Hints for use:

- **When viewing in a web browser**, hit F11 to toggle full screen mode.
- Use the bookmarks panel or table of contents to jump to the desired topic. Each page header has a quick link Tab to the table of contents, and a quick link Tab to the list of AlarmNet tasks.
- **When viewing on mobile devices**, use the table of contents to jump to the desired topic. You may also use the page header quick links.
# Table of Contents

Overview ............................................................................................................................................................................ 1

What’s New? ...................................................................................................................................................................... 1

Accessing AlarmNet 360 ............................................................................................................................................... 1

Obtaining a Central Station Account.................................................................................................................................................. 1

Obtaining a Dealer Account ............................................................................................................................................................... 1

Logging In .......................................................................................................................................................................................... 2

Navigating AlarmNet 360 .................................................................................................................................................................. 2

Finding the right AlarmNet tool ....................................................................................................................................................... 4

Tools .................................................................................................................................................................................... 6

DEVICES ▶ Device Status (central station) ........................................................................................................................................ 6

DEVICES ▶ Device History (central station) ....................................................................................................................................... 8

DEVICES ▶ SIM Activation / Status (central station and dealer) ....................................................................................................... 8

DEVICES ▶ Substitution PIN Generation (central station) .............................................................................................................. 10

ACCOUNTS ▶ View Accounts (central station) ................................................................................................................................ 10

AlarmNet Service Types ....................................................................................................................................................................... 12

ACCOUNTS ▶ Communication Failures (central station) ..................................................................................................................... 14

ACCOUNTS ▶ Account Generation (central station) ....................................................................................................................... 16

ACCOUNTS ▶ Account Cancellation (central station) ...................................................................................................................... 17

Creating Batch Files for Multiple Account Cancellations ..................................................................................................................... 18

ACCOUNTS ▶ Coverage Maps (central station and dealer) ............................................................................................................. 19

MY COMPANY ▶ My Profile (central station and dealer) ................................................................................................................ 19

MY COMPANY ▶ Manage Users (central station and dealer) ........................................................................................................... 19

User Authority Levels ........................................................................................................................................................................... 20

Adding a user ........................................................................................................................................................................................ 21

Editing a user ........................................................................................................................................................................................ 22

MY COMPANY ▶ Dealer Services Config (central station) ............................................................................................................. 24

MY COMPANY ▶ My History (central station and dealer) ................................................................................................................ 25

MY COMPANY ▶ Web Usage (central station) ............................................................................................................................... 25

MY COMPANY ▶ Company Information (central station super users, and dealer managers) ................................................................. 27
Overview

This guide explains how to use the **AlarmNet 360** online web application. AlarmNet 360 is a web based tool set for central station and dealer/installation companies to enable programming and testing of their AlarmNet communication devices and to create remote access service accounts. These tasks are easily accomplished from any PC with internet access. AlarmNet 360 enables you to perform the following:

- Search, display, and edit customer accounts.
- Add, delete, or replace communication devices, IP video, and automation devices.
- Display communication device types, their MAC IDs, and edit device information.
- Program, configure, test, and verify the status of devices.
- View, add, delete and edit user profiles.
- View a history of all AlarmNet 360 activity by company users.
- Create Total Connect accounts for your customers.
- Enables you to email AlarmNet 360 with questions or comments.

What’s New?

Reports

Accessing AlarmNet 360

Obtaining a Central Station Account

Central Stations can sign up by contacting AlarmNet Administration at 800-222-6525 and selecting option 3. (Administration hours are Monday thru Friday, 8:00 am to 5:00 pm ET)

Obtaining a Dealer Account

Dealers must sign up online by visiting the AlarmNet 360 website:

https://www.alarmnet360.com

Then simply complete the Dealer Signup procedure to obtain your User Name and Password. For validation purposes you will need to provide a city and central station ID number and have the MAC and CRC number from one of your communication devices. If you do not know your AlarmNet city and central station ID number, please call your central station.

---

This information is also available on the product box.
Only one sign-up per dealer is necessary; additional log in accounts for dealer personnel must be created by the initial user. Lastly you need a computer with internet access and a web browser.

Logging In

1. To access AlarmNet 360 visit the following link: https://www.alarmnet360.com

   After the page loads this is a good time to create a desktop or favorites bar shortcut by positioning the cursor over the address icon, left click the mouse and drag it to the desktop or favorites bar.

2. Navigate to the AlarmNet 360 home page using either the desktop shortcut (created in the last step) or by typing the address into the browser's address field. The Login page appears.

3. Enter your **User Name**, and **Password** then press **[Login]**. The Device Status window appears.

   **Note:** You can change the default landing page using the **My Company > My Profile** option.

4. Click on the **Browser Requirements** and ensure your browser meets the requirements.

Navigating AlarmNet 360

AlarmNet 360 is easy to navigate. Navigation starts with the **Tool Bar** at the top.

The AlarmNet 360 site is used by both the **Central Station** and **Dealers**.

**Note:** Since the Central Station has access to everything the Dealer has access to; tools such as **Take Ownership of Device** can also be used by the Central Station.
Further, each Central Station or Dealer can create subusers and assign Authority Levels and Features to their subusers. (See the "Manage Users" tool.)

At the tool bar, selecting a category brings up the associated tools. When a tool is selected, an information window appears where you can view, edit, add, or delete information. Some information can be printed, or saved as a file.

Central Station Tool Bar

### Devices
- Device Programming
- Device Status
- Device History
- Substitution PIN Generation

### Accounts
- View Accounts
- Communication Failures
- Account Generation
- Account Cancellation
- Manage TC 2.0 Accounts

### My Company
- Company Information
- Dealer Services Config.
- Manage Users
- Web Usage
- My History
- My Profile

### Tools
- Cellular Activation/Status
- Coverage Maps

### Reports
- Generate Reports
- My Dashboard

### Template

### Account Center

### API Documents
Finding the right AlarmNet tool

The AlarmNet 360 website is a collection of tools that enable you to manage communicator devices, accounts, users, check status, activate SIMs, etc.

The revised AlarmNet 360 interface is easy to navigate. It uses tool bar tabs that groups associated tools. For each tool, the workflow has been improved to naturally move you through a series of screens to complete a task.

For instance, programming communication devices is now accomplished using two wizards; Program New Device and Replace Other Device. Each wizard steps you through the proper procedure so the task is done easily and completely.

Below is a table showing various tasks and where the corresponding tool is located. Lastly, the tasks are hot linked, allowing you to jump to the proper help file topic.

**Please use this table as a roadmap for finding the right tool for the task.**

<table>
<thead>
<tr>
<th>Task</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>account, cancellation</td>
<td>Accounts ► Account Cancellation</td>
</tr>
<tr>
<td></td>
<td>Option available only for Central Stations</td>
</tr>
<tr>
<td>Account Center, portal access</td>
<td>Tool Bar ► Account Center (Log in, then refer to the online help)</td>
</tr>
<tr>
<td>accounts, editing</td>
<td>Devices ► Device Programming (Use Action column pulldown menu.)</td>
</tr>
<tr>
<td>accounts, generation</td>
<td>Accounts ► Account Generation Option available only for Central Stations</td>
</tr>
<tr>
<td>account reports, generate</td>
<td>(central station) Tool Bar ► Reports.</td>
</tr>
<tr>
<td></td>
<td>(dealer) Tool Bar ► Reports</td>
</tr>
<tr>
<td>account, view</td>
<td>Accounts ► View Accounts</td>
</tr>
<tr>
<td>automation devices, TUX series, adding</td>
<td>(central station) Accounts ► Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>(use this when adding to an existing</td>
<td>(dealer) Accounts ► Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>system)</td>
<td></td>
</tr>
<tr>
<td>automation devices, TUX series,</td>
<td>Devices ► Device Programming ► Program/Replace Device</td>
</tr>
<tr>
<td>enrolling (use this when TUX will stand</td>
<td></td>
</tr>
<tr>
<td>alone)</td>
<td></td>
</tr>
<tr>
<td>automation devices, TUX series,</td>
<td>Devices ► Device Programming ► Program/Replace Device</td>
</tr>
<tr>
<td>replacing</td>
<td></td>
</tr>
<tr>
<td>AlarmNet billing, payment</td>
<td>Tool Bar ► Account Center (Log in, then refer to the online help)</td>
</tr>
<tr>
<td></td>
<td>Option available only for Central Stations</td>
</tr>
<tr>
<td>API documents, request for cancelling</td>
<td>Tool Bar ► API Documents</td>
</tr>
<tr>
<td>accounts</td>
<td>Accounts ► Account Cancellation</td>
</tr>
<tr>
<td>communication failures</td>
<td>Accounts ► Communication Failures Option available only for Central</td>
</tr>
<tr>
<td>company information, manage</td>
<td>Company Information Option available only for Central Stations</td>
</tr>
<tr>
<td>coverage maps</td>
<td>(central station) Utilities ► Coverage Maps</td>
</tr>
<tr>
<td></td>
<td>(dealer) Utilities ► Coverage Maps</td>
</tr>
<tr>
<td>customer notifications</td>
<td>Tool Bar ► Customer Notification</td>
</tr>
<tr>
<td>dealer services, enable remote &amp; video</td>
<td>My Company ► Dealer Services Config. Option available only for Central</td>
</tr>
<tr>
<td>serv.</td>
<td></td>
</tr>
<tr>
<td>device, history</td>
<td>Devices ► Device History</td>
</tr>
<tr>
<td>device, program new</td>
<td>Devices ► Device Programming ► Program/ Replace Device</td>
</tr>
<tr>
<td>device, replace</td>
<td>Devices ► Device Programming ► Program/ Replace Device</td>
</tr>
<tr>
<td>device, show programmed devices</td>
<td>Devices ► Device Programming</td>
</tr>
<tr>
<td>device, status</td>
<td>Devices ► Device Status</td>
</tr>
<tr>
<td>device, substitution PIN generation</td>
<td>Devices ► Substitution PIN Generation Option available only for Central</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 4 -
<table>
<thead>
<tr>
<th>Task</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
<td><strong>Location</strong></td>
</tr>
<tr>
<td>device, take ownership</td>
<td>(central station) Devices ▶ Device Programming, then at the blue tool bar, select Take Ownership.</td>
</tr>
<tr>
<td></td>
<td>(dealer) Devices ▶ Device Programming ▶ Take Ownership</td>
</tr>
<tr>
<td>editing, account</td>
<td>Devices ▶ Device Programming</td>
</tr>
<tr>
<td>IP devices (TC1), adding, editing, deleting</td>
<td>Devices ▶ Device Programming</td>
</tr>
<tr>
<td>IP devices (TC2), adding, editing, deleting</td>
<td>(central station) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td></td>
<td>(dealer) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>notifications, customer</td>
<td>Tool Bar ▶ Customer Notification</td>
</tr>
<tr>
<td>ownership of device, task</td>
<td>(central station) Devices ▶ Device Programming ▶ Take Ownership.</td>
</tr>
<tr>
<td></td>
<td>(dealer) Devices ▶ Device Programming ▶ Take Ownership</td>
</tr>
<tr>
<td>PIN generation, substitution</td>
<td>Devices ▶ Substitution PIN Generation</td>
</tr>
<tr>
<td>program new device</td>
<td>Option available only for Central Stations</td>
</tr>
<tr>
<td>reports, account, generate</td>
<td>(central station) Tool Bar ▶ Reports.</td>
</tr>
<tr>
<td></td>
<td>(dealer) Tool Bar ▶ Reports</td>
</tr>
<tr>
<td>resetting the TC2 account username, email or password</td>
<td>(central station) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td></td>
<td>(dealer) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>SIM, activation/status</td>
<td>Utilities ▶ SIM Activation/Status</td>
</tr>
<tr>
<td>TC1 account, edit, delete</td>
<td>Devices ▶ Device Programming</td>
</tr>
<tr>
<td></td>
<td>(Use Action column pulldown menu.)</td>
</tr>
<tr>
<td>TC2 accounts, manage, edit, delete</td>
<td>(central station) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td></td>
<td>(dealer) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>TC2 accounts, reset username, email or password</td>
<td>(central station) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td></td>
<td>(dealer) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>TUX series automation devices, adding</td>
<td>(central station) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>(use this when adding to an existing system)</td>
<td>(dealer) Accounts ▶ Manage TC 2.0 Accounts</td>
</tr>
<tr>
<td>TUX series automation devices, enrolling</td>
<td>Devices ▶ Device Programming ▶ Program/ Replace Device</td>
</tr>
<tr>
<td>(use this when TUX will stand alone)</td>
<td></td>
</tr>
<tr>
<td>TUX series automation devices, replacing</td>
<td>Devices ▶ Device Programming ▶ Program/ Replace Device</td>
</tr>
<tr>
<td>users, manage</td>
<td>My Company ▶ Manage Users</td>
</tr>
<tr>
<td>users, my history</td>
<td>My Company ▶ My History</td>
</tr>
<tr>
<td>users, my profile</td>
<td>My Company ▶ My Profile</td>
</tr>
<tr>
<td>users, web usage</td>
<td>My Company ▶ Web Usage</td>
</tr>
<tr>
<td>video device configuration</td>
<td>Devices ▶ Device Programming</td>
</tr>
<tr>
<td>(use to configure TC1 or TC2 devices)</td>
<td></td>
</tr>
</tbody>
</table>
Tools

Each tool will be discussed in the order they appear on the Tool Bar.

DEVICES ▶ Device Status (central station)

This tool enables you to quickly check the status of a particular AlarmNet communication device.

Find the device by performing a search. You can search by entering the City code, Central Station and Subscriber number, or you can search by MAC. Enter the data and click the Search button. A detailed status screen for the device is then displayed.

All detailed information is grouped in subcategories and are described below.

**Current Status of the Device:**
This includes; MAC number, CRC, Device (communication type), Device Type (such as IGSMV4G), and Radio Version.

**Subscriber Status:**
- **New** - The account has not been registered.
- **Active** - The device has been activated in AlarmNet.
- **Partially Cancelled** - The account number is ready for re-use.
- **Full Cancelled** - The account number has been shutoff and cannot be re-used until changed to Partially Cancelled.

**Last Registered Date:** Displays the date and time the account was last registered.

**Supervision:** Indicates the supervision window of the device.
For example:

| US UL LINE SEC | [5 minute supervision] | WEEKLY | [7 day supervision] |
| CN UL LINE SEC | [3 minute supervision]  | MONTHLY | [30 day supervision] |
| DAILY          | [24 Hour supervision]  | NO SUPERVISION |

**Last Status Check IN:** Last Date and Time the device checked in.

**Next Status Check IN:** Next scheduled check-in Date and Time.

**Current State:** Shows the condition of the Subscriber. NORMAL, or COMM FAIL [Communication Failure]

**Ping Commands:** These commands will depend on the device. This drop-down field allows you to send a command to a GSM type device. [Commands marked with ** are limited to; 2 every 24hrs per account.] After making your choice, click **Ping**.

- **QOS (Status)** - Sends a command to have the GMS device report QOS status. (GSM type devices only.)
- **Test Alarm** - Sends a command forcing the device to send a test message of 555555559 to the central station. (Devices with Ethernet and GSM: it will try Ethernet first. If Ethernet is not available, it will try GSM.)
- **Test Alarm (Wired Ethernet)*** - Sends a command using the Ethernet to force the device to respond with a test message of 555555559 to be delivered to the central station. (For Internet devices only.)
- **Test Alarm (Cell)*** - Sends a command using GSM to force the device to respond with a test message of 555555559 to be delivered to the central station. (For GSM devices only.)
- **Register** - This command appears for certain users only. It forces the device to register or re-register on the AlarmNet Network. (For GSM Devices only.)
- **Reset** - This command appears for certain users only. It forces the device to reset and power up. A 5551 5555 6 will be sent to the central station. (For GSM devices only.)

**Current Status of SIM**

The basic information associated with the SIM. Its history can be accessed by clicking the “View SIM History” button.

**Subscriber Address Information**

The basic information associated with the subscriber and device location. This information can be edited by clicking the “Edit Subscriber” button.

**Sticky Notes**

Enables you to attach notes to this device or user as needed.

**Alarm History**

Displays the Alarms from the device and gives the ability to download the last 30 days of information if needed.
QOS Data (Quality of Service)

Shows basic information about the signal levels and input voltages of the device. (only available on AlarmNet GSM type devices.)

<table>
<thead>
<tr>
<th>Network</th>
<th>Good</th>
<th>OK</th>
<th>Marginal</th>
<th>Bad</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G</td>
<td>-20 dBm to -89 dBm</td>
<td>-90 dBm to -98 dBm</td>
<td>-99 dBm to -104 dBm</td>
<td>-105 dBm and under</td>
</tr>
<tr>
<td>3G / 4G</td>
<td>-20 dBm to -90 dBm</td>
<td>-91 dBm to -100 dBm</td>
<td>-101 dBm to -106 dBm</td>
<td>-107 dBm and under</td>
</tr>
</tbody>
</table>

**Received on (GMT)** - The date and time that the quality of service message came into the node. It is expressed as month/day/year and hour: minutes: seconds. The time is based on Greenwich Mean Time and is displayed in 24-hour military time.

**Line (V)** - This quantity represents the instantaneous DC voltage within the radio after the input power has been rectified; we are not measuring the voltage at the input terminals. This quantity is dependent on which wall transformer is used but is typically between 10.5 and 26 volts.

  - AC input: The QOS voltage will be approximately 1.414 times the input voltage.
  - DC input: The QOS voltage will be approximately the same as the input voltage.

**Battery (V)** - This quantity represents the voltage of the battery backup in the device at the instant the QOS data was sent. This quantity expresses an under load value that should reside above 6.0 volts to be considered normal.

**Net.** - Indicates the communication network used.

**Receiver Level** - The instantaneous relative level of the strength of the signal at the receiver at the time the data was transmitted. (Range: –150dBm to –10dBm, stronger)

**Min Signal** - The lowest relative level of the strength of the signal at the receiver since the last check in message was transmitted. (Range: –150dBm to –10dBm, stronger)

**Max Signal** - The highest relative level of the strength of the signal at the receiver since the last check in message was transmitted. (Range: –150dBm to –10dBm, stronger)

**DEVICES ➤ Device History (central station)**

This tool is useful when you want the device history. Use the Time Period drop-down menu to choose the range, enter the City-CS-Sub information, and click Search. You can also filter the displayed information using the Action drop-down menu.

**DEVICES ➤ SIM Activation/ Status (central station and dealer)**

This tool enables you to view the status of a SIM (Subscriber Identity Module) for a particular GSM or i-GSM series communication device or to activate the SIM. The SIM must be activated in order for the security system to report to AlarmNet.

Note, the SIM is activated when using the “Utilities” tool presented later in this guide. By default, all the SIMs are pre-activated at the factory.
1. Start by checking if the SIM is already activated.

2. In the MAC or AID field, enter the number. (Choose MAC for a SIM; or choose AID for the VISTA-GSM module used with the VISTA-21iP control panel.) Then click Get Status.

   **NOTE:** The SIMs used in the Canadian modules are all pre-activated.

3. If the SIM is already activated, its Current State will show it as SIM is activated (in green).

4. If the SIM is not activated, under Provision SIM, enter the CRC (or AID), and notification email so AlarmNet can notify you when the SIM is activated. Then click Activate, a confirmation screen appears.

5. When you receive notice the SIM is activated, you will be asked to complete the process by:

   To complete the activation process for mac number (00D02Dxxxxxx) please do the following:
   1) Power-Cycle the device by removing the input power and battery.
   2) Apply input power and plug in the battery.

   To program and register the radio logon to https://www.alarmnet360.com, or use a 7720p programmer, or call AlarmNet Technical Support at 800-222-6525:
   Select 'Technical Support'(Option #1) followed by 'Alarmnet GSM Device Activation/Registration'(Option #1) or for Lynx Touch, use the touch screen 'program radio' screen.
   Monday–Friday 8:00amET to 10:00pmET, and Saturdays 9:00amET – 5:30pmET.
   If device is already programmed, registration can be completed as follows:
   * Triple clicking the tamper switch on the device.
   * Using a 7720P programmer, press the SHIFT key then the UP ARROW key.
   * For Lynx Touch, use the touch screen registration command.
DEVICES ► Substitution PIN Generation (central station)

This tool enables you to generate a substitution PIN for communication devices when replacement is required. It provides an easy method to transfer the old device City, CS, and Subscriber number to the new device.

Read the on-screen instructions, then fill in the fields.

**Substitution Pin Generation**

<table>
<thead>
<tr>
<th>Primary City-CS-Sub</th>
<th>Primary City-CS-Sub</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is Dual Reporting?</td>
<td>Get PIN</td>
</tr>
</tbody>
</table>

Upon completion, click **Get PIN**.

ACCOUNTS ► View Accounts (central station)

This tool enables you to view accounts. Fill in the **Start Range** and **End Range** fields. You can further filter the search by using the **Select Services** and **Select Registration Status** check boxes.

Note there are security restrictions on what accounts a user can view. These restrictions are as follows:

**SuperUser, or Manager** - Has access to all the accounts for their company at all branch locations.

**Branch Manager, or Branch User** - Has access only to those accounts the user has been authorized to view.

Upon completion, click **Submit**. The search results are displayed.

The search results can be further sorted by clicking the **Sub**, **MAC**, **Service** and **Registration Status** column heads. The resultant sorted data can also be downloaded as a .csv (comma separated values) file for use by a spreadsheet.
For any particular account, detailed information can be displayed by double clicking the account's Sub number. An account details pop-up window appears.

### Terms . . .

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start/ End Range</strong></td>
</tr>
</tbody>
</table>

| **Select Services** | Filter the search by using the check boxes to select the service type. |

| **Select Registration Status** | Filter the search by using the check boxes to select the account status. |

- **New** - Account number is not currently associated with any devices and is ready for use.
- **Cancelled, service removed (Partial)** - The device has been cancelled by the central station and is no longer connected to the network. A new device may be registered to this account at any time.
- **Cancelled, still installed (Full)** - The device has been cancelled by the central station but may still be powered and transmitting. A new device may be registered to this account after submitting a cancellation as "Removed from Service", and then confirming that status has been changed on AlarmNet 360.
- **Active** - The device is actively using the network and may be billed.
- **Video Svcs** - All the account number appearing (in the color black) indicates it is a video service account.
### Terms . . .

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Details pop-up window</strong></td>
</tr>
<tr>
<td>Double clicking the account’s Sub number causes a details pop-up window to appear.</td>
</tr>
<tr>
<td>- The pop-up window will close after 5 minutes. If the pop-up is refreshed or any work is done in the pop-up window, it will reset the time to close back to 5 minutes.</td>
</tr>
<tr>
<td>- If the browser window is closed without logging out, ensure all pop-up windows are closed to log off the session. If no action is taken the pop-ups will close after 5 minutes.</td>
</tr>
<tr>
<td>- Closing the browser may not always log the user off the session. <strong>The user should always explicitly log out and not just close the browser window.</strong></td>
</tr>
</tbody>
</table>

### Pop-Up Window for; “A” type service
No information will be transferred if the user navigates to another page.

### Pop-up Window for; I, or Video Svcs
If the user navigates to Device Status, Programmerless Registration, or Substitution Pin Generation, the information will be filled out with the selected account information derived from clicking Details or the last pop-up the user was working with for I, or Video Svcs service only.

If the user clicked on Details and navigates to another page and then returns back to the View Accounts web page, all search criteria will be remembered on the View Accounts page, if the user continues working with the same account during the entire process.

If the user starts off in Device Status, Programmerless Registration, Substitution Pin Generation, or Outages, select a valid account to work with, then navigates to View Accounts. Search criteria for the account will be set up automatically.

---

### AlarmNet Service Types

The information below lists the Communication Device along with the applicable AlarmNet service type.

<table>
<thead>
<tr>
<th><strong>AlarmNet - A</strong></th>
<th><strong>AlarmNet - I</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>7720 series (1 way)</td>
<td>GSMV, IGMV, GSMV4G, IGMV4G</td>
</tr>
<tr>
<td>7820 series (1 way)</td>
<td>GSMV-EX</td>
</tr>
<tr>
<td>7920 series (2 way)</td>
<td>GSMHS, IGMHS, IGMHS4G</td>
</tr>
<tr>
<td>7810PC</td>
<td>GSMX, GSMX4G</td>
</tr>
<tr>
<td>8132i (Symphony)</td>
<td>GSMCF, IGMCF</td>
</tr>
<tr>
<td>7845i-GSM, and 7845i-ent series</td>
<td>IGMCFP4G</td>
</tr>
<tr>
<td>7847i</td>
<td>IPGSM-COM, IPGSM-DP, and IPGSM-DPC series</td>
</tr>
<tr>
<td>7810PC</td>
<td>IPGSM-4G</td>
</tr>
<tr>
<td>8132i (Symphony)</td>
<td>ILP5, GSMVLP, GSMVLP5, GSMVLP4G, GSMVLP54G</td>
</tr>
<tr>
<td>7845GSM, 7845i-GSM, and 7845i-ent series</td>
<td>7847i</td>
</tr>
<tr>
<td>7810PC</td>
<td>8132i (Symphony)</td>
</tr>
</tbody>
</table>

**Note:** Information above also applies to the Canadian product equivalents.
ACCOUNTS ► Communication Failures (central station)

This tool enables you to view which devices are experiencing communication failures.

Make your selections from the drop-down field. Upon completion, click **Search**. A listing of all communication devices that experienced failures will be listed.

For any particular account, detailed information can be displayed by clicking the account's Sub number. A device information details pop-up window appears.
ACCOUNTS ➤ Account Generation (central station)

This tool enables you to generate a new Subscriber account or range of subscriber accounts for distribution to a dealer.

Enter the data as required. Upon completion, click **Submit Request**. The request is sent to AlarmNet; when approved the new account numbers will appear for the central station.

The information below lists the Communication Device along with the applicable AlarmNet service type.

<table>
<thead>
<tr>
<th>AlarmNet – I</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GSMV, IGSMV, GSMV4G, IGSMV4G</td>
<td></td>
</tr>
<tr>
<td>GSMV-EX</td>
<td></td>
</tr>
<tr>
<td>GSMHS, IGSMHS, IGSMHS4G</td>
<td></td>
</tr>
<tr>
<td>GSMX, GSMX4G</td>
<td></td>
</tr>
<tr>
<td>GSMCF, IGSMCF</td>
<td></td>
</tr>
<tr>
<td>IGSMCFP4G</td>
<td></td>
</tr>
<tr>
<td>IPGSM-COM, IPGSM-DP, and IPGSM-DPC series</td>
<td></td>
</tr>
<tr>
<td>IPGSM-4G</td>
<td></td>
</tr>
<tr>
<td>ILPS, GSMVLP, GSMVLP5, GSMVLP4G, GSMVLP54G</td>
<td></td>
</tr>
<tr>
<td>7845GSM, 7845i-GSM, and 7845i-ent series</td>
<td></td>
</tr>
<tr>
<td>7847i</td>
<td></td>
</tr>
<tr>
<td>7810PC</td>
<td></td>
</tr>
<tr>
<td>8132i (Symphony)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Information above also applies to the Canadian product equivalents.
ACCOUNTS ► Account Cancellation (central station)

This tool enables you to cancel Subscriber accounts. When selected, the Account Cancellation form appears, allowing you to cancel one account or multiple accounts using a batch file.

1. Enter the information for the account to be cancelled.
2. Read each cancellation option and choose the appropriate option.
3. Click Submit Cancellation. The request is sent to AlarmNet, and billing is stopped. All of the associated data will be deleted and the SIM card will be deactivated after 30 minutes.
4. For multiple cancellations, submit the accounts as a batch file. Click Browse, and navigate to your batch file.
5. Click Submit Cancellation. The request is sent to AlarmNet, and billing is stopped.

For information on creating batch files see the next topic.
Creating Batch Files for Multiple Account Cancellations

1. Create the batch file by using either a spreadsheet or text editor such as “Notepad” to create the batch file.

   **For a spreadsheet, use the following format.**

<table>
<thead>
<tr>
<th>City</th>
<th>CSID</th>
<th>Subscriber #</th>
<th>Type of cancellation, use:</th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>10</td>
<td>1234 P</td>
<td>P = for transmitters removed from service.</td>
</tr>
<tr>
<td>63</td>
<td>10</td>
<td>1235 P</td>
<td>(partial cancel)</td>
</tr>
<tr>
<td>63</td>
<td>10</td>
<td>1236 F</td>
<td>F = for transmitters that are still installed.</td>
</tr>
<tr>
<td>63</td>
<td>10</td>
<td>1237 F</td>
<td>(full cancel)</td>
</tr>
</tbody>
</table>

   **For Notepad, separate the numbers by a comma and do not use spaces.**

   

2. If using a spreadsheet save the file as a `.CSV` file, or if using Notepad save the file as a `.TXT` file. The file name must be unique for each submission. If you create more than one file, increment the file number. Use the following file naming convention.

   COMPANYNAME_ME_2011-09-08_00001
   COMPANYNAME_ME_2011-09-08_00002
ACCOUNTS ► Coverage Maps (central station and dealer)

This tool enables you to display coverage maps for AlarmNet A, and G networks. Various search criteria are available. Choose the search criteria and click Submit Request, or click the area for a particular network. The resulting map can be zoomed in by clicking the desired area.

Click to return to AlarmNet360.

ACCOUNTS ► Coverage Maps (central station and dealer)

<table>
<thead>
<tr>
<th>AlarmNet-A Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater Atlanta Area Network - City 11</td>
</tr>
<tr>
<td>Chicago Metro Area Network - City 05</td>
</tr>
<tr>
<td>Dallas/Ft Worth Area Network - City 07</td>
</tr>
<tr>
<td>Detroit Metro Area Network - City 13</td>
</tr>
<tr>
<td>Houston Metro Area Network - City 26</td>
</tr>
<tr>
<td>Las Vegas Metro Area Network - City 34</td>
</tr>
<tr>
<td>Los Angeles Metro Area Network - City 09</td>
</tr>
<tr>
<td>Memphis Metro Area Network - City 22</td>
</tr>
<tr>
<td>Miami / Southeastern Florida Area Network - City 04</td>
</tr>
<tr>
<td>New York Tri-State Area Network - City 01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AlarmNet-G Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click below links to view coverage on provider’s sites:</td>
</tr>
<tr>
<td>United States</td>
</tr>
<tr>
<td>(GSM Digital Coverage Map)</td>
</tr>
<tr>
<td>Canada</td>
</tr>
<tr>
<td>(GSM Digital Coverage Map)</td>
</tr>
</tbody>
</table>

Click to return to AlarmNet360.

MY COMPANY ► My Profile (central station and dealer)

This tool enables you to edit your profile.

Edit your profile and click Update.

MY COMPANY ► Manage Users (central station and dealer)

This tool enables you to add users, assign features to users, and edit their profiles.
User Authority Levels

There are five user authority levels in AlarmNet, and each can be given different features they can invoke. The different authority levels follow the security restrictions below:

1. If a higher level attempts to edit a lower level, where the lower level profile has features enabled that the higher-level profile does not have, editing is prevented. This prevents a person from gaining access to features that have not been assigned to that person.

2. If a Branch Manager attempts to edit a Branch User, where the Branch User has authorization to accounts the Branch Manager does not have, editing is prevented. This prevents a Branch Manager from getting authorization to accounts that have not been assigned to the Branch Manager.

3. A higher level can only assign features that they possess.

The chart below provides detailed information for each authority level.

**SuperUser**
1. Has authority to “Create, Disable and Modify” others at the Same or Lower Levels: SuperUser, Master, Branch Manager, and Branch User.
2. Only other SuperUsers can “Create, Disable and Modify” another SuperUser.
3. Has account authorization for the entire company, covering all branches.
4. Can assign account authorizations for Branch Manager and Branch User.
5. Features that can be turned on for same/lower levels, only if they have been enabled for you.
   - Account Cancellation – Cancellation Feature
   - Account Generation – Generation Feature
   - Device Status Info and Ping Commands
   - Device Status Info
   - Enable: Daily Supervision Rate (for Device Status and Programmerless Registration)
   - Enable: Monthly Supervision Rate (for Device Status and Programmerless Registration)
   - Manage Users – “Create, Disable and Modify” (not available to be assigned for Branch User)
   - Programmerless Registration
   - Substitution Pin Generation
   - View Accounts
   - View/Download Reports

**Master**
1. Has authority to “Create, Disable and Modify” others at Lower Levels: Branch Manager, Branch User.
2. Has account authorization for the entire company, covering all branches.
3. Can assign account authorizations for Branch Manager and Branch User.
4. Features that can be turned on for same/lower levels, features can be assigned by you only if they have been enabled for you.
   - Account Cancellation – Cancellation Feature
   - Account Generation – Generation Feature
   - Device Status Info and Ping Commands
   - Device Status Info
   - Enable: Daily Supervision Rate (for Device Status and Programmerless Registration)
• Enable: Monthly Supervision Rate (for Device Status and Programmerless Registration)
• Manage Users - “Create, Disable and Modify” (not available to be assigned for Branch User)
• Programmerless Registration
• Substitution Pin Generation
• View Accounts
• View/Download Reports

Branch Manager
1. Has authority to “Create, Disable and Modify” others at Lower Levels: Branch User.
2. Have account authorizations that are assigned by Higher Levels: SuperUser and Master.
3. Can assign account authorizations for Branch User, but only those accounts that have been authorized for you.
4. Features that can be turned on for same/lower levels, features can be assigned by you only if they have been enabled for you.
   • Account Cancellation – Cancellation Feature
   • Account Generation – Generation Feature
   • Device Status Info and Ping Commands
   • Device Status Info
   • Enable: Daily Supervision Rate (for Device Status and Programmerless Registration)
   • Enable: Monthly Supervision Rate (for Device Status and Programmerless Registration)
   • Manage Users - “Create, Disable and Modify” (not available to be assigned for Branch User)
   • Programmerless Registration
   • Substitution Pin Generation
   • View Accounts
   • View/Download Reports

Branch User
1. Have account authorizations that were assigned by Higher Levels: SuperUser, Master and Branch Manager.
2. Features that are available for the Branch User are as follows:
   • Account Cancellation – Cancellation Feature
   • Account Generation – Generation Feature
   • Device Status Info and Ping Commands
   • Device Status Info
   • Enable: Daily Supervision Rate (for Device Status and Programmerless Registration)
   • Enable: Monthly Supervision Rate (for Device Status and Programmerless Registration)
   • Programmerless Registration
   • Substitution Pin Generation
   • View Accounts
   • View/Download Reports

Adding a user
1. Use the drop-down field to select the business location.
2. Click **Add User**. An information form appears.

3. Fill in all the fields and click **Submit**. A confirmation message appears, click **OK**.

4. You are brought to the **Edit User** window that enables you to assign privileges, etc.

   **Proceed to the next topic.**

### Editing a user

You can edit a user by simply clicking on the user which brings up the **Edit User** window. Note, that when adding a new user you are also brought to the Edit User window below.

Since the **Edit User** window is long, it will be presented in parts.
1. Edit the user by first assigning an Authority Level.
2. Assign Features for the user.
3. In the left pane select the desired features, then use the arrow buttons to transfer them to the right pane.
4. Assign which Locations to enable for the user.
5. Click Update.
6. Click Exit to Manage Users page.
MY COMPANY ▶ Dealer Services Config (central station)

Note that, by default “Dealer Services Config” is turned ON for all SuperUsers. This tool enables central stations to authorize certain Dealers to have Remote Services and Video Services.

**Video Services Only**  – If the dealer does not have GSM or Internet comm devices registered with their Central Station ID, initial access must be granted by AlarmNet. Please call 1-800-222-6525 option 1 then press #.

- Use the top drop-down menu to select the Central Station. When selected, the Dealers associated with that central station appear in a table.
- Using the Default option boxes, you can set the default authorizations for all new Dealers associated with the selected Central Station.
- In the two column heads you can select what options to apply to specific dealers.
- Upon completion, click Update.
- Use the Download button to download information for all dealers associated with the selected City/Central Station. The information will be a .csv (comma separated values) file for use by a spreadsheet.

In the example spreadsheet below, all the dealers associated with the City/Central Station and their device base (with account history) are broken down by Account, Supervision Rate, MAC Number, Product Type, Service Levels, etc.
MY COMPANY ▶ My History (central station and dealer)

This tool displays a history of access sessions, and actions taken by all of the users. You can filter the results using the various drop-down filters.

Information can further be sorted by clicking the Time, Action, User, City, and MAC column heads. The resultant sorted history data can be downloaded.

MY COMPANY ▶ Web Usage (central station)

This tool can display usage of the AlarmNet 360 website by users for all actions, at all companies. The depth of data displayed will vary according to your hierarchy. It provides a historical record of all access sessions and their actions.

Use the drop-down menus to filter the results.
MY COMPANY ► Company Information (central station super users, and dealer managers)

This tool enables you to manage Company Information and email lists to inform your staff of important information and notifications. Typical information includes:

- company information
- address information
- billing
- weekly reports
- network outages
- excess message usage
- new products and specials
- end user Sale/Service Requests. (These notifications are generated by LYNX Touch L5100 end users to request either service or sales to contact them.)

Managing Company Information and Staff Notifications

1. This is the information your staff members will see. Edit the fields as desired.
2. Click Save.
3. Search for the staff member you want to notify, or pick from the list below.
4. If necessary you can update their contact information.
   Note: When the email address is changed, a validation email is sent to the new address along with a link that must be clicked to complete the validation.
   The Email Validation icon will change to an envelop, and back again once validation is complete.
5. Choose the desired notifications for the staff member.
6. Click Save.

Note: The ability to manage this information can be assigned to other users. Go to My Company > Manage Users. Select the user and enable the “AND: Company Information” feature to their profile.
DEVICES ► Device Programming ► Program/ Replace (central station and dealer)

This tool enables you to search for all programmed devices by account number, or for a specific device by MAC number.

Example TC2 device drop-down menu.

Depending on the device, other choices may appear.

This button opens a Program New Device wizard. Please see the “Device Programming” topic.
Use the **Select a City-CS** drop-down menu or the **City-CS-Sub** field to set the search criteria, then click **Search**.

You can view details on a particular device by clicking the corresponding Acct #.

Or you may edit the device by using the **Actions** drop-down menu, selecting the action and clicking **GO**. After a change is made a confirmation message will appear, click **OK** to acknowledge.

**Editing the Account**

There is an extensive set of account configuration options that can be chosen by editing the account. From the **Actions** drop-down menu, select **Edit**, and click **GO**.

The details in each category can be viewed/edited by clicking the icon or link.

Save your changes by clicking **Finish**.

---

**IMPORTANT**: When editing the **Program Advanced Features** category, ensure you go back to the “Actions” column drop-down menu and perform a **Send Data** command.
Adding IP Video Devices (TC1 ready)

This procedure is for adding IP video devices that are used with “TC1 ready” Internet, GSM or combination I/GSM communication devices. To add IP video devices for TC2 ready communication devices, refer to the “Manage TC2 Accounts” topic.

Honeywell offers an array of IP based video devices such as the iPCAM-WI, iPCAM-PT, ACU Converter, etc., to add, delete, or edit the names of these devices you need the MAC number for the device. Refer to the installation guide if you need help in locating this number. Then perform the following steps:

1. Search for the GSM/I device as explained previously.

2. From the Actions drop-down menu, select Edit.

3. At this window, you can Edit existing video devices to change their name, or Delete the video device.

4. If you want to add a new video device, click the add video device icon. The Add Device window appears.
5. Enter the MAC number for the device, and a descriptive name (maximum of 6), then click **Save**.
DEVICE PROGRAMMING ► Program/ Replace Device (central station and dealer)

This is a wizard base tool that enables you to program a new GSM, i-GSM, or internet only communication device. The steps included in this tool are specifically tailored to task being accomplished. As you start to enter data, such as the MAC ID, AlarmNet will recognize the type of device and generate the next appropriate wizard screen.

Have the following information ready:

- Subscriber Account Number.
- MAC ID and CRC - For most communicators these are on the product carton, on the product’s PCB, or can be obtained using the 7720P Programming Tool.
  
  For TUX series devices, these are on the product carton, on the device back, or can be obtained by tapping the “tools” icon on the home screen. Then tap the “information” icon on the next screen.
- A name for the TC2 account.

1. Since this is a wizard based tool, just select the service you want for the account, and click Next. Follow the screen prompts.

2. If the new account will include Total Connect, about midway through the wizard a check box appears allowing you to Pre-Configure the TC 2.0 account for the customer.
This feature enables you to access the account after the wizard completes to configure the TC2 account for the customer. This is especially useful for accounts that employ advanced devices, and for those customers that do not have advanced web experience.

3. On the last wizard screen you will have a choice to immediately manage the TC2 account.

If you select “Manage TC2 Account” you are directed to the Manage Total Connect 2 Accounts screen, and can start the process by selecting PRE-CONFIGURE.

Please register the communicator first before using the PRE-CONFIGURE punch icon through, as the communicator will not sync if it is not registered first.
You are immediately logged into the account and can Pre-Configure it for the customer. After the TC2 account is configured, log out and you are returned to AlarmNet 360 to enable working with the newly created AlarmNet account. (The Pre-Configure button will remain active until the account is commissioned then the reverse arrow for normal punch through appears.)

4. If you selected “Begin Working with My Account” the wizard process is complete and you will remain in AlarmNet 360. Navigate DEVICES ► Device Programming. Then search for the device.

5. From the Actions column, select Send Data, then click GO. The Actions column has other choices that can be used to configure the communicator.

6. After a change is made a confirmation message appears, click OK to acknowledge.

DEVICE PROGRAMMING ► Program/ Replace Device (central station and dealer)

Instead of deleting the old communication device and starting over by programming a new comm. device, this tool enables subscriber information to be retained. The retained subscriber information and remote services (Total Connect) information is then linked to the new replacement comm. device.

This is a wizard based tool that enables you to replace an existing communication device with a new GSM, i-GSM, or internet only communication device. The steps included in this tool are specifically tailored to task being accomplished.

Have the following information ready:

- Subscriber Account Number.
- MAC ID and CRC for the existing device and the replacement device – For most communicators these are on the product carton, on the product’s PCB, or can be obtained using the 7720P Programming Tool.
  For TUX series devices, these are on the product carton, on the device back, or can be obtained by tapping the “tools” icon on the home screen. Then tap the “information” icon on the next screen.
- Substitution PIN obtained from AlarmNet (or your Central Station). Alternately you can search for the existing account, then from the Actions pulldown menu, select Get Substitute PIN.

1. Since this is a wizard based tool, just select the service you want for the account, and click Next. Follow the screen prompts.

2. After the wizard is completed, navigate DEVICES ► Device Programming. Then search for the device.

3. From the Actions column, select Send Data, then click GO.

4. After a change is made a confirmation message appears, click OK to acknowledge.
Accounts ► Manage TC 2.0 Accounts (central station and dealer)

This tool is for managing accounts associated with TC 2.0 ready Internet, GSM or combination I/GSM communication devices (and associated IP devices) that have been configured for a Total Connect 2 end user account.

Use the search filters on top to find the account. You then can manage the devices that are associated with the account.

Adding IP Video Devices

To add IP video devices to a TC2 account perform the following:

1. Select the account and click the adjacent + to expand.
2. Select the Location. (Accounts may have multiple locations.)
3. Under Action, click the icon to add a device. The Add Device window appears.
4. Enter a meaningful Device Name, then from the drop-down menu select the IP Camera.
5. Enter the MAC number for the device, and click Save.
6. The device has been added.
Adding TUX series Automation Devices

Note: You can use TUX only on Vista series panels.

To add TUX devices to a TC2 ready control panel (such as a VISTA 21-iP) perform the following:

1. Select the account and click the adjacent + to expand.
2. Select the Location. (Accounts may have multiple locations.)
3. Under Action, click the + icon to add a device. The Add Device window appears.

   ![Add Device to Location #1](image)

4. Enter a meaningful Device Name, then from the drop-down menu select the Automation.
5. Enter the MAC number and CRC for the device, and click Save.

   The device has been added.
Deleting a TC2 Account or Location

There are a few options for deleting a user or associated devices. First find the account using the Search Field and Search Text as appropriate. In the example below we used the City-CS-Sub filter, and entered the account number in the Search Text field (xx-xx-xxxx).

This brings up the window allowing you to delete the device, user, or the entire TC2 account. By only deleting the location, comm device or cameras, this retains the login and email info so you do not need to rebuild the account.

- Deletes just the camera. So it is no longer associated with any comm device.
- Deletes the comm device only. The camera is still associated with the subscriber account, and you can add a new comm device if desired.
- Deletes the comm device, camera and the location. So all items are not associated with the TC2 account.
- Deletes the entire TC2 subscriber account and associated locations and devices.

Getting permission to configure the customer's account:

If you need to make configuration changes, contact the customer and have them enable permission for you. Inform them this enables a limited 1 hour window for each permission session granted, and is limited to only one logon session.

Have the customer log into their TC2 account. Then open Users, and click on their Edit button. Next they need to check Security Professional Access, and confirm the pop-up security message. Lastly, click Save.
**Resetting the TC2 account username, email, or password**

If the Master User requests their username, email, or password be reset, first verify they are the Master User according to your local procedure. Then proceed.

1. Click the account’s Master User Management icon. A dialog screen appears.
2. Change any information as requested, then click **Save**.
3. To reset their password, click **Reset Password**. A “Password reset email has been sent” message appears.
4. The account’s Master User will then receive an email with a link that is active for **24 hours only** allowing their TC2 password to be updated.
5. After updating, a confirmation email will be sent.

**DEVICES ► Device Programming ► Take Ownership (central station and dealer)**

This tool enables you to take ownership of a device that was programmed by Honeywell Tech Support. Once the dealership takes ownership, they are able to manipulate the comm. device just like they would if it was programmed by the dealer.
API DOCUMENTS (central station and dealer)

**What is an API?**

The Application Programming Interface (APIs) are set of requirements that govern how one application can talk to another. For example, virtually all software has to request other software to do some things for it.

APIs are what make it possible to move information between programs. The APIs expose some of a program's internal functions to the outside world in a limited fashion. That makes it possible for applications to share data and take actions on one another's behalf without requiring developers to share all of their software's code.

APIs are specially crafted to expose only chosen functionality and/or data while safeguarding other parts of the application which provides the interface. Finally, the more applications that interact with your application the more popular it becomes.

**Why are APIs needed?**

Communication between applications is important and all this communication is made possible via APIs.

**How APIs work?**

These days, APIs are especially important because they dictate how developers can create new apps that tap into big Web services. For example, the developer of a game app can use the Dropbox API to let the end users store their saved games in the Dropbox cloud instead of working out some other cloud-storage option from scratch.

**Where can I find APIs?**

All the available APIs are listed under API Documents.

From the tool bar select API Documents. Click the required document to download.
<table>
<thead>
<tr>
<th>Devices</th>
<th>Device Programming</th>
<th>Device Status</th>
<th>Device History</th>
<th>Subscription PRI Generation</th>
</tr>
</thead>
<tbody>
<tr>
<td>[AlarmNet API Documents]</td>
<td>[TD2_Devices_Download]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[TD2_Devices_Download]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REPORTS (central station and dealer)

This tool enables you to generate and save detailed subscriber reports. From the tool bar select Reports > My Dashboard.

My Dashboard

The dashboard has multiple widgets, each one representing data in charts. You can click the icon next to every widget for more information.

Communication Failures

The Communication Failures widget displays the total count of accounts currently available under Comm Failure. Click the comm fail list for a detailed view of all the communication failures.

Communication Technology

The Communication Technology widget displays the distribution of devices in terms of their network capabilities, as in Radio capability.

Service Subscriptions

The Service Subscriptions widget displays the distribution of Accounts based on the services it has subscribed to, which are getting billed.

Each sub section in the subscriptions such as, Automation, Information, Advertising, Video, APL, and so on, the following details are displayed:

- Number of Accounts in % as well as the number against the total.
- Number of accounts serviced by that Central Station company/Dealer Company selected.
TC 2.0 Customer Engagement

The TC 2.0 Customer Engagement widget displays the Engagement level of the Customer using different mediums such as Web or mobile devices. The average Login per day is measured based on the following slab:

- **Frequent User**: > Avg(25) logins/day
- **Moderate User**: Avg(10) - Avg(25) logins/day
- **Occasional User**: < Avg (10) logins/day
**TC 2.0 No Login**

The **TC 2.0 No Login** widget displays the distribution of Accounts/Customers who have not logged on into the Total Connect 2.0 system.

![TC 2.0 No Login](image)

**Communicator Product**

The **Communicator Product** widget displays the distribution of security accounts by their Radio Type.

![Communicator Product](image)

**Device Installed**

The **Devices Installed** widget displays the distribution of devices (Lights, Locks, Thermostats) installed at the Customer Site (Total Connect).

![Device Installed](image)
**Top Noisy Accounts**

The **Top Noisy Account** report displays the list of top noisy accounts for the selected period. A maximum of 10 accounts are displayed.

---

**NOTIFICATION (central station and dealer)**

This tool provides notifications to the customer (Dealer/Installer). On the Tool Bar there is a status indicator. If the status indicator is displaying BLUE, please read the latest notifications.

*Note:* The dealer view includes a blue dot “You received new notification(s)!” message.

Blue = New notifications are posted.
Understanding Total Connect Services

The “Total Connect” suite of services provides additional flexibility to a powerful Honeywell security system. Because these services utilize various communication technologies outside of our control, the user should be aware how these impact the use of Total Connect. These services are intended as a convenience for the user, and do not replace Central Station reporting of critical events (alarms, troubles, etc.).

In addition, Honeywell provides many different control panel families, each having different feature sets. The current release of “Total Connect” services provides the most consistent operation when used with our Vista-10P/15P/20P series of panels. These services also function with our residential LYNX panels, and commercial Vista panels; namely the Vista-128BP class. However, there are some inconsistencies to be aware of. This topic provides helpful hints relative to the use of these new services.

### General

<table>
<thead>
<tr>
<th>Total Connect account creation</th>
<th>When programming a new GSM, IGSM or creating a Total Connect only (i.e., video services only) account the wizard will prompt you for the following information:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account Name</strong></td>
<td>Must be at least 8 characters.</td>
</tr>
<tr>
<td><strong>TC2 Master user name</strong></td>
<td>This is the &quot;Username&quot; for the customer to use when logging into Total Connect. Can be 6-80 character length (not case sensitive), valid entries are: 0-9, A-Z and ? ! @ # $ % ^ * - _ = + .</td>
</tr>
<tr>
<td><strong>TC2 Email address</strong></td>
<td>This is the email address provided by your customer. Your customer will receive a welcome email which contains the Total Connect 2.0 URL and username. They will also receive a second email containing their auto-generated password to login to Total Connect.</td>
</tr>
</tbody>
</table>

*** PLEASE NOTE ***

The “Master User” profile is not intended for your use”.

The “Master User” profile is intended to be managed by your customer. After initial setup in AlarmNet 360, the user profile will be maintained by the customer through their Total Connect website account. They can update and change their profile and assign subordinate user profiles via the Users module.

*** TECHNICAL TIP ***

In certain instances your customer may need hands on help to configure their Total Connect website account. If you are asked to make changes on your customers behalf another level of “Security Professional Access” is available. Have your customer (Master User Only):

1. Login to the Total Connect 2.0 web site.
2. Grant you access to their account by clicking; My Profile > then checking “Security Professional Access” (confirm the pop-up security message) > then click “Save”.
3. You will now have access up to 60 minutes to edit fields by accessing the account. Refer to the “Checking the customer’s TC2 account configuration” topic in this guide.

<table>
<thead>
<tr>
<th>auto stay arm</th>
<th>If the security system (or a partition) is configured with <strong>Auto Stay Arm</strong> enabled, using Remote Access or SMS to arm the system will result in the system (or partition) reverting to an Armed Stay state. This is because there is no detection that the premises has been vacated (complies with SIA requirements).</th>
</tr>
</thead>
<tbody>
<tr>
<td>service providers</td>
<td>Our remote services features are dependent upon the reliability and capability of the user’s service provider for the internet as well as the wireless carrier that may be involved. All networks are subject to outages and maintenance beyond our control, and as such, can prevent availability of connections or cause disruptions to the services.</td>
</tr>
<tr>
<td>web browser</td>
<td>Configure your web browser to always allow “pop-ups” from the services.alarmnet.com site.</td>
</tr>
</tbody>
</table>
control panel partition support

At this time, Total Connect 2.0 does not support control panel partitions two through eight. Partition support is limited to Partition One, even on panels that have more than one partition enabled.

**When using Total Connect 2.0 on multi-partitioned panels:**

1. Only zones assigned to partition one can be uploaded into Total Connect 2.0.
2. Notifications can be sent for events occurring on partition one only. This would apply to ALL events including: Alarm, Arming/Disarming, and zone notifications such as bypass or trouble.
3. The Quick Arm/Disarm buttons will arm/disarm partition one only.
4. The Total Connect 2.0 remote keypad MUST be assigned to partition one only, however, the remote keypad DOES support the Global Arming and GOTO functions (if enabled properly in the panel programming). Those functions will give the end user the ability to control other partitions on the system just like any keypad physically connected to the system.
5. System Status is provided for partition one only.

**When using Total Connect 2.0 User code synchronization on multi-partitioned panels:**

1. User Sync via Total Connect 2.0 is designed for use with user codes assigned to partition one only. User codes created via control panel keypad or Compass must have access to partition one for the code to be uploaded into Total Connect 2.0.
2. Users created via Total Connect 2.0 and assigned a user code for the control panel will be given “General authority” access to ALL enabled partitions when User Sync is performed. Caution must be exercised here so as to not give a user access to a partition they should not have access too. It is highly recommended to observe notes 3 and 4 below on multi-partitioned panels.
3. User codes originally created via control panel keypad or Compass will continue to function only in the partitions they were given access to when they were programmed, even after Total Connect 2.0 User sync is performed. These codes do not get assigned to all partitions when Sync is performed and will continue to work in the assigned partitions only.
4. On multi-partitioned panels, the best practice would be to program the user codes into the panel first, then use the User Sync function to pull the codes into Total Connect 2.0.

After the “Panel Only Users” are uploaded, modify them to create Total Connect 2.0 Users as desired (assign a login name and password, first/last name, email address, etc). It is recommended to follow this procedure in order to prevent giving undesired partition access to a Total Connect User.

**E-Mail**

**event notifications**

For event notifications, if no text has been added to describe the event on the Total Connect website (refer to the Configure Email topic in the Total Connect User Guide), a generic message (such as “Zone 1 Activated”) will be sent for the activated state.

**LYNXR-I, LYNX Plus, and LYNX Touch**

**fire zones**

Do not use email notification for zones configured as “Fire with verification.”

**panic keys**

The emulated keypad does not support single-button or two-button panic keys.

**time and date**

You cannot set the time and date or go into programming mode remotely.

**Remote Access**

**common partition**

Common Partition logic will work from the emulated keypad but not from the System Status screen.

**deleting users**

If you delete a user at the security system's control panel, when using Remote Access to Manage User Codes, the deleted user can still be retrieved since it is stored in the remote services database. If desired, delete that user from the remote services database (Remote Access > Users > Manage User Codes).
### fire zones, bypassing
When using Remote Access, if you attempt to bypass a fire zone, the fire zone WILL NOT be bypassed.

### keypad – full control
When using Remote Access, if the keypad type is set to “Full Control,” you may view status and control all partitions using the “System Status” tab (not the “Keypad” tab).

### panic keys
When using Remote Access, two-button panic keys such as 1+*, 2+#, and 3+# will not work. However single button panics (if programmed) will work.

### stay mode
The System Status screen does not support multiple stay modes. If you need to use a specific stay mode, use the Keypad screen.

### system status screen
The System Status screen does not support multiple stay modes. If you need to use a specific stay mode, use the Keypad screen.

### Text Message or SMS Commands (TC1 only)

| “Command issued, status unknown” reply message | When the network does not have sufficient information from the control panel to formulate a message in response to a command, instead of sending a “blank” reply message, it will send “Command issued, status unknown” to alert the user to retry getting status. Likewise, if the control panel information is not available at the time that the remote services application collects the status, the text message reply may be truncated. |
| commands | When a Remote Access session is active (using a PC), text message commands cannot be used to control the security system. If you desire to do text messaging, please shutdown the remote PC session and wait 15 seconds prior to sending a text command. |
| GOTO command | SMS Text Message commands do not support the GOTO command (applies to partitioned systems only). |
| multiple text message series | When the need or desire arises to send a series of text message commands, allow a 2-minute period after the reply of the first text message before sending the next text message. |
| out of order replies | Under certain network conditions, emails received by the user may be out of order. |
| output relay | You will not receive text message verification for turning an output relay on or off. You will, however, receive a system status message. |
| partition number | If you do not see the partition number in a reply message, contact your security system services provider to enable the control panel’s “Display Partition Number” field. |
| remote keypad – Full Control | If the remote keypad is set to “Full Control,” sending a text message command for arming or disarming a partitioned system without specifying a partition constitutes a global command for all partitions. If the user does not have global authorization, no action will be performed. Please make sure this is understood by the user when offering this service. |
| remote keypad – Keypad Only | If the remote keypad is set to “Keypad Only,” sending a text message command for arming or disarming a partitioned system without specifying a partition will affect only the partition the keypad is assigned to. Likewise, only the status of the partition assigned to the remote keypad will be retrieved. |
| short codes | Some wireless carrier service plans do not fully support SMS Text Message commands with short codes. While this is rare, the Total Connect service may not work with certain plans from your current carrier. Please consult with your carrier if this happens as you may need to upgrade your wireless plan to one that supports short codes. |
**text message commands**

When a Remote Access session is active (using a PC), text message commands cannot be used to control the security system. If you desire to do text messaging, please shutdown the remote PC session and wait 15 seconds prior to sending a text command.

**text message verification**

You will not receive text message verification for turning an output relay on or off. You will, however, receive a system status message.

**text messaging service**

Currently, the SMS Text Message command service operates in conjunction with a wireless service hosting company to support the short code used by Honeywell, which is “ALARM” or **25276**. This hosting service covers the vast majority of carriers supporting SMS service today. Whereas we realize the supported list is very broad, if for some reason the short code does not work with your wireless carrier, please contact them for assistance.

### Trouble Messages

**"Console ECP:2" message**

If the following screen appears, contact your security system services provider to program the control panel with the Remote Access keypad address that exists in the radio.

![Console ECP:2](image)

**"Panel Failed to Respond" message**

If, while using the SMS text message command feature, you receive a "Panel Failed to Respond, Please Retry" message, it may be a result of heavy network traffic, or the panel is busy responding to another Remote Access user. Please wait a minute and then try again.

**Setup/Programming Error message**

Setup/Programming Error is caused due to the lack of PSD (Panel Security Data) being sent from the Control Panel to Total Connect 2.0. There are a few causes, such as: no initial PSD received, incorrect Control Panel programming, or incorrect AlarmNet 360 programming.

To resolve this issue, try the following:

1. Arm and disarm the security system. This will force the PSD message to be sent if everything is programmed properly.

2. Ensure the following Control Panel settings are programmed:
   - For all control panels, verify “RIS” or “Delayed Reports” is enabled.
   - For Vista 15/20 control panels, verify field 91 is programmed to 8, 2. (In AlarmNet 360, the Device must be set to 25.)
   - For Vista Turbo control panels, one ECP address (recommended address 25) needs to be set to Type 12 RIS. Also in AlarmNet, the Device multimode address must match the multimode Device programmed in the control panel.
   - For LYNX series controls, verify the “Remote Access” is Enabled and “Email Notifications” are set to Total Connect 2.0 (Enhanced Rpts) in AlarmNet 360.

3. Ensure the following AlarmNet 360 settings are programmed:
   - For GSMV/IGSMV/GSMX and 7847i communicators, ensure “Remote Access” Enabled
and “Email Notifications” are set to Total Connect 2.0 (Enhanced Rpts) and MultiMode Address is either 25 for Vista 10/15/20 or matches the panel for Vista Turbo.

- For LYNX series controls, verify the “Remote Access” is Enabled and “Email Notifications” are set to Total Connect 2.0 (Enhanced Rpts) in AlarmNet 360.

4. After verifying the AlarmNet 360 device programming, ensure that the data is in the device by performing a “Send Data” command from the “Show Programmed Devices” page of AlarmNet 360.

5. Verify the “Transferred Date(ET)” shows a recent date and time and the arrow indicates down.

6. If you still have the Error 1000 ensure the control panel and AlarmNet device revision levels are support Total Connect 2.0. (Refer to the “Total Connect 2.0 Compatible Devices” topic in this help guide.)

7. If this issue has not been cleared, Contact AlarmNet Technical Support.

<table>
<thead>
<tr>
<th>VI STA commercial</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>arming command</td>
<td>When sending an arm text message command to a commercial panel with zero exit delay and a bypassed zone, the text message reply may not display that a zone is bypassed.</td>
</tr>
<tr>
<td>fire zone</td>
<td>If a fire zone is in a trouble condition (with all partitions disarmed), and you attempt to send a text message command to globally Arm Away, the reply message will indicate that all partitions are Armed Away, but may not indicate a fire trouble.</td>
</tr>
<tr>
<td>output relay</td>
<td>Even if a programmed output relay is restricted from being accessed in the control panel, its operation will function when commanded by an SMS text message.</td>
</tr>
<tr>
<td>sluggish response</td>
<td>For security systems that are heavily populated with a large number of zones and wireless devices, etc., the Remote Access response may be sluggish.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VI STA residential</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>restart exit delay</td>
<td>If the Restart Exit Delay field (*91) is enabled, sending text message commands to a residential control panel (e.g., Vist-10P, Vista-15P), may put the panel in an exit delay countdown condition before a successful completion of the command is sent.</td>
</tr>
</tbody>
</table>
Reference Information

Total Connect 2.0 Compatible Devices

<table>
<thead>
<tr>
<th>Control Panels</th>
<th>Version</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>LYNX 5100</td>
<td>ALL</td>
<td></td>
</tr>
<tr>
<td>LYNX 5000</td>
<td>ALL</td>
<td></td>
</tr>
<tr>
<td>LYNX L3000</td>
<td>20.1</td>
<td></td>
</tr>
<tr>
<td>VISTA-15P / FA148CP</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-15PCN / FA148CP-CN</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-20P / FA168CPS</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-20PCN / FA168CPS-CN</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-20PSIA / FA168CPSSIA</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-21IP / VISTA-21PSIA</td>
<td>3.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-128BPT / VISTA-128BPTSIA</td>
<td>10.1</td>
<td></td>
</tr>
<tr>
<td>VISTA-250BPT / VISTA-250BPTSIA</td>
<td>10.3</td>
<td></td>
</tr>
<tr>
<td>FA1660CT</td>
<td>10.1</td>
<td></td>
</tr>
</tbody>
</table>

For control panels verify compatibility by checking the product carton for a blue “TC2 Ready” label, or checking the version number that appears on the product carton and on the PCB board PROM label.

<table>
<thead>
<tr>
<th>Communicators 2G</th>
<th>Version</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSMVLP5 / iGSMVLP5</td>
<td>ALL</td>
<td>used with LYNX, see above</td>
</tr>
<tr>
<td>GSMVLP / GSMVLP CN</td>
<td>2.6.42</td>
<td>used with LYNX, see above</td>
</tr>
<tr>
<td>GSMV / GSMVCN</td>
<td>2.6.42</td>
<td></td>
</tr>
<tr>
<td>GSMX / GSMXCN</td>
<td>2.6.42</td>
<td></td>
</tr>
<tr>
<td>1GSMV / 1GSMVCN</td>
<td>2.6.42</td>
<td></td>
</tr>
<tr>
<td>VISTA-GSM / VISTA-GSMCN</td>
<td>ALL</td>
<td>used with VISTA-21IP, see above</td>
</tr>
<tr>
<td>7847i</td>
<td>2.6.42</td>
<td></td>
</tr>
<tr>
<td>7847i-L</td>
<td>2.6.42</td>
<td>internet only, used with LYNX, see above</td>
</tr>
</tbody>
</table>

For communicators, verify compatibility by checking the product carton for a blue “TC2 Ready” label, or checking the version number using the 7720P Programming Tool.

<table>
<thead>
<tr>
<th>Communicators 3G/ 4G</th>
<th>Version</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>ALL</td>
<td></td>
</tr>
</tbody>
</table>
Agreement Documents
Click on the following links to retrieve these documents.

AlarmNet Overview of Network Services

US - Subscriber Agreement

Canada - Subscriber Agreement

Technical Support
Before you contact Technical Support, be sure you:

• Referred to the online help.
• Entered all data correctly and did not enter the letter O for the number zero.
• Tried using the Feedback tool on the website to get help.
• Note your customer number and/or company name.

Having this information handy will make it easier for us to serve you quickly and effectively.

<table>
<thead>
<tr>
<th>Support</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. and Canada:</td>
<td>1-800-222-6525:</td>
</tr>
<tr>
<td>option 1 – AlarmNet Tech Support</td>
<td>Monday thru Friday, 8:00 am to 9:00 pm ET. Note, between 6 pm and 9 pm some AlarmNet products are not supported.</td>
</tr>
<tr>
<td>Extended support hours for GSM and activation ONLY. Saturday 9:00 am to 5:30 pm ET.</td>
<td></td>
</tr>
<tr>
<td>option 2 – AlarmNet General Product Information</td>
<td>Monday thru Friday, 8:00 am to 5:00 pm ET.</td>
</tr>
<tr>
<td>option 3 – AlarmNet administration and website support</td>
<td>Monday thru Friday, 8:00 am to 5:00 pm ET.</td>
</tr>
<tr>
<td>Latin America &amp; Caribbean region:</td>
<td>305-805-8188: Monday thru Friday, 8:00 am to 5:00 pm ET.</td>
</tr>
</tbody>
</table>

Notes