SYSTEM LINK

Click on the **Contents** tab for the Table of Contents.

Click on the **Index** tab for an alphabetical listing of help topics.

To search for an item, click on the **Contents** tab and then on the **Find** tab.

While working in System Link, you may press **F1** at any time for contextual help specific to the field that is currently active.

(This Help File is current for Version 1.70)

System Link™

© 2000 - 2014 Digital Monitoring Products, Inc.

System Link™ Software Product License Agreement

© 2000 - 2014 Digital Monitoring Products, Inc.

The terms of this Software Product License Agreement ("SPLA") for the Software Product(s) System Link™ and/or Remote Link™ are effective immediately upon you (either a single entity or individual) accepting a copy of the Software Product and the first use of it by you, your employees, or an authorized subcontractor. These Software Products are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. These Software Products are licensed, not sold.

Therefore, subject to the terms and conditions of this SPLA, your Provider Digital Monitoring Products, Inc., will provide you with a copy of Remote Link™ or, in the case of System Link™, your Provider either Digital Monitoring Products, Inc., or one of its authorized representatives will provide you with a copy System Link™ (which System Link™ and Remote Link™ singly or collectively according to context herein are referred to as the Software Product). You may not use the Software Product until you have read and accepted all of the terms of this SPLA by checking the "I accept" checkbox and clicking the "Finish" button. Digital Monitoring Products, Inc., (or "DMP") is the holder of the intellectual property holdings embodied in System Link™ and Remote Link™, including without limitation software modules such as Advanced Reporting, Alarm Monitoring, Command Center, Account Groups, or Link Server.

System Link™ and Remote Link™ include computer software and associated media, printed materials, and "online" or electronic documentation (referred to collectively or singly according to context as the Software Product). The System Link™ and Remote Link™ also include any updates, "plug-ins," modules and/or supplements to the original System Link™ or Remote Link™ provided to you by DMP or authorized representative.

By installing, copying, downloading, accessing or otherwise using System Link™ and/or Remote Link™, you agree to be bound by the terms of this SPLA. If you do not agree to the terms of this SPLA, do not install or use the Software Product. You may, however, return it for a full refund.

1. Permitted Uses and Restrictions on Use

A Remote Link™ licensee may install and use its DMP provided copy and install and use additional copies on any number of computers including a network server as well as laptops for the limited purposes of providing support service to end-users of Digital Monitoring Product, Inc.'s panel products and allied lines of alarm and security communications equipment; provided that all users are either employees of said Remote Link™ licensee or authorized subcontractors who are comparably restricted in usage of the Remote Link™ product, namely, that being for the limited purposes of providing support service to end-users of Digital Monitoring Product, Inc.'s panel products and allied lines of alarm and security communications equipment. A Remote Link™ licensee and/or every Remote Link™ user agrees not to copy, sell, resell, rent or sub-license (including offering Remote Link™-or any derivation or component thereof-to third parties on an applications service provider or time-sharing basis), lease, loan, redistribute, or create a derivative work of any portion of Remote Link™, or provide use of Remote Link™, or access to Remote Link™ in competition with sales or uses of System Link™ for and by end-users of Digital Monitoring Product, Inc.'s panel products and allied lines of alarm and security communications equipment.

A System Link™ licensee may install and use one copy of System Link™ on a single computer, including network server, for the purpose of providing communications management of Digital Monitoring

Product, Inc.'s panel products and allied lines of alarm and security communications equipment; provided that all such Digital Monitoring Product, Inc.'s panel products and allied lines of alarm and security communications equipment have duly registered accounts with Digital Monitoring Product, Inc., or authorized representative thereof. It being further provided that, all parties hereto contemplate that various devices including without limitation printers and the like are indeed communicators to a System Link™ machine but are not bound to be assigned an account. A System Link™ licensee agrees not to copy, sell, resell, rent or sub-license (including offering System Link™-or any derivation or component thereof-to third parties on an applications service provider or time-sharing basis), lease, loan, redistribute, or create a derivative work of any portion of System Link™, or provide use of System Link™, or access to System Link™ in competition with other sales or uses of System Link™ for and by other end-use parties of Digital Monitoring Product, Inc.'s panel products and allied lines of alarm and security communications equipment.

2. Your Registration Obligations

In consideration of your use of the Software Product, you agree to: (a) provide true, accurate, current and complete information about yourself as prompted your Provider's registration form(s) (such information being the "Registration Data") and (b) maintain and promptly update the Registration Data to keep it true, accurate, current and complete. If you provide any information that is untrue, inaccurate, not current or incomplete, or the Provider has reasonable grounds to suspect that such information is untrue, inaccurate, not current or incomplete, the Provider may suspend or terminate your license and you must discontinue any and all current or future use of the Software Product (or any portion thereof).

3. Fees

You agree to pay the then-current license fee associated with obtaining a copy of the Software Product. Your Provider reserves the right to modify its fee schedule with or without notice. For instance, each of one copy of either the native Remote Link™ product or the native System Link™ product will be provided pursuant to a one-time license fee set by the applicable provider thereof. "Plug-in" modules for either will be provided pursuant to a license fees computed on a basis such as the following:

Plug-in module licensee will pay a license fee according to (the reporting requirements therefor stated above) the total number of account numbers that are reporting into that licensee's System Link™ or Remote Link™ copy wherein the license fee schedule for such a "Plug-in" module will vary according to whether between 1-10 accounts are reporting, 11-50 accounts are reporting, 51-100 accounts are reporting, 101-500 accounts are reporting, 501-1000 accounts are reporting, 1001-2500 accounts are reporting, 2501-5000 accounts are reporting, or in excess of 5000 accounts are reporting.

4. Description of Other Rights and Limitations

Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the Software Product, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.

Separation of Components. The Software Product is licensed as a single product. Its component parts may not be separated for use on more than one computer.

Trademarks. This SPLA does not grant you any rights in connection with any trademarks or service marks of your Provider or DMP.

Termination. Without prejudice to any other rights, your Provider may terminate this SPLA if you fail to comply with the terms and conditions of this SPLA. In such event, you must destroy all copies of the Software Product and all of its component parts.

Back-up Copy. A System Link™ licensee, after installation of one copy of the System Link™ product pursuant to this SPLA, may keep the original media on which the System Link™ was provided by Provider solely for backup or archival purposes, or make one other backup or archival copy only solely for backup or archival purposes. Except as expressly provided in this SPLA, no licensee may otherwise make copies of the Software Product or the printed materials accompanying the Software Product.

5. Limited Warranty

DMP warrants that the Software Product will perform substantially in accordance with the accompanying written materials for a period of Three (3) Years from the date of receipt.

If an implied warranty or condition is created by your state/jurisdiction and federal or state/provincial law prohibits disclaimer of it, you also have an implied warranty or condition, BUT ONLY AS TO DEFECTS DISCOVERED DURING THE PERIOD OF THIS LIMITED WARRANTY (THREE (3) YEARS). AS TO ANY DEFECTS DISCOVERED AFTER THE THREE (3) YEAR PERIOD, THERE IS NO WARRANTY OR CONDITION OF ANY KIND. Some states/jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you. Any supplements, updates, plug-ins, or enhancement modules to the Software Product, including without limitation, any (if any) service pack or Software Update fixes provided to you after the expiration of the Three (3) Year Limited Warranty period are not covered by any warranty or condition, express or implied.

6. Limitation on Remedies; No Consequential or Other Damages

Your exclusive remedy for any breach of this Limited Warranty is as set forth below. Except for any refund elected by DMP, YOU ARE NOT ENTITLED TO ANY DAMAGES, INCLUDING BUT NOT LIMITED TO CONSEQUENTIAL DAMAGES, if the Software Product does not meet DMP's Limited Warranty, and, to the maximum extent allowed by applicable law, even if any remedy fails of its essential purpose. The terms "Exclusion of Incidental, Consequential and Certain Other Damages" below are also incorporated into this Limited Warranty. Some states/jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. This Limited Warranty gives you specific legal rights. You may have others which vary from state/jurisdiction to state/jurisdiction.

7. Your Exclusive Remedy

DMP's and its authorized representative's' entire liability and your exclusive remedy shall be, at DMP's option from time to time, (a) return of the price paid (if any) for, or (b) repair or replacement of, the Software Product that does not meet this Limited Warranty and that is returned to DMP with proof of license fee(s) paid.. You will receive the remedy elected by DMP without charge, except that you are responsible for any expenses you may incur (e.g. cost of shipping the Software Product to DMP). This Limited Warranty is void if failure of the Software Product has resulted from accident, abuse, misapplication, abnormal use or a virus. Any replacement Software Product will be warranted for the remainder of the original warranty period or One (1) Year, whichever is longer. Outside the United States or Canada, neither these remedies nor any product support services offered by DMP are available without proof of license fee(s) paid from an authorized international source.

8. Disclaimer of Warranties

The limited warranty that appears above is the only express warranty made to you and is provided in lieu of any other express warranties (if any) created by any documentation or packaging. Except for the limited warranty and to the maximum extent permitted by applicable law, DMP and its authorized representatives provide the Software Product and Support Services (if any) AS IS AND WITH ALL FAULTS, and hereby disclaim all other warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability, of

fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of workmanlike effort, all with regard to the Software Product, and the provision of or failure to provide Support Services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE PRODUCT.

9. Exclusion of Incidental, Consequential and Certain Other Damages

To the maximum extent permitted by applicable law, in no event shall DMP or its authorized representatives be liable for any special, incidental, indirect, or consequential damages whatsoever (including, but not limited to, damages for loss of profits or confidential or other information, for business interruption, for personal injury, for loss of privacy, for failure to meet any duty including of good faith or of reasonable care, for negligence, and for any other pecuniary or other loss whatsoever) arising out of or in any way related to the use of or inability to use the Software Product, the provision of or failure to provide Support Services, or otherwise under or in connection with any provision of this SPLA, even in the event of the fault, tort (including negligence), strict liability, breach of contract or breach of warranty of DMP or any authorized representative, and even if DMP or its authorized representative has been advised of the possibility of such damages.

10. Limitation of Liability and Remedies

Notwithstanding any damages that you might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of DMP or any of its authorized representatives under any provision of this SPLA and your exclusive remedy for all of the foregoing (except for any remedy of repair or replacement elected by DMP with respect to any breach of the Limited Warranty) shall be limited to the greater of the amount actually paid by you for the Software Product or U.S.$5.00. The foregoing limitations, exclusions and disclaimers described above shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

11. Survival

All representations, warranties, Sections, 5, 6, 7, 8, 9, 10 and 11 in this SPLA shall survive the termination of this SPLA.

12. General

You agree that this is the complete and exclusive statement of the Agreement among you and DMP and your Provider (if other than DMP), which supersedes all proposals, oral or written, and all other communications relating to the subject matter of this Agreement.

If any of the provisions, or portion thereof, of this Agreement are invalid under any applicable statute or rule of law, they are to that extent to be deemed omitted. This Agreement shall be governed by the laws of the State of Missouri.

Before using System Link, you should read and be familiar with the following documents:

Command Processor Programming and User Guides: There is a Programming, Installation, and User's Guide for each DMP Command Processor panel that fully details the various programming options and panel operation. There are also programming and installation guides for the hardware components that you may use to connect to alarm panels and to take full advantage of optional features.

You may 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, call DMP Customer Service at 1-800-641-4282 or contact your regional DMP Sales Representative.

You may also visit our document library at the DMP Web site at http://buy.dmp.com.

Before installing System Link, make sure that your computer hardware meets these minimum specifications listed in the table below.

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

Note: You need to have Administrator Authority or select 'Run as Administrator' to install System Link software.

You also need the following items:

- 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.

Note: If using System Link on Windows 7 or Windows Vista under Standard Operator authority, see **Installing Link on Windows Vista or Windows 7.**

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.

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 there 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 in to 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. For the purposes of this document, it will be assumed there are only two types of Link operators: administrators and standard operators. A Link administrator has Administrator special permissions, a standard operator does not. See the Operator Configuration section of the Link help for more information on operator priviledges.

Roles

There are three roles discussed in this section. Note that 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 document 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, System Link or 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. See Registering and Activating Modules section of Link Help.

Registry Keys

Once System 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\
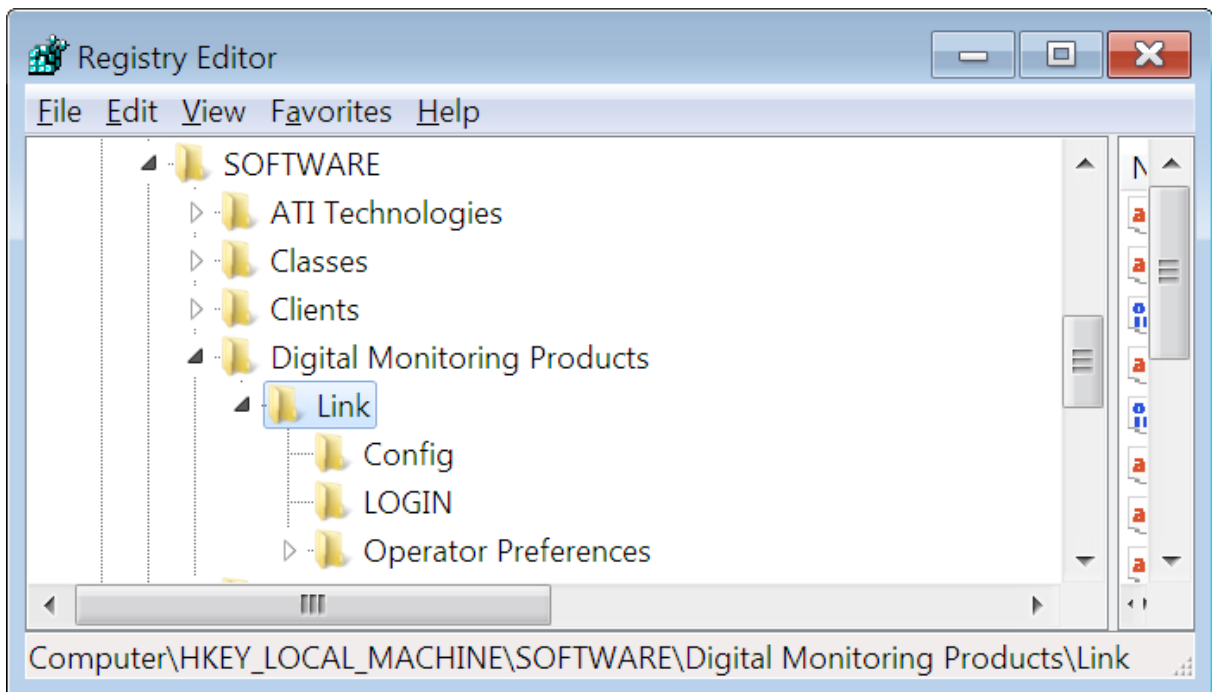
Registry Editor showing Link Registry Key

Database

This section discusses Database setup for Remote Link and System 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 subfolders) and the Link installation folder (and subfolders). This should be done irrespective of the database location.

Link Server

This section discusses information specific to Link Server. Link Server allows multiple System 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 System Link must be able to establish a TCP/IP connection to the DBISAM Database Server address and port.
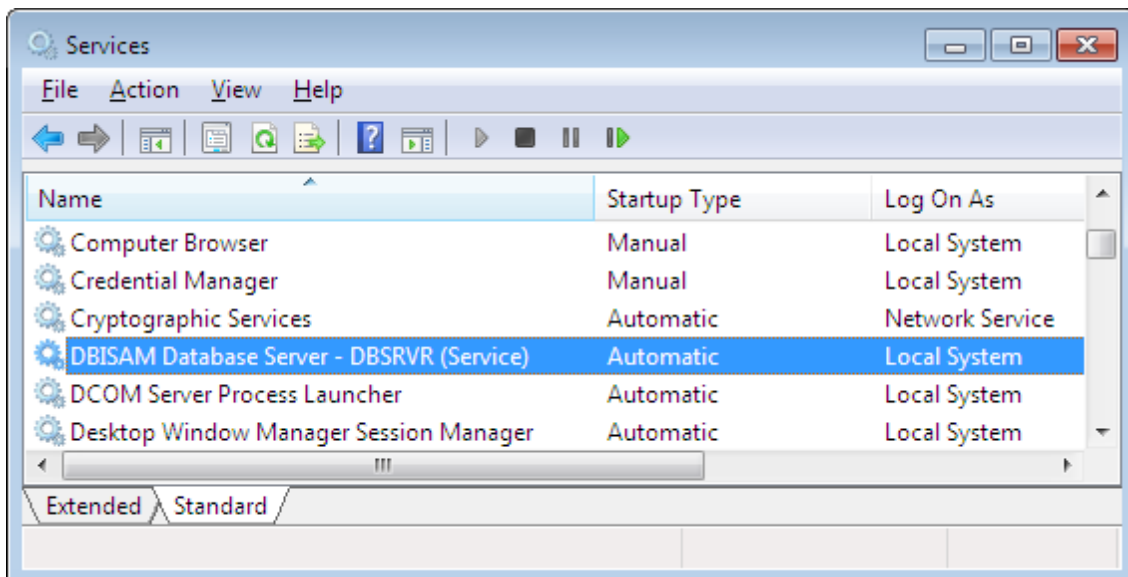
Link Server Database Service

System Link offers an updated interface that is simple to navigate, and provides easy access to the information you are most likely to need.

The **Window** menu allows you to switch between the windows you have open in System Link, or to organize the way you view them. You may also switch between windows within System Link by holding down the Ctrl and Tab buttons at the same time.

File > Close Panel will close the account file and all windows you currently have open.

File > Exit will close all windows you have open, disconnect you from a panel if you are connected, and exit from System Link.

Clicking **Apply** applies all changes you have made in that window.

Clicking **OK** saves any changes you have made in that window and closes the window.

Your System Link database contains your subscriber account information, your password information, and other valuable data. It is important to protect this information by performing regular backups of the database.

<p align="center">**Please backup your System Link database!**</p>

You can find the location of the System Link database by selecting **System > Configure > System Link** to open the System Link Configuration window. Click on 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 System Link database in a different location than the default folder, enter the location that you prefer for your System 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. See instructions about creating a new database location.

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 click **OK**, System Linkcreates 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 System Link database.

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

System > Log ON / OFF

Before using System Link, you must log in to the program with a user name and password. When you open System Link, the **Log On** window automatically displays. You may log off and then log in as another user any time the program is open.

The default log in is **new** for both your user name and password. Be sure the Caps Lock is not set.

> **Note:** Keep track of your passwords and remember to always keep them in a safe location.

To configure System Link to directly connect to a panel, follow the steps below:

Select the desired panel in **File > Panel Information**.

In the **Connection Information** group box, select **Direct** from the drop-down menu in the **Type** field.

Select the COM Port to which the panel is connected.

Select the Baud Rate of the COM Port.

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

After you have entered all the Connection Information, open the panel by clicking **OK**. Then go to **Panel > Connect** and click the **Connect** button. You are now connected to the panel.

To configure System Link to connect to a panel through an SCS-1, SCS-1R or SCS-105 Receiver using a dial-up connection, follow the steps below:

Select the desired panel in **File > Panel Information.**

In the **Connection Information** group box, select **SCS-1 / SCS-105** from the drop-down menu in the **Type** field.

Enter the Remote Key.

Enter the phone number of the panel.

Select **Yes** from the drop-down menu in the **Dial** field.

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

After you have entered all the Connection Information, open the panel by clicking **OK**. Then go to **Panel > Connect** and click the **Connect** button. You are now connected to the panel.

Using an XTL or XR150/XR350/XR550 panel

To configure System Link to connect to a panel through cellular communication, follow these steps:

1. Select the desired panel in **File > Panel Information**.

2. In the **Connection Information** box, select **Cellular** from the drop-down menu in the **Type** field.

3. In the Phone Number box, enter the phone number or SIM # for the cellular communication. Select OK to apply these changes.

  a. To retrieve the phone number or SIM/MEID #:

    i. For SecureCom Wireless users, select System > SecureCom Wireless Activations. This shows a list of all SecureCom activations. Right-click on the SIM/MEID # or phone number of the panel to copy the number and then paste into the phone number box of the connection information window.

    ii. For non SecureCom SIM cards, the SIM # is listed on the front of the SIM card. Enter this number into the phone number box.

(Alarm Monitoring, Command Center, or Advanced Reporting Module) Help > Registration

When you receive the module, you will also receive a manual and a certificate containing the serial number that is needed for proper activation of the program. Once the program is installed on your computer, enter the serial number in the **Help > Registration** window. Click the **Add** button and type the module's serial number as listed on the certificate.

> **Note:** You must right click on the System Link Icon and Run As Administrator before installing any modules.
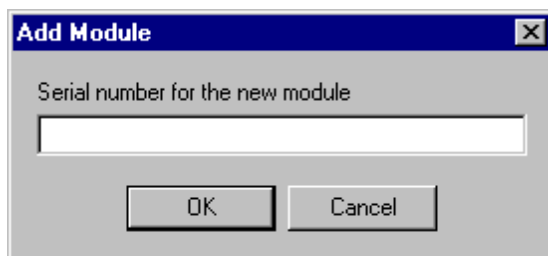
1. Go to **Help > Registration.**
2. Click **Add.**
3. In the field shown on the left, type the module's serial number as it appears on the certificate.
4. Click **OK**
5. A message box will appear reminding you to activate the module within 7 days.

> **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 wish to continue registering and activating the module, follow the steps described in **How to Activate the Module.**

Help > Registration

If you have purchased additional Modules to add-on to System 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. Refer to Entering the Module's Serial Number and Activating the Module for more information.

(Alarm Monitoring, Command Center, Advanced Reporting Module, Account Groups and SecureCom Wireless)

Help > Registration

Within the 7-day grace period, call DMP's Customer Service at to activate the module. You can reach DMP's Customer Service at (800) 641-4282 from 7 AM to 7 PM central standard time.

If activating the SecureCom Wireless service module, call Customer Service at 1-877-300-8030 for activation.

When you are ready to activate the module open **Help > Registration**. If you do not see the module listed, then the serial number has not been entered and the module has not been registered. To register the module, click the **Add** button, enter the serial number listed on the certificate and click **OK**.
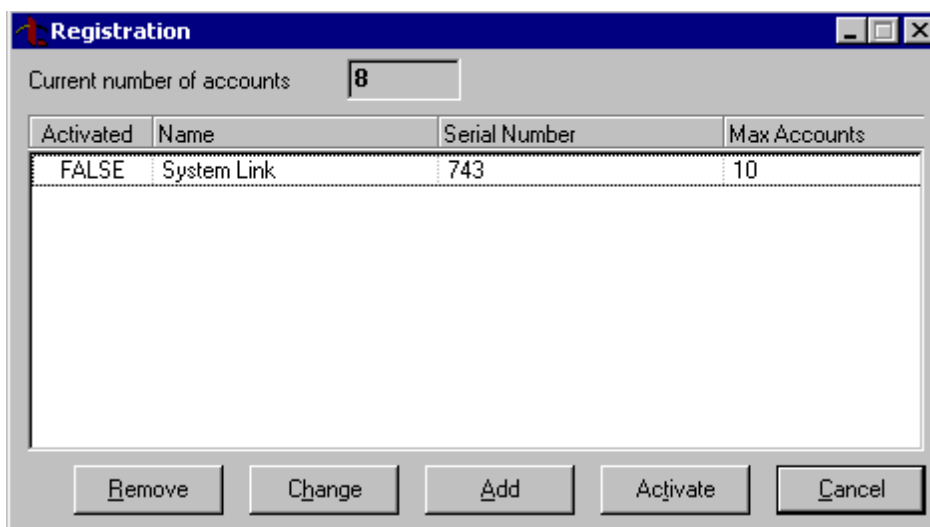
Select the module you wish to activate from the list of modules. Click the **Activate** button. System Link will automatically generate a Public Key for the module. The serial number and Public Key will be listed in a message box.

Call DMP Customer Service at (800) 641-4282 and have the serial number and the Public Key available. Customer Service will generate an Activation Code. Click **OK** in the message box to enter the Activation Code from DMP Customer Service. Click **Activate**. Now your Module is registered, activated, and ready to use.

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

(Alarm Monitoring, Command Center, or Advanced Reporting Module) Help > Registration

To upgrade the Account Level (the maximum number of allowable subscriber accounts), open **Help > Registration** after you receive the new CD-ROM and Certificate.
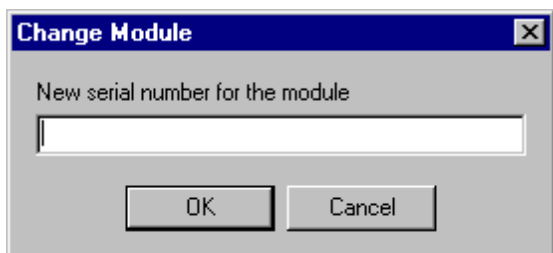
Select the module that you are upgrading and click **Change**. Enter the new Serial Number from the upgrade Certificate. Follow the instructions to activate the module with the new level of accounts.

(Alarm Monitoring, Command Center, or Advanced Reporting Module)
Help > Registration

If you decide to remove a module from your System Link program, follow the directions below.

Note: You need to have Administrator Authority to remove any modules from the program.

1. Click **Help > Registration** to open the Registration window.

2. Select the module that you wish to remove from the list in the Registration window. Click the Remove button.

3. A pop-up window will appear asking if you are sure you want to remove the module. Click Yes if you would like to remove the module.

4. You will then see a window that says, "Module Successfully Removed." Click **OK**.

5. Restart the program for the changes to take effect.
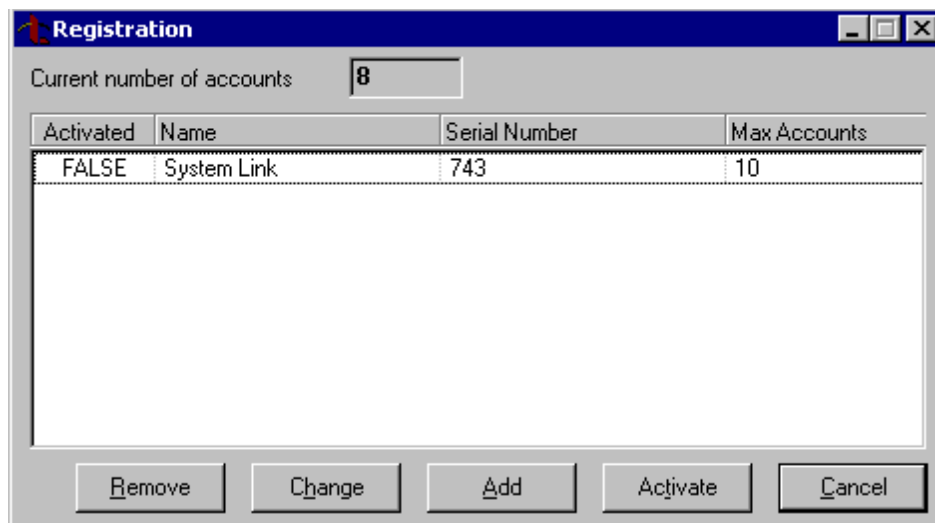
The SecureCom Wireless Activations window is used for managing control panel cellular service using SecureCom Wireless, LLC. To establish cellular service with SecureCom Wireless, go to www.securecomwireless.com and download the Network Service Agreement. This contract only needs to be completed once per company.

Once SecureCom Wireless service has been established, you will be e-mailed a Certificate of Authentication that bears a Serial Number which is needed to register and activate a SecureCom Wireless service module in System Link.
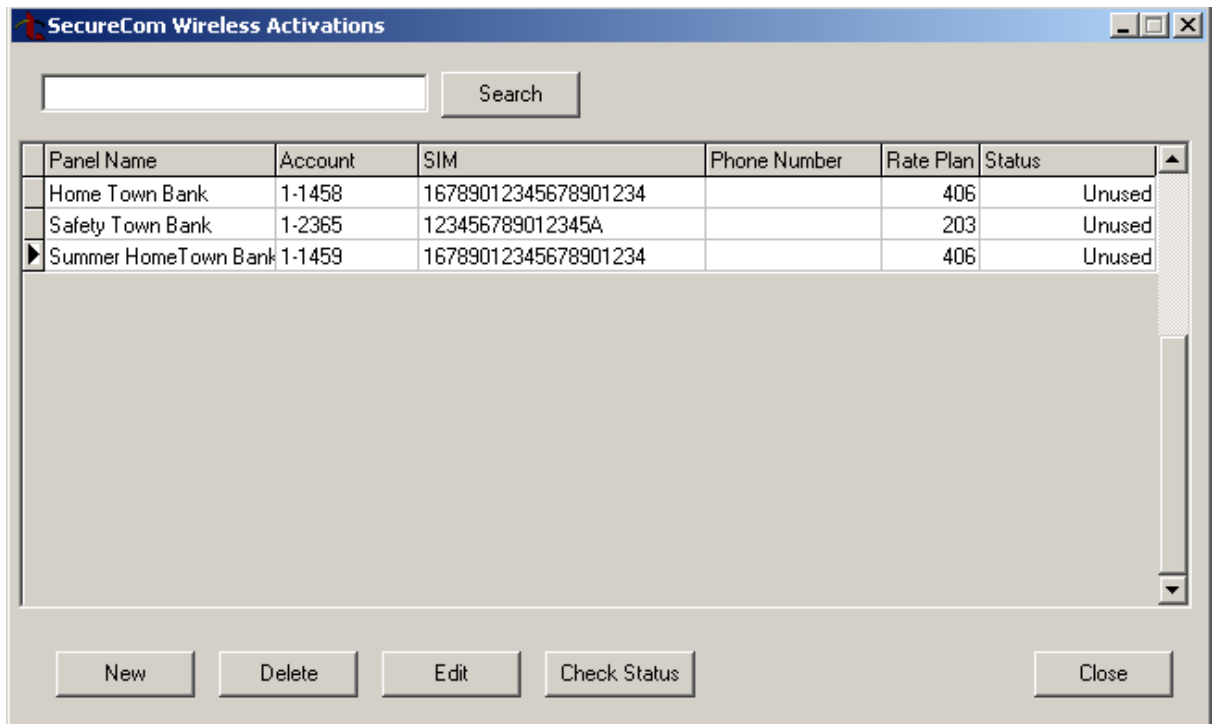
The serial number and activation is required for each installation of System Link. Contact SecureCom Wireless at 1-877-300-8050 for activation of additional installations of System Link.

Enter the Serial Number in **Help>Registration**. Refer to Activating the Module for additional information.

Access to the SecureCom Wireless Activations window is enabled through System>Operator Configuration. The Cellular Activations option must be enabled for an operator to manage SecureCom Wireless SIM cards.

Programming

The SecureCom Wireless Activations window can be accessed by selecting **System>SecureCom Wireless Activations**. In the SecureCom Wireless Activations window, select the SIM card to change and select the Edit button to open the Activate SIM window or select New to open up the Activate SIM window to add a SIM card.

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

The Activate SIM/MEID window can also be accessed by selecting Program>Communication. Select the path programmed for Cell communication and click on the Activate Button.

When the Activate SIM/MEID screen appears, enter all of the information before clicking on Activate.The following list explains the fields that appear on this screen:

Note: Complete all panel programming before activating the cellular path to ensure the correct rate plan is calculated for usage.

SIM Type: Select the type of SIM card you are activating. Select either 200, 400, or MEID.

SIM/MEID Card#: Enter the SIM (Subscriber Identity Module) or MEID (Mobile Equipment Identifier) number from the SecureCom AT&T Wireless SIM card, SecureCom T-Mobile Wireless SIM card, or the 263C/463C CDMA Cellular Communicator. The MEID number can be found on the label of the 263C or 463C.

Rate Plan: For XR100, XR500 Series, XR150/XR350/XR550, XT Series, and XTL panels, 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.

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

Using Model 380-400 or 380-400T SIM Card	SIM Card	Data Included
Plan 406: Back-up or primary path with a daily test	Level 400	50kb
Plan 408: Primary path with hourly check-in and O/C reports for up to 4 areas.	Level 400	200kb

Plan 410: Primary path with an hourly test and O/C reports for up to 8 areas.	Level 400	300kb
Plan 416: Primary path with a 6 minute check-in and O/C reports for up to 8 areas.	Level 400	1000kb
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	2000kb
Plan 435: Dual primary paths provide for 6 minute check-in and O/C reports for up to 8 areas.	Level 400	3000kb
Plan 445: Dual primary paths provide for 3 minute check-in OR 4 minute check-in with O/C reports for up to 16 areas.	Level 400	4000kb
XT: Daily test with a flat rate.	Level 400	N/A
XTL: Daily test with a flat rate.	Level 400	N/A

Status: This displays the current status of the SIM card. To update the status of the current SIM card, click on Update Status.

Unused: The SIM card 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 card.

Pend DeAct: A request to deactivate this SIM card has been sent and is pending.

Deactivated: This SIM card has been deactivated.

Invalid: The SIM card number entered is not a valid number. Reenter the number from the SIM card and retry the activation process.

Text Plan: Select the rate text plan for the SIM card. Plans available include:

Text Plans Available:	SIM Card	Available Panels:
None: Messaging is not included	Level 400	XR150/XR350/XR550, XR100, XR500,XT30, XT50, XTL
SMS100: 100 Messages per month	Level 400	XR150/XR350/XR550, XR100, XR500, XT30, XT50, XTL
SMS200: 200 Messages per month	Level 400	XR150/XR350/XR550, XR100, XR500, XT30, XT50, XTL
MyAccess: Unlimited messages	Level 400	XR150/XR350/XR550, XR100, XR500, XT30, XT50, XTL

Activating a SIM card

From the Activate SIM window, enter the SIM card number, select the SIM type as 200 or 400, and select a rate plan and text plan, if desired, for this SIM card. Click the **Activate** button to request activation.

The activation process could take up to 24 hours to complete.

Note: If using a SecureCom AT&T SIM card, the APN must be changed to SECURECOM400. If

using a SecureCom T-Mobile SIM card, the APN must be changed to GRID.T-MOBILE.COM.

Deactivating a SIM card

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

System > Configure > System Link > Receiver Tab

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

Current Receiver

Receiver General Options

Receiver Lengths

Default Receiver

System > Configure > System Link > Receiver Tab
Current Receiver

Model: Select the receiver from the drop-down menu to configure.

System > Configure > System Link > Receiver Tab

Communications 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 System 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
>
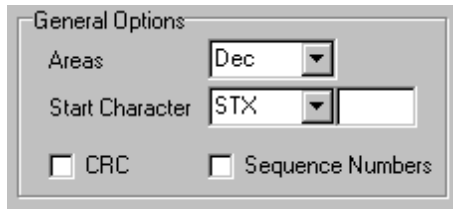> **SCS-1R/150 (using SCS-150):** Select 1-8
>
> **SCS-105:** Set this value to 1.

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.

System > Configure > System Link > Receiver Tab
General Options

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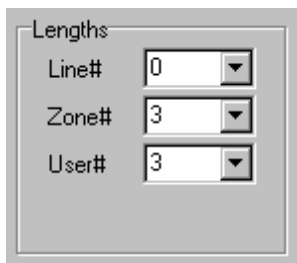
Other: If the SCS-1 or SCS-1R Receiver is set to a different Start Character than the available options, select Other and enter that Start Character in the field immediately to the right of the Start Character menu.

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.

System > Configure > System Link > Receiver Tab
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.

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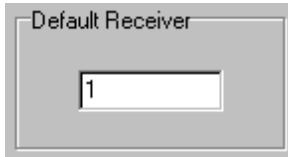
- **SCS-1 or SCS-1R Receivers:** This number must match the zone number programmed in the Host setup programming on the receiver.
- **CS-105 Receivers:** Use 3 for SCS-105 Single Line Receivers.

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.

(Must have an additional module to Use)
System > Configure > System Link > Receiver Tab

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.

If you do not enter a number in this field, the receiver number for host monitored accounts will default to 1 (one).

System > Configure > System Link > Modem Tab

Use the Modem tab to configure System Link when connecting to a DMP 462FM 9600 Baud Modem installed on a panel or when connecting to an XR500 Series or XR2500F for programming the panel at 2400 baud through the panel dialer. This allows you to connect to the panel using a standard computer modem.

System > Configure > System Link > Modem Tab

Communication Options

COM Port: Select the COM port that is connected to your modem. Use the Modem tab to configure System Link to connect to a panel that has a DMP Fast Modem installed or when connecting to an XR500 or XR150/XR350/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.
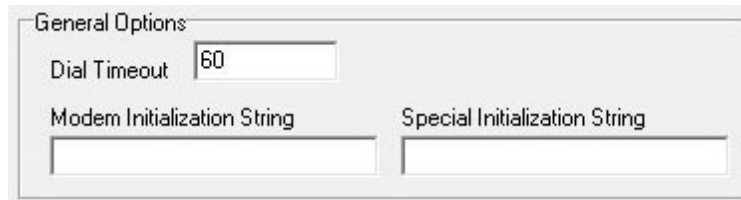
Note: These are for the local computer modem.

Baud Rate: Set the baud rate for System 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 XON/XOFF, 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.

System > Configure > System Link > Modem Tab
### General Options

Dial Time Out: Enter the length of time System Link will wait for the XR500 or XR150/XR350/XR550 Series panel or 462FM to pick up. Enter a range from 1 to 255 seconds. The default is 60 seconds. You may need to extend the Dial Time Out depending on the 462FM's programmed **Ring Count**. Extend the Dial Time Out about 10 seconds for each ring programmed in the **Ring Count**.

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.

## System > Configure > System Link > Database Tab
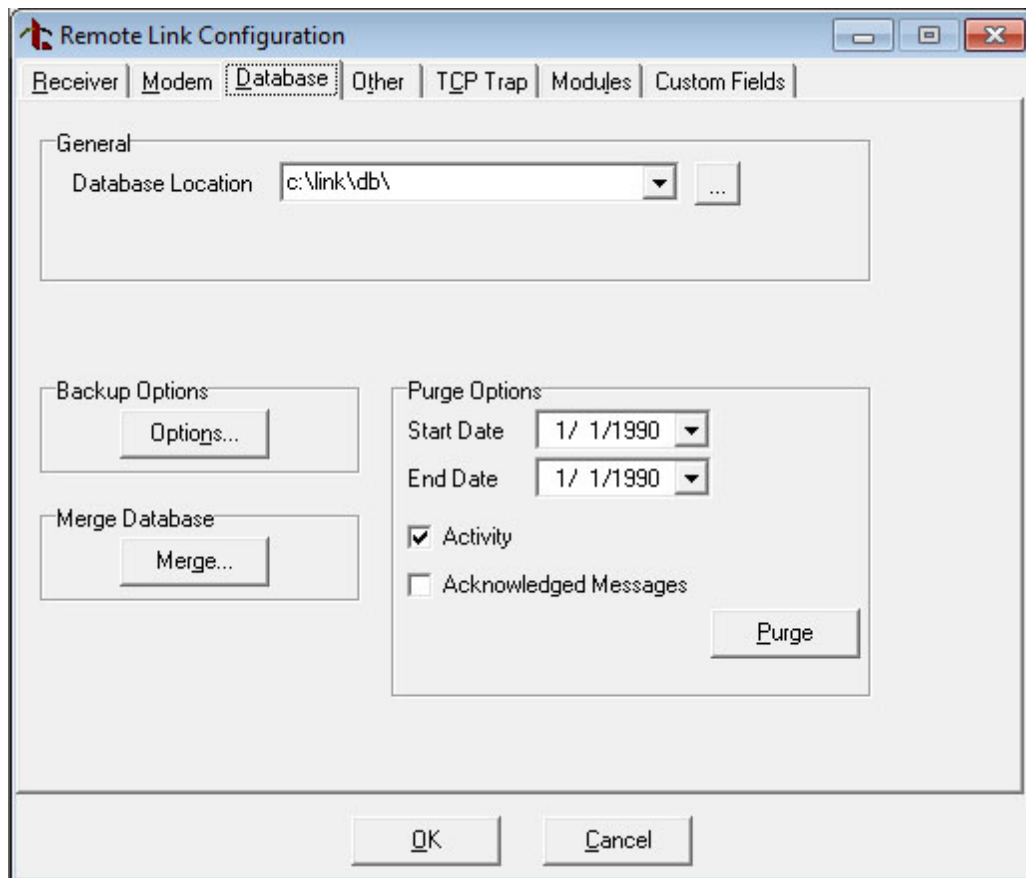
The settings in the **Database** tab allow you to change the location where System Link stores data on your computer's hard drive. It also allows you to backup and purge your System Link database, as well as merge another System Link database into the existing or import your Remote Access database into System Link.

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

You may move your System Link database to a folder on your computer hard drive, or to any connected network drive.

System > Configure > System Link > Database Tab

General Options
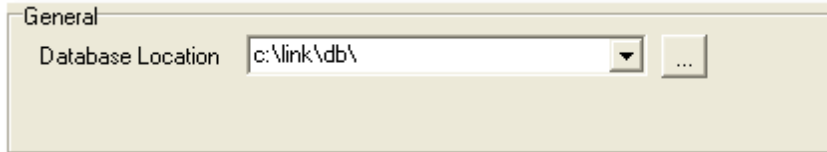
Database Location

Computer Hard Drive: Enter the path to the System Link database location on the computer or network hard drive. If you would like to store your System Link database in a different location than the default folder, type the location in the **Database Location** field. You may also browse for the folder where you would like to place your System Link database by clicking on the button just to the right of the Database Location field with three small dots.

The database may also be stored on a remote network server. This option allows more than three System Link computers to perform extensive database operations at the same time. Refer to the Link Server Installation Sheet (LT-0837).

Network Server: To use System Link with KLink Server, enter the network server IP address and port number to the System 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 System 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 System Link database, use Windows Explorer and copy the complete database folder (usually "C:\Link\Db") and paste to the desired location. Go to the Database Location field and either type the new location of the database into the field or click the browse button to locate where you have relocated the database.

If you change the location listed in the **Database Location** field without first moving the database manually, System Link displays a message asking, "Do you wish to create a new database?" If you click on **OK**, System Link creates a new database at the location that you just assigned and ignores the previous database. This means that System 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, System Link does not save the attempted relocation.

If System 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

System > Configure > System Link > Database Tab > Backup Options

As a safety measure, it is always wise to create a backup of your database. System 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.

Click on the **Options** button to open the **Backup Options** window.
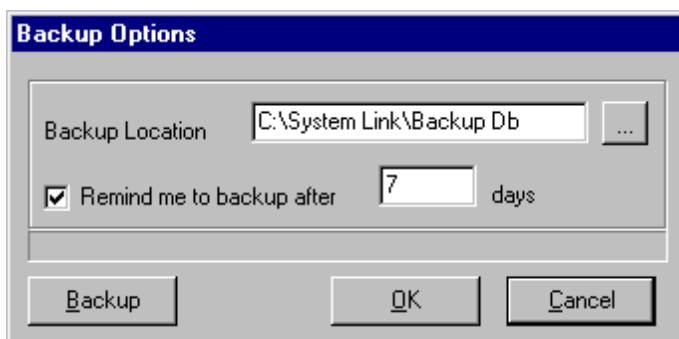
> **Note:** When using Link with SQL Server, all backup and repair operations must be performed by the database administrator, using SQL Server management tools. Remote Link does not perform these operations.

Backup Location: Enter the location where you want the Backup Database to reside. For example, C:\Backup tells System Link to place the Backup database in the Backup folder on the C drive of your computer.

You may also browse for the folder where you would like to place your System Link Backup Database. To browse for the location where you wish to place the database, click on the button with three small dots just to the right of the **Database Location** field.

When 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 System Link remind you when it is time to backup your database. Click the **"Remind me to backup after"** checkbox. Then enter the number of days you would like between backup reminders.

Click **OK** when finished entering in all of the fields. You may also click **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 when it is time to backup the database. If you select **Yes** the pop-up window closes and opens the **Backup Options** dialog box. Click the Backup button to perform the scheduled **Backup.**

If you select **No**, another pop-up window will appear the next time you log on to System Link.

> **Note:** Only the System Administrator can backup the System 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.

System > Configure > System Link > Database Tab > Merge

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

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

Go to **System > Configure > System Link** to open the **System Link Configuration** window. Click on the Database tab and then click the Merge button to open the Merge Database window.

In the **Merge Database** window, enter the path to another System Link database to merge with the existing database. You may also browse to the location of another System Link database by clicking on the button just to the right with three small dots. All of the accounts from the chosen database are copied and merged into the existing database.
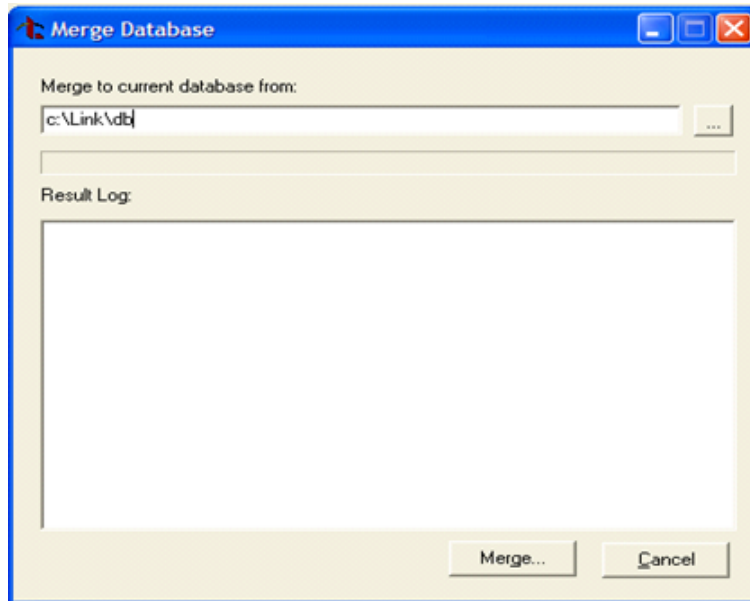
Note: Only a database located on a local or network drive can be merged. A database located on a remote server cannot be merged.
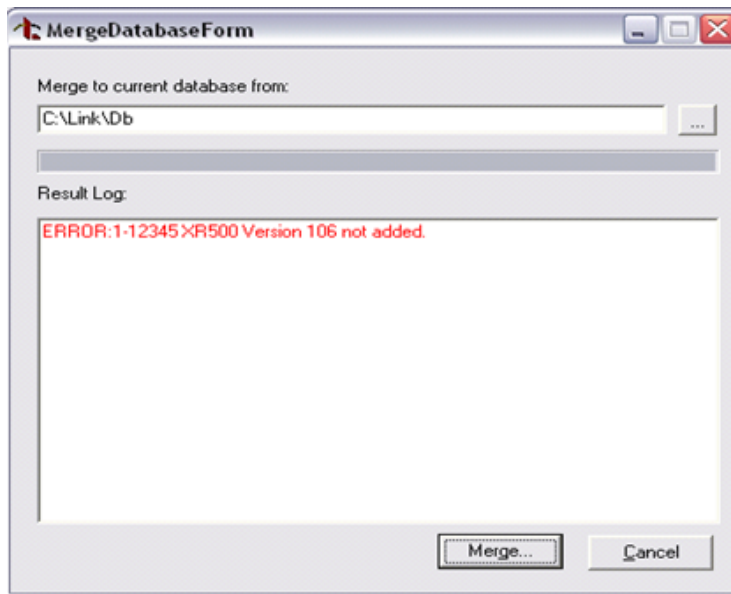

Note: If an account being merged has the same receiver and account number as one in the existing System Link database, an error message displays and the account is not merged.

After following the instructions above, click **Merge** to complete the merge operation.

System > Configure > System Link > Database Tab > Purge Options

Purge allows you to remove System Link activity from the database. Select the start and end dates, then select **Activity** or **Events**.

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.
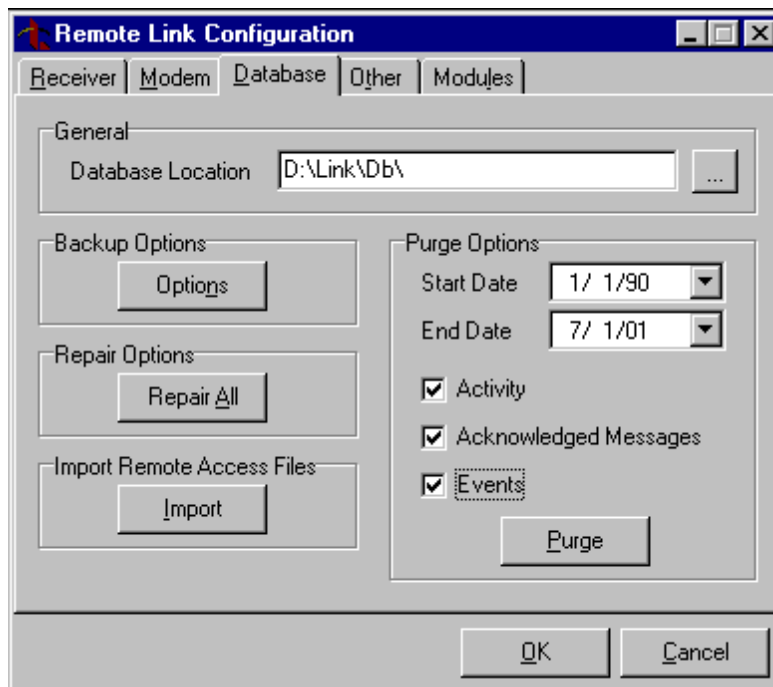
Start Date: Enter the first date that you would like to purge events. You may type the numbers, use the arrow keys, or use the drop-down calendar.

End Date: Enter the last date that you would like to purge events. You may type the numbers, use the arrow keys, or use the drop-down calendar.

Activity: Select Activity to remove the System 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, System 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.

Click the Purge button to remove all activity and/or events from the System Link database for the selected dates.

The **Restore from Backup** window automatically appears if your database is corrupt and you need to restore it.

> **Note:** To restore from a backup, you must have a backup file already made. Be sure to backup your System Link database frequently.

> **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.

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.

> **Note:** The Restore Location will typically be where your System Link database currently resides.

Press the Restore button to restore your database from the selected backup file.

> **Note:** If the Restore from Backup window does not automatically open, close System Link and follow the directions below.
>
> > • Go to Start > Programs > System Link.
> > • Click on Restore Database.

It is possible your System Link account database may be damaged if your computer experiences a power outage or a hardware or software problem that causes System Link to stop unexpectedly. The **Repair** feature attempts to repair corrupted account information, activity, panel programming, and

configuration files in your System Link database. If you believe your System Link database is damaged or corrupt, close System Link and follow the directions below.

- Go to Start > Programs > System Link.
- Click on 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.

System > Configure > System Link > Other Tab

Time Zone: Under the **Other** tab, select the appropriate time zone where your System 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 System Link to be saved in the debug table for diagnostic purposes. Uncheck the box to disable this function. When the box is unchecked, 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 System Link to display panel alarms and system event messages in the Alarm List. Uncheck this option when System

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 System 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.

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 System Link to stop responding such as an Access Violation or database corruption.
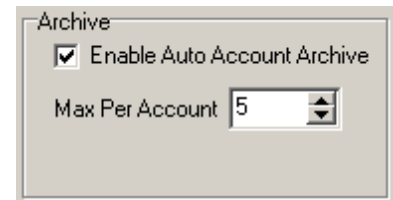
Archive
Pass Through Options
Admin Reader

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 unchecked.
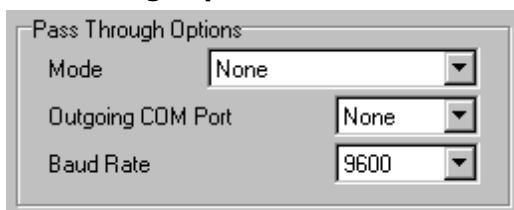
To archive panel account programming manually, select **File>Panel Information.**

Max Per Account: Select the maximum number of panel programming archive verisons allowed to be stored per account. Allowed range is 1 to 20 archives. Default is 5.

System > Configure > System Link > Other Tab

Pass Through Options

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

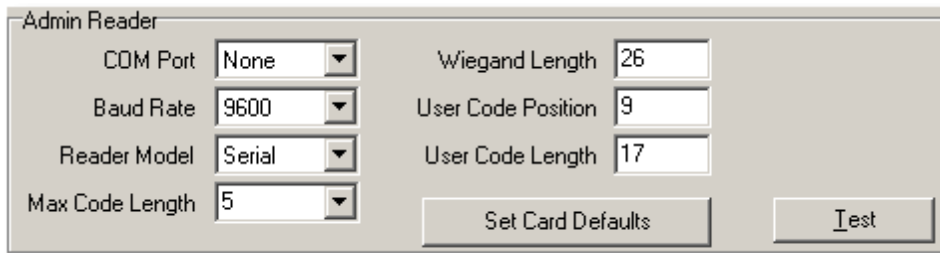> **None:** Select this option if you are not using Pass Through mode to relay signals to automation software.

Outgoing COM Port: Select the COM port that System 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.

System > Configure > System Link > Other Tab
Admin Reader

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

Note: The Admin 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/html/downloads.html

COM Port: Select the virtual COM Port to which the Admin Reader is connected.

Baud Rate: Select the baud rate at which the Remote Link communicates with the Admin Reader. The default Baud Rate is 9600.

Reader Model: Select the connection used for the Admin 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 Admin Reader fields based on the current value of the Max Code Length.

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

For more information about the Admin Reader feature, see Scanning a Proximity Card.

System > Configure > System Link > TCP Trap Tab

The options available on this tab are used to configure the TCP communication connection to the iCOM or iCOM-E version 103 or higher installed in the SCS-1 or SCS-1R receiver. This allows networks panels with a dynamic IP address to be trapped for System Link upload/download.

TCP Trap Enabled: Check this box to enable TCP Trapping.

Programming App. Address: Enter the IP address of the System Link computer used to program panels. If the System Link computer is behind a firewall, enter the IP address of the network router. This address is sent to the panel iCOM or iCOM-E to use for connection to System Link for a remote upload/download session.

Programming App. Port: This is the port used by the System Link computer to make the connection to the panel, iCOM and iCOM-E using TCP protocol. The default value is 2002.

Trap Server Address: Enter the IP address of the SCS-101, SCS-104, iCOM or iCOM-E 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, SCS-

104, iCOM or iCOM-E installed in the SCS-1 or SCS-1R.

Auto Send Traps: This enables System 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 System Link waits between resetting traps. Default is 180 seconds. Minimum is 30 seconds.
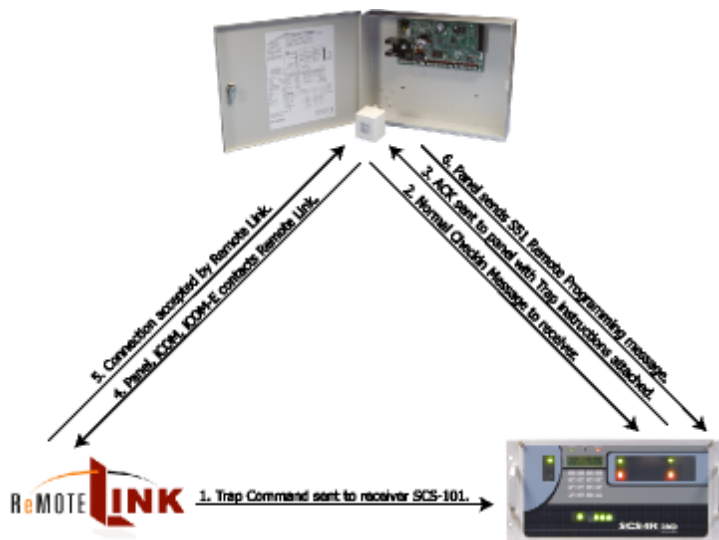
System > Configure > System Link > Modules Tab
Host Monitoring (Must have an additional module to use)

Host Monitoring: Select Host Monitoring to enable 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:** All XT Series, XR100, XR500, XR150/XR350/XR550 Series can track the Arm/Disarm status of the panel, however, for the XR200 Series, only the XR200 (version 110) and XR200-485 (version 204) have this capability.

System > Configure > System Link > 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.
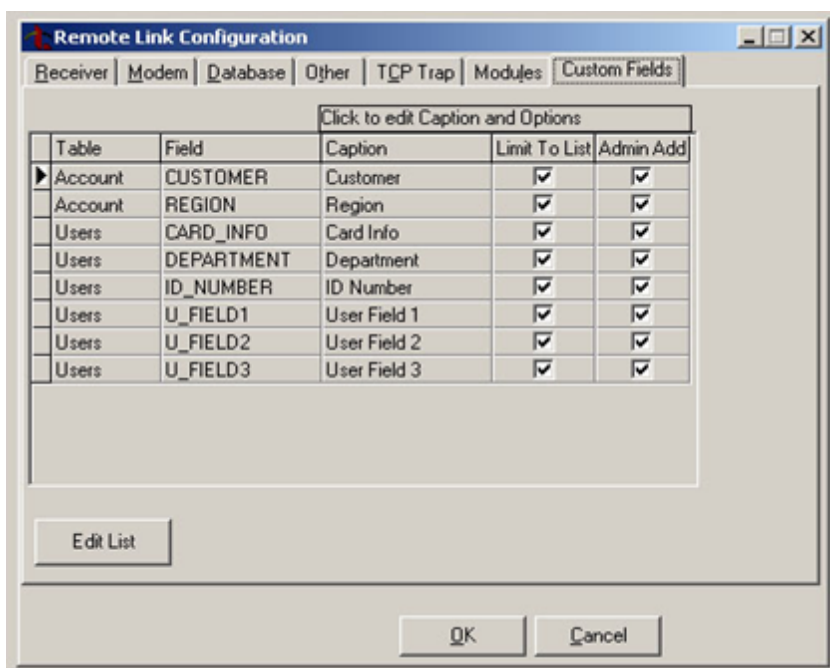
Edit List: The Edit List button allows the list of acceptable selections to be maintained by an Administrator. Select the field to change and click the Edit List button.

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
☐	☐	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.
☐	☑	All operators can add to the list. A prompt appears to confirm addition of the item to the drop down list.
☑	☐	Selections are strictly limited to items in the drop down list. Additions can only be made from the Remote Link Configuration screen.
☑	☑	Entries for non-Administrative operators are limited to items in the drop down list. Administrators can enter text not in the drop down list.

System > Operator Configuration > Operator Information

The programming options in the **System 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 System Link, select **System > Operator Configuration**.

Classic Login

Login Information: To authorize a new operator to log in to System Link, click on the **New** button 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 click the . . . button. In the Select Accounts window, place a checkmark next to the accounts the operator is authorized to access.
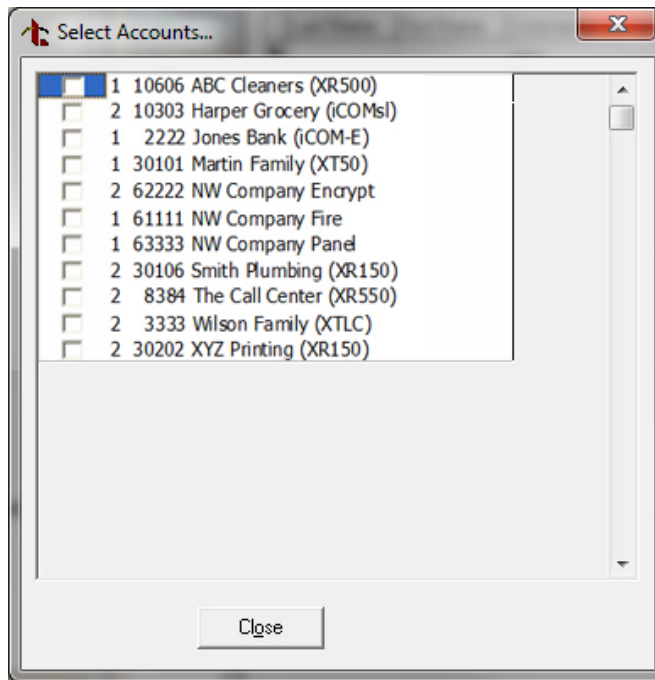
Note: The Account Access restrict option does not prevent an operator from using the trap function to send and/or retrieve changes made by other operators.

Note: 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. Click on the **View Only** option.

Administrator: Check the Administrator box to provide complete authority to perform administrative functions within System Link, such as adding new operators and configuring System 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 System Link Panel menu to be accessible to the user.

Single Sign-On

Single Sign-On allows a System Link operator to be associated with their Windows user account. When launched, System Link matches the Windows user currently logged in to an operator in the System Link database. This feature eliminates the need for Central Station operators to remember a System Link password and allows improved control of access to System Link. If a Windows user account fails to match a System Link operator an Application Access Denied dialog box displays and the user is denied access to System Link.

System 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:

From the main System Link screen, select System > Operator Information to display the Operator Configuration window. Click the Authentication… button at the bottom center of the screen. The Operator Authentication Method dialog displays detailing the two types of operator authentication. Click Next to continue or click the Cancel button to terminate the process.
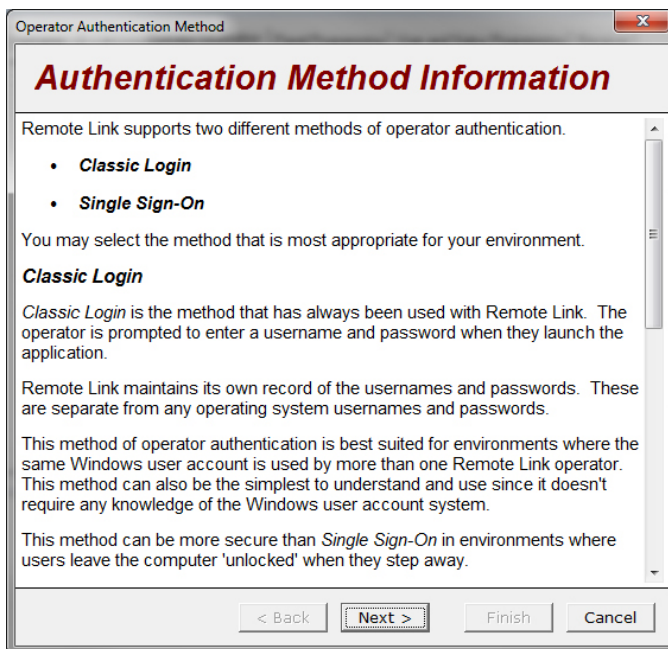
The Select Authentication Method dialog box displays with Classic Login and Single Sign-On checkboxes. Select Single Sign-On and click Next to continue or click Cancel button to terminate the process.
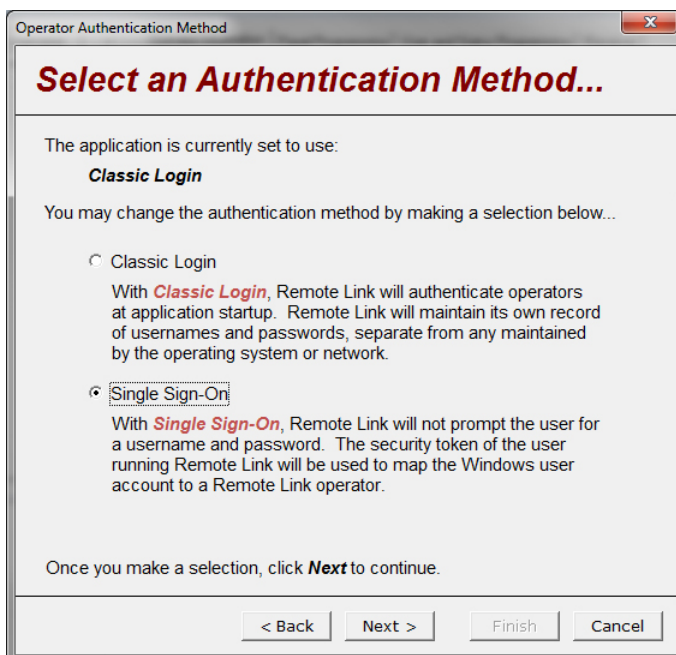
The Single Sign-On dialog box displays with the System Link administrator account and the Windows user account to be mapped. Click Finish to complete authorization. The Back button will return you to the Select Authentication Method screen or click the Cancel button to terminate the process.

Single Sign-On

By clicking **Finish**, Remote Link will switch from *Classic Login* to *Single Sign-On*.

Your Remote Link administration operator account,

new

will be mapped to the following Windows user account:

DMP\User1

which is the Windows user account that you are currently using. If necessary, you can change this in the *Operator Configuration* screen.

You will need to associate a Windows user account to each of the existing Remote Link operators. Until this is done, those operators will effectively be disabled.

You associate a Windows user account to an operator by clicking the **Edit...** button in the *Single Sign-On Information* area of the *Operator Configuration* screen.

Note that, for security purposes, an operator's password will be deleted once a Windows user account has been associated with the operator.

Click **Finish** to apply the new settings and exit this dialog.

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

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

Single Sign-On Information

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

- Object Types
- Locations
- Check Names

Object Types

The Windows User Object Type is automatically displayed.

Locations

Click the Locations button 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.
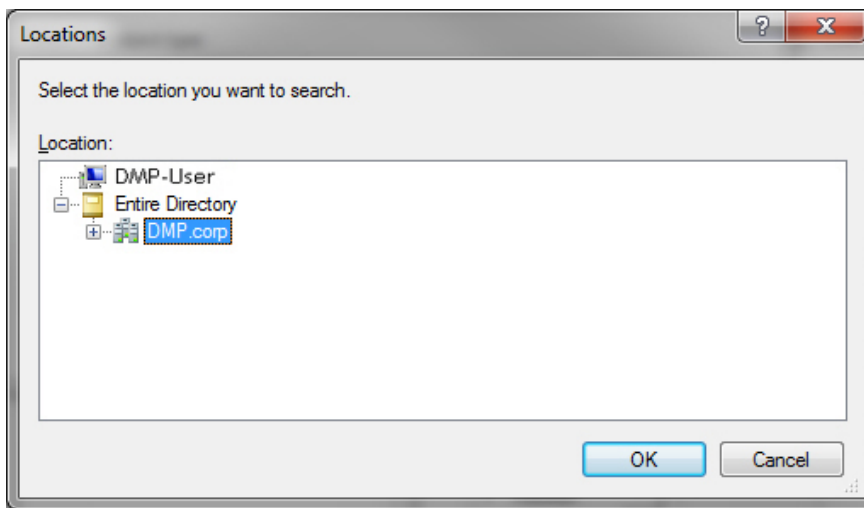
Check Names

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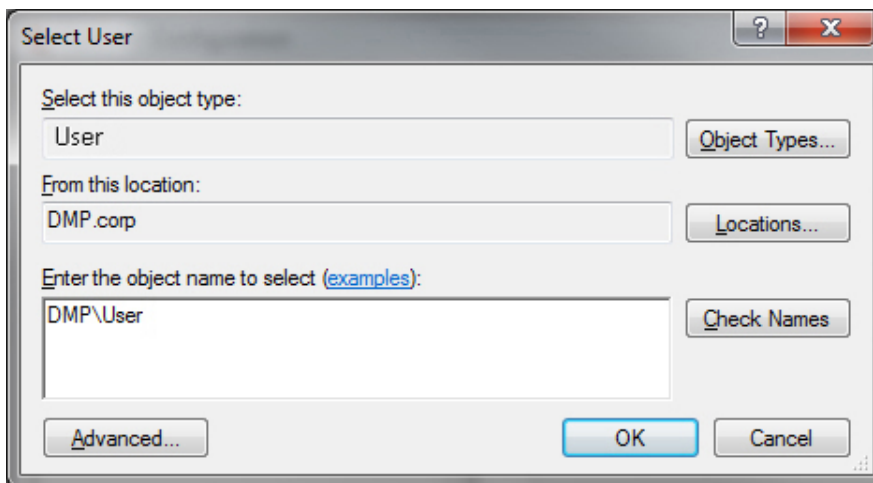
Advanced

Click the Advanced button to display the expanded search feature.

To add or remove available search criteria, click on the Columns button.

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

Choose Columns

Columns available:

- Assistant
- City
- Comment
- Company
- Country/Region
- Country/Region Abbrevia...
- Department
- Description
- Direct Reports
- Display Name

Add >

< Remove

Columns shown:

- Last Name
- First Name
- Name (RDN)
- E-Mail Address
- In Folder

OK   Cancel

Select User

Select this object type:

User   Object Types...

From this location:

DMP.corp   Locations...

Common Queries

Name: Starts with ▼

Description: Starts with ▼

Columns...

Find Now

Stop

☐ Disabled accounts
☐ Non expiring password

Days since last logon: ▼
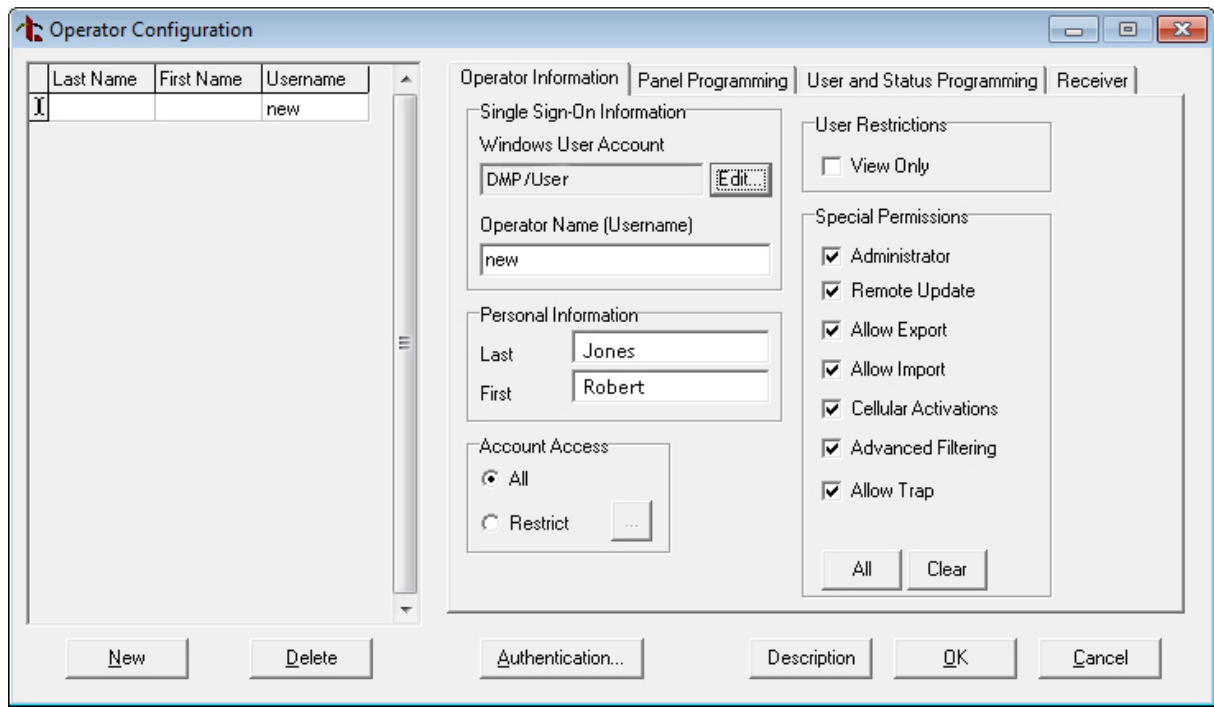
OK   Cancel

Search results:

Name (RDN)	E-Mail Address	In Folder	First Name	Last Name
Adminstrator			Adminstrator	
jking	jking@mail.com		James	King
rjones	rjones@mail.com		Robert	Jones

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 click the . . . button. In the Select Accounts window, place a checkmark next to the accounts the operator is authorized to access.

Note: 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. Click on the **View Only** option.

Administrator: Check the Administrator box to provide complete authority to perform administrative functions within System Link, such as adding new operators and configuring System 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 System Link Panel menu to be accessible to the user.

System > Operator Configuration > User and Status Programming
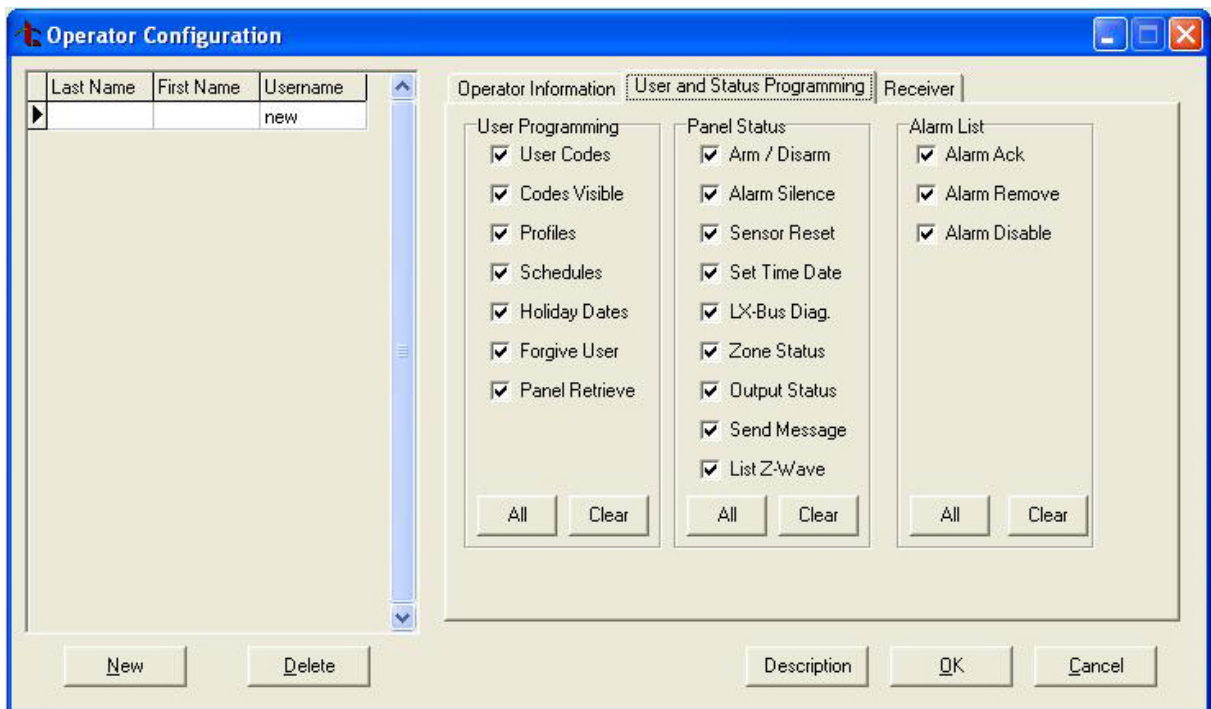
You may click the **All** button to select all options on the User and Status Programming Tab.

Click the **Clear** button 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 System Link versions the alarm authority options are automatically enabled.

System > Operator Configuration > Receiver
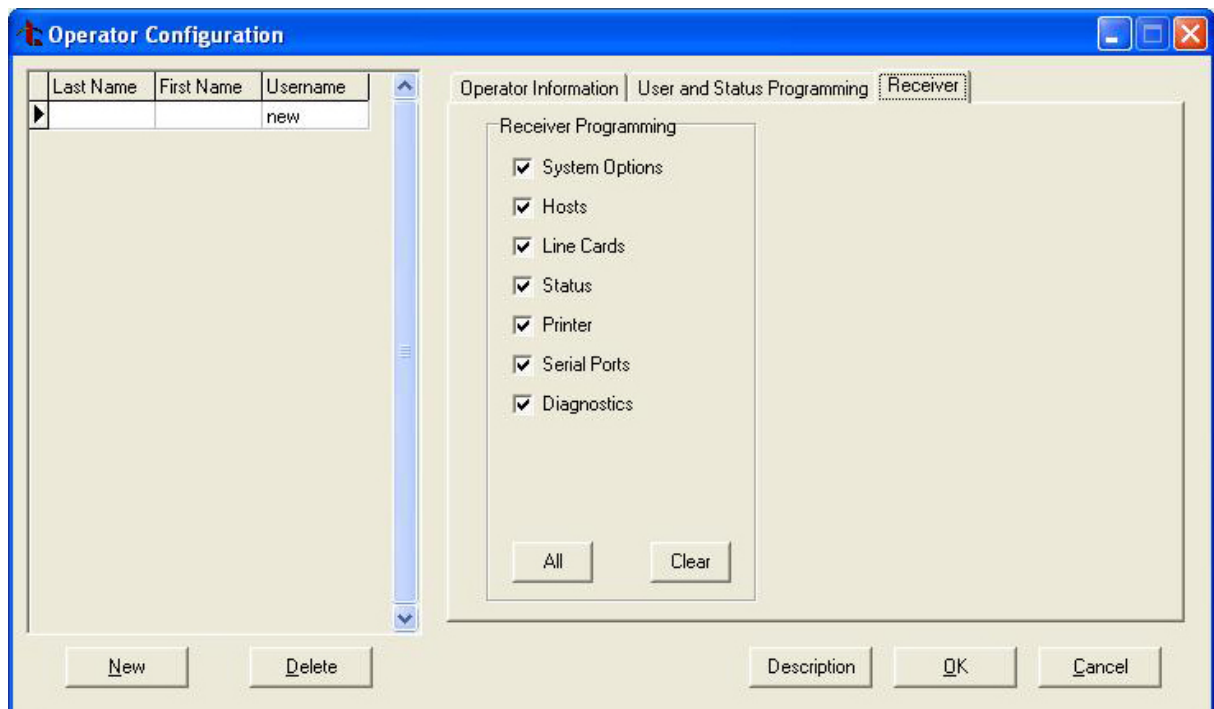
Each option refers to an SCS-150 programming window. Check each box to assign the operator authority to perform receiver programming options. You may click the **All** button to select all options on the Receiver Programming Tab. Click the **Clear** button to remove all options.

System > Toolbar Configuration

System 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, click 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.

System > Diagnostics or Alt + F10

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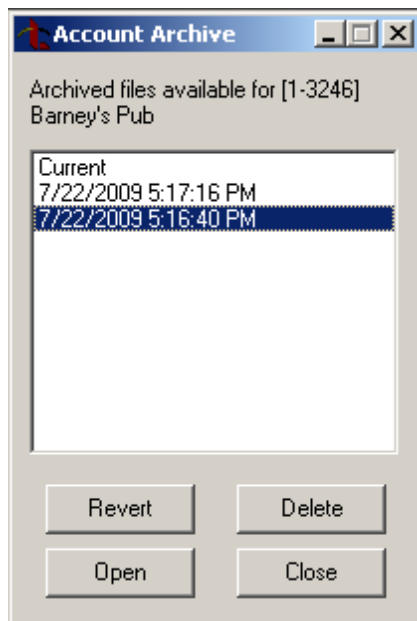
Account Archive can be accessed by selecting **Panel>Account Archive.** The Account Archive feature allows panel account programming to be stored for comparison or the archived version may be used to revert current panel programming to an archived version. System Link can be programmed to store up to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

Revert: This option reverts the current panel account programming to a previous programming

version. Select the archive version and click Revert. System 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.

File > Panel Information

If you wish to add, delete, or change accounts in System Link, click **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 XR150/XR350/XR550, XR100 and XR500 Series, XR2500F 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.

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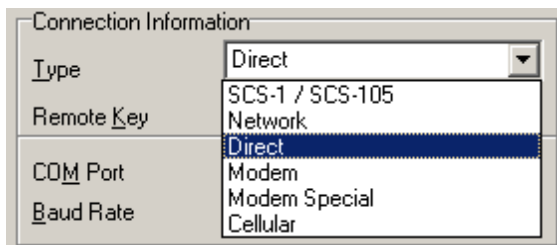
Enter a name for the account in the **Name** field in the **General Information** section. The receiver number and account number appear in this section of the **Panel Information** window as well. You may change the account number in the **Account #** field if necessary. Refer to Account Number Conventions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

File > Panel Information

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/XR2500F panel on-board Ethernet.

- The XR100N panel on-board Ethernet.

- The XR150/XR350/XR550 with Network panel on-board Ethernet.

- A 462N card and an iCOM™ Network Alarm Router or iCOM-E™ Encrypted Network Alarm Router.

- An XRSuper6/XR20/XR40 panel and an iCOMsl Network Alarm Router.

- An XT30/XT50 Series panel on-board 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 XR150/XR350/XR550 Series, XR500 Series or XR100 Series panel. First configure your computer's modem in the Modem Tab. Then configure the modem as described below.

Modem Special: for 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: System Link communicates with the panel through a cellular connection using a SIM 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 System Link computer. The panel must give the correct key to System 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

---

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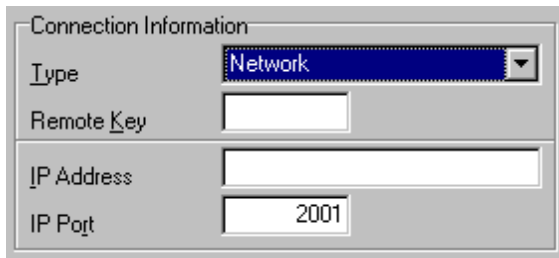
No: Do not dial the panel phone number to make contact with the panel. This is used mainly for multiplex and asynchronous accounts.

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 System Link pickup when the panel calls in to the receiver. This allows System Link to seize the panel when the panel calls in. The following example illustrates how to perform a Pickup Only using System 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 System 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). System Link will then seize the phone line and the Operator and Technician hang up their phones.

IP Address: Enter the IP address of the network device connected to the panel, such as the iCOM/iCOM-E or iCOMSL. 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. If the panel is an iCOMsl, ePAD, NRL-101, or iCOM/iCOM-E, the default is 9999. This field will appear only when you select **Network** in the **Type** field.

Note: When performing a Remote Update on an ePAD, the IP Port must be the same as the **Upgrade Port** programmed in the ePAD. When performing a Remote Update on an iCOM/iCOM-E or NRL-101, the IP Port must be the same as the Telnet Port programmed in the iCOM/iCOM-E or NRL-101. When programming an iCOMsl, the IP Port must be the same as the **Programming Port** programmed in the iCOMsl.

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 card was activated.

File > Panel Information

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 clicking on the Extra Information button. Clicking the Extra Information button opens the Extended Panel Information window.

File > Panel Information > Extended Panel Information

Click the **Extra Information** button 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, System Link will not look for an Automatic Recall Test for the account.

- If System 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, System Link begins counting down to look for the next Automatic Recall Test from the account. System Link's countdown adds two hours onto the entered number of days. For example, if 2 is entered in the Auto Recall Frequency field, System Link will look for the next test in 50 hours-48 hours plus two.

- Allow Test Deferrals: Check this box to allow System 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, System Link will accept the opening signal as the Automatic Recall test. System Link will then restart the timer after the opening signal is received.
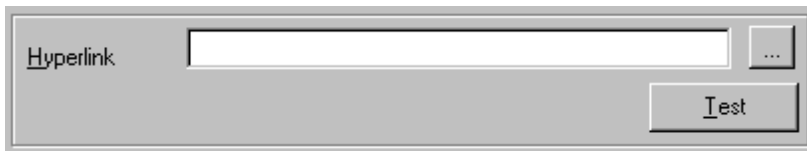
  Note: These two fields, Auto Recall Frequency and Allow Test Deferrals, should have the same value as the Test Frequency and Defer Test fields in Program > Communications > Test Timer tab.

- **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.

(Must have Alarm Monitoring Module or Command Center to Use)

File > Panel Information

Open **File > Panel** Information. Select the account to which to will assign the hyperlink. Click on the **Extra Information** button 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: Be sure to 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 loaded 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.

File > Panel Information > Configure Button

Configure: Click the **Configure** button beside the **Phone** field to open a dialog box that allows you to configure the 462FM Fast Modem.

Ring Count: Enter the number of times the site phone will ring before the 462FM picks up. Enter a number between 1 and 15. The default is 1 ring. You must increase the Dial Time Out about 10 seconds per ring.

Set Modem: Click this button to dial the phone number programmed in **Panel Information**. When the 462FM picks up, the Ring Count will be stored in the 462FM Module's programming. After the 462FM has stored the number, the 462FM will disconnect from System Link. A pop-up window will then appear stating, "Ring Count successfully sent."

File > Panel Information

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.

File > Panel Information> 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, click New, and enter the Version number, Receiver number, and Account number for the receiver and click 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.
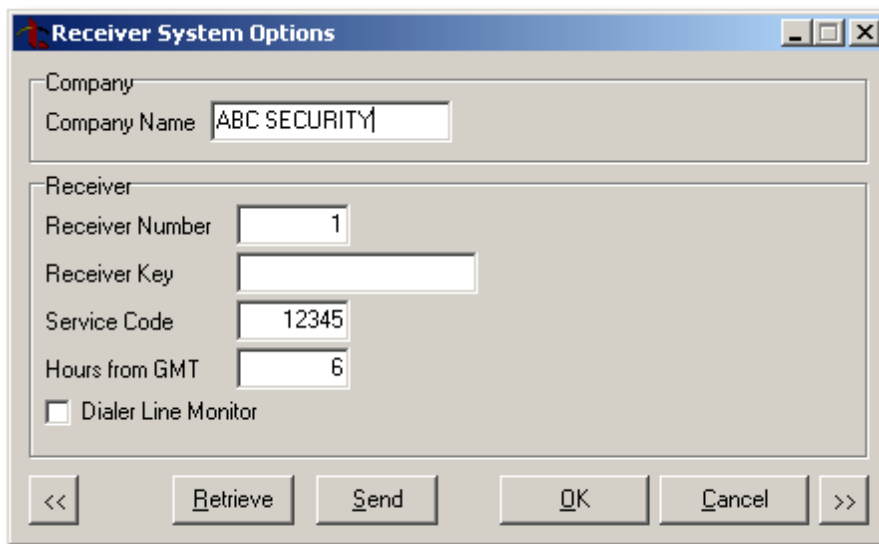
To copy an existing receiver, select the receiver from the list and click the Copy button. A new window appears, allowing changes to be made to the information. Once the new information has been added, click OK.

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

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

To filter accounts, select the Panel Filter button. This allows filtering of panel or user information.

Program > Receiver Sys Options
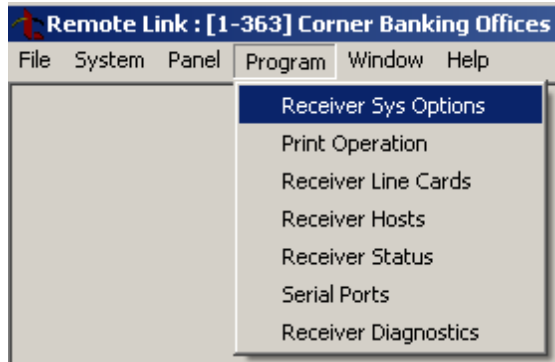
Note: Before continuing, click on the Retrieve button to import the current receiver information.

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

Program > 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.
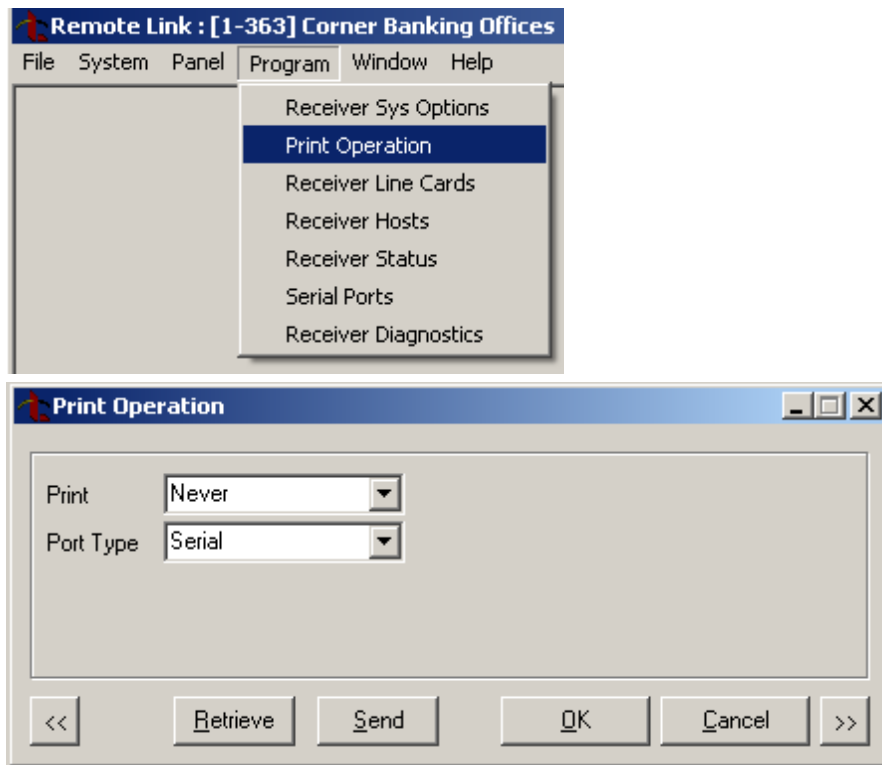
> **Note:** Before continuing, click on the Retrieve button to import the current receiver information.

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

Program > Receiver Line Cards

>> **Note:** Before continuing, click on the Retrieve button to import the current receiver information.

New: Select the NEW button near the bottom of the window to add a new line card.
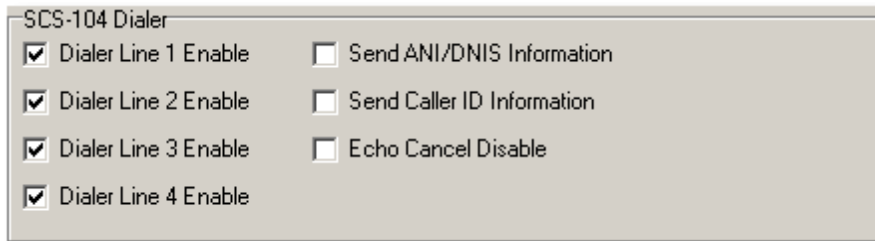
Card Number: Enter the card number, 1 through 8.

>> **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, 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 XR500 Series panels, but the data is not encrypted. The Passphrase is blank by default.

> **Note:** DO NOT LOSE THE PASSPHRASE. A lost or forgotten Passphrase requires that every XR500 Series 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.
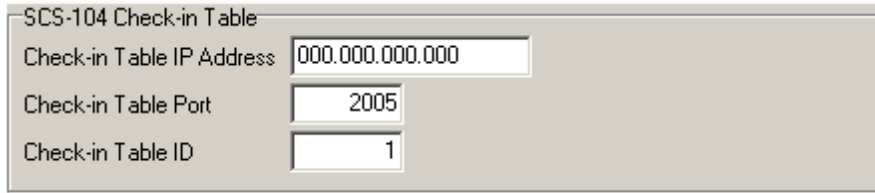
When enabled, the S17 Panel Response Restored message is sent to the automation computer each time a supervised account checks in for the first time after installation. This also occurs at an account's first check-in after the receiver or SCS-104 is powered-up. Default is disabled.

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: Click Send to send the Receiver Line Card programming to the SCS-1R.
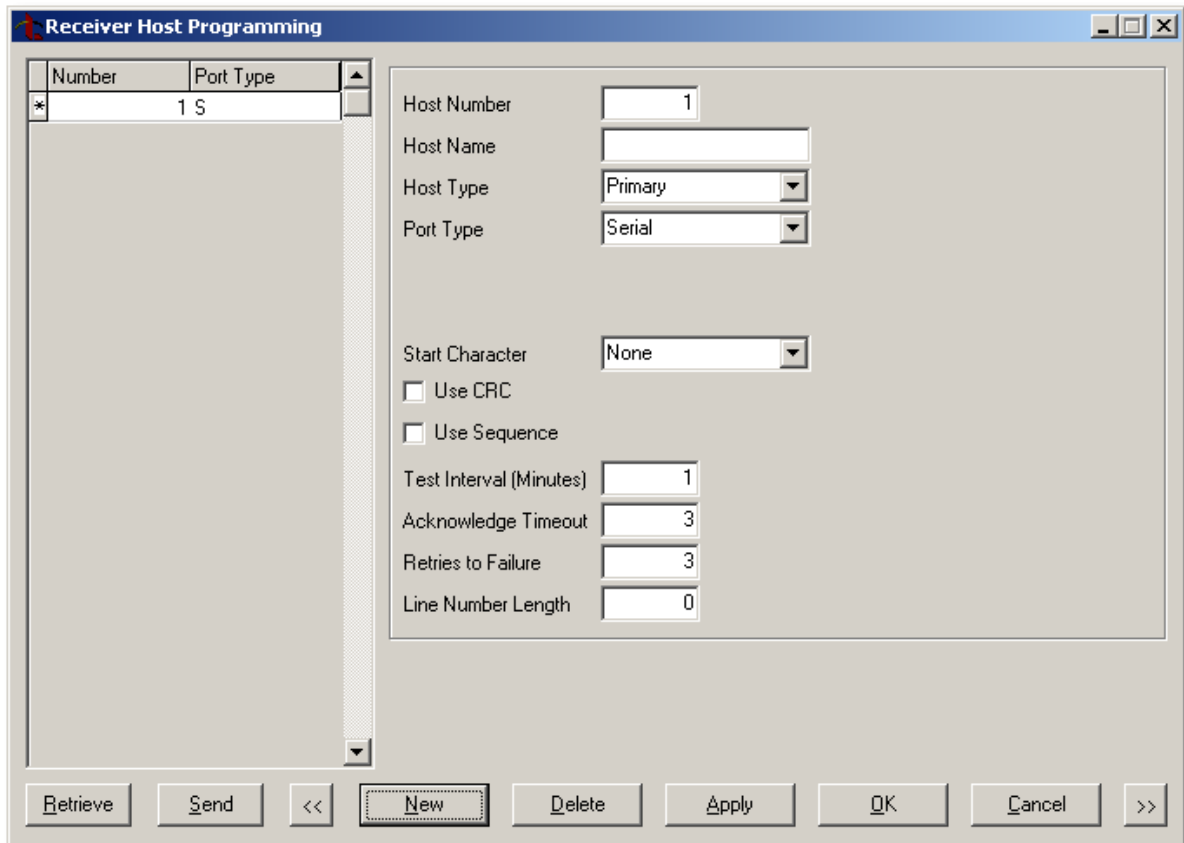
Program > Receiver Hosts

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.

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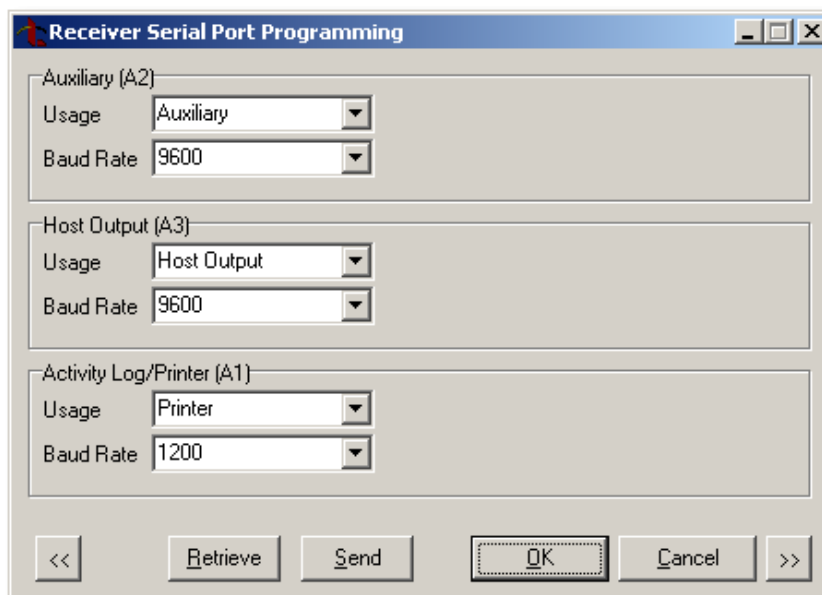
Send: Click Send to send the Receiver Host Programming to the SCS-1R.

Program > Receiver Status

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

Program > Serial Ports

Select to open the Receiver Serial Port Programming window.

> **Note:** Before continuing, click on the Retrieve button 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: Click Send to send the Receiver Serial Port Programming to the SCS-1R/SCS-150.

Program > Receiver Diagnostics

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

File > 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.
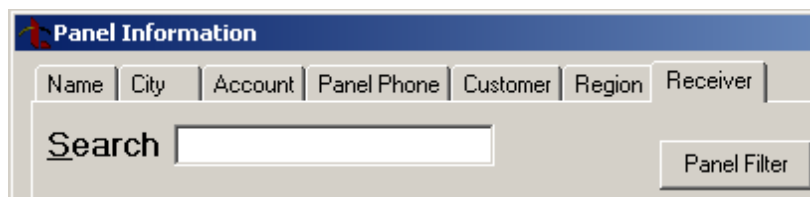
On the Panel Information Window, click the Panel Filter button. This allows filtering of panel or user

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.

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. Click 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.

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. Click 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.

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. Click on 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, click the Export button to export the information. If you want to export only certain users, select the users from the filtered information, click the Export Selected Users box, and click Export.

File > Panel Information > New button

To add a new account, click the **New** button 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 System 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, uncheck the box by clicking in the box. **Programming On File** is checked as default. See Programming Not on File for more information.

When you click on the drop-down arrow in the **Model** field, System Link displays a list of the panel models. Select the appropriate panel model number. For XR550 with Encryption, XR500E or XR2500F panels, select the XR550 with Network, 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 an XR500 Series panel, the Feature Set displays the available features and panel types. Check the enabled features of the panel for the account you are creating.

Click on Encryption when an XR550 with Encryption or XR500E panel is installed. The encryption feature allows the XR500E to send and receive data using 128 bit AES encryption. To complete encryption programming, enter a Passphrase in Network Options.

Click on XR2500F when an XR2500F Addressable Fire Alarm Control Panel (FACP) is installed.

Click on 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. See below for information about iCOMsl account numbers.

When you are finished completing all of the fields in the **New Panel** window click **OK** to close that window and return to the **Panel Information** window.

---

iCOMsl Account Numbers: In input mode, the account number entered here is reported to the receiver.

In keypad mode, the account number reported to the receiver originates from the panel attached to the iCOMsl. The account number entered here, when in keypad mode, is used for programming with System Link only. The iCOMsl and the panel have separate account numbers.

File > Panel Information

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

When using **Digital Dialer (DD)** 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 **Host/Net (HST/NET)** mode, the range of available account numbers is **1 through 65535**.

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.**

When using the iCOMsl, enter an account number between 1 and 65535.

File > Panel Information

To edit information on existing accounts, open the **Panel Information** window by clicking **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 clicking on the **Extra** Information button to open the **Extended Panel** Information window.

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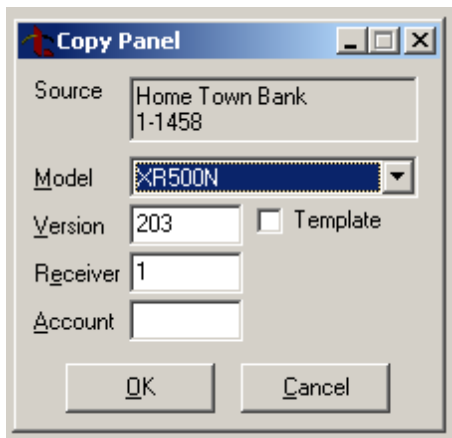
If you want to create a new account by using an existing account file as a template, open the **Panel Information** window by selecting **File > Panel Information**. Select the account file that you wish to use as a template by clicking on that account in the list. Then click on the **Copy** button at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

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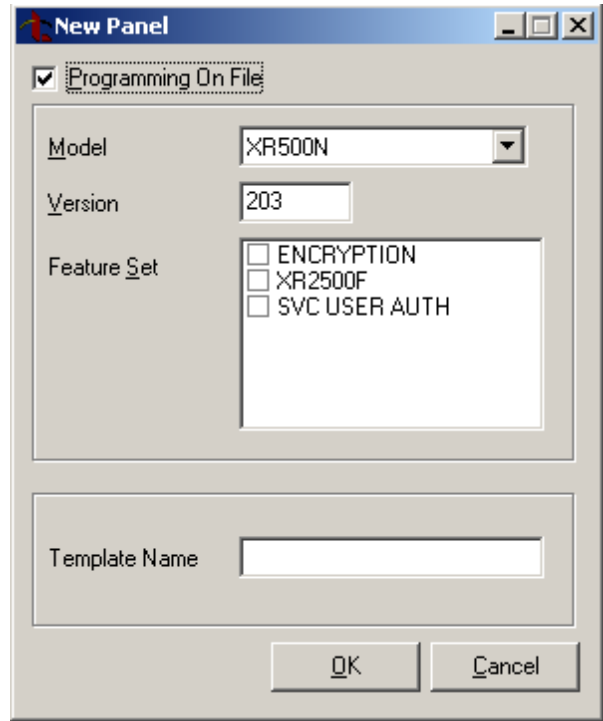
Any existing templates appear in the list with the **Name, Model and Version**.

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 click 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".

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. System 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>System Link>Other Tab.**

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

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

File > Import and Export > Export Accounts

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 System 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 clicking 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.

File > Import and Export > Import Accounts

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 System 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 clicking 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**.
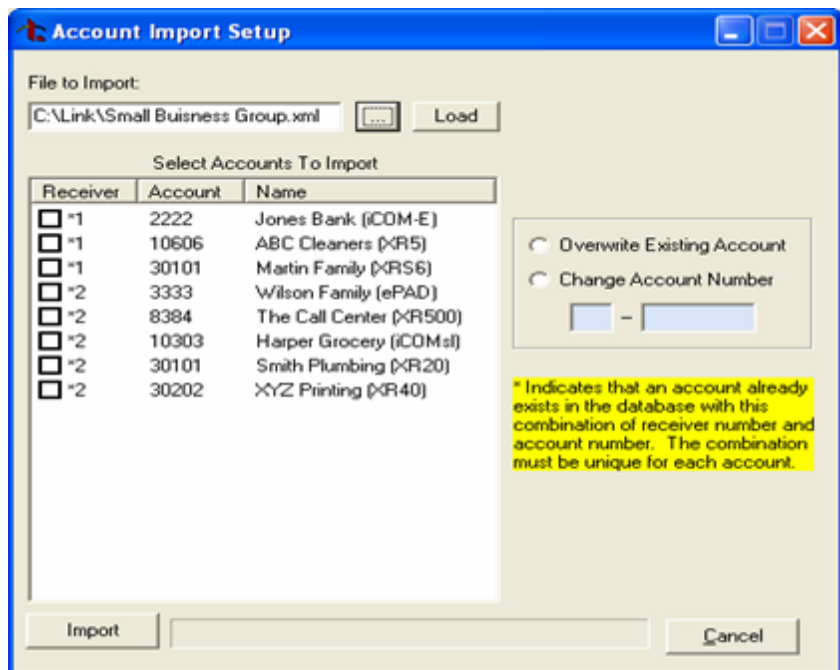
Enter Encryption Key: Enter the 4 to 64 character encryption key that was used when the file was exported. For security purposes, the exported data was encrypted to ensure panel programming was not compromised.
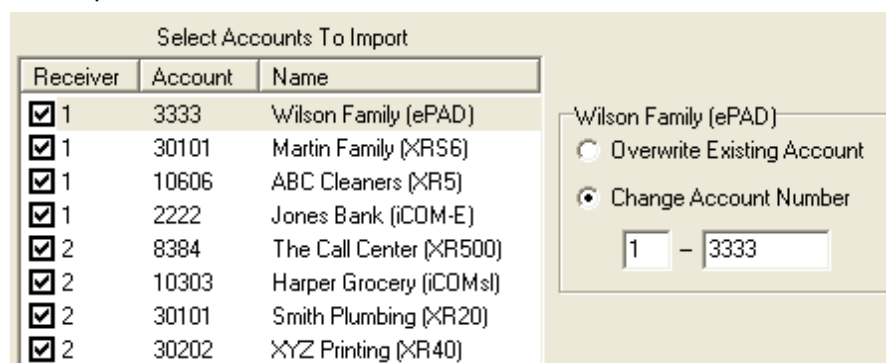
Select Accounts to Import: The receiver number, account number and panel name display. A * next tot he checkbox indicates that the panel currently exists in the System Link data base. Highlight the name and select the import process to use, overwrite or change, shown on the right of the screen. A checkmark 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 checkmarked 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.

File > Print

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.

Printing Account Information Reports

Printing Panel Programming Reports

Printing Activity Reports

Printing Events

Printing Advanced Reports (Must have the Advanced Reporting Module)

Printing the Recall Failure List

File > Print > Account Information

To print an account information report, select **File > Print > Account Information** to open the **Account Report Setup** window.
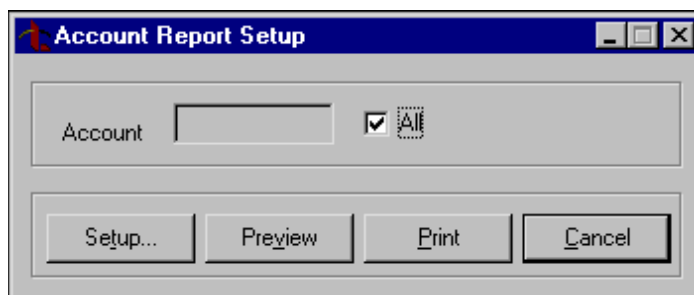
All: Check this box to print the account reports for all panel accounts. If the All checkbox is not selected, the account information for the panel that is opened in System Link will be printed.

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

Preview: Click 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: Click this button to print the account reports to an attached printer.

File > Print > Panel Programming

Prints panel programming for the account open in System Link.

Reports to Include

Check the box for each type of report that you wish to print. Click **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: Click on this button to enter the printer setup window to configure your print options.

Preview: Click 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: Click this button to print the account reports to an attached printer.

File > Print > Activity

Prints a report of System 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. Click the arrow to the right of the field to open the drop-down calendar, as shown above. Click on 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: Click on this button to enter the printer setup window to configure your print options.

Preview: Click 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: Click this button to print the account reports to an attached printer.

File > Print > 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, click **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. Click the arrow to the right of the field to open the drop-down calendar. Click on 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 System 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.

Print activation status reports for all SIM cards associated with an account. To print activation status reports, click **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.

File > Print > Alarm List

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:** Click on this button to enter the printer setup window to configure your print options.
- **Preview:** Click 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:** Click 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.

File > Print > Recall Failure List

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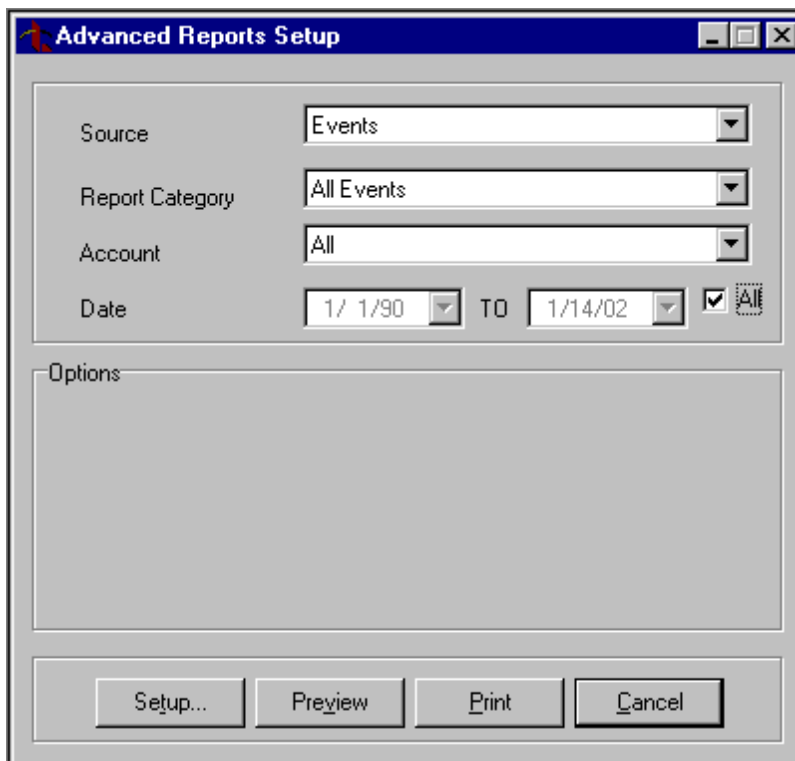
Preview: Click this button for a print preview on your computer screen. To save this report, press the button that looks like a floppy disk when in the preview mode. When you wish to print the report, got to **File > Print > Saved Report**.

Print: Click 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.

(Must have Advanced Reporting Module to Use)

File > Print > Advanced Reports

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

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

Preview: Click 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: Click this button to print the account reports to an attached printer.

Click here for a complete discussion of the **Advanced Reporting Module.**

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, click on the Load button 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 Aoounts 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 clicking 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 click on the **Load** button. The information from the selected comparison displays in the Accounts To Compare fields.

To delete a saved comparison from System Link, select the comparison name from the drop-down menu and click the **Delete** button.

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. Click 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 click 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.

File > Print > Export Data

To export data reports as CSV (Comma Separated Value) files that can be opened in Microsoft® Excel, click **File > Print > Data Export.** The account open in System 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.
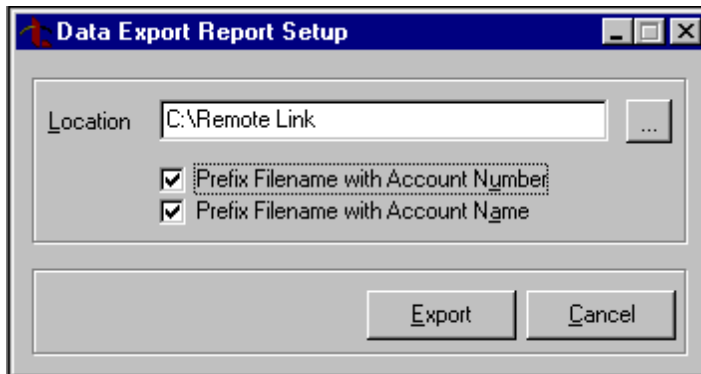
Prefix Filename with Account Number: Select this checkbox if you want all of the files to contain the account number in the file name. For example, a file name with the account number would read "1-12345 Area Information.csv."

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.

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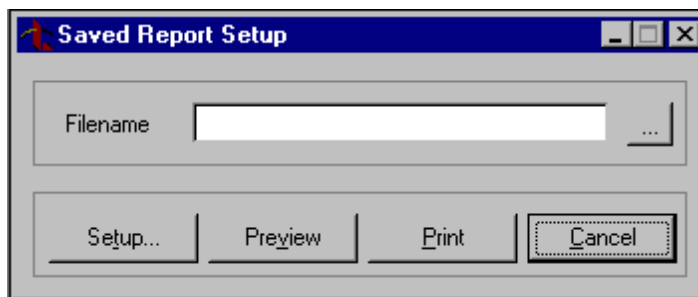
If you have saved a report and you now wish to print it, go to **File > Print > Saved Report**. Enter the filename of the saved report. Press the button to the right of the **Filename** field to browse for the saved report you wish to print.

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

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

Print: Click 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. See Exporting Reports.

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.

Panel > 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 clicking on the line for that account, then clicking **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, click **OK** to open the account.

```
┌─ Connection Status ──────────────── _ □ ✕ ┐
│ ┌─ Connection Information ──────────────┐ │
│ │  Account  [12345        ]             │ │
│ │  ┌────────────────────────────────┐   │ │
│ │  │                                │   │ │
│ │  │                                │   │ │
│ │  │                                │   │ │
│ │  │                                │   │ │
│ │  └────────────────────────────────┘   │ │
│ └───────────────────────────────────────┘ │
│  [ Connect ]  [ Abort ]  [ Disconnect ]  [ Cancel ] │
└────────────────────────────────────────────┘
```
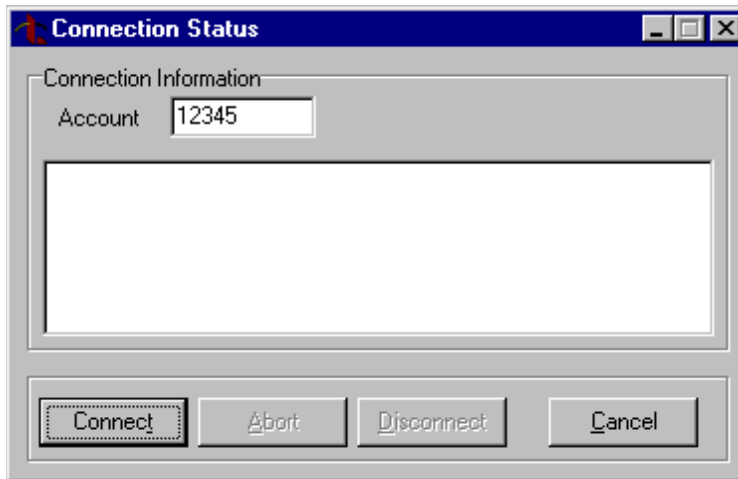
Now select **Panel > Connect** to open the **Connection Status** window and click **Connect**. The **Connection Status** window will close after System Link has connected to the panel.

This option allows you to connect the System 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 System 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. Click on **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, System Link will disconnect with the panel 1 minute later. System Link must be communicating with the panel using one of the following methods:

- The computer network card (NIC)
- The computer modem to a 462FM Fast Modem card or to the 2400 baud programming dialer of an XR500 Series or XR100 Series panel
- 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.

Errors While Connecting

The following messages indicate an error has occurred while System 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 System 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 > System Link (System Link Configuration window). Also verify that another application on the computer is not using a COM Port that is used by System 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. System Link cannot get a reply from the receiver. Check the following settings and items:

- In System > Configure > System 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. System 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 System 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. System Link did not receive a reply from panel.

Panel Connection Error: Invalid connect response. System 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 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: System 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 System Link was trying to send to the panel.

Panel > Disconnect

To disconnect from a panel, select **Panel > Disconnect** to open the **Connection Status** window. Click on the **Disconnect** button.

Panel > Send

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

> **Note:** Close all System 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, System Link tracks the status of the data transfer.
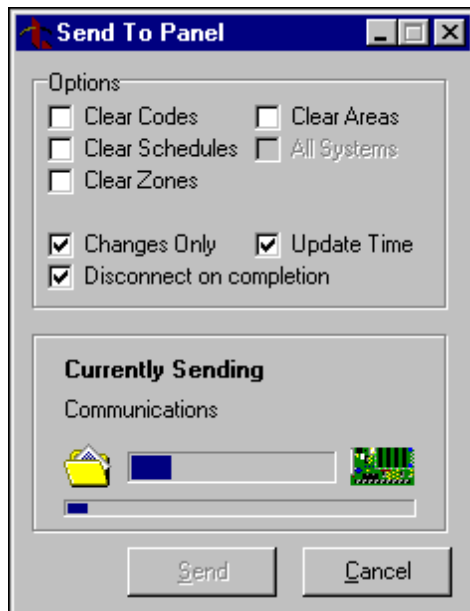
Before sending the file, you can also select to clear the codes, schedules, zone, and area information from the panel. Select **Changes Only** to send only the programming that has changed to the panel.

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 System Link and the panel. The bottom bar tracks the status of the entire file.

Panel > Retrieve

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

Note: Close all System 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.
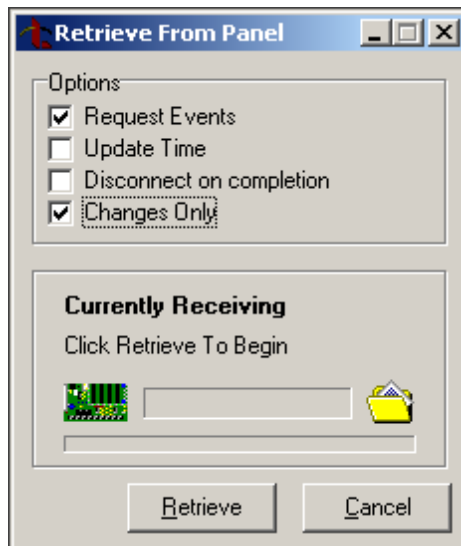
Select **Update Time** to send a time update to the panel after System Link has retrieved the data from the panel.

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

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

For XR150/XR350/XR550 and XR500 and XR100 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 System Link and the panel. The bottom bar tracks the status of the entire file.

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

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

Panel > 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
- Battery
- Line 1
- Line 2
- Tamper
- Ac Power
- 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.

Panel > System Status

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."

Panel > System Status

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."

Panel > System Status

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

Panel > System Status

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. Click 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 click **Send**.

To remove the message on-site, perform a J16 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 click the **Send** button.

> **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. System Link will confirm that your message was sent to the panel successfully, but System

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 m**an message to the panel. Enter the message in the **Message to Send** field, select **Service man**, and click **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.

Panel > System Status > Area Status

System 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 click on the Areas button.

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.

How to Arm and Disarm

- To arm or disarm an active area, select that area from the Area Status list and click on the arrow to open the drop-down menu, as shown in the picture above. Select Arm or Disarm form the drop-down list. Click on 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.
- Bad Zone Action
- Area Status Messages

Panel > System Status > Zone Status

The **Zone Status** window allows you to view the status of all zones assigned to a panel. Select **Panel > System Status** and click on 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 click on the **Request** button. Selecting the **24-hour box** will display all 24-hour zones, such as **Fire, Fire Verify, Supervisory, Emergency,** and **Panic** zones.

Panel > System Status > 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 click on the **Request** button. The Status column below the **Request** button displays the current status of each output; **Steady, Pulse, or Off**.

Turning Outputs On and Off

Door Control

Panel > System Status > 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 XR150/XR350/XR550 Series, XR500 Series, XR2500F, or XR100 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.

Panel > System Status > 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 click on the LX Bus Diagnostics button.

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

- XR550 and XR500 Series panels (Zones 500 through 999).
- XR350 Series panels (Zones 500 through 799).
- The 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.

Panel > System Status > Z-Wave Device Status
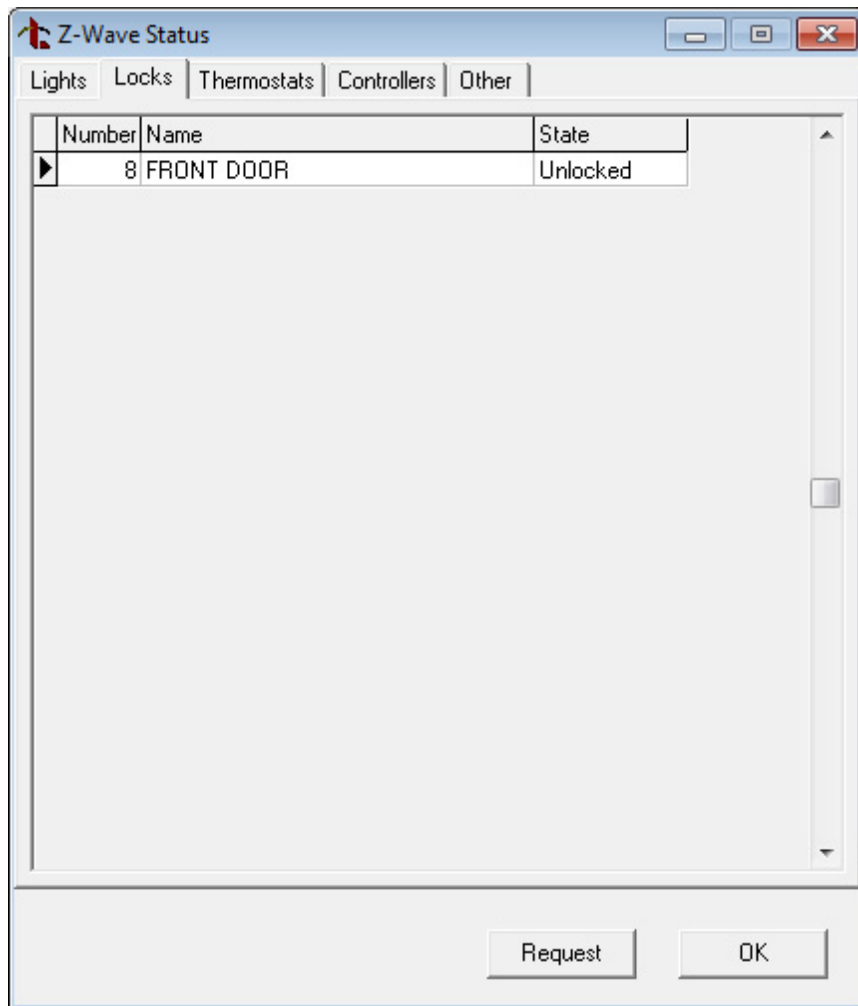
Each tab displays the Z-Wave devices that are currently programmed into the panel as well as their status. Select each tab to see a list of that device type.

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

Panel > System Status > Area Status

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.

    Bypass

    Force

Refuse

Panel > System Status > Area Status

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.

Panel > System Status > Zone Status

To bypass a zone, select the zone from the list in the **Zone Status** window and click the **Bypass** button. The zone remains bypassed until reset from System 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 click the **Reset** button. This removes the bypass from that zone.

Panel > System Status > Output Status > Output tab

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, click on 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 clicking once on that line.

After selecting an output, chose which action you wish to apply to that output by clicking on 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.

Panel > System Status > Output Status > Door Tab

The **Output Status** window allows you to lock and unlock doors and grant door access. Click on 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.

Panel > System Status

Click 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 ton restrict the site's access to authorized users only.

When the **Lockdown** button is pushed, System 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 XR150/XR350/XR550 Series, XR500 Series, XR2500F, XR100 Series, and XR200-485(B) Panels only.

Panel > 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 System Link database.

All Panels

Select **Disconnect on Completion** to automatically disconnect from the panel after the panel event buffer is downloaded into the System 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 clicking the Request button.

To continue, click the **Request** button. While System Link retrieves the events, a status bar appears on your screen that tracks System Link status while downloading events.

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

XR150/XR350/XR550 Series, XR500 Series, XR2500F, XR100 Series, or XR200-485 Panels

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

---

separately.
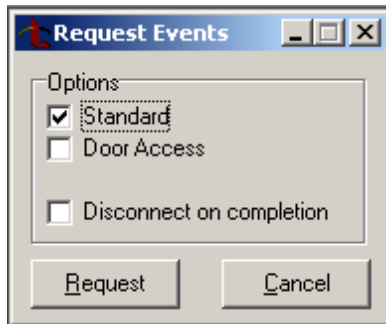
Standard: Requests all events except door access events.

Door Access: Requests only Door Access events.

XR150/XR350/XR550 Series, XR500 or XR100 Series or XR2500F Panels (version 117 or higher)

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
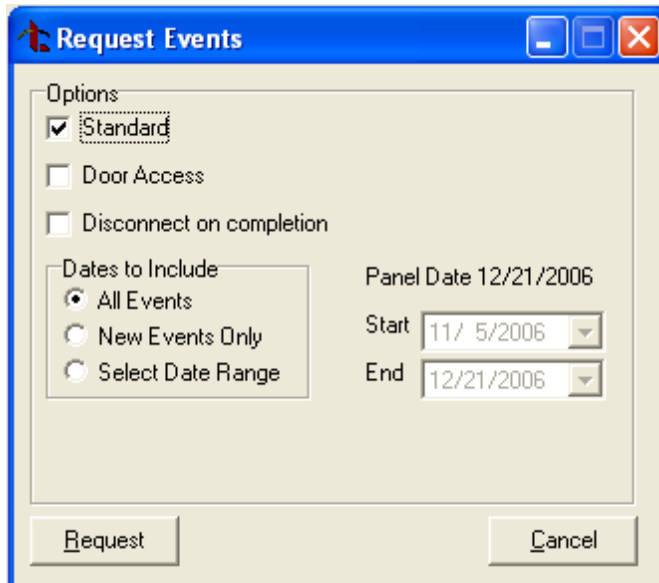
All Events: Requests all events stored in the panel event buffer based on the type of event selected. Uncheck this box to select specific dates.

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, System 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.

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

Panel programming options can also be changed by a service technician at the subscriber's premises. Changes made to a panel from a keypad in the field may not match an account file saved in the System 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 click the **Retrieve** button. 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 **Program** menu, one pointing left and one pointing right. These arrows lead to the previous or next item in the **Program** menu, making it easier to move through the programming windows.

Each panel from DMP offers different features. System 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.

Program > Schedules

The Schedules window allows you to schedule auto arming and disarming of individual areas. You may also create a schedule to limit user's access during specified times of the day. Schedules can also control what times of day a user has authority to arm and disarm the system.

The Schedules window allows you to program the times for each day of the week that you turn your burglary protection on and off. The system can then use this information to automatically arm or disarm the system.

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. Each panel type has a different method for assigning shift schedules.

Partition: Enter 1 through 4 to assign a partition to the shift you are programming. This option does not appear on the XR500 Series, XR2500F, or XR100 Series panels.

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 Partition Info or System 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.

Program > Schedules

These panels allow the assignment of two independent shifts with two unique options for assigning shifts. You may have either Permanent and Temporary schedules or Primary and Secondary schedules depending if Primary/Secondary Schedules is selected in Partition Information.

Shift: Choose Permanent / Primary to select a Permanent or Primary schedule that will operate until it is changed. Choose Temporary / Secondary to select a Temporary or Secondary schedule. The Temporary schedule will expire at the end of the schedule. The Secondary schedule will operate until changed.

Partition: Enter 1 through 4 to assign a partition to the shift you are programming.

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 Partition Info.

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.

Program > Schedules

These panels allow the assignment of four independent shifts. Choose 1st Shift, 2nd Shift, 3rd Shift, or 4th Shift from the drop-down menu.

Partition: Enter 1 through 4 to assign a partition to the shift you are programming. This option does not appear on the XR500 Series, XR2500F, or XR100 Series panels.

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 Partition Info.

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 supercedes all other schedules.

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. Click Apply when finished to save the schedule.

Area Schedules: Enter the Area number you want to assign to a Schedule. You can assign up to 8 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.
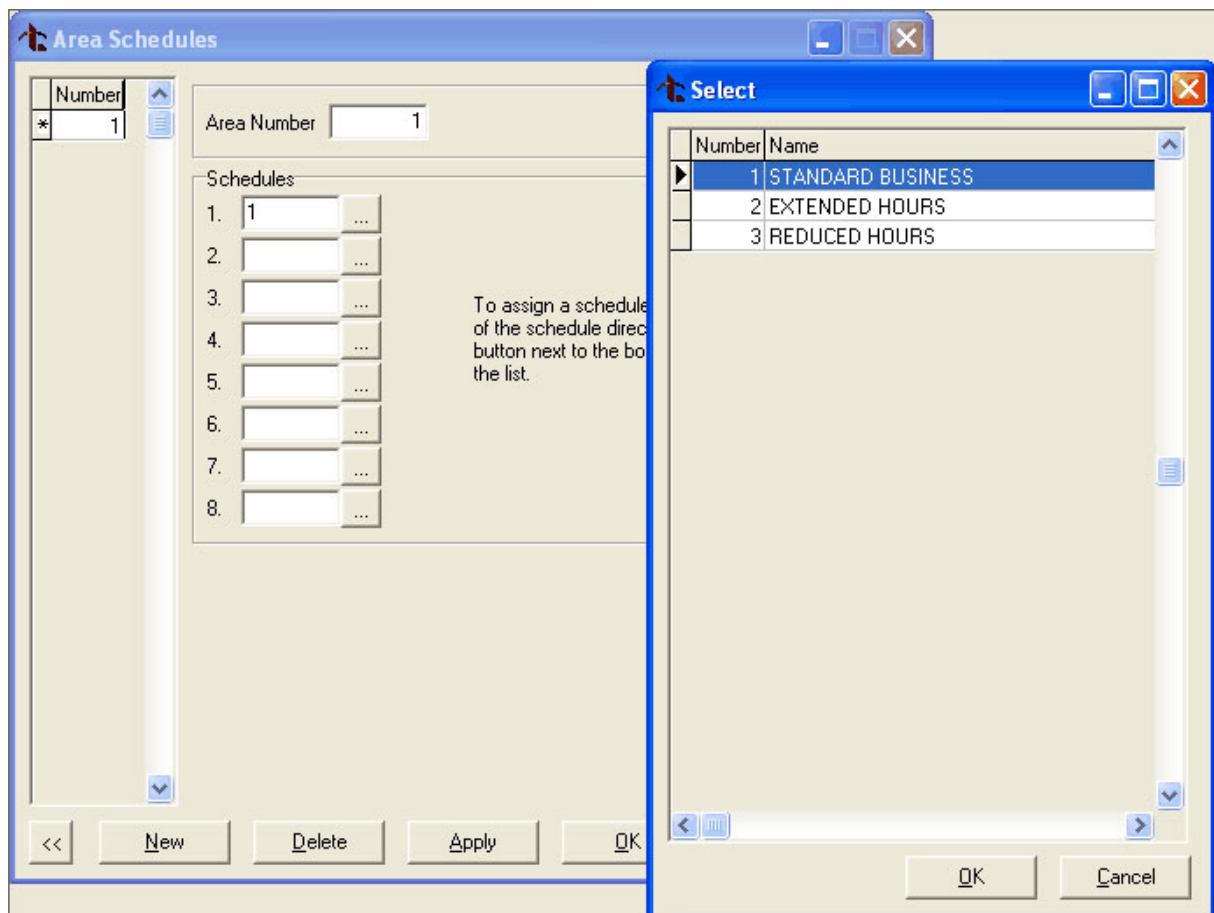
Output/Door/Favorite Schedules: Select the Output, Door, or Favorite number from the list to assign to a Schedule. You can assign up to 8 Schedules to each Output/Door/Favorite. Enter the Schedule number in the first available field or select the browse button next to the field to view the list of schedules. The list of schedules is programmed in the Time Schedules menu.
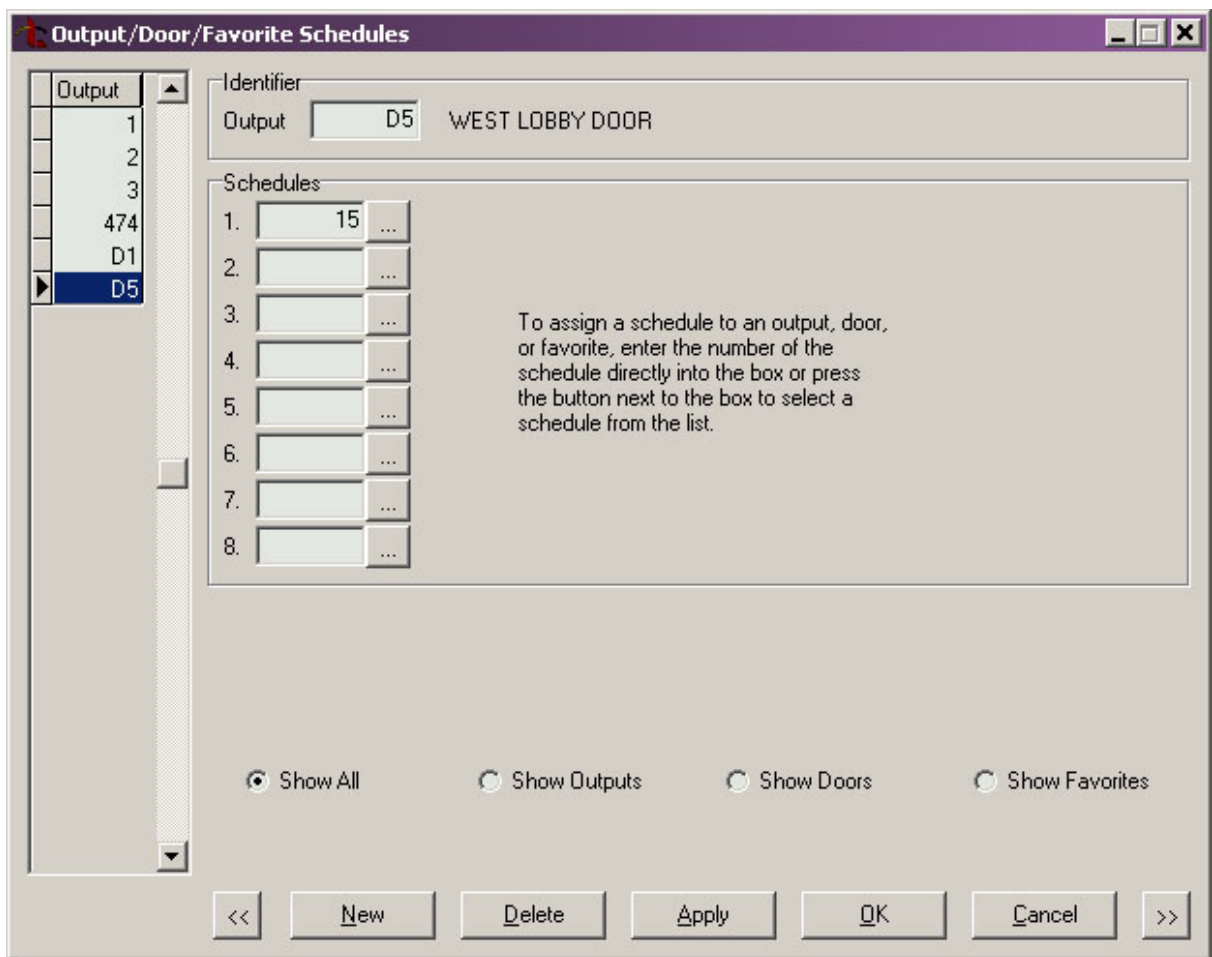
Holiday Schedules: Three Holiday Schedules are available. This allows an output, area, or door to have three different schedules for holidays. For example, Holiday Schedule A for those holidays when the building stays closed, Holiday Schedule B for a day that only opens for a morning, etc. Also, Holiday 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.

Program > Output Schedules

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.

To program door schedules, enter D and a device address number.

XR500 Series or XR2500F - select D01 to D16

XR100 Series - select D01 to D8

> **Note:** Door schedules are available on the XR500 Series, XR2500F, XR100 Series. All other panels program output schedules using output numbers only.

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:** XR500 Series panel and XR200-485 Enhanced only. You may enter the opening and closing times for three holidays (A, B, and C) as designated in Program > Holiday Dates. Holiday programming supercedes all other schedule programming.

Program > Favorite Schedules
XT30, XT50, XTL, XTLN, and XTLN-WiFi panels

Favorite Schedules allow you to set the times when your favorites connected to your system turn on and off automatically.

Favorite: Enter the favorite number (F1-F20) that you wish to assign a schedule.

Schedule:

    1. Select the day 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.

New: Select New to enter another Favorite Schedule. You can enter up to 7 schedules per favorite number.

Apply: Select Apply after entering the schedule to save.

Program > 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. 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 XR100/XR500 and XR150/XR350/XR550 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 XR150/XR350/XR550 Series, XR500 Series and XR2500F version 110 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 XR550 Series, XR500 Series or XR2500F

Areas 1 to 16 for XR350 Series

Areas 1 to 8 for XR150 Series, 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 in Programming Menu for more information.

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:** Always be sure that at least one administrator code in your system has a profile with all authorities and all areas.

Shifts (1 - 4) (XR150/XR350/XR550 Series panels): Check the box for each shift where you want to authorize access for this profile.

Schedules (XR150/XR350/XR550 Series panels): Enter each Schedule number you want to authorize access for this profile, up to 8 Schedules per profile.

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: 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.

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 720 minutes to allow the loading dock supervisor to load or unload a semi-truck.

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 (XR150/XR350/XR550): 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:** The Card Plus PIN option is only available on Area Systems.

Use this Profile Record to assist you when planning and programming an XR150/XR350/XR550 Series or XR100/XR500 Series system.

> **Note:** On XR150/XR350/XR550 Series and XR500 and XR100 Series panels configured for All/Perimeter or Home/Sleep/ Away operation use the default Profiles 1 to 10. For Home/Sleep/

Menu			Privilege	Number											
				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.

Program > User Codes>Panel Tab

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 and that user's code information, select the user from the list on the left side of the window and click on the Delete button at the bottom of the window.

To add a new user, click on the New button 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 XR200 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 passcode that you want to assign to this user. If you are using the Admin 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 Admin Reader feature, do not manually enter the User Code. Refer to Scanning Proximity Cards on page 121.
- User codes cannot begin with a 0 (zero). Three-digit codes cannot begin with 98.
- On XT30, XT50, XTL, XTLN, XTLN-WiFi, XRSuper6, XR20, and XR40 panels you can enter 4-digit User Codes.

- On XR200, XR200-485(B) panels you can enter from 3-digit to 5-digit User Codes.
- On XR2500F panels beginning with version 107 and XR100/XR500 Series, you can enter 3-digit to 6-digit User Codes. Previous XR2500F and 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.
- 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 and XR150/XR350/XR550 Series panels configured for All/Perimeter, Home/Sleep/Away or Home/Sleep/Away with Guest operation, only allow a 4-digit User Code.

Random (Not available on XRSuper6): Press the Random button to assign a random number to the User Codes 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 (XR2500F, XR100/XR500 Series, and XR150/XR350/XR550 Series): 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.

User PIN (XR500E and XR150/XR350/XR550 Series): 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 and XR150/XR350/XR550 Series): 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 inport, 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. Click on the links below to view authority levels for each panel type.

> Note: This option does not appear on the XR2500F, XR100/XR500 Series, XR150/XR350/XR550 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>System 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>System Link>Custom Fields Tab.

1512, 1812, and 1912 - The first digit of the five digit user code assigns the authority level. For example, the user code 12345 has a level 1 authority and the user code 92345 has a level 9 authority.

Level: Choose one of three 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.

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.

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.

Level: Choose level number 1 to 9 from the drop-down menu for pre-assigned authority levels.

Choose **Custom** from the drop-down menu to customize the functions you want the user to access. This allows users to have certain capabilities outside of a standard authority level. After choosing Custom, the user code authority checkboxes become active. Check the options you wish to assign to the user.

Choose **Temporary Custom** from the drop-down menu to assign this as a temporary code. Temporary codes expire in seven days.

Program > User Codes

To copy a user and the user code information to another partition or 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 Partition

In the User Codes window, select the user to be copied from the list on the left-hand side. Click the Copy button. Click the Paste button. This will automatically paste the user into the panel, allowing you to then change the Partition number

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 XR40 Command Processor™ Panel, the second panel must be an XR40.

In the User Codes window, select the user to be copied from the list on the left-hand side. Click the Copy button.

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 click the Paste button. This will paste all of the user code information you copied from the first panel into the second panel.

Program > 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.
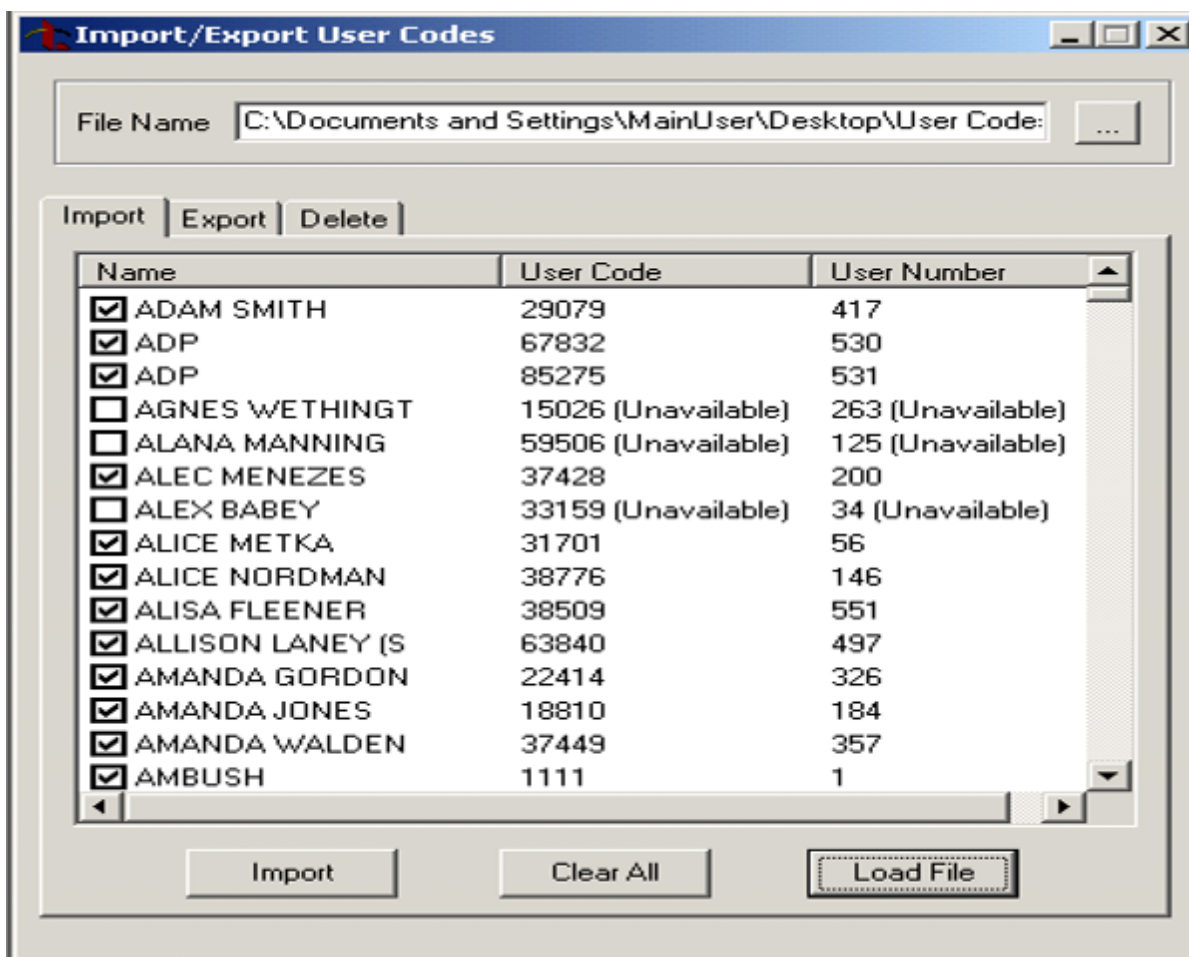
Import User Codes

To import User Codes, click on the Import tab. In the File Name field, select the Tab Delimited .txt file containing the user codes to import.

> **Note:** System 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.

System 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).

Click 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.

Click Import to add selected user codes to the panel.
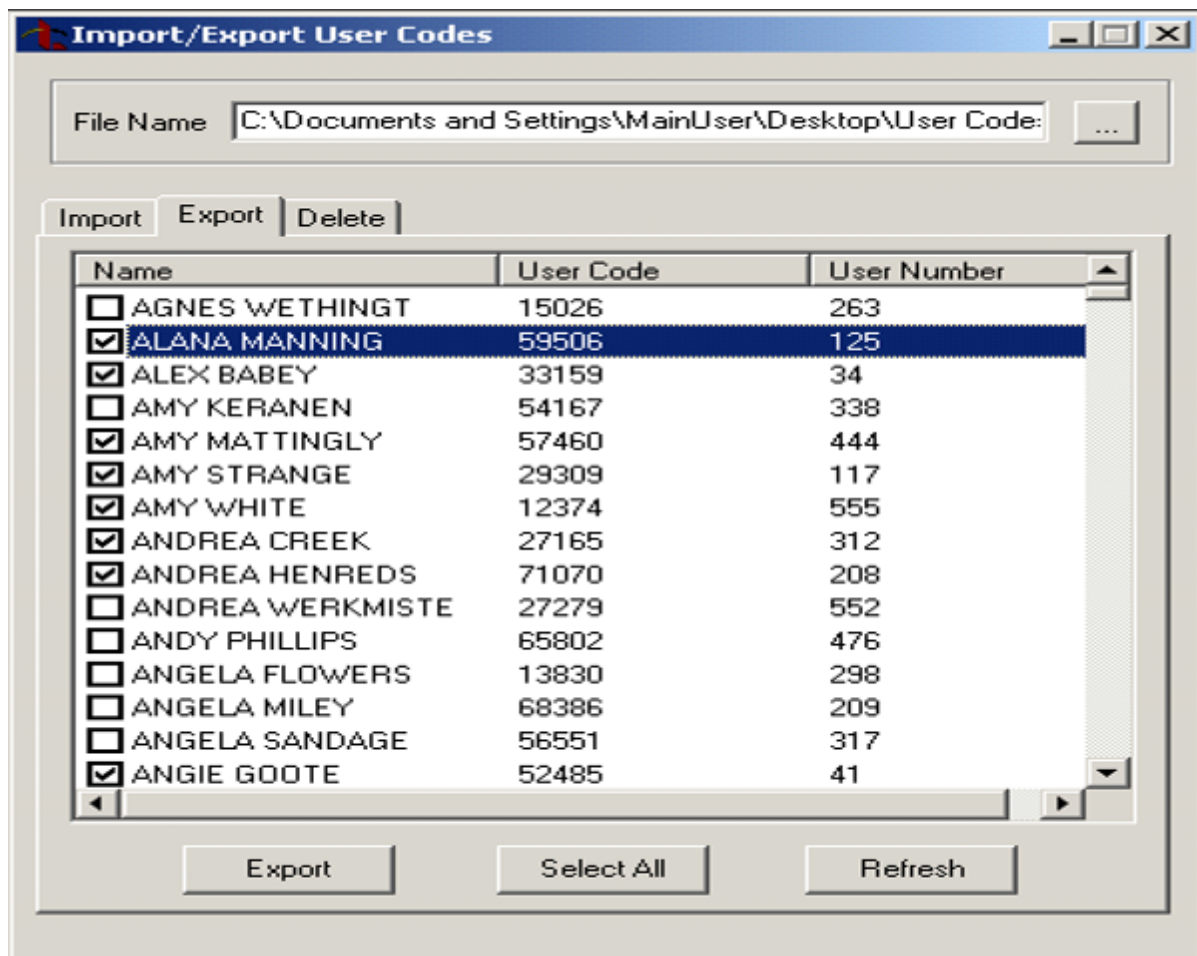
Export User Codes

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. Click on the check box next to the user code to export or Select All. When selection is complete, click Export.

> **Note:** The description field is not exported.
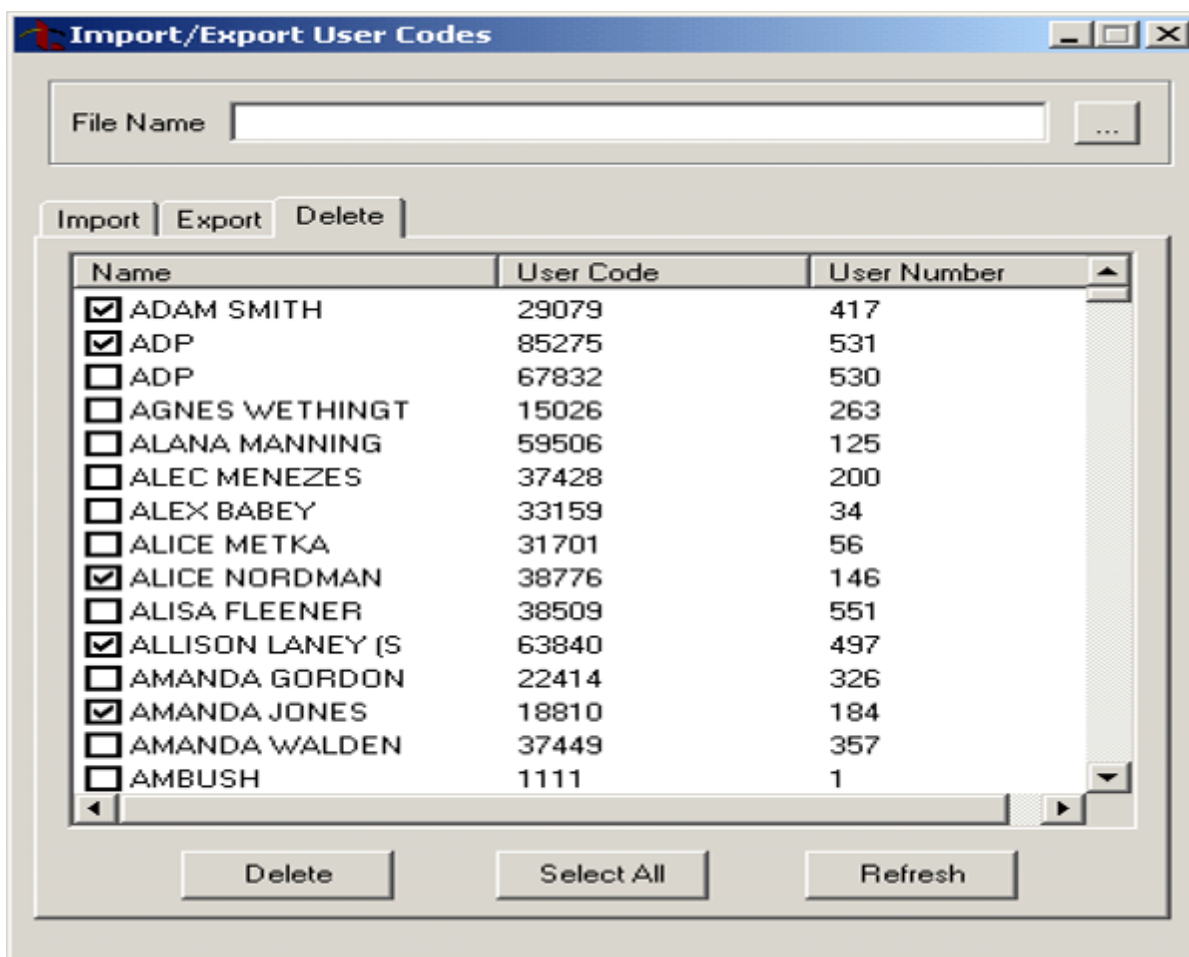
Delete User Codes

To delete User Codes from the panel file, select the Delete tab.

Click on the check box next to the user code to delete, or Select All. When selection is complete, click Delete.

Program > User Codes

Using an Admin Reader USB 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 Admin Reader USB. After properly connecting the Admin Reader USB to a COM port on your computer, go to System > Configure > System Link and select the Other Tab. Refer to Admin Reader for information on configuring System Link for the Admin Reader USB.

To enter a User Code using the Admin Reader 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 Admin Reader USB. The Admin Reader USB will automatically assign the card's code as the user's code. You can also use the Admin Reader USB when changing a user code.

System > Alarm List

 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 System Link before viewing and acknowledging any messages.
>
> With System Link, you have the ability to monitor multiple accounts from one Alarm List window. You can view the Alarm List while other System 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. System Link automatically closes the Alarm List after all messages have been acknowledged.

If an operator is not logged on when an alarm is received, System 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.

Alarm List Description

Organization of the Alarm messages

General Information

Location Information

Visible Alarms

Extended Information

Command Buttons

System > Alarm List

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 resize 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 clicking 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: System Link receives the time and date from the Windows Operating System. If a site

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.

System > Alarm List

When alarm and trouble messages are received, System 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.)

System > 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.

System > 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.

System > 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.

System > Alarm List

System Link allows you to view three different lists of messages:
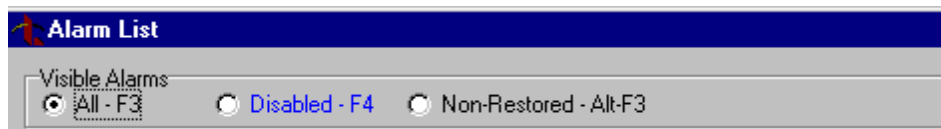
All - F3: View all messages, both acknowledged and unacknowledged. This is the standard Alarm List. Disabled messages do not display in the Alarm List.

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.

System > Alarm List

Six command buttons are provided so the operators can easily and quickly manage multiple signals.
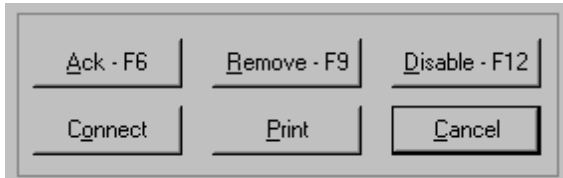
Ack - F6: Press to acknowledge the selected alarm and silence the alert tone.

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.

System > Alarm List

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 System 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

© 2014 Digital Monitoring Products

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.

System > Alarm List

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.

System > Alarm List

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.

System > 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.

System > 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 System 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.

System > Alarm List > Print

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: Click on this button to enter the printer setup window to configure your print options.
- Preview: Click 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: Click this button to print the account reports to an attached printer.

(Must have Alarm Monitoring Module to Use)

The sophisticated Alarm Monitoring Module expands the capabilities of the Alarm List present in

System 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 System Link.

Contact your dealer or visit http://www.dmp.com for more information about this product.

(Must have Alarm Monitoring Module to Use)
System > Alarm List

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 System Link before viewing and acknowledging any messages.

With System Link, you have the ability to monitor multiple accounts from one Alarm List window. You can view the Alarm List while other System 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, System 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. System 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, System 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.

Alarm List Description
Organization of the Alarm messages
General Information
Location Information
Extended Information
Visible Alarms
Command Buttons

(Must have Alarm Monitoring Module to Use)
System > Alarm List

The Alarm Monitoring Module expands the capability of the Alarm List already in System 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 System 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 System Link, if selecting File > Print > Events as described above.
- Date: Click the arrow to the right of the field to open the drop-down calendar, as shown above. Click on 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.

(Must have Alarm Monitoring Module to Use)
System > Alarm List

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: Click on this button to enter the printer setup window to configure your print options.
- Preview: Click 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: Click this button to print the account reports to an attached printer.

(Must have Command Center Module to Use)

System > Alarm Grid

The sophisticated Command Center Visual Alarm Command and Control Software expands the capabilities of the Alarm List present in System 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 click on 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 clicking on the Ack button. 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 System Link.

Contact your dealer or visit http://www.dmp.com for more information about this new product.

(Must have Command Center Module to Use)

System > 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. Click 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.)

(Must have Command Center Module to Use)

System > Alarm Grid

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.

(Must have Command Center Module to Use)

System > 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.

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

The segment remains the designated color until it is acknowledged in the Alarm List window.

(Must have Command Center Module to Use)
System > Alarm Grid

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 System 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, click once in 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.

(Must have Command Center Module to Use)
System > Alarm Grid

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.

(Must have Command Center Module to Use)
System > Alarm Grid

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.

(Must have Command Center Module to Use)
System > Alarm Grid

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 > System 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.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports

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 XR200 (version 111 and above), XR2400F (version 111 and above), and the XR200-485 (version 205 and above) Command Processor™ 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.

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 System Link Configuration. See the Advanced Reporting User's Guide (LT-0645) for more information.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports

The Advanced Reporting module can be used with the following panels that allow you to Request Events:

- XR200
- XR200-485
- XR2400F
- XR40
- XR20
- XRSUPER6
- 1912
- 1912XR
- 1512

You can also use the Advanced Reporting module with the XR200 (version 111 and above), XR2400F (version 111 and above), and the XR200-485 (version 205 and above) 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 Command Processor™ panels can be used with the Advanced Reporting Module if this method is used.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports

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 System 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.

Establish Direct Connection

To directly connect your alarm panel to the Advanced Reporting Module, connect the network cable from the panel's 462N Network Interface Card to a COM port on the computer running the Advanced

Reporting Module.

Enter all of the necessary information in the Connection[****]Information section of the Panel Information window. Also enter the proper information in the Modules Tab.

If you wish to assign a special identification number for events received over the direct connection, enter a Default Receiver number that will represent events received over the direct connection.

To establish the connection, open the panel in Panel Information. Then go to Panel > Connect and click the Connect button. You are now connected to the panel and ready to monitor the panel for event reports.

Enable Host Monitoring

To connect to a network to monitor for reports, connect the network cable from the panel's 462N Network Interface Card to an iCOM™ Internet Alarm Router or iCOM-E™ High Security Internet Alarm Router which connects to a network. Finally connect the network connection to the computer running the Advanced Reporting Module.

To monitor the network for panel events, enable Host Monitoring in the Modules Tab. Select System > Configure > System Link > Modules Tab and place a check in the Host Monitoring checkbox.

If you wish to assign a special receiver number for events received over the network, enter a Default Receiver number that will represent events received over the Host.

(Must have Advanced Reporting Module to Use)
File > Print > 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 XR200 (version 111 and above), XR2400F (version 111 and above), and the XR200-485 (version 205 and above). 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.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports

The Advanced Reports Setup window allows you to print reports of the alarm message information. Open the Advanced Reports Setup window by clicking File > Print > Events.

Source: Select the source of the reports.

Events: Selects the events sent from an XR200 (version 111 and above), XR2400F (version 111 and above), or an XR200-485 (version 205 and above) that has Host 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 GrantedAll 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. Clicking the arrow opens a calendar as shown in the screen shot. Click 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.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > Zone Action

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.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > Arming/Disarming

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.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > Area Late to Close

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

> Note: Area Late to Close reports will not be generated if Area Schedules is disabled in Partition Information.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > User Codes

Action: Select Added, Changed, or Deleted from the drop-down menu. Select All to generate a report for user code additions, changes, and deletions.

User: Select the user for which you will generate the report. Only users that have performed the user code change selected above will be displayed in the drop-down box. Select All to generate a report for all users who have made changes to user codes.

User Being Changed: Select the user for which you will generate the report. Only users that have been changed will be displayed in the drop-down box. Select All to generate a report for all users than have been changed.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > Door Access Granted

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

Door: Select the door for which you will run the report. Only doors that have granted door access will be displayed. Select All to create a report for all doors that have granted a door access.
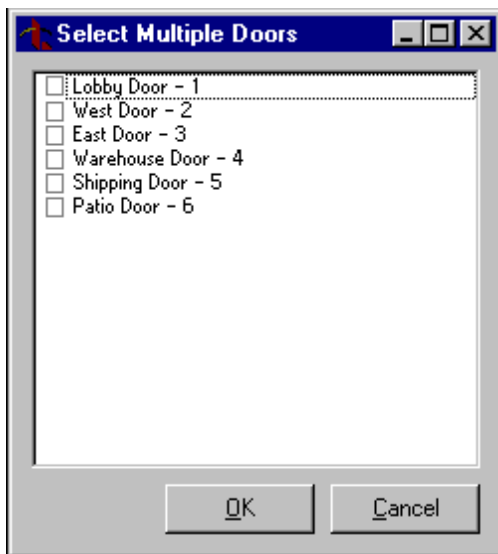
To create a report for multiple doors, select Select Multiple Doors from the drop-down menu. Then press the Select Doors button to open the Select Multiple Doors pop-up window. Click the box to the left of the door name and number to include that door in the report. The report can be created for any combination of doors.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > Door Access Denied

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

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. Click 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.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > Opening / Closing Schedule Changes

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.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > System Monitors

Component: Select the system component for which you will create the report. Select All to include all components in the report.

System Monitor Action: Select the action, trouble or restore, for which you will run the report. Select All to include all System Monitor Actions in the report.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > System Events

Event: Select the event for which you will run the report. Select All to include all events in the report.

Below is a list of all events available:

- Automatic Recall Test
- Unauthorized Entry
- System Late to Close
- Exit Error
- Alarm Bell Silenced
- Dialer Communication Failed
- Abort Message Sent

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

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports > All Events

Selecting All Events for the Report Category will create a report with all of the Report Categories. By default All is selected.

(Must have Advanced Reporting Module to Use)
File > Print > Advanced Reports

While in the preview mode, you may save the reports for printing later or in another application. Click the Save button that looks like a floppy disk. 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)

The DMP 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 DMP panel programming information.

The module also allows the administrator to export all existing DMP 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 your Remote Link and System Link software programs.

System 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:** System Link and SQL Server do not have to be installed on the same machine. Using System 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 System Link.

If System Link is configured to use SQL Server via a DSN and is not able to log in at startup, a login screen will appear:
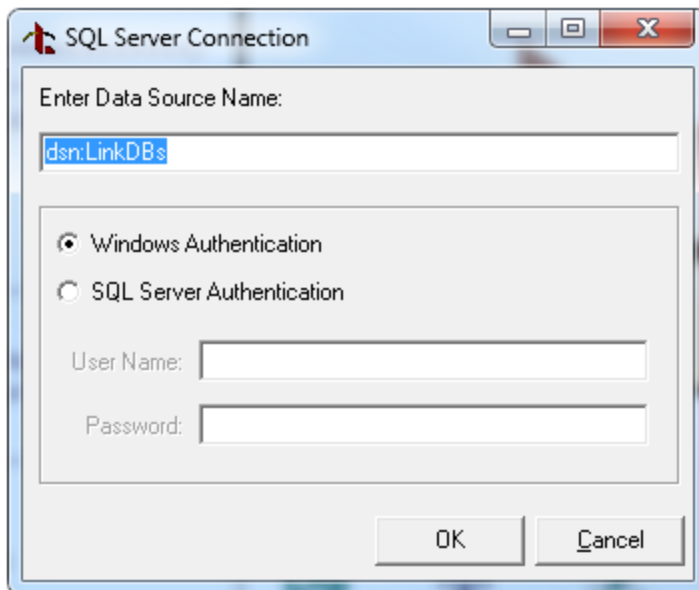
The user should contact the database administrator to find the correct options. If

SQL Server Authentication is chosen, a User Name and Password must be provided. This is the SQL username and password, not the System Link username and password.

The login screen will appear the first time the user runs System 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.

For users of System 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. System 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.

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.

To use Remote Link with Microsoft SQL Server, a ODBC Data Source must be set up on the user's machine.

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.

IMPORTANT: 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

The SQL Server Module allows the administrator to export all existing DMP 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. Click 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.

(Must have Account Groups Module to Use)

File > Account Groups Information

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. 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.

• System Link is not available to perform other operations while batch updates are in process.

• Compatible DMP Command Processor™ Panels

The Account Groups module can be used with the following panels:

    - version 108 or higher:

- XR500N
- XR500E
- XR2500F

    - all versions:

- XR100N
- XR150N
- XR350N
- XR550E
- XR550N

(Must have Account Groups Module to Use)

File > Account Groups Information

To update, change, or delete an account group, open the Account Groups window by clicking File > Account Group Information.
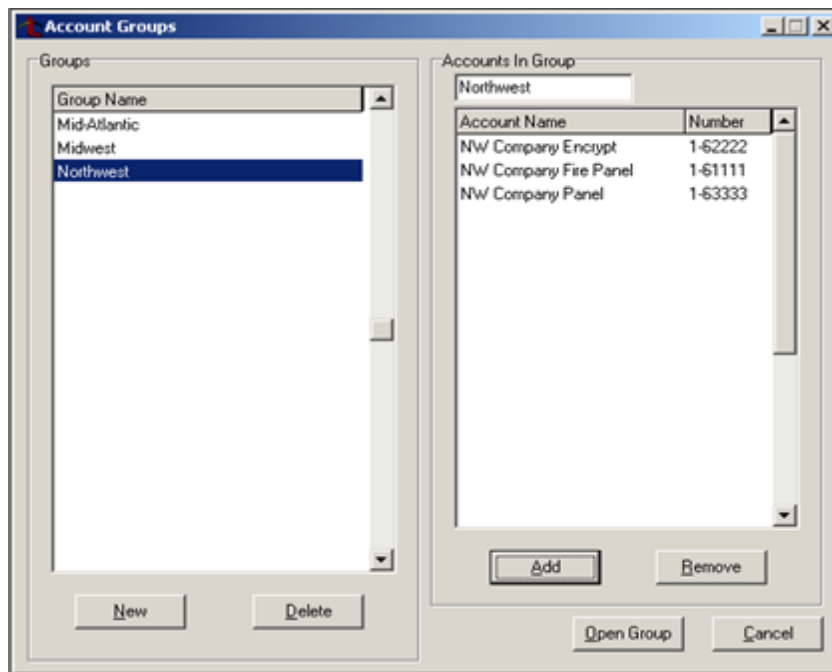
The window is divided into two sections. The left section, KGroups, lists the group names currently stored in the database and the New and Delete buttons. The right section, KAccounts in Group, lists the panel account names and numbers and the Add, Remove, Open Group, and Cancel buttons.

Only valid, 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. Click on the account to add to the group and press the Add button.

Remove: Allows you to delete an account from the group.

Open Group: 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 System Link or System Link in the display above the menu bar.**

Cancel: Exits the Account Groups window.
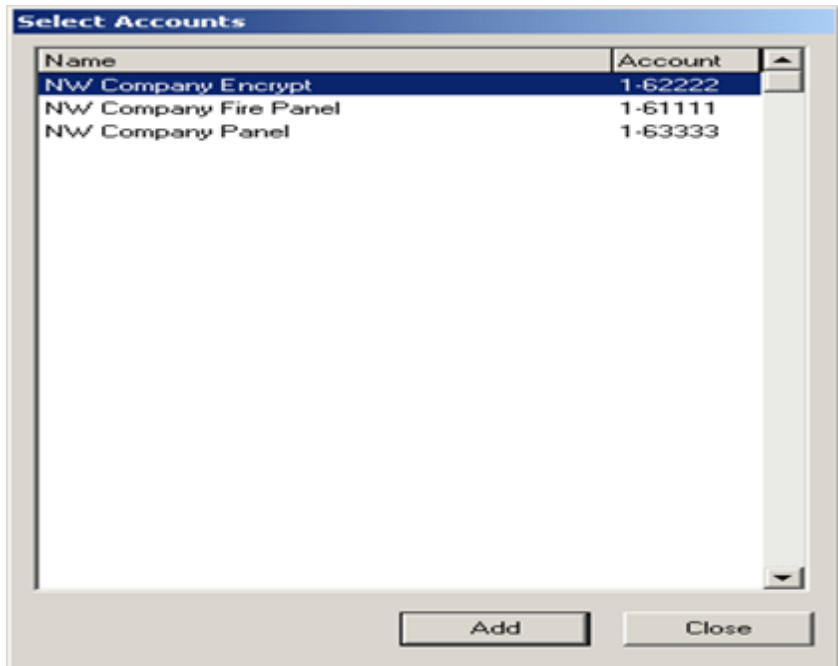
(Must have Account Groups Module to Use)

Program>Holiday Dates
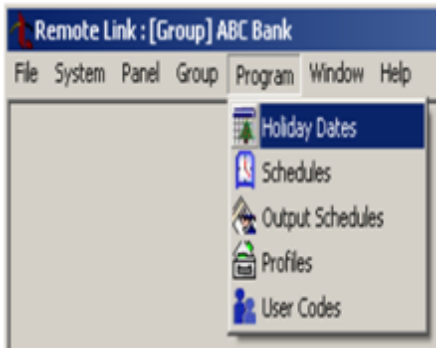
The Holiday Dates window allows you to enter dates that are used by the Holiday Schedules to override daily schedules.

To program Holiday Dates for a group, the group must first be opened or created. The currently opened group displays next to System Link or System 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.

- To add a new Holiday Date, click on the New button and enter information in each field. To accept the added information, click on the Apply button at the bottom of the window.
- To delete a Holiday Date, select the event from the list on the left side of the window and click on the Delete button 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.

(Must have Account Groups Module to Use)

Program>Output Schedules
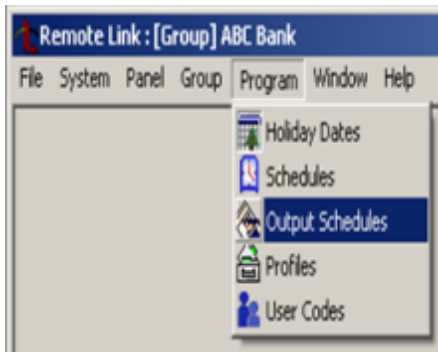
Output Schedules allow you to set the times when relay outputs connected to your system turn on and off automatically.

To program Output Schedules for a group, the group must first be opened or created. The currently opened group displays next to System Link or System 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, click on the New button and enter information in each field. To accept the added information, click on the Apply button 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 click on the Delete button 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.

- XR500 Series or XR2500F - select D01 to D16
- 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.

(Must have Account Groups Module to Use)
Program>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 System Link or System 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, click on the New button and enter information in each field. To accept the added information, click on the Apply button at the bottom of the window.
- To delete a Profile, select the schedule from the list on the left side of the window and click on

the Delete button 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 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 XR500 Series and XR2500F version 110 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 XR500 Series or XR2500F
- Areas 1 to 8 for 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 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.

(Must have Account Groups Module to Use)
Program>Schedules
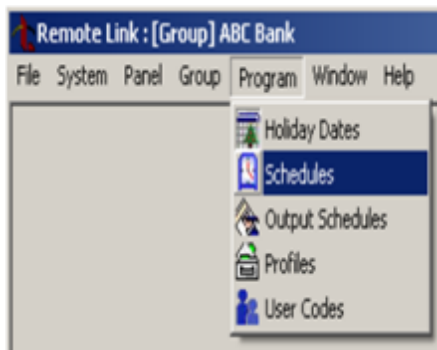
The Schedules window allows you to schedule auto arming and disarming of individual areas.

To program Schedules for a group, the group must first be opened or created. The currently opened group displays next to System Link or System 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, click on the New button and enter information in each field. To accept the added information, click on the Apply button at the bottom of the window.
- To delete a Schedule, select the schedule from the list on the left side of the window and click on the Delete button 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.

(Must have Account Groups Module to Use)
Program>User Codes
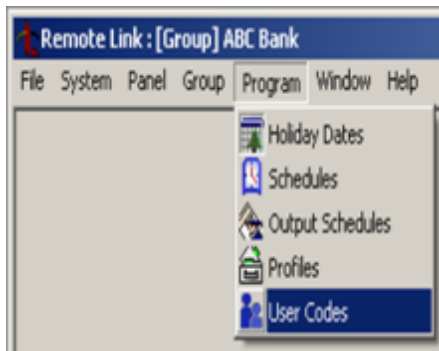
To program User Codes for a group, the group must first be opened or created. The currently opened group displays next to System Link in the display above the menu bar. The Program>User Codes window allows you to enter or make changes to the user code information in the group database file.

To add a new user, click on the New button and enter information in each field. To accept the added information, click on the Apply button 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 click on the Delete button at the bottom of the window.
- To sort user codes, click on the desired method in the title bar: For example, if you wish to sort the user codes alphabetically, click on 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.

(Must have Account Groups Module to Use)

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

In the User Codes window, select one User to be copied from the list on the left-hand side. Click the Copy button.

Click the Paste button 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.

In the User Codes window, select one User to be copied from the list on the left-hand side. Click the Copy button.

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.

Select Program > User Codes and click the Paste button. This pastes all of the user code information you copied from the first panel or group into the second panel or group.

(Must have Account Groups Module to Use)

Open the group from the File > Account Groups window before sending any program information to a group. The currently opened group displays next to System 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. System Link or System 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 System Link or System 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
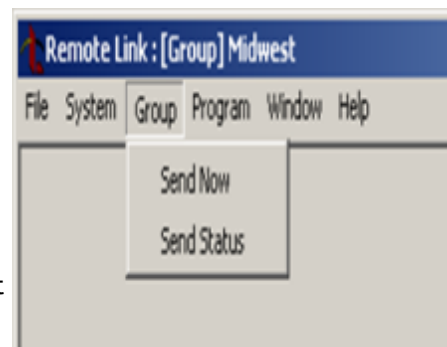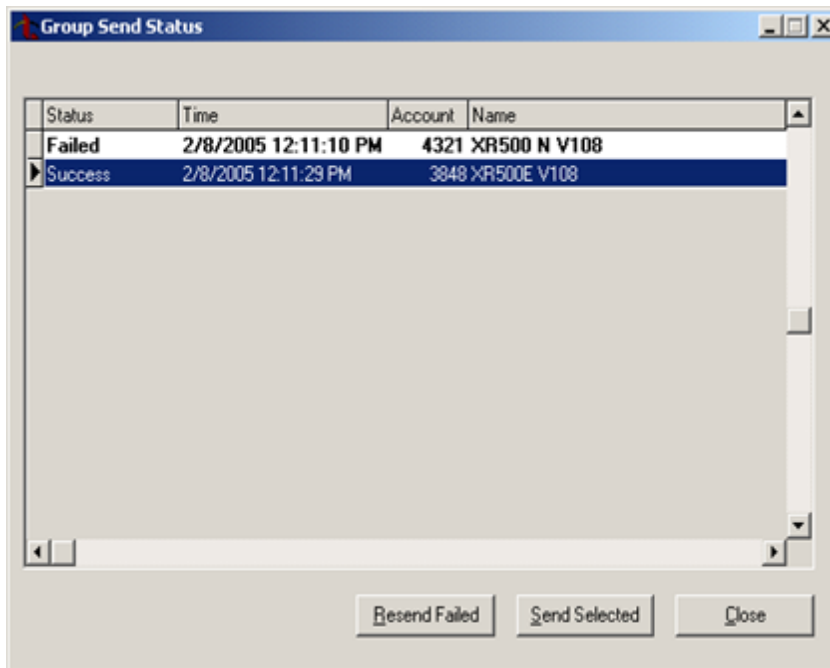
The Group Send Status window displays a list of the panels System Link attempted to connect to when the group send process was started. Any communications that fail are listed first.

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.

Q. How do I make the SCS-105 receiver dial DTMF?

A. In the System > Configure > System Link window, click on 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.

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.

Q. Is System Link compatible with Windows 3.1?

A. No. System Link is designed to work with Windows 95, 98, 2000, NT, and XP.

Q. I just installed System Link. Now what do I do?

A. You first need to log in and configure the System Link program. See System Link Configuration for more information.

Q. What do I need to do for normal maintenance on my System 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. There are also utilities available on your system such as SCANDISK and DEFRAG that should be used regularly.

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.

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.

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.

Q. What is the default Log on user name and password?

A. New

Q. Where do I enter Closing Code, Area Schedules, and other Area Information options?

A. From the Area Information window, click on the Partition Info button on the lower left side of the screen. This is where you program items that affect the entire partition.

Q. I've logged on to System 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.

Q. A new panel will not stay on-line with System 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. See the note in the Connect section of this help file for detailed instructions.

4-2 Communication definition - 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.

"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 on-board 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.

"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.

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 a DMP 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 on-board 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.

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.

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.

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.

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.

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.

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.

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 DMP System 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.

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.

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.

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.

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.

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 a DMP 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.

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 System 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 on-board 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.

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 DMP 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.

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.

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.

volt/amp (VA) rating - the products of rated input voltage multiplied by the rated current. This establishes the apparent energy available to accomplish work.

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.

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 retard - a false alarm reduction feature that allows fire, supervisory, auxiliary one, and auxiliary two zones to be programmed to delay from one to 250 seconds. If the zone remains shorted for the entire length of the zone retard delay time an alarm is initiated.

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.

The following keys on the keyboard can be used in a window or a full screen when you are in the System Link program.

Press To

F1 Display Context-sensitive Help

Alt + F10 Display Diagnostics window

F11 Display Log On / Off window

Ctrl + Tab Switch between System Link windows

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.

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.

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 -

- A -

- B -

- C -

- D -

- E -