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

Accessing AlarmNet 360 ................................................................................................................... 1
  Obtaining a Central Station Account .......................................................................................... 1
  Obtaining a Dealer Account ........................................................................................................... 1
  Logging In ........................................................................................................................................ 2
  Navigating AlarmNet 360 ............................................................................................................... 3

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

Tools ................................................................................................................................................. 6
  DEVICES ▶ Device Status (central station) .................................................................................. 6
  DEVICES ▶ Device History (central station) ................................................................................ 8
  TOOLS ▶ Cellular Activation / Status (central station and dealer) .............................................. 9
  TOOLS ▶ Substitution PIN Generation (central station) .............................................................. 10

Editing a Lyric device ...................................................................................................................... 10

LYRIC DEVICE ▶ Account Overview .......................................................................................... 10
  LYRIC DEVICE ▶ Account Overview > Save as Template ...................................................... 11
  LYRIC DEVICE ▶ Account Overview > Sync ........................................................................ 11
  LYRIC DEVICE ▶ Settings ......................................................................................................... 12
  LYRIC DEVICE ▶ Users ............................................................................................................. 12
  LYRIC DEVICE ▶ Users > New User ......................................................................................... 13
  LYRIC DEVICE ▶ Sensors .......................................................................................................... 13
  LYRIC DEVICE ▶ Sensors > Add New Sensor .......................................................................... 14
  LYRIC DEVICE ▶ Sensors > Cross Zones ................................................................................... 14
  LYRIC DEVICE ▶ Sensors > Cross Zones ................................................................................... 15
  LYRIC DEVICE ▶ Keyfobs ......................................................................................................... 15
  LYRIC DEVICE ▶ Keyfobs > Add Keyfob .................................................................................. 16
  LYRIC DEVICE ▶ Keypads .......................................................................................................... 16
  LYRIC DEVICE ▶ Keypad > Add New Keypad .......................................................................... 17
  LYRIC DEVICE ▶ Reporting Test .............................................................................................. 17
  LYRIC DEVICE ▶ System Test > Add Reporting Test ............................................................... 18
  LYRIC DEVICE ▶ Diagnostics .................................................................................................... 18
  LYRIC DEVICE ▶ Diagnostics > Communicator Diagnostics .................................................... 18
  LYRIC DEVICE ▶ Diagnostics > Panel Diagnostics ..................................................................... 19
  LYRIC DEVICE ▶ Diagnostics > Installation Quality .................................................................... 19
800-11248 Rev. A

LYRIC DEVICE ▶ Event Log ................................................................. 20
LYRIC DEVICE ▶ Activity Log ............................................................. 22
ACCOUNTS ▶ View (Central Station) ...................................................... 23
   AlarmNet Service Types ..................................................................... 24
ACCOUNTS ▶ Generate (Central Station) ................................................. 25
ACCOUNTS ▶ Cancel (central station) ...................................................... 26
   Creating Batch Files for Multiple Account Cancellations ..................... 26
TOOLS ▶ Coverage Maps (central station and dealer) ............................ 27
MY PROFILE (central station and dealer) ............................................... 28
MY ACTIVITIES (central station and dealer) ............................................. 29
MY COMPANY ▶ Web Usage (central station) .......................................... 29
   Uploading Dealer Logos .................................................................. 30
   Dealer Branding (dealer managers) .................................................. 30
   Company Info (central station super users, and dealer managers) ......... 30
      Managing Company Information and Staff Notifications .............. 31
DEVICES ▶ Programming (central station and dealer) .......................... 33
   Editing the Account ........................................................................ 33
   NEW ACCOUNT ▶ Other Communicators (central station and dealer) . 34
   Programming ▶ Drafts ..................................................................... 35
ACCOUNTS ▶ Replace Device (central station and dealer) ....................... 36
DEVICES ▶ Manage TC 2.0 Accounts (central station and dealer) ........... 37
   Adding IP Video Devices .................................................................. 37
   Adding TUX series Automation Devices ........................................... 38
   Deleting a TC2 Account or Location .................................................. 39
   Checking the customer’s TC2 account configuration .......................... 39
   Getting permission to configure the customer’s account ...................... 40
   Resetting the TC2 account username, email, or password .................. 40
DEVICES ▶ Templates (central station and dealer) .................................. 41
   Viewing or Searching for a Template ................................................ 41
   Creating a New Template ............................................................... 42
DEVICES ▶ Checklist (central station and dealer) .................................... 42
   Viewing or Searching for a Checklist ................................................ 42
   Creating a Checklist ...................................................................... 43
DEVICES ▶ User Management ............................................................... 47
   Users ......................................................................................... 47
   Viewing or Searching for a User ....................................................... 47
   Adding a User ............................................................................. 48
   Groups ...................................................................................... 49
   Viewing or Searching for a Group .................................................... 49
   Creating a Group ........................................................................ 49
   Editing a Group .......................................................................... 50
   Roles ....................................................................................... 51
   Viewing or Searching for a Role ...................................................... 52
   Creating a Role .......................................................................... 52
   Editing a Role .......................................................................... 53
DEVICES ▶ TAKE OWNERSHIP (central station and dealer) ................... 53
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.
- Upload and download programming data.
- 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.

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 EST)

Obtaining a Dealer Account

Dealers must request a User Name and Password from their central station or sign up online by visiting the AlarmNet 360 website:

https://services.alarmnet.com/AlarmnetDirectP_SignUp/

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.

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.

Sim= 12345678901234567890
Mac=00DXXXXX5  Mac  CRC XXXX
Imei=123456789012345
01-05-2010      10:24:17        IGSMV
Logging In

1. To access AlarmNet 360 visit the following link: https://services.alarmnet.com/AlarmNetDirect/

   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.

![Desktop Shortcut](image)

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.

![Login Page](image)

3. Click on the Browser Requirements and ensure your browser meets the requirements. Also you can access online help by clicking Help at the bottom of any window.

4. Enter your User Name, and Password then click Login. The Device Status window appears.
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.

**Dealer Tool Bar**

**Central Station Tool Bar**
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.

AlarmNet 360 is easy to navigate, it uses tool bar tabs that group associated tools. And 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 GSM/I and Replace Other Device. Each wizard steps you through the proper procedure so the task is done easily and completely.

Since there are a broad band of tasks and many tools, finding the right starting point may not be easy. 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>Account Center, portal access</td>
<td>Account Center  (Log in, then refer to the online help)</td>
</tr>
<tr>
<td>accounts, cancelling</td>
<td>Accounts ▶ Account Cancellation</td>
</tr>
<tr>
<td>accounts, editing</td>
<td>Devices ▶ Programming (Use Action column pulldown menu.)</td>
</tr>
<tr>
<td>accounts, generation</td>
<td>Accounts ▶ Generate</td>
</tr>
<tr>
<td>account reports, generate</td>
<td>Insights, then at the Accounts Map page, click Export.</td>
</tr>
<tr>
<td>account, view</td>
<td>Accounts ▶ View</td>
</tr>
<tr>
<td>automation devices, TUX series, adding</td>
<td>Devices ▶ Manage TC 2.0</td>
</tr>
<tr>
<td>(use this when adding to an existing system)</td>
<td></td>
</tr>
<tr>
<td>automation devices, TUX series, enrolling</td>
<td>Devices ▶ Programming</td>
</tr>
<tr>
<td>(use this when TUX will stand alone)</td>
<td></td>
</tr>
<tr>
<td>automation devices, TUX series, replacing</td>
<td>Devices ▶ Replace Device</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>API documents, request for</td>
<td>(dealer) My Company▶ API Documents</td>
</tr>
<tr>
<td>cancelling accounts</td>
<td>Accounts ▶ Cancel</td>
</tr>
<tr>
<td>company information, manage</td>
<td>My Company ▶ Company Info</td>
</tr>
<tr>
<td>Task</td>
<td>Location</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>coverage maps</td>
<td>(central station) Tools ➤ Coverage Maps</td>
</tr>
<tr>
<td></td>
<td>(dealer) Tools ➤ Coverage Maps</td>
</tr>
<tr>
<td>customer notifications</td>
<td>Tool Bar ➤ Customer Notification</td>
</tr>
<tr>
<td>dealer services, enable remote &amp; video serv.</td>
<td>My Company ➤ Dealer Services.</td>
</tr>
<tr>
<td>device, history</td>
<td>Devices ➤ Device History</td>
</tr>
<tr>
<td>device, program new</td>
<td>Devices ➤ Programming</td>
</tr>
<tr>
<td>device, replace</td>
<td>Devices ➤ Replace Device</td>
</tr>
<tr>
<td>device, show programmed devices</td>
<td>Devices ➤ Show Programmed Devices</td>
</tr>
<tr>
<td>device, status</td>
<td>Devices ➤ Device Status</td>
</tr>
<tr>
<td>device, substitution PIN generation</td>
<td>Tools ➤ Substitution PIN Generation</td>
</tr>
<tr>
<td>device, take ownership</td>
<td>Devices ➤ Programming ➤ Take Ownership</td>
</tr>
<tr>
<td>editing, account</td>
<td>Devices ➤ Programming</td>
</tr>
<tr>
<td></td>
<td>(Use Actions column pulldown menu.)</td>
</tr>
<tr>
<td>IP devices (TC1), adding, editing, deleting</td>
<td>Devices ➤ Programming</td>
</tr>
<tr>
<td></td>
<td>(Use Actions column pulldown menu.)</td>
</tr>
<tr>
<td>IP devices (TC2), adding, editing, deleting</td>
<td>Devices ➤ Manage TC 2.0</td>
</tr>
<tr>
<td>notifications, customer</td>
<td>Tool Bar ➤ Customer Notification</td>
</tr>
<tr>
<td>PIN generation, substitution</td>
<td>Tools ➤ Substitution PIN Generation</td>
</tr>
<tr>
<td>program new device</td>
<td>Devices ➤ Programming</td>
</tr>
<tr>
<td>reports, account, generate</td>
<td>Insights, then at the Accounts Map page, click Export.</td>
</tr>
<tr>
<td>resetting the TC2 account username, email or password</td>
<td>Devices ➤ Manage TC 2.0</td>
</tr>
<tr>
<td>SIM, activation/status</td>
<td>Tools ➤ Cellular Activation/Status</td>
</tr>
<tr>
<td>ownership of device, take</td>
<td>Devices ➤ Programming ➤ Take Ownership</td>
</tr>
<tr>
<td>TC1 account, edit, delete</td>
<td>Devices ➤ Programming</td>
</tr>
<tr>
<td></td>
<td>(Use Actions column pulldown menu.)</td>
</tr>
<tr>
<td>TC2 accounts, manage, edit, delete</td>
<td>Devices ➤ Manage TC 2.0</td>
</tr>
<tr>
<td>TC2 accounts, reset username, email, or password</td>
<td>Devices ➤ Manage TC 2.0</td>
</tr>
<tr>
<td>TUX series automation devices, adding</td>
<td>Devices ➤ Manage TC 2.0</td>
</tr>
<tr>
<td>(use this when adding to an existing system)</td>
<td></td>
</tr>
<tr>
<td>TUX series automation devices, enrolling</td>
<td>Devices ➤ Programming</td>
</tr>
<tr>
<td>(use this when TUX will stand alone)</td>
<td>(Use Actions column pulldown menu.)</td>
</tr>
<tr>
<td>TUX series automation devices, replacing</td>
<td>Devices ➤ Programming</td>
</tr>
<tr>
<td>(Use Actions column pulldown menu.)</td>
<td></td>
</tr>
<tr>
<td>users, manage</td>
<td>My Company ➤ Manage Users</td>
</tr>
<tr>
<td>users, my profile</td>
<td>Main Page ➤ 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 ➤ Programming</td>
</tr>
<tr>
<td>(use to configure TC1 or TC2 devices)</td>
<td>(Use Actions column pulldown menu.)</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 Device**

**Device Type:**
This includes; City-CS-Sub, 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.

- **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 GSM device report in it 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 6.5 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.

<table>
<thead>
<tr>
<th>Time (GMT)</th>
<th>Action</th>
<th>User ID</th>
<th>City</th>
<th>CS</th>
<th>Sub</th>
<th>MNC</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-27 10:30:57</td>
<td>Status Retrieved</td>
<td>CS Branch Manager, Kitchick</td>
<td>89</td>
<td>21</td>
<td>1012</td>
<td></td>
<td>103.232.224.249</td>
</tr>
<tr>
<td>2017-03-27 10:30:56</td>
<td>Status Requested</td>
<td>CS Branch Manager, Kitchick</td>
<td>89</td>
<td>21</td>
<td>1012</td>
<td></td>
<td>103.232.224.249</td>
</tr>
<tr>
<td>2017-03-27 10:30:26</td>
<td>Status Retrieved</td>
<td>CS Branch Manager, Kitchick</td>
<td>89</td>
<td>21</td>
<td>1012</td>
<td></td>
<td>103.232.224.249</td>
</tr>
<tr>
<td>2017-03-27 10:30:22</td>
<td>Status Requested</td>
<td>CS Branch Manager, Kitchick</td>
<td>89</td>
<td>21</td>
<td>1012</td>
<td></td>
<td>103.232.224.249</td>
</tr>
</tbody>
</table>
TOOLS ► Cellular 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 "Program New Devices GSM/I" tool presented later in this guide. However there may be times when you want to see if a SIM is already activated, or may want to pre-activate a SIM to simplify installing communication devices in the field.

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://services.alarmnet.com/AlarmnetDirect, 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.
TOOLS ► 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.

- Upon completion, click GET PIN.

Editing a Lyric device

You can edit a Lyric device by clicking the Edit option in the AlarmNet main window.

LYRIC DEVICE ► Account Overview

You can log into the customer’s account to check if their account is properly configured. You can also view the location details, account status, and other panel related specifications.
**LYRIC DEVICE ➤ Account Overview ➤ Save as Template**

The **Save as template** option in the **Account Overview** page allows you to save the template.

1. Click **Save as Template** in the **Account Overview** page.

2. Enter the **Template Name** and **Template Description**.

3. Click **SAVE**.

**LYRIC DEVICE ➤ Account Overview ➤ Sync**

The **Sync** option in the **Account Overview** page allows you to sync the account with the panel.

1. Click **SYNC** in the **ACCOUNT OVERVIEW** page.

2. Based on the requirement, select **Alarmnet** or **Panel**.

3. Click **Start Sync**.
LYRIC DEVICE ► Settings

You can modify the settings for the following:

- System
- Area
- Communicator
- Reporter

LYRIC DEVICE ► Users

This tool enables you to add users, assign features to users, and edit their profiles.
LYRIC DEVICE ► Users > New User

1. Click NEW USER in the USERS page.

2. Fill in all the fields and click Save.

OR

You can also click Save and Add Another to save the current details and another new user.

LYRIC DEVICE ► Sensors

The sensor detects events or changes in quantities and provides the corresponding output. You can add a single sensor or add multiple sensors.
LYRIC DEVICE ► Sensors > Add New Sensor

1. Click **ADD SENSOR** in the **SENSORS** page.

2. Fill in all the fields and click **Save**.

   **OR**

   You can also click **Save and Add Another** to save the current details and another new sensor.

LYRIC DEVICE ► Sensors > Cross Zones
LYRIC DEVICE ► Sensors > Cross Zones

1. Click ADD CROSS ZONE under Cross Zones, in the SENSORS page.

![Add Cross Zone](image1)

2. Fill in all the fields and click Save.

LYRIC DEVICE ► Keyfobs

The built-in authentication of the keyfob enables you to control security system present in each zone.
LYRIC DEVICE ➤ Keyfobs ➤ Add Keyfob

1. Click **ADD KEYFOB** in the **KEYFOBS** page.

2. Fill in all the fields and click **Save**.

   OR

   You can also click **Save and Add Another** to save the current details and another new keyfob.

LYRIC DEVICE ➤ Keypads

The flexible, easy-to-use keypads enable security and convenience at your fingertips.
LYRIC DEVICE ► Keypad > Add New Keypad

1. Click **ADD KEYPAD** in the **KEYPADS** page.

   ![Add New Keypad screenshot]

2. Fill in all the fields and click **SAVE**.
   
   OR
   
   You can also click **SAVE AND ADD ANOTHER** to save the current details and another new keypad.

LYRIC DEVICE ► Reporting Test

This tool enables you to view the previously performed reporting test reports and raise a reporting test request. The reporting test ensures that the alarm from each sensor is accurately reported to the Central Station.

![Reporting Test screenshot]
1. Click **NEW REPORTING TEST** in the **REPORTING TEST** page.

2. Select **I have informed the Central Station**.

3. Click **START TEST**.

**LYRIC DEVICE ► Diagnostics**

The **Diagnostics** page enables you to diagnose any issue with the configuration of

- Communicators
- Panels

**LYRIC DEVICE ► Diagnostics ► Communicator Diagnostics**

The **Communicator Details** pane displays the details of the configured communicator.
• Click **Communicator** in the **DIAGNOSTICS** page.

The details of the communicator is displayed under **Communicator Details**.

---

**LYRIC DEVICE ► Diagnostics > Panel Diagnostics**

The **Panel** page displays the details of the configured panels.

• Click **Panel** in the **DIAGNOSTICS** page.

Under Panel Status pane, you can click:

• **Time on Panel**: To monitor the panel time.

• **AC Power Status**: To monitor the status of the AC Power to the panel.

• **Battery Status**: To monitor the battery status of the panel.

---

**LYRIC DEVICE ► Diagnostics > Installation Quality**

The **Installation Quality** page enables you to verify the Quality of Installation by validating against a checklist which you have created.
• Click **Installation Quality** in the **DIAGNOSTICS** page.

  • Evaluation of a checklist is done against the data in AlarmNet 360. Hence, to obtain accurate results, it is recommended to ensure that the data in AlarmNet 360 is latest.

**NOTES:**

• **Last Evaluated Result** enables you to view:
  
  o **All Rules**: Displays the list of configured rules for the selected checklist.
  
  o **Failed Rules**: Displays the list of failed rules.
  
  o **Checklist Name**: Displays the name of the last evaluated checklist. If you delete any checklist after evaluation, then, the **Checklist Name** displays **Deleted**.

• **Results**: Displays the date and time of the evaluation.

• Click 📄 to print the evaluation result.

• Click 📝 to export the evaluation result to an .xls file.

The **Last Evaluated Result** is refreshed only after you a select a checklist for evaluation.

**LYRIC DEVICE ➤ Event Log**

The Event Log page enables you to view the list of events.

You can generate an event log based on the following filters.

• **Date Range**

• **Open/Close Events**

• **Non-Security Events**

• **Trouble Events**

• **Alarm Events**

• **Bypass Events**

• **All**
<table>
<thead>
<tr>
<th>Date and Time [UTC]</th>
<th>Event Description</th>
<th>Event Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-03-30 05:20:50</td>
<td>System log entry</td>
<td>E</td>
</tr>
<tr>
<td>2017-03-30 05:20:50</td>
<td>Sensor 1 log</td>
<td>E</td>
</tr>
<tr>
<td>2017-03-30 11:15:50</td>
<td>Sensor 1 log</td>
<td>E</td>
</tr>
<tr>
<td>2017-03-30 12:00:00</td>
<td>System log entry</td>
<td>E</td>
</tr>
<tr>
<td>2017-03-30 12:00:00</td>
<td>Sensor 1 log</td>
<td>E</td>
</tr>
<tr>
<td>2017-03-30 12:00:00</td>
<td>Sensor 2 log</td>
<td>E</td>
</tr>
</tbody>
</table>

Note: Event Log data will be available only for last 10 days.
LYRIC DEVICE ➤ Activity Log

The Activity Log displays the list of activities performed.

You can generate an activity log with the following details:

- Date and Time
- Activity Type
- Operation Type
- Activity
- Performed By
ACCOUNTS ▶ View (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>Terms . . .</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start/End Range</strong></td>
<td>Filter the search by specifying a range of values to limit the subscriber numbers in the results. Enter a Starting Range value or End Range value, or both. Note, the End Range must be greater than the Starting Range.</td>
</tr>
<tr>
<td><strong>Select Services</strong></td>
<td>Filter the search by using the check boxes to select the service type.</td>
</tr>
</tbody>
</table>
| **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** — The device is actively using the network and may be billed. |
| **Account Details pop-up window** | Double clicking the account’s Sub number causes a details pop-up window to appear.  

- 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.  
- 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.  
- Closing the browser may not always log the user off the session. The user should always explicitly log out and not just close the browser window. |
| **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>AlarmNet — A</th>
</tr>
</thead>
<tbody>
<tr>
<td>7720 series (1 way)</td>
</tr>
<tr>
<td>7820 series (1 way)</td>
</tr>
<tr>
<td>7920 series (2 way)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AlarmNet — I</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSMV, IGSMV, GSMV4G, IGSMV4G</td>
</tr>
<tr>
<td>GSMV-EX</td>
</tr>
<tr>
<td>GSMHS, IGSMHS, IGSMHS4G</td>
</tr>
<tr>
<td>GSMX, GSMX4G</td>
</tr>
<tr>
<td>GSCMF, IGSCMF</td>
</tr>
<tr>
<td>IGSCMF4G</td>
</tr>
<tr>
<td>IPGSM-COM, IPGSM-DP, and IPGSM-DPC series</td>
</tr>
</tbody>
</table>
ACCOUNTS ➤ Generate (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, then select the Service Type. 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 – A</th>
<th>AlarmNet – I</th>
</tr>
</thead>
<tbody>
<tr>
<td>7720 series (1 way)</td>
<td>GSMV, IGSMV, GSMV4G, IGSMV4G</td>
</tr>
<tr>
<td>7820 series (1 way)</td>
<td>GSMV-EX</td>
</tr>
<tr>
<td>7920 series (2 way)</td>
<td>GSMHS, IGSMHS, IGSMHS4G</td>
</tr>
<tr>
<td></td>
<td>GSMX, GSMX4G</td>
</tr>
<tr>
<td></td>
<td>GSMCF, IGSMCF</td>
</tr>
<tr>
<td></td>
<td>IGSMCFP4G</td>
</tr>
<tr>
<td></td>
<td>IPGSM-COM, IPGSM-DP, and IPGSM-DPC series</td>
</tr>
<tr>
<td></td>
<td>IPGSM-4G</td>
</tr>
<tr>
<td>IPGSM-4G</td>
<td>ILP5, GSMVLP, GSMVLP5, GSMVLP4G, GSMVLP54G</td>
</tr>
<tr>
<td>ILP5, GSMVLP, GSMVLP5, GSMVLP4G, GSMVLP54G</td>
<td>7845GSM, 7845i-GSM, and 7845i-ent series</td>
</tr>
<tr>
<td>7847i</td>
<td>7847i</td>
</tr>
<tr>
<td>7810PC</td>
<td>7810PC</td>
</tr>
<tr>
<td>8132i (Symphony)</td>
<td>8132i (Symphony)</td>
</tr>
</tbody>
</table>

**Note:** Information above also applies to the Canadian product equivalents.
ACCOUNTS ➤ Cancel (central station)
This tool enables you to cancel Subscriber accounts.
This brings up the Account Cancellation form, 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 **Choose File**, 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></td>
<td></td>
<td></td>
<td>P = for transmitters removed from service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(partial cancel)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>F = for transmitters that are still installed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></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

**TOOLS ► 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.
MY PROFILE (central station and dealer)

Click the user profile icon appearing at the top right corner of the main page and then click **MY PROFILE**. This option enables you to edit your profile.

- Edit your profile and click **UPDATE**.

This field will appear for Central Stations only
MY ACTIVITIES (central station and dealer)

Click the user profile info icon appearing at the top right corner of the main page and then click MY ACTIVITIES. This option 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 ► Dealer Branding (dealer managers)

This tool displays the option to upload:

- dealer logo
- dealer contact information
- images that appear as a slideshow when the panel is in idle state

**Uploading Dealer Logos**

1. Click **MY COMPANY > Dealer Branding**.

2. Under **Logo**, click ![open file icon] to browse and select the logo image or icon. The uploaded image appears as a preview.

3. Under **Contact Information**, click ![open file icon] to browse and select the dealer contact information in an image format. The uploaded image appears as a preview.

4. Under **Slide Show**, click ![open file icon] to browse and select images that appear as a slideshow when the panel is in idle state. The uploaded image appears as a preview.

5. Click **CONFIRM**.

MY COMPANY ► Company Info (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 envelope, 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 Users > Manage Users.

Choices will vary depending on privilege level.
| Select the user and enable the "AND: Company Information" feature to their profile. |  |
DEVICES ► Programming (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.

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 blue bar category can be viewed/edited by clicking the icon or link.

Save your changes by clicking Finish.
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 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 select "Begin Working with My Account", the wizard process is complete and you will remain in AlarmNet 360. Navigate DEVICES ► 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.

DEVICES ► Programming ► Drafts

This option enables you to pre-program an account before installation. While you are creating an account, you can enter all the relevant details pertaining to the account, without the City-CS-Sub and MAC address, and then save the account as a draft.
After you obtain the City-CS-Sub and MAC address, you can update the details.

1. In the Programming page, click Drafts.
2. From the Actions column, select Edit against the required account and then click ☑.
   The Account Overview page, with the message, Account is in Draft State, appears.
3. Click CREATE ACCOUNT at the top right corner of the page.
4. From the drop-down list, select the Communicator Type.
5. Based on the selected communicator type, you can enter the following details:
   - Cellular/Ethernet MAC or WiFi MAC
   - Cellular/Ethernet CRC or WiFi CRC
   - Alarm Reporting Number
6. Click CONTINUE to verify the entered details.
7. Select TOTAL CONNECT 2.0 to:
   - Create a TC account
     OR
   - Associate an existing TC account
8. Click CONFIRM to create the account.

ACCOUNTS ► 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. In the Accounts page, type the MAC ID and search for the device.
2. From the Actions column, select Replace Device, then click .

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

**DEVICES ► Manage TC 2.0 Accounts (central station and dealer)**

This tool is for managing accounts associated with TC2 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. 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**.

The device has been added.

**Adding TUX series Automation Devices**

*Note:* TUX can only be used on Vista series panels.

To add TUX devices to a TC 2.0 ready control panel (such as a VISTA 21iP) 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 an appropriate **Device Name**.
5. Select the **Device Type** as **Automation**.
6. Enter the **MAC** number and the **CRC** for the device.
7. Click **NEXT** to verify the MAC and CRC.
8. Once verified, then click **Save**.

**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.

![Image showing TC2 account management](image)

**Checking the customer’s TC2 account configuration**

You can log into the customer’s TC2 account to check if their account is properly configured. This feature, also referred to as “TC2 Punch Through”, is a READ ONLY mode. To ensure the customer’s privacy video will not be visible. Follow the steps below.

- To enable this feature, click the **Security Professional Access** icon.
The customer’s TC2 account will open in READ ONLY mode to enable you to check it.

**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 ► Templates (central station and dealer)**

This option enables you to create a new template, view, and delete the existing templates. Templates are used to create “master” files to speed up programming of a new account. A template gives you a very quick and easy way to add a customer’s panel programming information.

**Viewing or Searching for a Template**

The Template page lists the templates, along with the template Name, Description, Panel Name, Communicator Name, Created On and Created By.

To search for a template:

1. In the AlarmNet 360 home page, click the icon. From the list select **DEVICES > Templates**.
The Templates page appears.

2. Type the Template Name in the search bar and then press Enter.

The relevant template, with all the details, is listed.

Creating a New Template

The New Template (custom template), option enables you to create a new template.

To create a new template:

1. In the Templates page, click NEW TEMPLATE. The Create Template pane appears.

   ![Create Template pane](image)

   2. Enter the following details.
      - Name: Type the name of the template.
      - Description: Type the description for the template.
      - Panel: From the list, select the type of panel. The panels are categorized, grouped, and then listed.
      - Panel Revision: From the list, select a revision number for the panel.
      - Template Default: From the list, select to set a default template for the newly created custom template.

   3. Click SAVE AND CONFIGURE TEMPLATE. The Configure Template page appears.

   NOTE: Click Cancel to cancel creating a template.

4. You can view/edit the following options available in the Configure Template page.
   - Settings: Click to modify the System, Area, Communicator, and the Reporter options.
   - Users: Click to modify the user options.
   - Sensors: Click to modify the sensor options.

5. Click Done.

DEVICES ▶ Checklist (central station and dealer)

The Checklist option helps in validating the Installation Quality by verifying the configuration done by the Installer during commissioning.

Viewing or Searching for a Checklist

The Checklist page lists the checklists, along with the checklist Name, Description, Created On, and Created By.

To search for a checklist:

1. In the AlarmNet 360 home page, click the icon. From the list select DEVICES > Checklist.

   The Checklists page appears.
2. Type the **Checklist Name** in the search bar and then press **Enter**.

The relevant checklist, with all the details, is listed.

**Creating a Checklist**

1. In the **Checklists** page, click **NEW CHECKLIST**. The **Checklist** page appears.

2. Type a **Name** for the checklist.

3. Type a **Description** for the checklist.

   **NOTE:**

   You can search through the list of configured rules or categories. Type the rule name and then press **Enter**. The rule, along with the configured detail, appears.

4. Under **AVAILABLE RULES**, click to add a new rule.

   **NOTE:**

   Whenever you configure a new rule, the **CONFIGURATION DETAILS** are updated alphabetically.

   For example, to create **AlarmNet Services** rule, navigate

   - Click **AlarmNet Services > Lyric Lock**.

   On the right pane, under **CONFIGURATION DETAILS**, the selected rule appears.

   Similarly, you can add and configure multiple rules.

   **NOTE:**

   Rules that can be used only once becomes inactive after configuration. However, there are few exceptions for certain rules and can apply the same rule for a different condition.
5. You can select parameters and set conditions for the following:

- By default, the first drop-down, **Rule Name**, is disabled.
- The second drop-down, **Logic**, enables you to select a condition for the rule.
- Based on the selected rule and condition, you can set the third column, **Value**, with the relevant parameter.

**A few examples are described below.**

i. To convert the following requirement

- 'Partition' as a rule in the user interface, you must perform the following:
  
  a. By default, the first drop-down, is set to **Rule Name** as **Auto Stay Arming**.
  
  ![Image](image1.png)

  b. From the second drop-down, select to set the **Logic** for the parameter.

  ![Image](image2.png)

  c. From the third drop-down, select a value for the condition.

  ![Image](image3.png)

  d. Click **SAVE**.

  ii. To convert the following requirement

  - 'Sensor' as a rule in the user interface, you must perform the following:
    
    a. By default, the first drop-down, is set to **Rule Name** as **Device Type**.
b. From the second drop-down, select to set the condition for the parameter.

c. From the third drop-down, enter a value for the condition.

d. Click the icon to add a condition for the parameter.

**NOTES:**

You can click the:

- + icon to add multiple conditions.
- - icon to delete all the conditions.

- Under **Condition Name**,  
  - From the first drop-down list, click and select **Condition Name**.
  - From the second drop-down list, click and select the logic as **IS**.
From the third drop-down list, click to set the **Value** to **Entry Exit 1**.

**NOTE:**

To enable the **CR** condition, you need to add two or more conditions.

- Click the **+** icon to add an additional condition.

  ![Diagram](image1)

- Configure the **Condition Name**, **Logic**, and **Value**.

  ![Diagram](image2)

- Click the **+** icon to add an additional condition.

  ![Diagram](image3)

- Configure the **Condition Name**, **Logic**, and **Value**.

  ![Diagram](image4)

- Click **SAVE**.

iii. **To convert the following requirement**

   - **'Automation Device'** as a rule in the user interface, you must perform the following:

     a. From the first drop-down, select to set parameter as **Device Name**.

     ![Diagram](image5)

     b. From the second drop-down, select to set the condition for the parameter.

     ![Diagram](image6)
c. From the third drop-down, enter a value for the condition.

6. Click **SAVE**.

**DEVICES ➤ User Management**

The **User Management** option enables you to manage:

- Users
- Groups
- Roles

**Users**

The **USERS** option in **Manage Users** enables you to add and view user details.

**Viewing or Searching for a User**

The **USERS** tab lists the following:

- User Name
- Associated Group
- Contact Information
- Modified By
- Last Modified
- Last Login
- Status

In the **USERS** page, you can click any associated group to view the user details.

The **User** dialog box enables you to:
- View the user configuration details
- View the associated groups and roles
- Edit the user
- Access link to manage groups

**NOTE:**
- The search bar enables you to search users by:
  - Name
  - Group Name
  - Email
- The **Advanced Search** option enables you to search users based on various filters.

**Adding a User**

**NOTE:**
- You must first ensure to:
  - Create **Roles**.
  - Create **Groups** to associate the role/s.

For companies with few users, you can directly assign roles to a user, without creating groups.

**To add a user:**

1. In the **USERS** tab, click **CREATE USER**. The **CREATE USER** dialog box appears.

![CREATE USER Dialog Box](image)

2. Enter the **First name** and the **Last name** of the user.
3. Type the **Email address** of the user.
4. Optionally, you can also type the **Employee ID**.
5. Under **GROUPS**, select to associate the user to a group.
6. Click **SAVE**. A confirmation message appears.
7. Click **OK**.

**NOTE:**
- The **BACK** option in the **CREATE USER** dialog box, enables you to:
Save the unsaved changes
OR
Click CANCEL to exit the message
OR
Click CONTINUE to proceed without saving the changes

Groups

The GROUPS option in Manage Users enables you to create groups and associate role/s. The search option enables you to search through the list of role names.

Viewing or Searching for a Group

The GROUPS tab lists the following:
- **Group Name**: Displays the name of the group, along with the associated features
- **Description**: Describes the group
- **Roles**: Displays the role the group is associated to
- **Labels**: Displays the City-CS-Sub code selected for the relevant group.
- **Last Modified**: Displays the last modified time and date
- **Modified By**: Displays the user details of those who last modified the group

In the GROUPS page, you can click any group to view the group details.

The Group dialog box enables you to:
- View the roles assigned to the relevant group
  - SHOW ALL FEATURES to expand and view the associated features of the selected role
  - HIDE ALL FEATURES to collapse the associated features of the selected role
- Create a copy of the group
- Edit the group
- Access link to manage roles

Creating a Group

The CREATE GROUP option enables you to create a group and associate roles to the created groups.

NOTE:
You must have a minimum of one role to create a group.

To create a group:
1. In the **GROUPS** tab, click **CREATE GROUP**. The **CREATE GROUP** dialog box appears.

![CREATE GROUP dialog box]

2. Type the **Group Name**.
3. Type a **Description** for the group name.
4. Under **ROLES**, click **ASSIGN ROLE**.
5. From the **Role Name** drop-down list, select a role.

**NOTES:**
- **ASSIGN ANOTHER ROLE** enables you to assign a different role for the selected group.
- You cannot assign the same role within a group. For example, you cannot assign two administrator roles for the same group.
6. Under **ACCOUNT ACCESS**, you can search and associate one or more City CS code.
7. The **Available City CS** list displays the list of associated City CS codes.
8. Click **SAVE**.

**NOTES:**
- The **BACK** option in the **CREATE GROUP** dialog box, enables you to:
  - Save the unsaved changes
  - Click **CANCEL** to exit the message
  - Click **CONTINUE** to proceed without saving the changes

**Editing a Group**

The **EDIT** option enables you to edit the:
- name and description of the group
- selected roles
- access labels

**To edit a group:**
1. In the **GROUPS** tab, click **EDIT**. The **EDIT** dialog box appears.
2. Modify the **Group Name** and the **Description** for the group name.
3. Under **ROLES**, click to modify the assigned roles.
4. Click **SAVE**.

**NOTES:**
- Click **BACK** to view the **GROUP** dialog box.
- OR
- Click **UNDO CHANGES** to exit without saving the changes.

**Roles**

The **ROLES** option in **Manage Users** enables you to:
- Search a role by name
- Create a role
- View role details
- Sort roles

Roles are classified as:
- **Standard Role**: Standard roles enables you to:
  - Replicate the existing roles
  - Edit the replicated features

  By default,
  - five standard roles are available to the dealer and central station user.
  - two standard roles are available to the Honeywell user.

  **NOTE:**
  Administrator role cannot be replicated.

  The Standard roles, displayed in the following list, is denoted with the  icon and cannot be edited.
  - Accounts Payable
  - Administrator
  - Data Manager
  - Sales Support
  - Service Support

- **Custom Role**: Custom role enables you to create a new role and assign features.

  You can create a maximum of 45 custom roles.
Viewing or Searching for a Role

The ROLES tab lists the following:

- **Name**: Displays the name of the role, along with the associated features
- **Description**: Describes the role
- **Associated Groups**: Displays the group the role is associated to
- **Last Modified**: Displays the date and time of the role that was last modified
- **Modified By**: Displays the user details of those who last modified the role

Creating a Role

The CREATE ROLE option enables you to add a new role. Every role contains a list of features associated with it. Based on the login credentials, you can configure different access levels to the feature.

**NOTES:**

- You must ensure that each role must contain a minimum of one feature.
- You cannot edit or delete a standard role.
- You cannot duplicate the **Role Name** or the **Features**.

To add a new role:

1. In the Roles tab, click **CREATE ROLE**. The CREATE ROLE dialog box appears.

   ![CREATE ROLE dialog box](image)

2. Type the **Role Name**. The name must begin with an alphabet and should not exceed 50 characters. It can contain alphanumeric characters.

3. Type a **Description** for the role. Maximum character limit is 150.

4. Under **FEATURES**, select to associate the feature to the role.
   - System Programming
   - Alarmnet Insights 360
   - Diagnostics
   - Device Programming
   - Cellular Configuration
   - Account Management
   - User Management
   - Billing
- API Management
- G3 Billing
- Total Connect 1
- Total Connect 2.0
- **TC 2.0 PreConfigure**: This feature is available only when you enable Total Connect 2.0.

5. Click **SAVE**. A confirmation message appears.

**NOTES:**
- The **BACK** option in the **CREATE USER** dialog box, enables you to:
  - Save the unsaved changes
  - OR
  - Click **CANCEL** to exit the message
  - OR
  - Click **CONTINUE** to proceed without saving the changes

**EDITING A ROLE**

The **EDIT** option enables you to edit the:
- name and description of the role
- selected features

**To edit a role:**
1. In the **ROLES** tab, click **EDIT**. The **EDIT** dialog box appears.
2. Modify the Role Name and the Description for the role name.
3. Under **FEATURES**, click to modify the assigned features.
4. Click **SAVE**.

**NOTES:**
- Click **BACK** to view the **ROLE** dialog box.
  - OR
- Click **UNDO CHANGES** to exit without saving the changes.

**DEVICES ➤ TAKE OWNERSHIP (central station and dealer)**

This option 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.
DEVICES ► MANAGE OWNERSHIP (central station and dealer)

Managing Account Ownership

AlarmNet 360 provides the ability to manage dealer ownership of your accounts. This provides the flexibility for AlarmNet Dealers to take and relinquish ownership of accounts or transfer them to the Central Station as needed.* Dealers and Central Stations are encouraged to communicate with each other directly on any ownership changes.

To manage ownership of your accounts through AlarmNet 360, follow the steps below.

1. Click “Device Programming” on the Navigation Bar
2. Search for the account by entering the City-CS-Sub number or the 12-Digit MAC ID of the communicator, then click “Search”
3. Once the Account Information appears, click the “Actions” dropdown and select “Manage Ownership”
4. Choose the appropriate option, type “I Agree,” then click “Submit”
5. Once submitted you will receive a “Success” message stating that the action you selected has been done

NOTE: If the account is one location of a multi-site Honeywell Total Connect Remote Services account, a pop-up will appear stating that ownership cannot be managed through AlarmNet 360. Please contact AlarmNet Customer Service for assistance at 1(800) 222-6525, option 3, or contact securitycustomersupport@honeywell.com.

*AlarmNet Central Stations will always have access to their accounts.

DEVICES ► ACCOUNT MIGRATION (central station and dealer)

LYNX Touch panels that were originally programmed using the Compass Downloader or locally at the control panel can be moved to AlarmNet 360. Once the panel has been migrated, the following operations can be performed using AlarmNet 360.

- Panel Programming (e.g. Entry/Exit Delays, Bell Timeout, Report Options, etc.)
- Zone Programming [Sensors, User Codes, Wireless Keys (Keyfobs), etc.]
- View Panel and Zones Status
- View Panel Event Logs

Before migration can be completed, the following conditions must be met:

- The panel must be equipped with an AlarmNet communication module (e.g.; GSMVLP5-4G/GSMVLP5CN4G, 3GL/3GLC, 4GL/4GLC, CDMA-L57, ILP5 or L5100-WiFi)
• The communicator must have been programmed using AlarmNet Direct or AlarmNet 360
  
  o If the Communicator was registered locally from the control panel or via Honeywell Tech support, you must take ownership of the account through the AlarmNet 360 Device Programming page

**Panel Migration**

For LYNX Touch 5200, 5210 and 7000 control panels that were not programmed remotely using the Compass Downloader, skip Steps 1 – 3 and proceed directly to Step 4.

If the Compass Downloader was used to program the panels, AlarmNet 360 requires the CSID and Account Number from Compass to connect to the panel.

1. Update Compass to the latest version (2.2.25.3 and higher). The Compass software can be downloaded from MyWebTech at: [https://mywebtech.honeywellhome.com/](https://mywebtech.honeywellhome.com/).

2. Open the Compass application and log in (as any user with “View CSID/Proprietary ID in Panels” permission level.). Select “Reports” from the toolbar and select “Account Information” from the reports list. Select “Generate Report” to download the report, which exports encrypted CSIDs and account numbers for all LYNX 5200, 5210 and 7000 Control Panels, to your computer.

3. Log into AlarmNet 360, select the menu item “Import Compass Data.” The page opens in a new browser tab or window. Dealer Manager, Super User, Master User or Branch Manager access is required. Browse the Account Information Report and select the “Import Compass Data” button. Once the import is complete, those panels are ready to be programmed using AlarmNet 360.

4. Locate the account in AlarmNet 360 by searching the City-CS-Sub or MAC ID from the Device Programming option. Select "Edit" from the Actions dropdown and click the arrow button to the right of the dropdown. The account will open in a new browser tab or window.

5. At the top right corner of the screen, select the "Sync" button and initiate a “Fetch All”. AlarmNet 360 will connect to the panel and start uploading the programming data. Once complete, new menu items including Sensors, User Codes, Panel Settings, etc., will appear on the left navigation bar.

**NOTE:** Once panel data has been moved to AlarmNet 360 (a successful ‘Fetch All’ completion), the Compass Downloader can no longer be used for those systems.
ACCOUNT CENTER (central station)

This provides a direct link to the Account Center website allowing authorized users to manage their AlarmNet payments.

From the tool bar select Account Center, then log in and refer to the online help.

MY COMPANY ► 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.

This brings up a form to request API documents.
From the tool bar select API Documents. Complete the form and click Submit.

**INSIGHTS (central station and dealer)**

This option enables you to generate and save detailed subscriber data. From the tool bar, select Insights.

This page enables you to:

- View subscription details
- Filter information
- View account status
- View list of accounts
- Export the list of accounts
CUSTOMER NOTIFICATION (central station and dealer)

Click the 📨 icon appearing at the top right of the main page.

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

**Note:** The dealer view includes a yellow flashing "You received new notification(s)!" message.

Yellow (flashing) = New notifications have been 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

| Total Connect account creation | 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:
| Account Name – Must be at least 8 characters. |
| TC2 Master user name – This is the "Username" 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 ! @ # $ % ^ * - _ = + . |
| TC2 Email address – 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. |
| *** 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 customer’s 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. |

### auto stay arm

If the security system (or a partition) is configured with Auto Stay Arm 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).

### service providers

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.

### web browser

Configure your web browser to always allow "pop-ups" from the services.alarmnet.com site.
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 to. 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**

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).
<table>
<thead>
<tr>
<th>fire zones, bypassing</th>
<th>When using Remote Access, if you attempt to bypass a fire zone, the fire zone WILL NOT be bypassed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>keypad – full control</td>
<td>When using Remote Access, if the keypad type is set to &quot;Full Control,&quot; you may view status and control all partitions using the &quot;System Status&quot; tab (not the &quot;Keypad&quot; tab).</td>
</tr>
<tr>
<td>panic keys</td>
<td>When using Remote Access, two-button panic keys such as 1+6, 6 +#, and 3 +# will not work. However single button panics (if programmed) will work.</td>
</tr>
<tr>
<td>stay mode</td>
<td>The System Status screen does not support multiple stay modes. If you need to use a specific stay mode, use the Keypad screen.</td>
</tr>
<tr>
<td>system status screen</td>
<td>The System Status screen does not support multiple stay modes. If you need to use a specific stay mode, use the Keypad screen.</td>
</tr>
<tr>
<td>zone descriptors</td>
<td>The security system's zone descriptor information will only be copied to the Remote Services database if there is no zone descriptor in its database for a particular zone. The descriptor in the database takes precedence over what might be in the security system control panel. If you want to copy the zone descriptor that is in the control panel, simply delete the zone descriptor from the database (Remote Access &gt; Setup &gt; Name Zones), then click Save Zone Names. When you start another session, the zone type, along with its descriptive name, is retrieved from the control panel.</td>
</tr>
</tbody>
</table>

**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. |
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.

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

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.

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.

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.

Error 1000 is caused 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 191 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.

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>VISTA 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>VISTA residential</th>
</tr>
</thead>
<tbody>
<tr>
<td>restart exit delay</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 / FA168CP</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-20PCN / FA168CP-CN</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-20PSIA / FA168CP-SIA</td>
<td>9.12</td>
<td></td>
</tr>
<tr>
<td>VISTA-21iP / VISTA-21iPSIA</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 / GSMVLP5CN</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>IGSMV / IGSMVCN</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.

**AlarmNet360 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><strong>U.S. and Canada:</strong> Resideo Technologies, Inc.</td>
<td><strong>1-800-222-6525:</strong></td>
</tr>
<tr>
<td>2 Corporate Center Drive</td>
<td><strong>option 1 – AlarmNet Tech Support</strong></td>
</tr>
<tr>
<td>Suite 100</td>
<td>Monday thru Friday, 8:00 am to 9:00 pm ET.</td>
</tr>
<tr>
<td>Melville, NY 11747</td>
<td>Note, between 6 pm and 9 pm some AlarmNet products are not supported.</td>
</tr>
<tr>
<td></td>
<td><strong>option 2 – AlarmNet General Product Information</strong> Monday thru Friday, 8:00 am to 5:00 pm ET.</td>
</tr>
<tr>
<td></td>
<td><strong>option 3 – AlarmNet administration and website support</strong> Monday thru Friday, 8:00 am to 5:00 pm ET.</td>
</tr>
<tr>
<td><strong>Latin America &amp; Caribbean region:</strong> Resideo Technologies, Inc. Latin American &amp; Caribbean Division</td>
<td><strong>305-805-8188:</strong> Monday thru Friday, 8:00 am to 5:00 pm ET.</td>
</tr>
<tr>
<td>9315 NW 112th Avenue</td>
<td></td>
</tr>
<tr>
<td>Miami, FL 33178 USA</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>MyWebTech</strong> (Online technical database.) <a href="https://mywebtech.honeywellhome.com/">https://mywebtech.honeywellhome.com/</a></td>
</tr>
</tbody>
</table>