time expires
- the output is reset from the keypad menu
- toggled off

21.3.3. FA Series Wireless Options

These options only apply when using an FA400-DMP Remote Receiver through a DMP 472 FA Series 900MHz Interface Card. Refer to the XR500 Series Programming Guide (LT-0679), XR200 Programming Guide (LT-0196), or XR200-485 Programming Guide (LT-0466) as needed for wireless operation.

Note: For XR500 Series panels set the House Code to 99 to enable FA Series Wireless. Refer to System Options.

Wireless: Select this field if the zone you are programming is FA Series wireless. These options only apply when using an FA400-DMP Remote Receiver through a DMP 472 FA Series 900MHz Interface Card. Refer to the specific panel programming guide as needed for wireless operation.

Check-in Time: Select the check-in time required for the wireless zone. The wireless transmitter must check-in at least once during this time or a missing condition is indicated for that zone. Select 3, 15, or 60 minutes. Select None for unsupervised operation. Default is 60 minutes.

Note: When the panel is reset or a receiver is installed or powered down and powered up, or Remote Link disconnects, the supervision time restarts for all wireless zones.

Internal Contact: Select this field to use an internal contact on the wireless transmitter. Leave this box empty to use an external contact.

End-of-Line Resistor: Select this field to supervise an external contact connected to the wireless transmitter. Leave this box empty if you are not installing an End-of-Line resistor.

Normally Open: Select this field if the external contact connected to the wireless transmitter is a normally open (N/O) type. Leave this box empty if the external contact connected to the wireless transmitter is a normally closed (N/C) type.

21.4. Advanced Tab

Swinger Bypass (XR150INT/XR550INT, XR150/XR550, XR100/XR500): Allows the zone to be bypassed by the panel according to the specifications programmed in Swinger Bypass Trips and Swinger Reset in the System Options window.

Swinger Bypass (XT30INT/XT50INT, XT30/XT50, XTL/XTLN/XTLN-WiFi): Allows the zone to be bypassed by the panel after two alarms, troubles, or local trips within one hour. The bypass condition displays in the keypad

Status List.

Retard (XR150INT/XR550INT, XR150/XR550, XR100/XR500): This option is only available for the following zone types: Fire, Auxiliary 1, Auxiliary 2, Arming, Panic or Supervisory. Programs the zone to operate with the zone retard delay as specified in the Retard Delay field in the System Options window. Zone retard functions only in zone short conditions. The zone must remain shorted for the full length of the retard delay before the panel recognizes the shorted condition. If the arming zone has Maintain as the style, the retard delay also occurs when the zone returns to a normal state.

Fast Response (XR150INT/XR550INT, XR150/XR550, XR100/XR500): Provides a zone response time of 327ms. Leave this field blank to provide a normal zone response time of 500ms. LX-Bus zones have a fixed response time of 200ms.

Cross Zone: Enables cross zoning for this zone. Cross zoning requires one or more armed zones to fault within a programmed time before an alarm report is sent to the central station. The length of the programmed time is designated in the Cross Zone Seconds field in Program >> System Options.

Note: To operate correctly, all cross-zone zones need to be programmed as the same zone type.

When a cross-zoned zone trips, the output action assigned to the zone activates and the cross-zone time specified in Program >> System Options begins to count down. If another cross-zoned zone faults or if the first zone restores and faults again before a sensor reset is performed, the panel sends an alarm report to the central station. If no other cross-zoned zones trip before the cross-zone time expires, the panel sends only a zone fault report to the central station.

Note: You cannot enable cross zoning for Fire Verify zones or for any Fire zone type that is programmed with a retard delay.

Priority Zone : Requires this zone to be in a normal condition before arming its assigned area.

Fire Panel Slave (XR150INT/XR550INT, XR150/XR550, XR100/XR500): This option is available on Fire Zones (FI) only and allows a fire zone the ability to provide slave communication operation for a separate fire alarm control panel. If selected, this zone will transmit a restoral immediately when restored by the fire panel being monitored. A sensor reset is not required to generate the restoral message.

If not selected, this zone will operate as a standard fire type zone and a sensor reset is required before the zone will return to normal.

Traffic Count (XT30INT/XT50INT, XT30/XT50, XTL, XTLN, XTLN-WiFi, XR150/XR550 Series Version 109 or higher): This option is only displayed for Night (NT) and Exit (EX) type zones. If selected, provides reporting to the receiver of the number of zone trips per area while in a disarmed state. Traffic Count data for the 10 lowest numbered zones with Traffic Count set to YES will also be reported to the Virtual Keypad app if enabled at DMPDealerAdmin.com. Default is NO.

Tamper (XT30INT/XT50INT and XR150INT/XR550INT Series): Select to enable Dual EOL zone operation. See Section 10.2 Operational Parameters of the XT30INT/XT50INT Series Installation Guide (LT-0980INT) or XR150INT/XR550INT Series Installation Guide (LT-1232INT) for additional information. The control panel reports a zone open circuit as a tamper condition. Select NO for Single EOL operation. Default is NO.

Real-time Status (XR500 Series/XR100 Series Version 203 or higher): If selected, this allows Real-time Status reports, such as Door Open or Closed with zone number or output condition, to be sent using PC Log reporting. Selecting NO disables Real-time Status for this zone. Default is NO.

Zone Audit Days (XT30INT/XT50INT Series, XT30/XT50 Series Version 103 or higher, XTL/XTLN/XTLN-WiFi, XR150INT/XR550INT Series, XR150/XR550 Series, XR100/XR500 Series Version 205 or higher): Specify the number of days, 0 to 99 for XT30/XT50 Series or 0-365 for XR100/500 Series, XR150/XR350/XR550 Series or XR150INT/XR550INT Series, allowed to elapse without this zone being tripped before a fault message is sent. The message is sent to the receiver(s) programmed to receive Supervisory/Trouble Reports at 10:00 am

following the expiration of the timer. Each time the zone is tripped, the Zone Audit Days timer restarts and begins to countdown the number of days programmed. After the countdown expires, a fault message is sent and the Zone Audit Days timer restarts and begins to countdown the number of days programmed. Available for all zone types except fire and fire verify. Enter 0 (zero) to disable this function. Default is 0 (zero). This feature is used to monitor a zone for inactivity.

Receiver Routing (XT30INT/XT50INT, XT30/XT50 Series Version 103 or higher, XTL, XTLN, and XTLN-WiFi): If Auxiliary 1 or Auxiliary 2 is selected as Zone Type, select from the following routing options:

- Normal: Sends Alarm and Supv/Trbl messages from this zone to receiver 1 or receiver 2 as programmed.
- 1: Sends Alarm and Supv/Trbl messages from this zone to receiver 1 only, regardless of the programming for that receiver.
- 2: Sends Alarm and Supv/Trbl messages from this zone to receiver 2 only, regardless of the programming for that receiver.
- Both: Sends Alarm and Supv/Trbl messages from this zone to both receivers, regardless of the programming for either receiver.

Door Number (XR100/XR500 Series Version 203, 204 or 205): If Real-time Status is selected, enter a door number (keypad bus address) of 1-16 for XR500 Series panel or 1-8 for XR100 Series panels. When a door number is selected, the door number is included in the status report instead of the zone number. Enter 0 (zero) to disable this feature and report the zone number. Default is 0 (no door).

Report with Account Number for Area (XR150INT/XR550INT Series, XR150/XR550 Series, and XR100/XR500 Series Version 206 or higher):

This option is only available for 24-hour zone types (Fire, Fire Verify, Panic, Emergency, or Supervisory). Enter the area number (1-32) to assign as a 24-hour zone type. This option sends the account number of the programmed area with messages. If the entered area number does not exist or is not valid, the account number programmed in the Communication section is sent. Select 0 (zero) to have the report sent with the account number programmed in Communication. Default is 0.

Chime Sound: This option allows you to assign a Doorbell, Ascend, or Descend tone to a Night or Exit zone. Having access to three distinct tones allows end users to easily differentiate between chime-enabled zones.

Prewarn: Enter the keypad addresses that you want to prewarn during the entry delay. All keypad addresses designated in this field display "ENTER CODE: -"

To enter a keypad address, select the field and type the number key for the desired keypad address. The number appears in the field. To turn off an address number, type the number that appears in the Prewarn field that you wish to remove.

Note: On XR150INT/XR550INT Series, XR150/XR550 Series, XR500 Series, and XR100 Series panels, the prewarn tone stops at the keypad when the first user code digit is entered. If no keys are pressed for five seconds or an invalid user code is entered, the prewarn tone resumes. XR550INT Series, XR550 Series, and XR500 Series panels support up to 32 keypads. All other panels support up to eight keypads.

Presignal: If Retard is selected for a zone, the Prewarn field changes to the Presignal field. A presignal tone is indicated by a warning tone sounding from the keypad, but not from any other notification devices, and no signal is sent to the central station. Presignal allows you to enable any combination of keypad addresses to sound a presignal tone during the time a zone is in retard delay. Retard only functions in zone short conditions.

Armed Areas (XT30INT/XT50INT, XT30, XT50, XTL/XTLN/XTLN-WiFi): When Arming is selected as the Zone Type, the Prewarn field changes to Armed Areas. Select the area numbers to be armed when this zone is faulted.

Entry Delay Number: Select the entry timer for this zone. The Entry Delay Number refers to the Entry Delay fields in the System Options window. Enter a number (1 to 4) to assign the entry delay time for each exit-type

zone.

Lockdown: Enable the Lockdown box to trigger Lockdown for panic zones. This allows users to quickly put a system in a Lockdown state using the programmed Panic type zone. Keep in mind, if the panic zones are not programmed to trigger a lockdown, it will only send a panic when they are triggered.

21.5. Zone Types

The following Zone Types can be programmed. Select the desired type from the drop-down menu. Only those that apply to the panel and mode are shown in the drop-down menu.

Blank (--): Selecting Blank will program the zone to send all alarm data to the central station, but will suppress the name of the zone from displaying at the central station.

Night (NT): A controlled instant zone used for perimeter doors and windows and interior devices such as motion detectors and glass break detectors.

Day (DY): Used for emergency doors or fire doors to sound the keypad buzzer and display the zone name when the zone is faulted. Day zones will send alarm reports to the receiver during the system's armed periods.

Exit (EX): Initiates the entry delay timer when its assigned area is armed. It also initiates an exit delay timer to allow a user to exit an area after the arming process has started.

Panic (PN): Used for connecting to devices that allow a user to signal an emergency alarm. Panic zones can provide either a silent or audible alarm with or without reporting to a central station receiver.

Emergency (EM): Used for reporting medical or other non-panic emergencies to the central station receiver.

Auxiliary 1 (A1) and Auxiliary 2 (A2): These zones are similar to a Night zone and are typically used to protect restricted areas within a protected premise.

The Zone Retard Delay time (1 -to 250 seconds) for A2 and Arming zones keeps momentary blockages or shadows from tripping the zone.

Supervisory (SV): Used to provide 24-hour zone supervision to devices associated with fire systems. Typical applications are tamper switches on Post Indicator Valves (PIVs), gate valves, and low and high temperature gauges.

Fire (FI): Used for any type of powered or mechanical fire detection device. Typical applications are for smoke detectors, sprinkler flowswitches, manual pull stations, and beam detectors. Retard, cross zoning, and pre-signal options are available for the Fire zone type.

Fire Verify (FV): Used primarily for smoke detector circuits to verify the existence of an actual fire condition. When a Fire Verify zone initiates an alarm, the panel performs a Sensor Reset. If any Fire Verify zone initiates an alarm within 120 seconds after the reset, an alarm is indicated. If an alarm is initiated after another 120 seconds, the cycle is repeated.

Arming Zone (AR): This zone allows you to connect a keyswitch on a zone and use it to arm and disarm one or more areas within a partition. In the XR200 and XR2400F version 112 and higher, and the XR200-485 version 206 and higher, when connecting to a light sensor, using Maintain with Retard Delay will allow arming at dusk and disarming at dawn, ignoring momentary changes in light intensity, such as shadows or headlights.

AR Style: When programming an Arming zone, some panels allow you to select an Arming Style. This allows for different actions of the arming zones.

The options in the AR Style menu are:

Toggle: When the zone changes from normal to shorted, the programmed areas toggle between the armed or disarmed condition. When restored to normal, no action occurs. When the zone is opened from a normal (disarmed) state, a trouble is reported. When opened from a shorted (armed) state, an alarm is reported and the zone is disabled until you disarm the area(s) from either a keypad or Remote Link computer.

Arm: When the zone is shorted, the programmed areas are armed. When restored to normal, no action occurs.

When the zone is opened from a normal (disarmed) state, a trouble is reported. When opened from a shorted (armed) state, an alarm is reported.

Disarm: When programmed as an Area system, a short will disarm the programmed areas. When programmed as an All/Perimeter or Home/Away system, a short will disarm all areas. When restored to normal, no action occurs. When the zone is opened from a normal (disarmed) state, a trouble is reported.

Step: When programmed as an Area system, a short will arm the areas and beep the keypads once. When programmed as All/Perimeter or Home/Away, on the first short Home (Perimeter) will arm and beep the keypads once. On the second short, Sleep will arm for Home/Away systems and beep the keypads twice. When programmed as All/Perimeter, the interior will arm and beep the keypads twice. On the third short, Away will arm and beep the keypads three times. A normal condition will cause no action. An open condition will disarm the programmed areas and beep the keypads for one second.

Note: This arming style is designed for wireless arming pendants. When using an arming/disarming keyswitch locate the keyswitch within the protected area.

Maintain: When the zone is shorted, the programmed areas are armed. When restored to normal, the programmed areas are disarmed and any alarm bells are silenced. When the zone is opened from a normal (disarmed) state, a trouble is reported. If opened from a shorted (armed) state, an alarm is reported and the zone is disabled until you disarm the area(s) from either a keypad or Remote Link computer.

21.6. Miscellaneous Zone Options

Prewarn: Enter the keypad addresses that you want to prewarn during the entry delay. All keypad addresses designated in this field display "ENTER CODE: -"

To enter a keypad address, select the field and type the number key for the desired keypad address. The number appears in the field. To turn off an address number, type the number that appears in the Prewarn field that you wish to remove.

Note: On XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series, XR2500F, XR100 Series, and XR40 panels, the prewarn tone stops at the keypad when the first user code digit is entered. If no keys are pressed for five seconds or an invalid user code is entered, the prewarn tone resumes.

Note: XR500 Series and XR2500F panels support up to 16 keypads. XR350 Series panels support up to 16 keypads. All other panels support up to eight keypads.

Presignal: Enter the keypad addresses that you want to sound a presignal tone during the time a zone is in retard delay. The presignal tone silences when the zone restores or the retard delay expires. You may only select Presignal when Retard is selected.

Armed Areas (XT30INT/XT50INT, XT30/XT50, XRSuper6, XR20, XR40): When Arming is selected as the Zone Type, the Prewarn field changes to Armed Areas. Select the area numbers to be armed when this zone is faulted.

Entry Delay Number: Select the entry timer for this zone. The Entry Delay Number refers to an Entry Delay field in the System Options window. Enter a number from 1 to 4 to assign the entry delay time for each exit-type zone.

Swinger Bypass: Selecting this box allows the zone to be bypassed by the panel according to the specifications programmed in Swinger Bypass Trips and Reset Swinger Bypass the System Options window. The bypass condition will be displayed in the keypad Status List. Leaving this box empty will disable swinger bypassing for this zone.

How It Works

If within one hour, a zone trips the total number of times as specified in Swinger Bypass Trips, the panel

bypasses it until the following conditions occur;

- the area in which the zone is assigned is disarmed
- the zone is manually reset through the Bypass Zones? keypad User Menu function
- the Reset Swinger Bypass is enabled

Retard: Selecting this box programs the zone to operate with the zone retard delay as specified in the Zone Retard Delay field in the System Options window. Zone retard only functions in zone short conditions. The zone must remain shorted for the full length of the retard delay before the panel recognizes the shorted condition. If the arming zone has Maintain as the style, the retard delay also occurs when the zone returns to a normal state. If you leave this field blank, the zone operates without a retard delay.

Fast Response: Select this box to provide a zone response time of 167ms. Leave this field blank to provide a normal zone response time of 500ms. LX-Bus zones have a fixed response time of 200ms.

Cross Zone: Select this field to enable cross zoning for this zone. Cross zoning requires one or more armed zones to fault within a programmed time before an alarm report is sent to the central station. The length of the programmed time is designated in the Cross Zone Time field in Program >> System Options.

Note: To operate correctly, all cross-zone zones need to be programmed as the same zone type.

When a cross-zoned zone trips, the bell action assigned to the zone activates and the cross zone seconds specified in System Options begins to count down. If a second cross-zoned zone faults, or if the first zone restores and faults again before a sensor reset is performed, the panel sends an alarm report to the central station. If no other cross-zoned zone trips before the cross-zone time expires, the panel sends only a zone fault report to the central station.

Note: You cannot enable cross zoning for Fire Verify zones or for any Fire zone type that is programmed with a retard delay.

Priority Zone: Select this box to require this zone to be in a normal condition before its assigned area can be armed.

Traffic Count: If selected, provides reporting to the receiver of the number of zone trips per area for Night and Exit type zones while in a disarmed state. Default is NO

Zone Audit Days (XT30/XT50 Series Version 103 or higher, XT30INT/XT50INT): Specify the number of days, 0 to 99, allowed to elapse without this zone being tripped before a fault message is sent. The message is sent to the receiver(s) programmed to receive Supervisory/Trouble Reports at 10:00 am following the expiration of the timer. Each time the zone is tripped, the Zone Audit Days timer restarts and begins to countdown the number of days programmed. After the countdown expires, a fault message is sent and the Zone Audit Days timer restarts and begins to countdown the number of days programmed. Available for all zone types except fire and fire verify. Enter 0 (zero) to disable this function. Default is 0 (zero). This feature is used to monitor a zone for inactivity.

Receiver Routing (XT30/XT50 Series Version 103 or higher, XT30INT/XT50INT): If Auxiliary 1 or Auxiliary 2 is selected as Zone Type, select from the following routing options:

Normal: Sends Alarm and Supv/Trbl messages from this zone to receiver 1 or receiver 2 as programmed.

1: Sends Alarm and Supv/Trbl messages from this zone to receiver 1 only, regardless of the programming for that receiver.

2: Sends Alarm and Supv/Trbl messages from this zone to receiver 2 only, regardless of the programming for that receiver.

Both: Sends Alarm and Supv/Trbl messages from this zone to both receivers, regardless of the programming for either receiver.

Real-time Status: If selected, this allows Real-time Status reports, such as Door Open or Closed with zone number or output condition, to be sent using PC Log reporting. Selecting NO disables Real-time Status for this

zone. Default is no.

Door Number: If Real-time Status is selected, enter a door number (keypad bus address) of 1-16 for XR500 systems or 1-8 for XR100 systems. When a door number is selected, the door number is included in the status report instead of the zone number. Enter 0 (zero) to disable this feature and report the zone number. Default is 0 (no door).

22. Holiday Dates and Schedules

Setting 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.

Three Holiday Schedules are available. This allows an output, area, or door to have three different schedules for holidays. For example, Holiday Schedule A for those holidays when the building stays closed, Holiday B for a day that only opens for a morning, etc. Also, Holiday Schedules can be used to cross multiple days or to arm only specific areas of a building.

Number: Assign a number to the holiday date. You may assign up to 20 holiday dates for XR100/XR500 Series or up to 40 holiday dates for XR150INT/XR550INT Series and XR150/XR350/XR550 Series panels.

Name: Enter up to 32 characters for the name of the holiday.

Note: XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series Version 205 or higher accept names up to 32 character.

Class: The Class menu allows you to assign one of three different schedules to a holiday. Each holiday class assigns a different schedule to a holiday. Choose A, B, or C from the drop-down menu.

Holiday: Enter the date of the holiday or choose the holiday from the drop-down calendar.

Description: This field allows you to enter a note about the holiday that you are scheduling.

Holiday Schedules

Three Holiday Schedules are available. This allows an output, area, or door to have three different schedules for holidays. For example, Holiday Schedule A for those holidays when the building stays closed, Holiday Schedule B for a day that only opens for a morning, etc. Also, Holiday Schedules can be used to cross multiple days. These schedules become active and supersede the current day's schedule when a Holiday Date occurs. You can assign up to a total of 40 Holiday Schedules.

Similar to the Time Schedules menu, enter a Begin and End Time for Holiday Schedules A, B, and C.

23.1 Schedules

23.1. Schedules

See the following User Guide for detailed information on Schedules:

- CellComSL Installation/Programming Guide LT-1339
- XTLC/XTLN/XTLN-WiFi User Guide LT-1109
- XT30INT/XT50INT Series User Guide LT-0982INT
- XT30/XT50 Series User Guide LT-0982
- XR100/XR500 Series User Guide LT-0683
- XR150/XR350/XR550 Series User Guide LT-1278
- XR150INT/XR550INT Series User Guide LT-1278INT

CellComSL, DualCom, XT30INT/XT50INT Series, XT30 Series, XT50 Series, XTLC/XTLN/XTLN-WiFi Series panels

The Schedules window allows you to program the times at which you normally turn your burglary protection on and off each day of the week. This information can then be used by the system to automatically arm or disarm the burglary protection.

You can also use the Closing Check/Extend feature with Schedules to ensure your system is armed by an authorized user at a specific time. This option sounds the keypad buzzer and displays CLOSING TIME! when a schedule expires. Users still on the premises are required to arm the system or extend the schedule. If the system is not armed, or the schedule is not extended, a report can be sent to the central station and/or an email address or cell phone. When a schedule expires and CLOSING TIME! displays, the keypad next displays ENTER CODE: -. To silence the keypad buzzer and extend the schedule for one hour, a user must either enter a valid user code or present a card to the card reader.

Permanent Schedules are used for automatic arming and disarming an area and will always occur at the same time until you change or delete the schedule. When you turn on Auto Arm or Auto Disarm in Area Information, the area will use this schedule to arm or disarm automatically. One schedule is available for one or all areas.

XR100/XR500 Series panels

Schedules are ideal for individual area auto arming and disarming and for creating Opening/Closing windows during which users can access the building or disarm the system. Having separate schedules allows you to create Opening/Closing windows for each day. One could be for normal business activity and another could be for cleaning crews or a second shift. Once created, these schedules operate continually until changed.

The Schedules function allows you to program into the system the times at which you normally turn your burglary protection on and off each day of the week. If you system does not use automatic arming, you can use the Closing Check/Extend feature with Schedules to help ensure your system is armed manually at a specific time. This option sounds the keypad buzzer and displays CLOSING TIME! or AREA LATE! when a schedule expires. This reminds the users still on the premises to arm the system or extend the schedule to a late time.

The XR100/XR500 Series panels allow the assignment of four independent shifts. Choose 1st Shift, 2nd Shift, 3rd Shift, or 4th Shift from the drop-down menu. Shifts are assigned to profiles assigned to individual User Codes.

Shift: The Shift drop-down menu allows you to program access and arm/disarm schedules. Select which shift you want to schedule from the drop-down Shift menu. Shifts can be assigned to a profile which then is assigned to a user code.

Area: Enter the area number that you are assigning to the schedule. In order for this feature to be available, Area Schedules must be selected in Area Information.

Opening: Enter the time that you want to schedule for the opening (disarm) time. Repeat for each day of the week that you wish to program.

Closing: Enter the time that you want to schedule for the closing (arm) time. Repeat for each day of the week that you wish to program. The opening time must be before the closing time.

Note: When programming area schedules, you must enter both an opening and a closing time for each day that you are programming. The panel will disregard a schedule if it sees only an opening time, but no closing time, and vice versa.

If you want a schedule to run over multiple days, that is, you want the system to disarm on one day and remain disarmed until later that week, you may schedule this when you enter the closing time. In the closing field,

enter the time and day of the week that you want to schedule the closing.

Example: In the Monday Opening field enter 8:00 AM. In the Monday Closing field enter 5:00 PM FRI. With this schedule, the system will disarm at 8:00 AM Monday morning and arm Friday at 5:00 PM.

Note: Some panels allow the entry of Holiday schedules. The Holiday fields will display at the bottom of the Opening and Closing columns if they are available on the panel type. Enter the opening and closing time for the holiday, then choose the dates you wish to assign for the holiday schedule in Program > Holiday Dates. Holiday programming supersedes all other schedules.

XR150INT/XR550INT/XR150/XR350/XR550 Series Panels

Your system provides you with the following schedules menus.

Time Schedules

This menu allows you to program up to 99 access, arm/disarm and holiday schedules. Select New or the schedule you want to program from the list. Enter the times you want to Open/Begin/Activate and Close/End the Schedule in the boxes on the right. Select Apply when finished to save the schedule.

Check the Temporary Schedule box and enter a Begin and End Date to create a temporary schedule. A temporary schedule expires at the set end date and is automatically deleted from the system. You can apply a temporary schedule to areas, doors, outputs, and/or favorites. This feature is only available for XR150/XR550 Series panels.

Sunrise/Sunset Schedules use a panel's weather zip code to stay synced with sunrise and sunset times throughout the year. Choose either Sunrise or Sunset from the drop-down menu, and then set the before or after and day options for the schedule. This feature is available for XT30/XT50, XTLplus, and XR150/XR550 Series panels.

Area Schedules

Enter the Area number you want to assign to a Schedule. You can assign up to 16 Schedules to each Area. Enter a Schedule number in the field or select the browse button next to the field to view the list of schedules. The list of schedules is programmed in the Time Schedules menu.

24. Output Schedules

XT50, CellComSL, and DualCom

Output Schedules allow you to set the times when relay outputs connected to your system turn on and off automatically.

Output: Enter the output number that you wish to assign a schedule.

- XT50 Series - select 1 - 4, 31 - 34, 41 - 44
- CellComSL and DualCom Series - select 1 - 2

XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series, and XR100 Series

Output Schedules allow you to set the times when relay outputs connected to your system turn on and off automatically.

Output: Enter the output number that you wish to assign a schedule.

- XR550 Series, XR550INT Series, or XR500 Series: Select 1 - 6, 500 - 999

- XR350 Series: Select 1 - 6, 500 - 699
- XR150 Series, XR150INT Series, or XR100 Series: Select 1 - 6, 500 - 599
- XT30INT/XT50INT Series or XT50/XT30 Series: Select 1 - 4, 31 - 34, 41 - 44
- CellComSL and DualCom Series: Select 1 - 2

Door: To program door schedules, enter D and a device address number.

- XR350, XR550 Series, XR550INT Series, or XR500 Series: Select D01 - D16
- XR150 Series, XR150INT Series, or XR100 Series: Select D01 - D08

Note: Door schedules are available on the XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series, and XR100 Series. All other panels program output schedules using output numbers only.

Outputs Favorites

Schedule: Enter the schedule number that you want to program. The Schedule field allows you to set up to 100 different scheduled times for relay outputs and door access relays connected to your system to turn on and off automatically. The maximum number of schedules you may assign per door access relay or relay output is 8.

On: Enter the time that you want to turn on the output. Repeat for each day of the week that you wish to program.

Off: Enter the time that you want to turn off the output. Repeat for each day of the week that you wish to program.

Note: XR150INT/XR550INT, XR150/XR350/XR550 Series, and XR500 Series panel only. You may enter the opening and closing times for three holidays (A, B, and C) as designated in Program >> Holiday Dates. Holiday programming supersedes all other schedule programming.

Sunrise/Sunset: Sunrise/Sunset Schedules use a panel's weather zip code to stay synced with sunrise and sunset times throughout the year. Choose either Sunrise or Sunset from the drop-down menu, and then set the before or after and day options for the schedule. This feature is available for XT30/XT50, XTLplus, and XR150/XR550 Series panels.

25. Favorite Schedules

XT30INT/XT50INT, XT30/XT50, CellComSL, DualCom, XR150/XR350/XR550, and XR150INT/XR550INT Series panels

Favorite Schedules allow you to set the times when your favorites connected to your system activate automatically.

New: Select New to enter a Favorite Schedule. You can enter up to 7 schedules per Favorite number.

Favorite: Enter the Favorite number (F1-F20) that you wish to assign a schedule.

Sunrise/Sunset: Sunrise/Sunset Schedules use a panel's weather zip code to stay synced with sunrise and sunset times throughout the year. Choose either Sunrise or Sunset from the drop-down menu, and then set the before or after and day options for the schedule. This feature is available for XT30/XT50, XTLplus, and XR150/XR550 Series panels.

Activate

1. Select the days and times you want to program.
2. Enter all schedule times using a 12 hour clock. For example, to enter 6 AM you would enter a 6:00 AM. For 11:30 PM you would enter 11:30 PM.

Apply: Select Apply after entering the schedule to save.

26. Output, Favorite, and Door Schedules

Output/Door/Favorite Schedules: Select the Output, Door, or Favorite number from the list to assign to a Schedule. You can assign up to 8 Schedules to each Output/Door/Favorite. Enter the Schedule number in the first available field or select the browse button next to the field to view the list of schedules. The list of schedules is programmed in the Time Schedules menu.

27.1 Profiles

27.1. Profiles

The Profiles window allows you to add, delete, or change user profiles. A profile defines the authority of each user code in the system. Up to 4 profiles can be assigned to each user code. Use the Profile Record to assist you when programming Profiles.

Profile: Enter a number to assign to the profile. Each profile may be assigned a number from 1 to 99.

Note: On XR150INT/XR550INT, XR150/XR350/XR550, or XR100/XR500 Series panels, Profiles cannot be changed at the keypad for All/Perimeter or Home/Sleep/Away operation. Use the default Profiles 1 to 10.

Name: Enter a name to assign to the profile you are programming. Each profile may be assigned a 16-character name.

Arm / Disarm Areas: Enter the number for the areas that you want to authorize this profile to arm and disarm. Beginning with XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR500/XR100 Series, you can specify separate arm and disarm authority for a profile.

Each profile may be assigned specific areas of the burglary part of the system for arming and disarming. When profiles 1 to 98 are created, no areas are assigned by default. By default, profile 99 is assigned authority to all areas.

Access Areas: Enter the number for the areas you want to authorize access for this profile.

Areas 1 to 32 for XR550INT Series, XR550 Series, or XR500 Series

Areas 1 to 16 for XR350 Series

Areas 1 to 8 for XR150INT Series, XR150 Series, or XR100 Series

Each profile may be assigned door access to specific areas. When profiles 1 to 98 are created, no areas are assigned by default. By default, profile 99 is assigned authority to all areas.

Note: On XR500 or XR100 Series panels set to All/Perimeter or Home/Sleep/Away operation, Access Areas should be left at factory default settings.

Output Group: You may assign each profile to an output group number from 1 to 20. See Output Groups for more information.

Re Arm Delay: Allows the entry of 0 to 720 minutes to be used to delay automatic rearming when the user disarms an area outside of schedule. If zero is selected, the rearming occurs based on Late/Arm Delay programming in the panel Area Information.

Re Arm Delay is also used to delay a late to close message to the central station when the panel does not use automatic arming.

If the user has Extend Schedule authority, 2HR 4HR 6HR 8HR displays at disarming. If the user does not make a choice, the Re Arm Delay is used to extend the schedule.

Applications example: An exit door near the trash is scheduled to be armed at all times. When the custodian needs to remove trash, program 10 minutes for the activity. Or, an overhead door only requires access when a delivery is made. Program up to 250 minutes to allow the loading dock supervisor to load or unload a semi-truck.

Inactive User Audit Days: This option allows you to 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 to inactive. The range is 0-425 days. The default is 0. This feature is only available for XR550 Series panels.

Profile Options

Each user profile may be assigned any of the profile options. Select each box for the options you wish to assign to the profile.

Note: At least one administrator code in your system must have a profile with all authorities and all areas.

Arm: Allows you to arm areas specified in Arm / Disarm Areas:.

Disarm: Allows you to disarm areas specified in Arm / Disarm Areas:.

Alarm Silence: Allows the user see Alarm Silence in the User Menu.

Lockdown: Enables the Lockdown prompt in the User Menu for this profile. Lockdown immediately locks all public doors, and sends a lock command to each Z-Wave lock, and a close command to all Z-Wave garage doors.

Door Lock/Unlock: Enables the Door Lock/Unlock prompt in the User Menu for this profile. Door Lock/Unlock is used to immediately lock or unlock a door.

Sensor Reset: Enables the Sensor Reset prompt in the User Menu for this profile. Also known as fire reset, the sensor reset is used to reset smoke and glassbreak sensors and to activate and deactivate a Lockdown.

Door Access: Enables the Door Access prompt in the User Menu for this profile. Door Access turns on the door strike relay for 5 seconds.

Armed Areas: Enables the Armed Areas prompt in the User Menu for this profile. Pressing any select key displays the area name of the armed areas. Pressing CMD forwards to the next armed area name. When the last armed area name is displayed, pressing CMD returns the keypad to the Status List.

Outputs On Off: Enable the Outputs On/Off and Z-Wave Setup (XR550) prompts in the User Menu for this profile. Allows the user to manually turn on or off an output that has not been entered in as an Output Action in Zone Information.

Zone Status: Enables the Zone Status prompt in the User Menu. Displays a list of armed, bypassed, or alarmed zones. Also allows you to check the status of individual zones. Zone Status can be used to give you a list of zones by category or display the current status of an individual zone number.

Bypass Zones: Enables the Bypass Zones prompt in the User Menu for this profile. Allows you to bypass a zone prior to arming. Bypassing is usually done when a zone cannot be restored to normal. A significant benefit of bypassing a zone is to allow a zone in a faulted or bad condition to be bypassed so arming can occur. The faulted zone can then be serviced the next day.

Zone Monitor: Enables the Zone Monitor prompt in the User Menu for this profile. Allows the system to monitor selected disarmed zones (doors, windows, or motion detectors) and display their name at the keypad as they are faulted. This feature could be used to monitor an access door. Zone Monitor works with any disarmed zone and also sounds the keypad monitor tone when the zone faults. The zone name displays at all keypads designated for the area in your system. You can place any combination of disarmed zones in the Zone Monitor but only the most recent zone faulted will display on the keypad. The displayed zone name clears automatically after a short time or when the zone is armed.

System Status: Enables the System Status prompt in the User Menu for this profile. Displays the current condition of internal system hardware. System status shows the panel condition of AC power, battery power, and optional panel tamper. When System Status is selected, each monitor displays followed by OKAY or TRBL (Trouble) to indicate the current condition.

System Test: Enables the System Test prompt in the User Menu for this profile. System Test is used to test

battery, alarm bell or siren, and central station communication. The System Test function begins automatically as soon as you select SYSTEM. Zone Test is used to perform a Walk Test on zones. The Walk Test function begins automatically as soon as you select ZONES. NOTE: If an area is in an armed state, the system test will not operate.

Profiles: Enables the User Profiles prompt in the User Menu for this profile. Add, delete, or change User Profiles, that define the authority of each user code in the system, Several characteristics define the authority of each User Profile within the system. Always make sure that at least one administrator in your system has a profile with all authorities and all areas. Up to four profiles may be assigned per user.

In All/ Perimeter or Home/Sleep/Away operation, Users Profiles will not display in the User Menu. When adding User Codes, use the default profiles 1 through 10.

In Home/Sleep/Away with Guest house system, the User Profiles option does not display in the User Menu but when adding User Codes, enter a profile number 1 through 9 for the main house system, profiles 11-19 for the Guest 1 house system and profiles 21-29 for the Guest 2 house system (XR550 only). Profiles 2-9 will default to have Arming/Disarming for all eight areas, while profiles 12-19 and 22-29 only Arm/Disarm assigned to Guest 1 and Guest 2 respectively. Profiles 1, 11, and 21 do not have any Arming/Disarming authority assigned. Refer to the Users Profiles Chart below.

Menu Display			Authority	Predefined Profile Number											
				1	2	3	4	5	6	7	8	9	10	11-98	99
ALM SLNC	NO	YES	Alarm Silence	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SNSR RST	NO	YES	Sensor Reset	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
LOCKDOWN	NO	YES	Lockdown	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
DOOR LOCK/UNLOCK	NO	YES	Door Lock/Unlock	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
DOOR ACS	NO	YES	Door Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
ARM AREA	NO	YES	Armed Areas	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
OUTPUTS	NO	YES	Outputs ON/OFF	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
ZN STATS	NO	YES	Zone Status	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
BYPAS ZN	NO	YES	Bypass Zones	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	Yes
ZONE MON	NO	YES	Zone Monitor	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SYS STAT	NO	YES	System Status	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SYS TEST	NO	YES	System Test	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
PROFILES	NO	YES	User Profiles	No	No	No	No	No	No	No	No	Yes	No	No	Yes
USR CODE	NO	YES	User Codes	No	No	No	No	No	No	No	No	Yes	No	No	Yes
EXTEND	NO	YES	Extend Schedules	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	Yes
SCHEDULS	NO	YES	Schedules	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
TIME	NO	YES	Time	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
DIS EVNT	NO	YES	Display Events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SERV REQ	NO	YES	Service Request	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
FIRE DRILL	NO	YES	Fire Drill	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
TEMP CODE	NO	YES	Temp User Code	No	No	No	No	No	No	No	No	No	No	No	No
ANTI PASS	NO	YES	Anti-Passback	No	No	No	No	No	No	No	No	No	No	No	No
ACCESS SCHEDULES	Sch. 1-99		Access Time	-	-	-	-	-	-	-	-	-	-	-	-
RE ARM DLY	0 – 720		Re-Arm Delay	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
EASY ARM/DISARM	NO	YES	Arm/Disarm	No	No	No	No	No	No	No	No	No	No	No	No
SEC LANGUAGE	NO	YES	Preferred Language	No	No	No	No	No	No	No	No	No	No	No	No
CARD PLUS PIN	NO	YES	Card Plus Pin	No	No	No	No	No	No	No	No	No	No	No	No
WIFI SETUP	NO	YES	WiFi Setup	No	No	No	No	No	No	No	No	Yes	No	No	Yes
TECHNICIAN USER	NO	YES	Technician User	No	No	No	No	No	No	No	No	No	No	No	No

User Codes: Enables the User Codes prompt in the User Menu for this profile. This options allows you to add, delete, or change a user code. You may also assign specific User Profiles to individual users.

Schedules: Enables the Schedules prompt in the User Menu for this profile. This option allows you to assign up to eight Schedules to a profile for door access. Note: To program a profile with anytime access, do not assign the profile number to any Schedules.

Schedules are ideal for individual area auto arming and disarming and for creating Opening/Closing windows during which users can access the building or disarm the system. The Schedules function allows you to program into the system the times at which you normally turn your burglary protection on and off each day of the week. Your system may be pre-programmed at installation to allow automatic arming and disarming. When pre-

programmed, you can enter a schedule for the arming and disarming times. If your system does not use automatic arming, you can use the Closing Check/Extend feature with Schedules to help ensure your system is armed manually at a specific time. This option sounds the keypad buzzer and displays CLOSING TIME! or AREA LATE! when a schedule expires. This reminds users still on the premises to arm the system or extend the schedule to a later time.

Set Time: Enables the Time prompt in the User Menu for this profile. Allows you to change the current date and time displayed on the keypad and used by the system.

Display Events: Enables the Display Events prompt in the User Menu for this profile. Allows you to review up to 12,000 past door access and system events.

Service Request: Enables the Service Request prompt in the User Menu for this profile. Allows you to simply press any Select key when SERVICE REQUEST? displays from the User menu, and have the system automatically send a "Request for Service" message to the central station. The display changes momentarily to REQUEST MADE to confirm your request was sent.

Fire Drill: Enables the Fire Drill prompt in the User Menu for this profile.

Extend: Enables the Extend Closing prompt in the User Menu for this profile.

Temp Code: With Temporary User Codes enabled, an Expiration Date and Expiration Time can be applied to a User Code with the Profile attached. On the Expiration Date, within one hour of the Expiration Time, the User Code is deleted from the panel.

Anti Passback: Enables the Anti-Passback feature for this profile. Anti-passback requires users to properly exit an Area. To do so, they need to access one of the Egress Areas assigned to the door they formerly accessed. If they fail to access an Egress Area, a Failed to Exit message is presented on the keypad and they are not granted access. The user must exit the area by accessing the proper door or someone with User Codes authority must Forgive Failure to Exit from the User Menu to allow entry to the area.

Shifts (1 - 4) (XR100/XR500 Series panels): Check the box for each shift where you want to authorize access for this profile.

Schedules (XR150INT/XR550INT Series or XR150/XR350/XR550 Series panels): Enter each Schedule number you want to authorize access for this profile, up to 8 Schedules per profile. Profiles with no assigned Schedules will have 24-hour access. See Schedules.

Easy Arm/Disarm: When entering a code that has Easy Arm/Disarm enabled, the system will automatically arm or disarm all areas that are assigned to the code. The ALL NO YES? Option does not display when this option is enabled in the user profile.

Anytime (XR100/XR500 Series panels): Check this box if you would like this profile to operate without regard to schedules.

Note: You may select multiple shifts for each profile. For example, a profile may be allowed Shift 1 and Shift 2. You may not select individual shifts if you select Anytime.

Use Secondary Language: Allows the programmed secondary user language to display when the Easy Arm/Disarm option is enabled and the user presents their credentials or enters their user code at the Status List.

Card Plus PIN (XR150INT/XR550INT Series or XR150/XR550 Series panels): When checked, all existing user codes assigned to that profile will need a PIN number assigned. Program the PIN number in Program >> User Codes. For door access, arm/disarm, or User Menu access, the first code must be entered from a proximity patch, credential card, fob, etc., on a reader from a DMP Keypad (Models 7063, 7163, 7073, 7173, 7872, 7873) or an external reader. The second code is a PIN number keyed in at the keypad or can be a second credential.

For users with multiple profiles, when Card Plus PIN is checked, a PIN is only required for the Arm/Disarm or Access areas assigned to that profile.

Note: Card Plus PIN for XR100/XR500 Series panels is located as an option in System Options.

Note: The Card Plus PIN option is only available on Area Systems.

Technician User: If Technician User is enabled in a profile, the user cannot disarm a system that has been armed by a standard user. If the Technician User armed the system, then he or she can disarm it. This feature allows technicians to arm and disarm a system for testing purposes only. This feature is only available on XR150/XR550 Series panels with Verison 171 firmware or higher.

Lockdown Override: Any user who has Sensor Reset and Lockdown Override enabled in their profile will have the ability to return the Lockdown system back to its previous state.

27.2. Profile Record

Use this Profile Record to assist you when planning and programming an XR150INT/XR550INT Series, XR150/ XR350/XR550 Series or XR100/XR500 Series system.

Note: On XR150INT/XR550INT Series, XR150/XR350/XR550 Series and XR100/XR500 Series panels configured for All/Perimeter or Home/Sleep/ Away operation use the default Profiles 1 to 10. For Home/Sleep/Away with Guest systems use the default profiles 1 through 9 for the main house system, default profiles 11-19 for the Guest 1 house system, and default profiles 21-29 for the Guest 2 house system.

				Number											
Menu			Privilege	1	2	3	4	5	6	7	8	9	10	11-98	99
ARM/DIS	NO	YES	Arm & Disarm	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
ALM SLNC	NO	YES	Alarm Silence	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SNSR RST	NO	YES	Sensor Reset	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
LOCKDOWN**	NO	YES	Lockdown	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
DOOR LOCK/UNLOCK**	NO	YES	Door Lock/Unlock	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
DOOR ACS	NO	YES	Door Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
ARM AREA	NO	YES	Armed Areas	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
OUTPUTS	NO	YES	Outputs ON/OFF	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
FAVORITES**	F01-	F20	Z-Wave Favorites	No	No	No	No	Yes	Yes	Yes	Yes	Yes	No	No	Yes
ZN STATS	NO	YES	Zones Status	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
BYPAS ZN	NO	YES	Bypass Zones	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	Yes
ZONE MON	NO	YES	Zone Monitor	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SYS STAT	NO	YES	System Status	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SYS TEST	NO	YES	System Test	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
PROFILES	NO	YES	User Profiles	No	No	No	No	No	No	No	No	Yes	No	No	Yes
USR CODE	NO	YES	User Codes	No	No	No	No	No	No	No	No	Yes	No	No	Yes
EXTEND	NO	YES	Extend Schedules	No	No	No	No	No	Yes	Yes	Yes	Yes	No	No	Yes
SCHEDULS	NO	YES	Schedules	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
TIME	NO	YES	Time	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
DIS EVNT	NO	YES	Display Events	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes
SERV REQ	NO	YES	Service Request	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
FIRE DRILL	NO	YES	Fire Drill	No	No	No	No	No	No	No	Yes	Yes	No	No	Yes
TEMP CODE	NO	YES	Temp User Code	No	No	No	No	No	No	No	No	No	No	No	No
ANTI PASS	NO	YES	Anti-Passback	No	No	No	No	No	No	No	No	No	No	No	No
ACCESS SCHEDULES**	Sch.	1-99	Access Time	-	-	-	-	-	-	-	-	-	-	-	-
1234 ANYTIME	____	ANYTIME	Shift/Time Access	1234	1234	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any
RE ARM DLY*	0-	720	Re-Arm Delay	No	No	No	No	No	No	Yes	Yes	Yes	No	No	Yes
EASY ARM/DISARM	NO	YES	Arm/Disarm	No	No	No	No	No	No	No	No	No	No	No	No
SEC LANGUAGE	NO	YES	Preferred Language	No	No	No	No	No	No	No	No	No	No	No	No

*This option is only available on XR100/XR500 Series and XR2500F panels Version 106 or higher.
**This option is only available on XR150/XR350/XR550 Series panels.

Use this Profile Record to assist you when planning and programming an XR200-485 system.

Profile #	Profile Name	Arm/Disarm Area	Access Area	Output Group	Arm/Disarm	Alarm Silence	Sensor Reset	Door Access	Armed Areas	Outputs On/Off	Zone Status	Bypass Zones	Zone Monitor	System Status	System Test	User Profiles	User Codes	Schedules	Time	Display Events	Service Request	Fire Drill	Extended Schedules	Temp User Code	Anti-passback	Shift/Time Access
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A
		12345678	12345678																							1234A

28.1 User Codes

28.1. XR Series Panels

User Codes for XR150INT/XR550INT Series, XR150/XR350/XR550 Series, and XR100/XR500 Series

The User Codes window allows you to enter or make changes to the user code information in the panel or database file.

To delete a user, select the user from the list on the left side of the window and select Delete at the bottom of the window.

To add a new user, select New and enter information in each field as described below.

You may copy and paste user code information between panels that have the same panel type. For example, if Jane Jones will be working regularly at two sites that both have XR550 systems, you could copy her information instead of re-entering all of the information manually. For information on copying user codes between panels and partitions, see Copying User Code Information.

To scan a user's proximity card, press the Scan Card button. See Scanning a Proximity Card for more information.

User Number: Enter the number you are assigning to this user. This is the number that identifies a user to the system. The User Number can only be as high as the number of users allowed on the panel type.

User Code: Enter the user code that you want to assign to this user. If you are using the proximity reader feature, do not manually enter the User Code. Refer to Scanning Proximity Cards.

Note: When assigning user codes, keep the following in mind:

- When using the proximity reader feature, do not manually enter the User Code. Refer to Scanning a Proximity Card.
- On XT30INT/XT50INT, XT30/XT50, XTL, XTLN, and XTLN-WiFi, you can enter 4-digit User Codes.

- On XR100/XR500 Series, you can enter 3-digit to 6-digit User Codes. Previous XR500 Series versions support 3-digit to 5-digit User Codes.
- XR150/XR350/XR550 Series panels with versions 100 and 101, you can enter 3-digit to 10-digit User Codes for credentials.
- XR150/XR350/XR550 Series panels with version 102, you can enter 3-digit to 12-digit User Codes for credentials.
- XR150INT/XR550INT Series and XR150/XR350/XR550 Series panels you can enter 3-digit to 6-digit User Codes for Arming and Disarming using the keyboard at the keypad.
- XR100/XR500 Series, XR150/XR350/XR550, and XR150INT/XR550INT Series panels configured for All/ Perimeter, Home/Sleep/Away or Home/Sleep/Away with Guest operation, only allow a 4-digit User Code.

Random: Press the Random button to assign a random number to the User Code being entered. The randomly assigned User Code displays in the User Code field. The number of digits assigned to the random User Code is based on the maximum number of digits allowed by the panel or the system configuration.

User Name: Enter the User Name that you are assigning to the user. You may enter up to 32 characters.

Profile Number: Enter a number, from 1 to 99 that will designate the areas and functions that a user may access. Profile numbers are programmed in the Programs >> Profiles window. Press the button to the right of the Profile Number field to display a list of profile numbers and names. Up to 4 profiles can be assigned to each User Code.

Temp Date (XR100/XR500 Series, XR150/XR350/XR550 Series, XR150INT/XR550INT): If the Profile you entered is for a temporary user, select the date the temporary User Code is to expire. You may type the numbers, use the arrow keys, or use the drop-down calendar.

Active User (XR150/XR550 Series): When you add or edit a user code in Remote Link, you have the option to make the user active or inactive. In the User Codes window, check the Active User box to make the user you are creating or editing active, or deselect it to make the user inactive.

User PIN (XR500E, XR150/XR350/XR550, XR150INT/XR550INT): Enter up to a 6-digit number (to 999999) you are assigning to this user as a PIN to enter when the Card Plus PIN option is enabled in Program >> System Options. Each user needs to enter their PIN into the keypad after presenting their card/ proximity credential to the reader when accessing system functions.

Random (XR500E, XR150/XR350/XR550, XR150INT/XR550INT): Press the Random button to assign a random PIN to the user code being entered. The randomly assigned PIN displays in the User PIN field.

Areas (Not available on XRSuper6): Enter the area numbers that you wish to assign arm and disarm capability.

Description: You may enter a description or note regarding the user code entry you are programming.

Copy: Allows you to copy a user and the user code information to another panel of the same model.

Paste: Allows you to copy and paste a user and the user code information from another panel of the same model.

Batch: The Batch option allows you to import, export, and/or delete large numbers of users from a panel file at one time.

Level

Each panel has a different method for assigning user authority levels. Select the links below to view authority levels for each panel type.

Note: This option does not appear on the XR100/XR500 Series, XR150/XR350/XR550 Series, or XR150INT/ XR550INT Series panels.

Program >> User Codes >> Custom Tab

Department: Select the department for the current user from the drop down menu. If the required department is not listed in the drop down menu, additional options can be added by entering the text in the department field or using System >> Configure >> Remote Link >> Custom Fields Tab.

ID Number: Enter the number you are assigning to identify the user to the system.

Card Info: Enter any notes or information pertaining to the user card.

User Field 1/2/3: These customizable fields are available for additional sorting and filtering use. Define these fields using System >> Configure >> Remote Link >> Custom Fields Tab.

28.2. XTL Series Panels

User Codes XTL, XTLN, and XTLN-WiFi

Level: Choose one of two levels from the drop-down menu.

Standard: A Standard authority level is a mid level user. This level allows all options except Schedules, Time Set, and User Codes.

Master: A Master authority level assigns all options to the user code.

Temporary Standard: A Temporary Standard authority level has the same capabilities as a Standard level, however the code will expire in seven days.

28.3. XT Series Panels

User Codes XT30INT/XT50INT, XT30, and XT50

Level: Choose one of four levels from the drop-down menu.

Scheduled: A Scheduled authority level only functions during a valid schedule, except for arming which can be done anytime. Disarming is allowed outside of a schedule, but an "Unauthorized Entry" report is sent to the central station.

Limited: A Limited authority level is a low level user with limited authority.

Standard: A Standard authority level is a mid level user. This level allows all options except Schedules, Time Set, and User Codes.

Master: A Master authority level assigns all options to the user code.

Temporary: Check this box to make this a temporary code. Leave this box empty to assign this as a permanent code.

Arm Only: Check this box to assign this user Arm Only capability. Leave this box empty to allow arming and disarming.

Send Code to Locks: Check this box to send the selected user code to all Z-Wave locks associated with the system. This feature is only available for XT30/XT50 and XTLplus Series panels.

28.4. Copying User Code Information

To copy a user and the user code information to another panel of the same model, open the panel from which you will copy the user code information. Select Program >> User Codes.

Note: Profiles must be the same in both panels and both partitions to accurately copy and paste user code information.

Pasting User Information into a Different Panel

Note: To copy a user to a different panel, the two panel models must be the same. For example, to copy a user from an XR550 Panel, the second panel must be an XR550.

In the User Codes window, select the user to be copied from the list on the left-hand side. Select Copy.

Select File >> Close Panel to close that panel. Then select File >> Panel Information and open the panel to which you will copy the user code information.

Select Program >> User Codes and select Paste. This will paste all of the user code information you copied from the first panel into the second panel.

28.5. Batch Modify User Codes

The Batch Import/Export User Codes window allows you to import, export and/or delete large numbers of users from a panel file at one time.

Import User Codes

To import User Codes, select the Import tab. In the File Name field, select the Tab Delimited .txt file containing the user codes to import.

Note: Remote Link requires the imported User Name data to be in all capital letters. If the User Name data from the import file is not in all capital letters, please correct before importing.

Remote Link requires the following data in this specific order for a successful user import. A header row is not required.

User Number (maximum 4 digits)

User Name (maximum 16 characters for XR500 Series and 32 characters for XR550 Series)

User Code (maximum 12 digits)

User Profile (maximum 2 digits)

User Pin (maximum 6 digits) typically 0 (zero)

Description (maximum 1024 characters)

Note: The User Pin column is required for user code import. If the panel does not use the Feature Key Duress + 2, populate this field with 0 (zero).

Select Load File to display the user codes contained in the selected .txt file. All user codes eligible for import are automatically checked. A user that already exists in the panel cannot be selected for import.

Select Import to add selected user codes to the panel.

Export User Codes

To export User Codes, select the Export tab. In the File Name field, select a file name and the location to save the User Codes you are exporting. The file is saved as a Tab Delimited .txt file.

All the User Codes programmed in the panel display for selection. Select the checkbox next to the user code to export or Select All. When selection is complete, select Export.

Note: The description field is not exported.

Delete User Codes

To delete User Codes from the panel file, select the Delete tab.

Select the checkbox next to the user code to delete, or Select All. When selection is complete, select Delete.

28.6. 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. Refer to LT-0619 for information about installing the proximity reader USB. 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 the Scan Card button 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.

29. 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 make changes to the panel's programming through the keypad, they must enter the designated access code.

To assign an access code, enter a number in the Code field in the Access Code window and select OK. This number must not be higher than 65535 or less than 3 digits, (0, 100 to 65535) for XR Series panels and 0 to 65535 for XT30/XT50 Series panels.

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

Part . Alarm List

The Alarm List allows operators to receive and process signals from subscriber accounts. View the Alarm List by pressing the F3 key or by navigating to System >> Alarm List.

Note: You must log into Remote Link before viewing and acknowledging any messages.

With Remote Link, you have the ability to monitor multiple accounts from one Alarm List window. You can view the Alarm List while other Remote Link windows are open. If an alarm signal is received while you have other windows open, the Alarm List automatically opens and comes to the front of all other windows with the new alarm message selected.

An audible alert tone sounds on your computer's internal speaker when an 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 the Acknowledge button. 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.

1. Alarm List Description

The main group in the Alarm List window displays all alarm signals. When alarm signals are received, they display on a violet background until acknowledged. After the alarm signal is acknowledged, the color changes according to the type of message received. See Ack - F6 for a list of acknowledged colors.

The most recently received and highest priority messages display on the top of the list. The audible alert tone continues to sound until all messages have been acknowledged.

Note: You may re-size the columns in the Alarm List by placing your cursor in the top row containing the column headings. Drag the column to the right or left to adjust the size of the column. To make an account active, select a message in the Alarm List by selecting anywhere in the message line.

Account: Lists the account number that is transmitting an alarm message. This is the first column on the left-

hand side of the screen.

Message: Lists all of the pertinent information for the incoming signal. The Message field can hold up to three lines of text. The information listed in the Message field is as follows:

Zone Number: The zone number that is in alarm is listed here. If the signal does not include a zone number, a Report Identifier is displayed here. Common Report Identifiers are warning, alert, and abort.

Zone Name: The zone name that is in alarm is displayed here. The zone name can be up to 16 characters long.

Report Type: The type of signal displays, such as Alarm, Panic, or Trouble.

No Account Record: If a signal has been received from an account that is not in the database, "No account record" will display in the second line of the Message field.

Restoral Status: If a signal has been received, but a restoral signal was not received "Not Restored" will display in the second line of the Message field. When the restoral signal is received, "Not Restored" will no longer display in this field.

Rpt. (Repeat Count): Lists the number of times repeat signals have been received. If a signal has been received one time, a 0 (zero) displays here. If the exact same message is received from the same account, the Repeat Count increases to 1 (one). The message returns to the violet color, indicating its unacknowledged state. The alert tone also sounds until the message is acknowledged. The repeat count increases by increments of one each time repeat signals are received.

Time (Time Received): Lists the time and date the alarm signal was received. In the case that a signal has been received multiple times, also called a Repeat Count message, the Time column displays the date and time of the first signal received. To view the other dates and times a Repeat Count signal occurred, print a report by pressing the Print button.

Note: Remote Link receives the time and date from the Windows Operating System. If a site is in a different time zone than the central station receiver, alarm signal's date and time would be based upon the central station's date and time.

Ackn. (Acknowledge Time): Displays the time and date the signal was acknowledged by the operator. In the case that a signal has been received multiple times, also called a Repeat Count message, the Ackn. column displays the date and time of the last time the signal was acknowledged.

2. Organization of the Alarm List

When alarm and trouble messages are received, Remote Link displays them in the Alarm List. The last signal to be received is displayed on the top row of the Alarm List. Incoming signals are displayed on a violet background until you acknowledge them.

Messages are sorted by priority. First, they are sorted by acknowledged and unacknowledged, with the unacknowledged signals above the acknowledged signals. Within these two categories, signals are then sorted by event type and time received. Messages with the highest priority and those that were received the most recently display at the top of the Alarm List.

Example: If a fire alarm was received at the same time a zone trouble was received, the fire alarm would appear above the zone trouble signal. This is to ensure that proper and timely action is taken on each incoming signal.

If more than one unacknowledged message is displayed in the Alarm List, the messages are prioritized in the following order:

1. Fire Alarms
2. Panic Alarms
3. Burglary Alarms
4. All Supervisory

5. All Emergency
6. Auxiliary 1 and Auxiliary 2 Alarms
7. Fire Troubles
8. Other Fire (CleanMe™, zone fault, etc.)
9. Other Burglary (zone trouble, zone fault, etc.)
10. All Other Messages (AC fail, low battery, etc.)

3. General Information in Alarm List

This section of the Alarm List window provides you with the name and account number for the account that is currently active in the Alarm List. The information entered in the General Information fields in the Panel Information window when setting up the account will appear here. You may not edit the information here: You must edit the information in the Panel Information window to change the General Information in the Alarm List window.

4. Location Information in Alarm List

The Location Information fields automatically reflect the site's information for the account currently active in the Alarm List. This information is the same as that entered in the Location fields in the Panel Information window. The operator may view the information from this screen, but all editing to Location Information must be completed in the Panel Information window. Location Information includes the following information:

- Address
- City
- State
- Zip Code
- Voice Phone
- Night Phone

An additional button labeled Hyperlink is available when using the Alarm Monitoring module or the Command Center. Refer to the Creating a Hyperlink for more information.

If a message is selected that does not have an account record on file, "No Account Record" displays in the second row of the message and all fields in the Location box are empty.

5. Extended Information in Alarm List

There are several options provided for you to gain more information about an account in the Extended Information window: Site Password, Response, Notes, and Call List.

The Site Password displays for the account currently active in the Alarm List.

Hyperlink: (Must have a module to Use) Press the Hyperlink button to open the linked file or Web page. Hyperlinks are created in the Extended Information window. See Creating a Hyperlink for more information.

Pressing any of the three buttons labeled Response, Notes, or Call List displays a window containing the information entered in the Panel Information window. Any editing to this information must be completed in the Panel Information window.

6. Visible Alarms in Alarm List

Remote Link allows you to view three different lists of messages:

All - F3: View all messages, both acknowledged and unacknowledged. This is the standard Alarm List. Disabled messages do not display in the Alarm List.

Disabled - F4: View messages that have been disabled. If messages are in this list, Disabled - F4 is in blue text. To re-enable a message in this list, press the Enable button. The message then returns to the Alarm List.

Note: Disabled messages are removed from the Alarm List until they have been re-enabled. If the same alarm signal is received again, the alarm message does not appear in the Alarm List and the tone does not sound. The repeat count continues to increase, though, as multiple disabled messages are received. Be sure that the signal is a false alarm or a runaway before disabling.

Non-Restored - Alt-F3: View all messages that have not been restored. Non-restored messages indicate the zone that is in alarm must be restored to normal. If a Non-Restored signal is sent with the alarm message, "Not Restored" appears in the alarm message. When the restoral signal is received from the panel, "Non-Restored" is removed from the alarm message automatically.

7. Command Buttons

Six command buttons are provided so the operators can easily and quickly manage multiple signals.

Ack - F6: Press to acknowledge the selected alarm and silence the alert tone.

Remove - F9: Press to delete the message from the Alarm List.

Disable - F12: Press to disable the alarm and remove it from the Alarm List.

Connect: Press to connect to the account that is selected in the Alarm List.

Print: Press to print customized reports of the accounts in the Alarm List.

Cancel: Press to exit the Alarm List window.

8. Acknowledging Alarm Messages (F6)

Acknowledge: Press the Acknowledge button to acknowledge the active signal in the Alarm List and silence the audible alert tone. If unacknowledged signals remain in the Alarm List, the audible alert tone continues to sound until you have acknowledged all alarms.

F6 is the function key that has been assigned to Acknowledge. Simply press F6 to acknowledge the alarm active in the Alarm List.

Note: You must be logged onto Remote Link before acknowledging any alarm signals.

After you have acknowledged a message, the color of the message field changes to indicate that the message has been acknowledged. The message field changes to a specific color that is unique to the type of message that was acknowledged.

Violet: Unacknowledged alarm messages

Red: Fire Alarm, Fire Trouble, and Fire Restore messages

Yellow: Burglary Alarm or Burglary Trouble messages

Green: Emergency messages

Gray: Auxiliary 1 and Auxiliary 2 messages

Orange: Supervisory Zone Messages

Light Green: Panic messages

Light Yellow: System messages and all other messages

After you have acknowledged a message, it remains in the Alarm List until you remove or disable the message. The Activity Log records that the operator has acknowledged the message.

You also have to option to purge events and acknowledged messages. See Purge Options for more information.

9. Removing Alarm Messages (F9)

Remove: Press the Remove button to delete the selected message from the Alarm List. You must Acknowledge an alarm message before you can remove it from the Alarm List. The Activity Log records that the operator has removed the message from the list.

F9 is the function key that has been assigned to Remove. Simply press F9 to remove the selected alarm from the Alarm List.

Note: You must be logged in before removing any messages.

10. Disabling Alarm Signals (F12)

Disable: Press the disable button to disable the selected message and remove it from the Alarm List. You must Acknowledge an alarm message before it can be disabled. The Activity Log records that the operator has disabled the message.

Note: You must be logged in before disabling any messages.

F12 is the function key that has been assigned to Disable. Simply press F12 to disable the selected alarm.

Note: Disabling an Alarm message removes it from the Alarm List until it has been re-enabled. If the same alarm signal is received again, the alarm message does not appear in the Alarm List and the tone does not sound. The repeat count continues to increase, though, as multiple disabled messages are received. Be sure that the signal is a false alarm or a runaway before disabling.

To re-enable a disabled alarm, press the Disable List radio button above the Alarm List. Then select the desired message and press the Disable button. The message returns to the Alarm List.

11. Connecting in Alarm list

Connect: The Connect button in the Alarm List window allows you to quickly connect to the selected account. After you press the Connect button, the Connection Status dialog box opens with the selected account number in the account field. Select Connect in the Connection Status box to connect to the account.

Note: If you attempt to connect to an account that has no programming on file, you must connect to the Main Account.

12. Printing the Alarm List

You can print events from the Alarm List in two ways:

- Go to File >> Print >> Events.
- Go to System >> Alarm List and press the Print button.

Note: Printing through the Alarm List window prints the active account in the Alarm List. Printing from File >> Print >> Events prints the account active in Remote Link.

After pressing the Print button or selecting Print >> Events, the Event Reports Setup dialog box appears containing the following fields:

Panel: Enter the range of account numbers you wish to print. You can check All to print all account records. The Account field defaults to the active account in the Alarm List.

Date: Enter the range of dates you wish to print. Enter the first and last dates in the Date field using mm/dd/year format. The year must be entered in 4-digit format. Selecting All will print all of the dates for the selected record.

Messages in the Report: You can select which messages you would like to print.

If you have the Alarm Monitoring module or the Advanced Reporting module, there are extra features available to you in the Print Events window. For a description of these features, read Alarm Monitoring and Advanced

Reporting module.

13. Messages in the Alarm List Report

Check the box next to the event type that you would like to print. You may select any combination of the following event types:

- Alarm
- Trouble
- Restoral
- System

All: Selecting All will check all boxes.

Clear: Selecting Clear will clear all boxes.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to File >> Print >> Saved Report.

Print: Select this button to print the account reports to an attached printer.

Part . Alarm Monitoring Module

The Alarm Monitoring module is a separate product from Remote Link. Contact your dealer or visit the DMP website for more information about this product.

1. Alarm Monitoring

The sophisticated Alarm Monitoring module expands the capabilities of the Alarm List present in Remote Link by allowing you to receive 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 an easy 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.

To obtain optimum results from the Alarm Monitoring module, it is highly recommended that you install the software on a computer dedicated solely to the Alarm Monitoring module and Remote Link.

2. Alarm List with Alarm Monitoring Module

The Alarm List allows operators to receive and process signals from subscriber accounts. You may view the Alarm List at any time by pressing the F3 key, or by opening System >> Alarm List.

Note: You must log on to Remote Link before viewing and acknowledging any messages.

With Remote Link, you have the ability to monitor multiple accounts from one Alarm List window. You can view the Alarm List while other Remote Link windows are open. If an alarm signal is received while you have other windows open, the Alarm List will automatically come to the front of all other windows. If you do not have the Alarm List window open and a new message is received, Remote Link will automatically open the Alarm List and select the new alarm message.

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

If an operator is not logged on when an alarm is received, Remote Link will sound an audible alert tone and display 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.

3. Printing with the Alarm Monitoring Module

The Alarm Monitoring module expands the capability of the Alarm List already in Remote Link by giving you the ability to print Opening and Closing Reports, and Door Access Reports.

You can print Door Access and Opening/Closing events from the Alarm List in two ways:

- Go to File >> Print >> Events.
- Go to System >> Alarm List and press the Print button.

Note: Printing through the Alarm List window will print the active account in the Alarm List. Printing from File >> Print >> Events will print the account active in Remote Link.

After pressing the Print button or selecting Print >> Events, the Event Reports Setup dialog box will appear containing the following fields:

Summary: Select Summary to print a report of events sorted by account number.

Customer Mailout: Select Customer Mailout when printing reports to send to customers. This option sorts the events by account and automatically breaks the pages when a new account is detected allowing you to mail the reports to each customer.

Account: Enter the range of account numbers you wish to print. Enter the receiver number then the account number, for example 1-12345 with 1 being the receiver number and 12345 the account number. Check All to print all account records. The Account field defaults to the active account in Remote Link, if selecting File >> Print >> Events as described above.

Date: Select the arrow to the right of the field to open the drop-down calendar, as shown above. Select the date to select the desired date. You may also type in the appropriate date. Selecting All will print all of the dates for the selected record.

Messages in the Report: You can select which messages you would like to print.

4. Printing Messages with the Alarm Monitoring Module

Check the box next to the event type that you would like to print. You may select any combination of the following event types:

- Alarm
- Trouble
- Restoral
- System
- Open/Close
- Other (such as Door Access, Bypass events, code changes, etc.)

All: Selecting All will check all boxes.

Clear: Selecting Clear will clear all boxes.

Setup: Select this button to enter the printer setup window to configure your print options.

Preview: Select this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to File >> Print >> Saved Report.

Print: Select this button to print the account reports to an attached printer.

Part . Command Center Module

The Command Center module is a separate product from Remote Link. Contact your dealer or visit the DMP website for more information about this product.

1. Command Center

The sophisticated Command Center Visual Alarm Command and Control Software expands the capabilities of the Alarm List present in Remote Link by allowing you to receive 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 Command Center enables you to visually monitor alarm activity on subscriber accounts using an SCS-1 or SCS-1R Receiver, SCS-105 Receiver, or an Ethernet host monitoring network connection.

The Command Center enables you to visually monitor alarm activity on subscriber accounts using an SCS-1 or SCS-1R Receiver, SCS-105 Receiver, or an Ethernet host monitoring network connection.

The Command Center is composed of two different windows: The Alarm Grid window is a segmented grid and the Alarm List contains alarm information for each account. The Alarm Grid window organizes your subscriber accounts by account number in the grid. Each account is assigned one square, or segment, in the Alarm Grid window. Each account also has its own Alarm List: When you select the account's segment in the Alarm Grid window, the Alarm List opens displaying the account's alarm and account information.

Once in the Alarm List window, acknowledge alarm signals by pressing the F6 key or by selecting Ack. You may view account information while in the Alarm List window and open hyperlink files.

If more than one unacknowledged alarm signal is pending, the warning tone will continue until you acknowledge all alarm signals. In addition, the Command Center displays the message "Unacknowledged Alarms: X" in red text at the bottom of the screen. "X" represents the number of unacknowledged alarms.

You can open the Alarm Grid window by selecting System >> Alarm Grid from the menu. Pressing F3 also opens the Alarm Grid window.

Refer to the Alarm List topics in this help file to learn more about the Alarm List within the Command Center.

To obtain optimum results from the Alarm Monitoring module, it is highly recommended that you install the software on a computer dedicated solely to the Alarm Monitoring module and Remote Link.

2. Alarm Grid

The Alarm Grid window enables you to view all account alarm activity by simply watching a grid. Each segment of the grid represents one subscriber account. When the mouse moves over each segment of the grid, the account information is displayed in a small pop-up window. Select once to open the account's Alarm List that displays information about the account and the alarm signals.

Arranging the Alarm Grid Window

The accounts in the Alarm Grid window are arranged in numerical order, according to receiver number and account number. The segments are filled from left to right and top to bottom: The lowest account number will be listed before higher account numbers. For example, account 1-12 appears before account 1-22.

Also, all accounts reporting to receiver 1 are listed before those reporting to receiver 2 and above. For example, account 1-12345 appears before account 2-12345.

Use the scrollbar on the right of the grid to move up and down in the grid. When an alarm occurs on an account that is not in the screen, the Command Center automatically scrolls to the necessary segment.

Prioritizing Alarm Signals in the Alarm Grid Window

Messages are sorted by priority according to event type and time received. The Command Center will display the segments with messages that have the highest priority and those that are received more recently before scrolling to others.

If two alarms occur at the same time but cannot fit on the screen together, the Command Center first displays the account segment with the higher priority alarm. After the highest priority alarm is acknowledged, the Command Center then brings the next highest priority account segment to view.

For example, if a fire alarm is received at the same time a zone trouble is received, the Command Center scrolls to the segment with the fire alarm and then the segment with the zone trouble. This is to ensure that proper and timely action is taken on each incoming signal. Messages are prioritized in the following order:

1. Fire Alarms
2. Panic Alarms
3. Burglary Alarms
4. All Supervisory
5. All Emergency
6. Auxiliary 1 and Auxiliary 2 Alarms
7. Fire Troubles
8. Other Fire (CleanMe™, zone fault, etc.)
9. Other Burglary (zone trouble, zone fault, etc.)
10. All Other Messages (AC fail, low battery, etc.)

3. Viewing Account Information

As you move the mouse over each segment of the grid, pop-up windows appear containing general information about each account. The pop-up window includes the account number, name, and location. This information is that entered in the Panel Information window.

The pop-up windows allow you to easily identify each account without the need to open the Alarm List to determine account information. Once the mouse is removed from the segment, the pop-up window disappears.

4. Identifying Signals with the Alarm Grid

When the Command Center first receives an alarm message, the grid segment changes from white to a specific color that indicates the type of signal received. The color designation allows you to quickly gain information about the alarm signal.

Color	Alarm Signal
Red	Fire Alarm, Fire Trouble, and Fire Restore messages
Yellow	Burglary Alarm or Burglary Trouble messages
Green	Emergency messages
Gray	Auxiliary 1 and Auxiliary 2 messages
Orange	Supervisory Zone messages
Light Green	Panic messages
Light Yellow	System messages and other messages

The segment remains the designated color until it is acknowledged in the Alarm List window.

5. Managing Alarm Signals

When the Command Center receives an alarm signal from a subscriber account, several things occur to inform you of the new alarm signal:

- An audible tone sounds until all signals have been acknowledged.
- The Alarm Grid window automatically opens on the screen and comes to the front of other windows open in Remote Link.
- The account's segment turns a designated color to indicate that an alarm has been received for this account.
- The Command Center automatically scrolls so the proper account segment is visible when an alarm is received.
- Acknowledging Alarm Signals.
- After Command Center has received the alarm signal, select the account's segment where the alarm has occurred. This opens that account's Alarm List. From the Alarm List, you can view the alarm messages to learn the type of alarm, the zone the alarm occurred on, and other important information.

6. System Segment

The System segment is located in the top left-hand corner of the grid. The System segment contains information about system messages and signals received form accounts with no information on file.

When a system message is received that is not associated with an account, such as receiver messages, the System segment will turn light yellow. The name field will display the receiver number followed by the account number of zero (0). For example, the name field will display 1-0.

When a system message is received for an account that is not in the Command Center's database, the System segment will change to the color of the type of signal received. The Alarm List will display "No account record" on the second line of the message.

When a system message is received that is associated with an account, the account's segment will change to light yellow. You must then process the system message as any other alarm message.

7. Tracking Automatic Recall Tests

An icon shaped like a clock indicates that a scheduled automatic recall test has not been received from the account. When the automatic recall test is received, the icon will no longer be displayed.

Note: The clock icon will only display when Auto Recall Frequency field has been filled-in with a number of days in the Extended Panel Information window.

8. Tracking Armed Status

An icon shaped like a padlock will appear in an account's segment to indicate that the account is fully armed. The icon will appear in every account's segment that has been fully armed. When any area is disarmed, the icon is no longer displayed.

Note: The padlock icon will only display when Track Armed Status is selected. Go to System >> Configuration >> Remote Link and select the Modules Tab.

Note: Only the XR200 version 110 and XR200-485 version 204 support this feature. The other panels will be revised to include this feature soon.

Part . Advanced Reporting Module

The Advanced Reporting module is a separate product from Remote Link. Contact your dealer or visit the DMP website for more information about this product.

To configure the Advanced Reporting module to accept signals through a direct connection or a network connection, make the appropriate selections in the Modules Tab of Remote Link Configuration.

1. 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's event buffer, or you may create reports using the Host Log Reports feature in the XT30/XT50, CellComSL, DualCom Series, XR150/XR350/XR550 Series, and XR500/XR100 Series panels. You can also generate reports received from an SCS-105, SCS-1 Receiver. Additionally, you may connect to the Advanced Reporting module through a direct connection or network connection.

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.

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 or the Command Center.

2. Compatible Panels

The Advanced Reporting module can be used with the following panels that allow you to Request Events:

- XT30/XT50
- CellComSL
- DualCom Series
- XR150/XR350/XR550 Series
- XR500/XR100 Series

You can also use the Advanced Reporting module with the XR150/XR350/XR550 Series, XR500/XR100 Series, and XT30/XT50 Panels with the Host Log Reports programming option.

You can also generate reports using the signals received from an SCS-105 or SCS-1 or SCS-1R Receiver. All DMP panels can be used with the Advanced Reporting module if this method is used.

3. Establishing a Connection

To obtain the data necessary to create advanced reports, establish a direct connection or a network connection. If you are generating reports from an SCS-105 or SCS-1 or SCS-1R Receiver, use the current connection method already established in Remote Link.

Note: If you are using the Request Events method to create advanced reports, use your standard connection method to Request Events. See Obtaining Data for Advanced Reports for more information.

4. Obtaining Data for Advanced Reports

The Advanced Reporting module creates reports from the panel's activity. You must obtain the data necessary to create the reports using one of the methods listed below.

You may create advanced reports using the data gathered by requesting the events from the panel. Refer to Request Events for instructions. After you have properly requested the panel's events, select Panel Event Buffer for the Source of the Advanced Report.

Some panels may be programming to send Host Log Reports. The panels that can send Host Log Reports are the XR150/XR350/XR550 Series, XR500/XR100 Series, and XT30/XT50 Panels. If the panel is programmed to send these reports, you do not need to request events from the panel before creating an advanced report.

You may use the messages received from an SCS-105 or SCS-1 Receiver. You may also use the Advanced Reporting module with another module, such as Alarm Monitoring. When using the two modules together or with a receiver, you do not need to request events to obtain advanced reports data. The Advanced Reporting module will use the same data received to generate reports.

5. Printing with the Advanced Reporting Module

The Advanced Reports Setup window allows you to print reports of the alarm message information. Open the Advanced Reports Setup window by selecting File >> Print >> Events.

Source: Select the source of the reports.

Events: Selects the events sent from an XT30/XT50, CellComSL, DualCom, XR150/XR350/XR550 Series, XR500/XR100 Series that has 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.

Note: 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 the 10 Report Categories:

Zone Action	Door Access Denied
Arming/Disarming	Opening/Closing Schedule Changes
Area Late to Close	System Monitors
User Code	System Events
Door Access Granted	All Events

Account: Enter the account number for which you are running the report. Select the All box 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 the All box to print all available dates.

Options: The Options group box changes depending on which Report Category is selected.

6. Zone Action Report Category

Select Zone Action to 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.

7. Arming/Disarming Report Category

Select Arming / Disarming to 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.

Note: 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.

8. Area Late to Close Report Category

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.

Note: Area Late to Close reports will not be generated if Area Schedules is disabled in Partition Information.

9. User Codes Report Category

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.

10. Door Access Granted Report Category

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, select Select Multiple Doors from the drop-down menu. Then press the

Select Doors button to open the Select Multiple Doors pop-up window. 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.

11. Door Access Denied Report Category

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.

Note: 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, select Select Multiple Doors from the drop-down menu. Then press the Select Doors button to open the Select Multiple Doors pop-up window. 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.

12. Schedule Change Report Category

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.

Note: 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.

13. System Monitors Report Category

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 which you will run the report. Select All to include all System Monitor Actions in the report.

14. System Events Report Category

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 Late to Close 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.

15. All Events Report Category

Selecting All Events for the Report Category will create a report with all of the Report Categories. By default All is selected.

16. Exporting 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)

Part . SQL Server Module

The SQL module allows larger corporate users to take advantage of existing Microsoft SQL Server installations they already have in place. This module allows an administrator to configure an ODBC connection to an existing Microsoft SQL Server installation, on which it will then create the database structure necessary to store all of the panel programming information.

The module also allows the administrator to export all existing panel programming information from the standard DBISAM database, and then import that information into a newly created Microsoft SQL database. The SQL module is an add-on module to Remote Link.

1. SQL Server Installation

Remote Link is designed to use Microsoft SQL Server 2008 R2. All editions of Microsoft SQL Server 2008 R2 are supported, including the SQL Server 2008 Express edition.

Both the 32-bit and 64-bit versions of SQL Server are supported by Link. Install the version that corresponds to the operating system version of the machine which the Server will operate. For example, if running the server on Windows 7 64-bit, install the 64-bit version of SQL Server.

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.

Installing SQL Server 2008 R2 Express also installs the database and management tools including SQL Server Management Studio (SSMS). This tool can be used to connect and examine the database used by Remote Link.

If Remote Link is configured to use SQL Server via a DSN and is not able to log in at startup, a login screen will appear.

The user should contact the database administrator to find the correct options. If SQL Server Authentication is chosen, a User Name and Password must be provided. This is the SQL username and password, not the Remote Link username and password.

The login screen 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 on the database side.

2. SQL Server Administration

For users of Remote Link in mission-critical applications (such as central station monitoring), it is recommended 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 configuration.

When using 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 Link with the built-in database engine, or with Link Server, Link can still be used to perform database backup and repair operations.

3. Setting up SQL Server Database for Link

The database administrator should create an empty database.

Any user created to be used for SQL Server authentication must have permission to read, write, modify and delete all tables.

An ODBC Data Source will need to be created to allow Link to connect to the new Link database. For more information, go to Setting up ODBC Data Source.

4. Setting up ODBC Data Source

To use Remote Link with Microsoft SQL Server, a ODBC Data Source must be set up on the user's machine.

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 is odbcad32.exe can be found within `C:\Windows\System32\`.

Add a System DSN for SQL Server

1. For Windows XP: Start >> Settings >> Control Panel >> Administrative Tools >> Data Sources (ODBC) to open ODBC Data Source Administrator.
   For Windows 7: Start >> Control Panel >> Administrative Tools >> Data Sources (ODBC) to open ODBC Data Source Administrator.
2. Select System DSN tab.
3. Press Add.
4. In Create New Data Source window, select 'SQL Server', then press Finish
5. In Create a New Data Source to SQL Server window

a. Give the data source a Name and Description. Make note of the name you assign.

b. Select the server from the dropdown.

Note: 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'`

c. Press Next

d. Consult with your database administrator to determine whether to use Windows NT Authentication or SQL Server Authentication. If using SQL Server Authentication, use the Login ID and Password priovided by the administrator.

e. Press Next

f. Change default database to the Link database.

g. Press Next

h. Press Finish

6. Test Data Source

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 is odbcad32.exe and can be found within `C:\Windows\System32\`

5. Importing Panel Programming into SQL Database

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 newly created Microsoft SQL database.

1. Backup database. While using the SQL Server module, Remote Link does not automatically backup the database.

2. Make sure Remote Link has been upgraded to 1.60 including updating the database.

3. Export database accounts. Go to File >> Import and Export >> Export Accounts. For more information on Exporting Accounts, see Export Account Information.

4. Go to System >> Configure >> Remote Link >> Database Tab. Within the Database Tab, type in the name you gave the ODBC data source you created in the previous section "Setting up ODBC Data Source". The location must start with "dsn:"

5. Select OK to exit configuration.

6. Restart Remote Link.

7. When Remote Link restarts, select Yes to initialize database.

8. Import database accounts. Go to File >> Import and export >> Import Accounts. For more information on Importing Accounts, see Import Account Information.

Part 1. Account Groups Module

1. Account Groups

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. Using the Account Groups module, you can group panels together under one name and associate the groups by location, business, or other logical grouping. Once grouped, you can update all the panels within the group in one operation. You can also update panels and send that information to multiple account groups in one operation. There is no limit on the number of groups you can create.

Basic Requirements

Complete Account Group module updates 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.
- Compatible DMP Command Processor™ Panels

Compatibility

The Account Groups module can be used with the following panels:

Version 108 or higher

- XR500N
- XR500E

All versions

- XR100N
- XR150N
- XR350N
- XR550E
- XR550N
- XR550INT

2. Using Account Groups

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

The window is divided into two sections. The left section, Groups, lists the group names currently stored in the database and the New and Delete buttons. The right section, Accounts in Group, lists the panel account names and numbers and the Add, Remove, Open Group, and Cancel buttons.

Existing accounts display in the Accounts in Group window and can be included in a group account. To modify the information contained in an account group, refer to the details below.

- Group Name: This field 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: Pressing Add displays the Select Accounts window. Select the account to add to the group and press the Add button.
- Remove: Allows you to delete an account from the group.
- Open Group: This option opens the group currently highlighted in the Groups window. Open the group to program holiday dates, schedules, output schedules, profiles, and user codes and to send that information to a group. The group name displays next to Remote Link in the display above the menu bar.
- Cancel: Exits the Account Groups window.

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 the Batch button. From here, select either Add Account(s) to this Group to group add accounts to the selected group that haven't already been grouped yet, or Remove Account(s) from this Group. You can also

select the Edit button to display a list of all the systems in programmed Remote Link and filter your account search. Select the OK button when finished. Select the Done button when you are finished adding or removing accounts from the group.

3. Programming Holiday Dates

The Holiday Dates window allows you to enter dates that are used by the Holiday Schedules to override daily schedules.

To program Holiday Dates for a group, the group must first be opened or created. The currently opened group displays next to Remote Link in the display above the menu bar.

The Program >> Holiday Dates window allows you to enter or make changes to the Holiday Dates information in the group database file.

Add a New Holiday Date

Select New and enter information in each field listed below. To accept the added information, select Apply at the bottom of the window.

- Number: Assign a number to the holiday date. You may assign up to 20 holiday dates.
- Name: Enter up to 16 characters for the name of the holiday. The name does not show up on the panel, but does appear on reports.
- Class: Allows you to assign one of three different schedules to a holiday. Each holiday class assigns a different schedule to a holiday. Choose A, B, or C from the drop-down menu.
- Holiday: Select the date of the holiday from the drop-down calendar.
- Description: To enter a note or description regarding the holiday entry you are programming, type the information in the Description field or press the Description button to open the Edit Rich Text window. After you type your note, go to File >> Save and Exit to save your work and close the Edit Rich Text window. Your note appears in the field above the Description button. This information does not show up on the panel, but does appear on reports.

Delete a Holiday Date

Select the event from the list on the left side of the window and select Delete at the bottom of the window.

4. Programming Output Schedules

Output Schedules allow you to set the times when relay outputs connected to your system turn on and off automatically.

To program Output Schedules for a group, the group must first be opened or created. The currently opened group displays next to Remote Link in the display above the menu bar. The Program >> Output Schedules window allows you to enter or make changes to the Output Schedule information in the group database file.

- To add a new Output Schedule, select New and enter information in each field. To accept the added information, select Apply at the bottom of the window.
- To delete an Output Schedule, select the schedule from the list on the left side of the window and select Delete at the bottom of the window.

Output: Enter the output number that you wish to assign a schedule. To program door schedules, enter D and a device address number.

- XR550INT Series, XR350/XR550 Series, or XR500 Series: Select D01 to D16

- XR150INT Series, XR150 Series or XR100 Series: Select D01 to D08

Schedule: Enter the schedule number to program. The Schedule field allows up to 100 different scheduled times for relay outputs and door access relays connected to your system to turn on and off automatically. The maximum number of schedules you may assign per door access relay or relay output is 8.

On: Enter the time to turn on the output. Repeat for each day of the week that you wish to program.

Off: Enter the time to turn off the output. Repeat for each day of the week that you wish to program.

5. Programming Profiles

The Profiles window allows you to add, delete, or change User Profiles. A profile defines the authority of each user code in the system.

To program Profiles for a group, the group must first be opened or created. The currently opened group displays next to Remote Link in the display above the menu bar. The Program >> Profiles window allows you to enter or make changes to the Profiles information in the group database file.

- To add a new Profile, select New and enter information in each field. To accept the added information, select Apply at the bottom of the window.
- To delete a Profile, select the schedule from the list on the left side of the window and select Delete at the bottom of the window.
- Profile: Enter a number to assign to the profile. Each profile may be assigned a number from 1 to 99.
- Note: On XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 and XR100 Series panels, Profiles cannot be changed via keypad for All/Perimeter or Home/Sleep/Away operation. Use the default Profiles 1 to 10.
- Name: Enter a name to assign to the profile you are programming. Each profile may be assigned a 16-character name.
- Arm/Disarm Areas: Enter the number for the areas that you want to authorize this profile to arm and disarm. Beginning with XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 Series and XR100 Series, you can specify separate arm and disarm authority for a profile.
- Each profile may be assigned specific areas of the burglary part of the system for arming and disarming. When profiles 1 to 98 are created, no areas are assigned by default. By default, profile 99 is assigned authority to all areas.
- Access Areas: Enter the number for the areas you want to authorize access for this profile.
- Areas 1 to 32 for XR550INT Series, XR550 Series, or XR500 Series
- Areas 1 to 16 for XR350 Series
- Areas 1 to 8 for XR150INT Series, XR150 Series or XR100 Series

Each profile may be assigned door access to specific areas. When profiles 1 to 98 are created, no areas are assigned by default. By default, profile 99 is assigned authority to all areas.

Note: On XR150INT/XR550INT Series, XR150/XR350/XR550 Series, XR500 or XR100 Series panels set to All/Perimeter or Home/Sleep/Away operation, Access Areas should be left at factory default settings.

Output Group: You may assign each profile to an output group number from 1 to 20. See Output Groups for more information.

Re-Arm Delay: Allows the entry of 0 to 250 minutes to be used to delay automatic rearming when the user disarms an area outside of schedule. If zero is selected, the rearming occurs based on Late/Arm Delay programming in the panel Area Information.

Re-Arm Delay is also used to delay a late to close message to the central station when the panel does not use automatic arming.

If the user has Extend Schedule authority, 2HR 4HR 6HR 8HR displays at disarming. If the user does not make a choice, the Re-Arm Delay is used to extend the schedule.

Profile Options: Each user profile may be assigned any of the profile options. Select each box for the options you wish to assign to the profile.

Shifts (1-4): Check the box for each shift where you want to authorize access for this profile.

Anytime: Check this box if you would like this profile to operate without regard to schedules.

Note: You may select multiple shifts for each profile. For example, a profile may be allowed Shift 1 and Shift 2. You may not select individual shifts if you select Anytime.

Description: To enter a note or description regarding the profile entry you are programming, type the information in the Description field or press the Description button to open the Edit Rich Text window. After you type your note, go to File >> Save and Exit to save your work and close the Edit Rich Text window. Your note appears in the field above the Description button.

6. Programming Schedules

The Schedules window allows you to schedule auto arming and disarming of individual areas.

To program Schedules for a group, the group must first be opened or created. The currently opened group displays next to Remote Link in the display above the menu bar. The Program >> Schedules window allows you to enter or make changes to the Schedule information in the group database file.

- To add a new Schedule, select New and enter information in each field. To accept the added information, select Apply at the bottom of the window.
- To delete a Schedule, select the schedule from the list on the left side of the window and select Delete at the bottom of the window.

Shift: The Shift drop-down menu allows you to program access and arm/disarm schedules. Select which shift you want to schedule from the drop-down Shift menu.

Area: Enter the area number that you are assigning to the schedule. In order for this feature to be available, Area Schedules must be selected in System Area Information.

Opening: Enter the opening (disarm) time. Repeat for each day of the week to program.

Closing: Enter the closing (arm) time. Repeat for each day of the week to program. The opening time must be before the closing time.

Note: When programming area schedules, enter both an opening and a closing time for each day that you are programming. A message displays if the time entered is invalid. For example, if there is only an opening time, but no closing time, and vice versa.

If you want a schedule to run over multiple days-that is, you want the system to disarm on one day and remain disarmed until later that week-you may schedule this when you enter the closing time. In the closing field, enter the time and day of the week that you want to schedule the closing.

Example: In the Monday Opening field enter 8:00 AM. In the Monday Closing field enter 5:00 PM FRI. With this schedule, the system will disarm at 8:00 AM Monday morning and arm Friday at 5:00 PM.

7. Programming User Codes

To program User Codes for a group, the group must first be opened or created. The currently opened group displays next to Remote Link in the display above the menu bar. The Program >> User Codes window allows you to enter or make changes to the user code information in the group database file.

To add a new user, select New and enter information in each field. To accept the added information, select Apply at the bottom of the window.

- To delete a user and their associated user code information, select the user from the list on the left side of the window and select Delete at the bottom of the window.
- To sort user codes, select the desired method in the title bar: For example, if you wish to sort the user codes alphabetically, select Name in the title bar.
- User Number: Enter the number to assign to identify the user to the system. The User Number can only be as high as the number of users allowed on the panel.
- User Code: Enter the 3-digit to 6-digit passcode to assign to this user.

Note: User codes cannot begin with a 0. Three-digit codes cannot begin with 98.

- Random: Press the Random button to assign a random number to the user code being entered. The randomly assigned user code displays in the User Code field. The number of digits assigned to the random user code is based on the maximum number of digits allowed by the panel.
- User Name: Enter the user name to assign to the user. The user name can have up to 16 characters.
- Profile Number: Enter a number from 1 to 99 to designate the areas and functions that a user may access. Program profile numbers individually for each panel in the Program >> Profiles window.

Note: To create a new profile for a user, exit the open group and open the panel account where the profile is needed. Create the profile, save the changes, and return to the group.

- Description: To enter a note or description regarding the user code entry you are programming, type the information in the Description field or press the Description button to open the Edit Rich Text window. After you type your note, go to File >> Save and Exit to save your work and close the Edit Rich Text window. Your note appears in the field above the Description button.

8. Copying/Pasting User Code Information for Account Groups

To copy a user and user code information, open the panel or group from which you want to copy the user code information. Select Program >> User Codes.

Note: The copy function works with one user at a time.

Pasting User Information into the Current Panel or Group

1. In the User Codes window, select one User to be copied from the list on the left-hand side. Select Copy.
2. Select Paste and edit the name and user information as required.

Pasting User Information into a Different Panel or Group

Note: Profiles must be the same in both panels and both areas to accurately copy and paste user code information.

1. In the User Codes window, select one User to be copied from the list on the left-hand side. Select Copy.
2. Select File >> Close Panel to close that panel. Then select File >> Panel Information and open the panel or group to which you want to copy the user code information.
3. Select Program >> User Codes and select Paste. This pastes all of the user code information you copied from the first panel or group into the second panel or group.

9. Sending Program Information to a Group

Open the group from the File >> Account Groups window before sending any program information to a group. The currently opened group displays next to Remote Link in the display above the menu bar.

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.

Note: If changes were made to Holidays, Schedules, Output Schedules, or Profiles, the new information sent to the account group overwrites any existing panel programming. All panel programming not previously sent to the panel, or that has been changed in the file since the last update is also sent.

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.

In the example, the XR500N panel with account number 4321 failed to update. The XR500E panel with account number 3848 successfully updated.

To resend all accounts that failed to update, press Resend Failed. To send a single account, select that account and press Send Selected. After the resend process, the Status column in the Group Send Status window updates.

Part 1. Hardware Setup

1. Hardware Connection

In order to use Remote Link, you must have a connection that will let your computer communicate with the alarm panel. There are five basic types of connection available:

- Direct cable
- SCS-1 / SCS-105
- Modem Special: For when a slower baud rate that does not fluctuate is needed to ensure data integrity when connecting to a panel. Modem Special allows this type of control when using a computer modem to dial out.

Note: Only one modem can be used. Select the correct one for your operation.

- onboard Ethernet connector
- Cellular connection

More information

Refer to the installation guides that came with your product for information on hardware connections and configuration.

2. SCS-1 or SCS-1R Receiver

SCS-1 or SCS-1R Receiver - The SCS-1 or SCS-1R Receiver is a rack-mountable receiver that accepts up to five line cards.

Complete instructions for the SCS-1 or SCS-1R Receiver are packaged with the SCS-1 or SCS-1R Receiver. The SCS-1R Installation/User Guide (LT-1037) can be found in the document library at the DMP website.

3.1 SCS-1 / SCS-1R Configure

3.1. SCS-1 or 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-1, SCS-1R, or SCS-105 receiver, follow the instructions below.

Enter the SCS-1 System Configuration window by selecting System >> Configure >> SCS-1 System. You also configure SCS-105 Single Line Receivers in this window.

System Number: If your central station has more than one SCS-1, SCS-1R or SCS-105 receiver, enter the number of the appropriate receiver in the System Number field.

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 in the Receiver Key field.

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 see the "Invalid receiver number" error message, and the panel and the receiver will not be able to communicate.

Once you enter the Receiver Key, it is important that you write it down on the SCS-1 or SCS-1R System Configuration Record Sheet provided in the Remote Link User Guide appendix, and store it in a safe place.

3.2. SCS-1 Line Configuration

Select System >> Configure >> SCS-1 Line to display the SCS-1 Line Configuration window. You must configure each line card used in the SCS-1 or SCS-1R Receiver.

Line Number: Enter the number of the communication line assigned to the line card in the SCS-1 or SCS-1R Receiver that you are programming. Enter a single digit from 1 to 9.

Line Type: Select the type of communication line the receiver is connected to from the Line Type menu.

None: Select None to clear all programmed information for the line prior to programming.

Multiplex (MPX): Select this option when you are using multiplex communication through an SCS-1 Receiver using a polled communication line.

Digital Dialer (DD): Select Digital Dialer when you are using DMP's proprietary (SDLC) format for communication over standard telephone lines through an SCS-1, SCS-1R or SCS-105 receiver.

DDMX: Select DDMX if the line card in the SCS-1 Receiver is configured for digital dialer/multiplex accounts. You may have up to 128 DDMX accounts on one line card.

ASYNCH: Select ASYNCH if the line card is configured for asynchronous network communications.

Phone Number: Enter the phone number of the telephone line connected to the receiver.

Billing Number: Enter the billing number that the telephone company has assigned to the telephone line connected to this line card.

Comment: Enter any comments that might assist you in billing or system maintenance.

Checkboxes 0 to 127: Select the checkbox next to the number that corresponds to each multiplex account connected to this line card.

Repeat this process for each line card in use.

4. SCS-1 Receiver Firmware Requirements

The SCS-1 Receiver must contain firmware revision level 801 or higher. If your receiver firmware level is less than 801, contact DMP Customer Service for an SCS-1 Firmware Update kit.

If you are not sure which revision level your receiver is currently running, follow the steps below:

1. Open the front of the receiver by turning the four quick disconnect screws counterclockwise.

2. Remove the plexiglass cover and press the Processor Restart button on the far left side of the SCS-120 Power Supply board.

The receiver restarts and displays its firmware revision level on the CRT for about three seconds before returning to the Operator Sign On screen.

5. SCS-105 Receiver

The SCS-105 receiver is a single line receiver that is essentially an external modem that allows you to communicate with a single alarm panel over a standard telephone line.

Complete instructions are packaged with the SCS-105 Receiver. The SCS-105 Installation Guide (LT-0153) can be found in the document library at the DMP website.

6. SCS-105 Firmware Requirements

To be compatible with Remote Link, the SCS-105 Receiver must contain firmware revision level 204 or higher. If your SCS-105 firmware level is less than 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, follow the steps below:

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 revision number is on a label on top of the chip.

Part 1. Frequently Asked Questions

1. How do I dial DTMF?

Q. How do I make the SCS-105 receiver dial DTMF?

A. 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-1 or SCS-1R receiver will always pulse dial.

2. How do I set a schedule that runs through midnight?

Q. Can I set a schedule that disarms in the evening and arms in the morning?

A. 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. Is Remote Link compatible with my operating system?

Q. Is Remote Link compatible with Windows 3.1?

A. No. Remote Link is designed to work with Windows 95, 98, 2000, NT, XP, Vista, 7 and 8.

4. What do I do first?

Q. I just installed Remote Link. Now what do I do?

A. You first need to log in and configure the Remote Link program.

5. What do I need to do for maintenance?

Q. What do I need to do for normal maintenance on my Remote Link computer?

A. As with any computer running Windows and Windows applications, you should have a program of regular maintenance to keep the system optimized. The Microsoft® Windows™ User's Guide has a chapter titled Maintaining Windows with Setup that you should refer to for information. Set a regular schedule to backup your database files.

6. What happens to codes when I change partitions?

Q. What happens to my user codes when I change the account number on a panel or when I change the number of partitions in a 1912XR, XR200, XR200-485 or a XR2400F panel?

A. When you change the number of partitions in a panel, all of the user codes are deleted and the factory default code 99 is loaded for each partition. This is to prevent user codes from being assigned to the wrong partition. It is recommended that you print a copy of your user codes before changing partition numbers.

7. What is the Receiver Timeout Message?

Q. What is the Receiver Timeout Message? Why do I get an hourglass mouse cursor before I get this message?

A. The receiver and computer are not communicating correctly. Check the connections between your computer and receiver.

8. What is the correct account number?

Q. In some places I see my account number listed as 12345, while in other places it is listed as 1-12345. Which is it?

A. 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.

9. Where do I program Closing Code?

Q. Where do I enter Closing Code, Area Schedules, and other Area Information options?

A. From the Area Information window, select the Partition Info button on the lower left side of the screen. This is where you program items that affect the entire partition. In XTL Series, XT30/XT50 Series, and XT30INT/ XT50INT Series, Control Panels, Closing Code is in System Options Section of Programming. In XR100/XR500 Series, XR150/XR350/XR550 Series, and XR150INT/XR550INT Series, Closing Code is programmed in Area Information.

10. Why aren't all of the options available?

Q. I've logged on to Remote Link but several of the options are not available.

A. 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.

11. Why won't the panel stay online?

Q. A new panel will not stay on-line with Remote Link. The panel will seize the line then immediately hang up.

A. 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.

Part 1. Glossary

1. 4-2

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.

2. 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 ten-minute 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.

3. 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.

4. 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-1 or 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.

control or control panel - see alarm panel.

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. See also the DMP cross zoning application note LT-2000.

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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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-1 or SCS-1R Receiver to get a check-in report (s70) periodically to verify the communication link with the panel.

10. 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.

11. 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.

12. 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. The LX-Bus™ is available using an expansion interface card.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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. 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.

21. 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.

22. 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.

23. 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.

Part . 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.

Press	To
F1	Display Context-sensitive Help
Alt + F10	Display Diagnostics window
F11	Display Log On / Off window
Ctrl + Tab	Switch between Remote Link windows

1. Menu Keys

Use the following keys to select menus and choose commands.

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.

2. Editing Keys

Use the following keys to edit text in a dialog box or window.

Backspace

Delete the character to the left of the insertion point.

Del

Delete the character to the right of the insertion point.

3. Dialog Box Keys

Use the following when working in a dialog box.

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	Carry out a command.
Esc; or Ctrl + F4	Close a dialog box without completing the command.
F1	Open the topic of the Help File that directly relates to the active field or dialog box.

Index

- 4 -

- 7 -

- A -

- B -

- C -

- D -

- E -

- F -

- G -

- H -

- I -

- K -

- L -

- M -

- N -

- O -

- P -

- R -

- S -

- T -

- U -

- W -

- X -

- Z -

Designed, engineered, and
manufactured in Springfield, MO
using U.S. and global componenets.
LT-0565 19194

INTRUSION - FIRE - ACCESS - NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877
800.641.4282 | DMP.com