tyco | American Dynamics

# ITv2 Integration for victor Unified Client User Guide

January 2023

8200-1147-1215 F

5.4.1

www.americandynamics.net

Johnson Controls

**eNotice**

The information in this manual was current when published. The manufacturer reserves the right to revise and improve its products. All specifications are therefore subject to change without notice.

**Copyright**



**Customer Service**

Thank you for using American Dynamics products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at www.americandynamics.net.

**Trademarks**

# Table of Contents

# Introduction

## ITv2 Overview

The ITv2 integration provides advanced, seamless integration between victor Unified systems and DSC Intrusion panels. This integration allows users of victor Unified Client to monitor and configure their DSC Neo and Pro Panel, alarms and personnel from the victor environment.

This document provides information about the ITv2 Integration from within the victor environment. All the features and functionality explained here are with respect to the victor platform.

## Product Components

- The victor Unified Client application is configured with ITv2 objects.
- **ITv2 Objects**: Physical or logical ITv2 entities within the victor environment. Following are the ITv2 objects:
  - **Panel**: Panel refers to the DSC PowerSeries Neo and Pro Panel Hardware which is connected to one or more keypads, sensors and detectors.

**NOTE** DSC Power series Neo and Pro panel functions in the victor Unified Client platform integrated with ITv2 integration and uses the ITv2 protocol for communication.

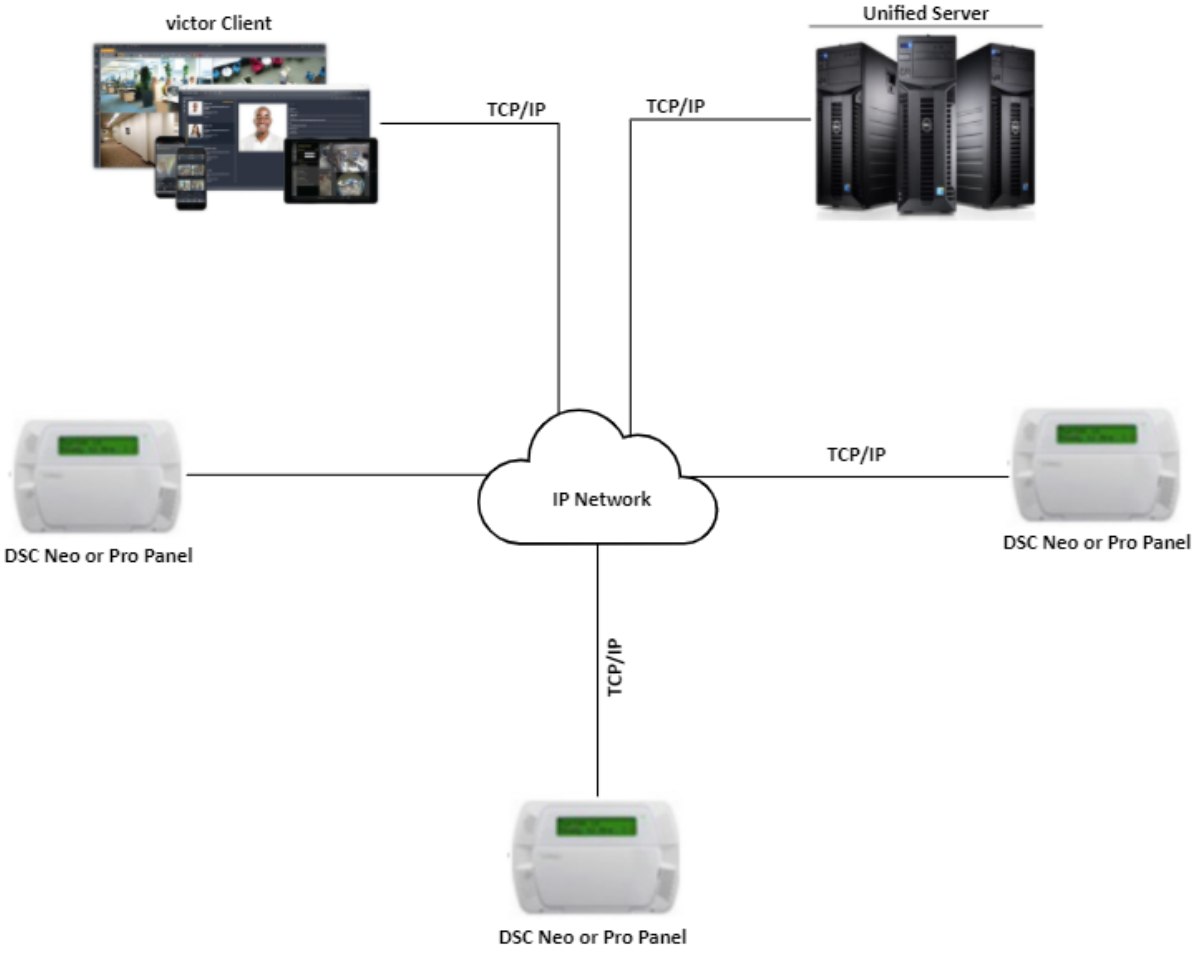
  - **Partition**: ITv2 Partition refers to a area defined in the panel. The Neo Panel supports a maximum of 8 partitions, and the Pro Panel supports a maximum of 32 partitions.
  - **Zone**: ITv2 Zone refers to the physical interface or sensors in the Neo or Pro Panel hardware. The DSC PowerSeries Neo Panel supports a maximum of 128 zones, and the Pro panel supports 248 zones.
  - **Virtual Zone**: Virtual Zone is used by the third party hardware devices to report alarms to a central monitoring station using DSC Neo and Pro panels. DSC PowerSeries Neo and Pro Panels support a maximum of 32 virtual zones.
  - **Output**: The Output object refers to an event or input to a relay on a Neo or Pro Panel. DSC PowerSeries Neo and Pro Panels support a maximum of 164 outputs

**NOTE** Zones from 21 to 36 are kept for future use, so only 148 zones will be available.

  - **Users**: The ITv2 integration can support a maximum of 1000 Users.
  - **ITv2 Server Component**: The heart of the integration, facilitates and maintains communication with the DSC Neo and Pro panels and created partitions, zones, outputs and virtual zones based on the panel capabilities.

After installing the driver, all the relevant ITv2 object editors are available from victor's intrusion ribbon bar.

**Figure 1:** System Overview: IP Configuration




## Features

The objective of the ITv2 Integration is to provide a standard, single interface between DSC Neo and Pro alarm panel and American Dynamics' victor - Video Management product.

ITv2 Integration supports:

- DSC PowerSeries Neo and Pro Panels
- TCP/IP communication
- Synchronization of the following objects from the Panel:
  - Partition
  - Zones
  - Output
  - Virtual Zones
  - Users
  - Associations
  - Attributes to the panel
- Synchronization of the following objects to the Panel:

    - Partition
    - Zones
    - Output
    - Users
    - Associations
    - Attributes to the panel
- The following actions to control the ITv2 objects:
    - Partition: Arm or Disarm.
    - Zone: Bypass or Reset.
    - Output: Activate or Deactivate.
- Create and Apply Templates for the panel
- Alarm Filtering
- Virtual Keypad
- victor Roles and Object Association
- victor Client-side Event Management
- Devices on victor Maps and Health Dashboard
- Supports TLS 1.2 for security

## Versions Supported

The victor ITv2 Integration supports the following firmware versions:

**Table 1:** Neo Versions Supported

| Hardware Version | Hardware Model | Firmware Version Supported |
|---|---|---|
| UA621 REV03 | HS2016 / HS2032 / HS2064 / HS2128 / HS2128E | v01.12.01.13 / v01.14.01.10 / v1.20.01.31 / v1.21.01.01 / v01.30.01.08 / v01.30.01 / v1.31.01.01 / v1.35.01.07 |
| UA601 Rev03 | TL280 / TL280R / TL2803G | v04.11.04.31 |
| UA628 Rev03 | HS2LCD | v01.10.01.51 / v01.11.01.1 3 / v1.20.01.29 / v1.30.01.04 / v1.35.01.03 |
| UA685 Rev01 | TL280 / TL280R / TL2803G / TL280E / TL280RE | v5.00.04.27 / v05.20.01.29 / v05.02.04.0 3 / v5.03.04.04 / v5.41.04.01 |

**Table 2:** Pro Versions Supported

| Hardware Version | Hardware Model | Firmware Version Supported |
|---|---|---|
| UA718Rev03 | HS3128PCB / HS3248PCB | v1.30 |
| UA628 Rev03 | HS2LCD | v2.30 |

**NOTE** The Communication mode supported by the ITv2 Integration is Network (TCP/IP).

# Installation

## Installation Overview

Like the victor system, the ITv2 Integration has client and server components. You must install the client components on every computer that runs victor Unified Client applications and install the server components on the victor Application Server.

## Pre-Installation Tasks

Before installing the ITv2 Intrusion Integration, ensure the following:

On the victor Application Server:

- You must have appropriate Windows permissions.
- You must be a member in the local Administrators group, or have equivalent privileges.
- victor Application Server must be installed with the ITv2 Intrusion Integration.
- To install the ITv2 Intrusion Integration on victor Application Server, you must install the .NET Framework 3.5 on victor server.

On the Clients:

- You must have appropriate Windows permissions.
- You must be a member in the local Administrators group, or have equivalent privileges.
- victor client must be installed.

## Qualified Hardware and Firmware

The ITv2 Integration has the same hardware, software, and disk space requirements as C•CURE 9000. If the target computer can install victor Application Server, then it satisfies ITv2 Intrusion Integration requirements.

Supported hardware:

- DSC Intrusion Integration Panels
  - DSC PowerSeries Neo Panels
  - DSC PowerSeries Pro Panels
- Expansion Module: Output expander / Zone expander (HSM2108 / HSM2208)
- Wireless Module: HSM2HOST / PG4984 / PG4945

The ITv2 Intrusion Integration requires the following firmware:

**Table 3:** Neo Versions Supported

| Hardware Version | Hardware Model | Firmware Version Supported |
|---|---|---|
| UA621 REV03 | HS2016 / HS2032 / HS2064 / HS2128 / HS2128E | v01.12.01.13 / v01.14.01.10 / v1.20.01.31 / v1.21.01.01 / v01.30.01.08 / v01.30.01 / v1.31.01.01 / v1.35.01.07 |

| Hardware Version | Hardware Model | Firmware Version Supported |
|---|---|---|
| UA601 Rev03 | TL280 / TL280R / TL2803G | v04.11.04.31 |
| UA628 Rev03 | HS2LCD | v01.10.01.51 / v01.11.01.1 3 / v1.20.01.29 / v1.30.01.04 / v1.35.01.03 |
| UA685 Rev01 | TL280 / TL280R / TL2803G / TL280E / TL280RE | v5.00.04.27 / v05.20.01.29 / v05.02.04.0 3 / v5.03.04.04 / v5.41.04.01 |

**Table 4:** Pro Versions Supported

| Hardware Version | Hardware Model | Firmware Version Supported |
|---|---|---|
| UA718Rev03 | HS3128PCB / HS3248PCB | v1.30 |
| UA628 Rev03 | HS2LCD | v2.30 |

## Software Requirements

The ITv2 Integration requires the following software:

- victor Application Server: v5.4.1
- victor unified client: v5.4.1

## Installing ITv2

**NOTE**

- You must install the ITv2 Intrusion Integration in the same folder as victor. If the correct version of victor is not installed, a message prompting you to install the correct version is displayed.
- It is recommended to stop the CrossFire services before initiating the installation of ITv2 Intrusion Integration.

### Procedure - Installing ITv2 on victor Application Server

1. Close all running programs and stop all services.
2. Navigate to http://www.americandynamics.net and download the appropriate version of the ITv2 Software Driver.
3. Double-click the `DSC_ITV2-x.x.xxx.x.exe file`. The Install Wizard begins and the **Welcome to ITv2 Intrusion Integration** window appears.
4. Click **Next** and follow the Install Wizard.
5. Read the The End User License Agreement EULA and select the **I accept the terms in the license agreement** button, then click **Next**.
6. Click **Install**. The program begins to install. After completion, the InstallShield Wizard Complete window appears.

**NOTE** The Start the Tyco CrossFire services check box is selected by default. If this check box is not selected, then the CrossFire services will not start automatically.

7. Click **Finish** to complete the installation.
8. Restart the system installation.
9. Restart services on victor Application Server that may have been stopped during installation.

### Procedure - Configuring the Server Services

1. Launch the Server Configuration Application:
   a. From the Windows **Start** menu, click **All Programs** and then click **Tyco**.
   b. Right-click **Server Configuration** and then **click Run as Administrator**. Server Configuration Application page opens.
2. Restart the CrossFire Services:
   a. On the **Server Configuration Application** page, click to open the **Services** tab.
   b. In the **Framework Services** area, click the **Stop** button beside Crossfire Framework Service to stop all services. Wait for the status to change to **Stopped**.
   c. Click the **Start** button beside **Crossfire Framework Service** and wait for the status to change to **Running**.
   d. Click the **Start** button beside **Crossfire Server Component Framework Service** and wait for the status to change to **Running**.
   e. In the **Extension Services** area, locate the **ITv2 Driver Service**. Select the **Enabled** check box and then click the **Start** button. The status of the ITv2 Driver Service changes to **Running**.

### Procedure - Uninstalling ITv2

1. Close all running programs.
2. Open **Control Panel** and click **Programs and Features**.
3. Right-click **ITv2** and select **Uninstall**.

   The Modify Setup dialog box appears dialog box opens.
4. Click **Uninstall**. The Drop Database dialog box appears.
5. Select one of the following options:
   - Click **Yes** to delete the database used in the ITv2 integration configuration.
   - Click **No** to retain the database used in the ITv2 integration configuration.

   The **Setup Successful** dialog box appears.
6. Click **Close** to exit from the uninstallation wizard.

**NOTE** The ITv2 integration shuts down and restarts the CrossFire services. Therefore, the ITv2 integration uninstall should be planned accordingly.

# Administration

This chapter provides information about integration support in victor Client. For more information about victor Client or victor Unified Client, refer to the *victor Administration and Configuration Guide*.

## Roles

victor Roles support ITv2 Integration device privileges, therefore all context menu actions associated with the devices are added to existing victor Roles which can be edited accordingly. For more information on Roles, refer to the victor Unified Client Configuration and User Guide.

## Associations

victor's Object Association supports ITv2 Integration objects. Object Association refers to linking unrelated victor objects with the intent of enabling incident building capability. For more information on Object Associations, refer to the victor Unified Client Configuration and User Guide.

## Reports

victor's Reports selection tool and Find in Journal feature support ITv2 Integration objects. For more information on Reports and the Find in Journal feature, refer to the victor Unified Client Configuration and User Guide.

## Events

victor Events supports ITv2 Integration objects support allowing you to detect, monitor and record specific activities on the system. For further information on Events, refer to the victor Unified Client Configuration and User Guide.

## Maps

victor Maps and Find on Map features support ITv2 Integration objects.

# Configuration

## ITV2 Configuration File

The driver configuration file, `ITV2Configuration.xml` is located in `Tyco\CrossFire\ServerComponents`. You can configure the following properties:

**NOTE** Restart the driver after changing the configuration file.

### CommandTimeout

It is the duration the ITv2 integration waits for a response to a command sent to the Panel. The default value is 10000 milliseconds.

### BatchCount

It is the number of panels that can synchronize simultaneously. The default value is 10, which means that a maximum of 10 panels can synchronize simultaneously. You can change this value depending on the system configuration.

### RetryCount

The default value is 3, which means that the driver will try a maximum of 3 times if it does not receive the required response for a command from the panel.

### Heartbeat Interval

The default value is 20000 milliseconds, which means that the driver sends heartbeat to the panel once in every 20 seconds. You can configure this value to a maximum of 29000 milliseconds.

### Enable Context Logging

The default value is FALSE, if it is set to TRUE, then the sequence number exchanges between the Driver and the Panel is captured in the CrossFire log.

### Enable Raw Data Logs

The default value is FALSE, if it is set to TRUE then the raw data/byte stream exchanges between the Driver and the Panel is captured in the CrossFire log.

### Enable Additional Panel Event Logs

The default value is FALSE, if it is set to TRUE then the Keypad access events are logged in the Activity Viewer.

For Example: *6 access by User “User1”

### Time Sync Interval

This is used to synchronize the time between the Driver and Panel. The default value is 60 minutes, which means that the time-date push from Driver to Panel happens once in every 60 minutes. You can configure this value.

### Max Thread Count

The default value is 10, which means that a maximum of 10 threads are used for all the panels. You can configure this value depending on the system configuration.

## Configuring DSC PowerSeries Neo and Pro Panel Hardware using the Keypad

The ITv2 Integration supports DSC PowerSeries Neo and Pro Panels. This section provides instructions to perform basic configurations in the DSC PowerSeries Neo and Pro Panels that enable them to communicate with the Unified server.

**NOTE** The Communication mode supported by the Integration is Network (TCP/ IP).

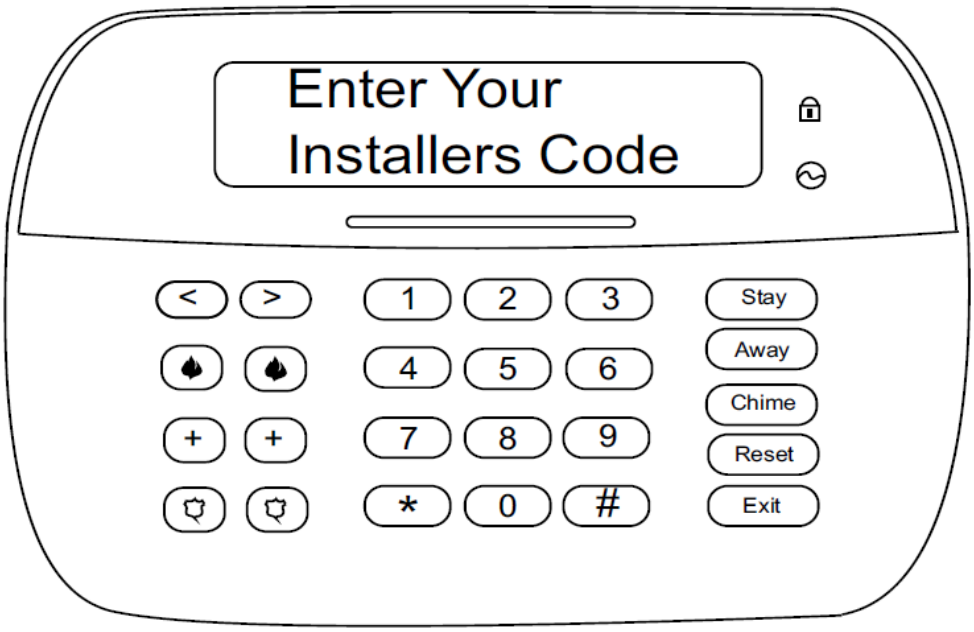
Following basic configurations must be performed in the DSC PowerSeries Neo or Pro Panel to connect it to victor:

| Procedure | Configurations |
|---|---|
| Procedure 1 | Procedure - Enabling the Alternate Communicator |
| Procedure 2 | Procedure - Configuring the Communicator |
| Procedure 3 | Procedure - Viewing the Panel Account Number (subsection 651) |
| Procedure 4 | Procedure - Enabling the DSC PowerSeries Neo or Pro Panel over Ethernet (subsection 663) |
| Procedure 5 | Procedure - Configuring the ITv2 Server IP Address (subsection 693) |
| Procedure 6 | Procedure - Configuring the Port Number (subsection 694) |
| Procedure 7 | Procedure - Configuring the Panel IP Address (subsection 992) |
| Procedure 8 | Procedure - Viewing the Remote Panel Account Code (subsection 652) |
| Procedure 9 | Procedure - Enabling TCP Communication (subsection 664) |

### Procedure - Enabling the Alternate Communicator

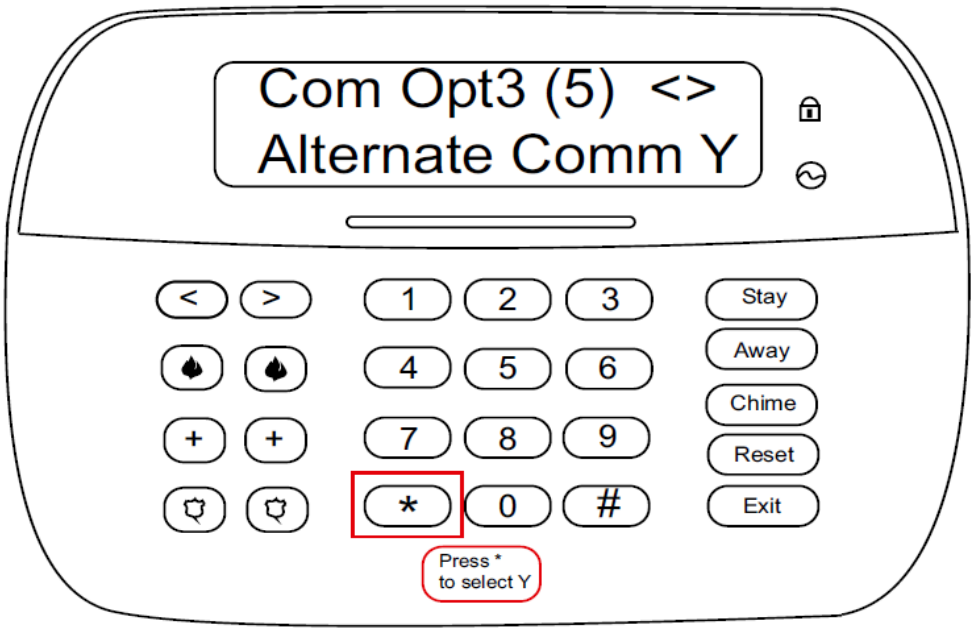
1. Using DSC PowerSeries Neo or Pro Panel Keypad, press [*] [8].

   Enter Your Installers Code message appears on the keypad, as shown in the following figure:




2. Enter the Installer Code using the keypad. The default Installer code is 5555.
3. Press [382] using the keypad.
4. Use the > to scroll to subsection [5].

   **Com Opt3 <5> Alternate Comm** message appears, as shown in the following figure:



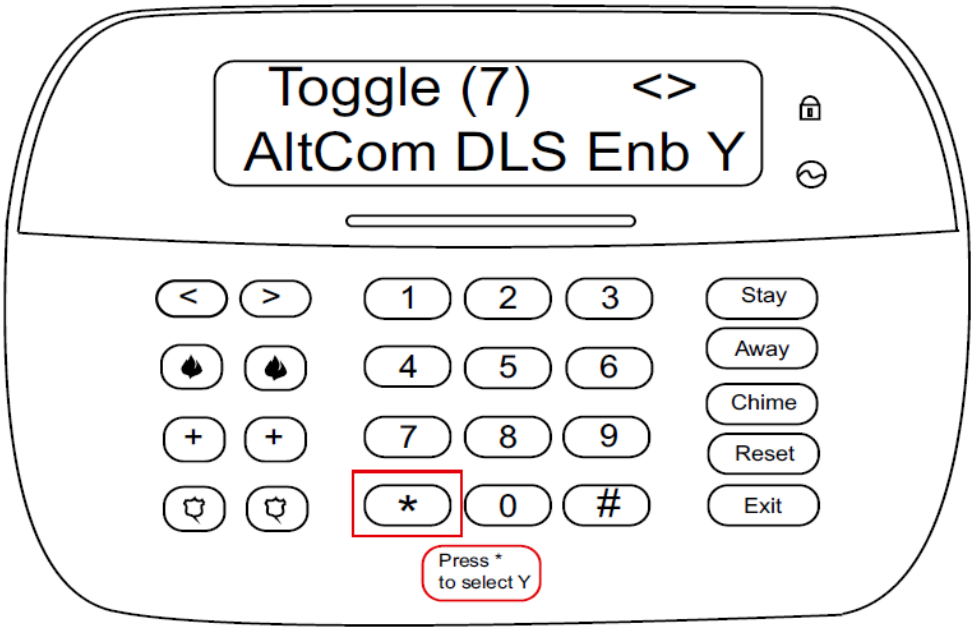

5. Select one of the following options:
   - For Neo panels: Verify if Alternate Comm option is **Y**. If not, select **Y** using [*] button on the keypad.
   - For Pro panels: Verify if Alternate Comm option is **N**. If not, select **N** using [*] button on the keypad.

**NOTE**

Press [*] to toggle between **Y** and **N**.

6. Press # to exit the subsection.
7. Press [401].
8. Use the > to scroll to go to subsection [7].

   **Toggle <7> AltCom DLS Enb** message appears, as shown in the following figure:



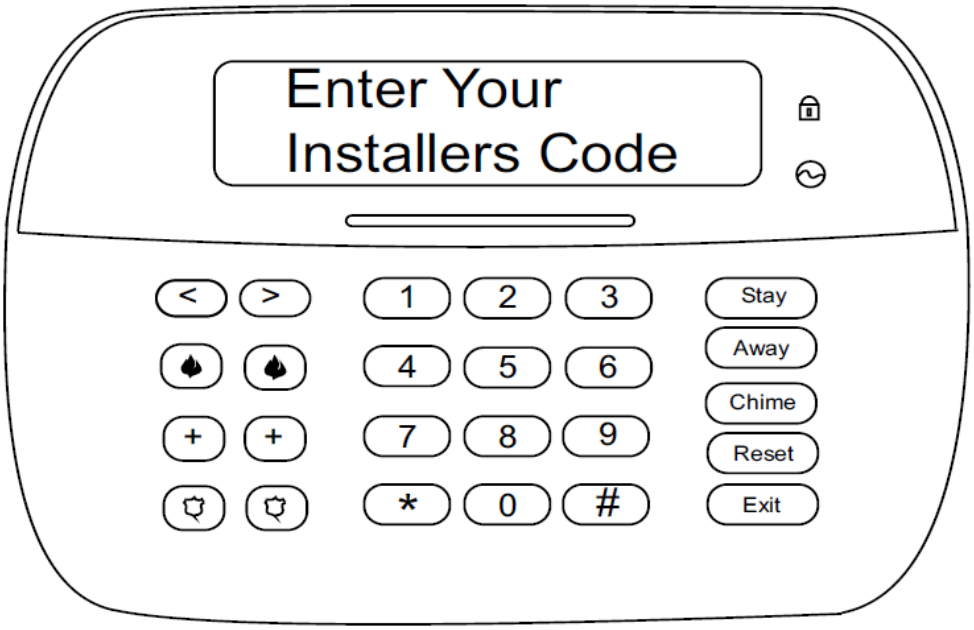

9. Verify if Alternate Comm option is **Y**. If not, select **Y** using [*] button on the keypad.

**NOTE** Press [*] to toggle between **Y** and **N**.

10. Press # to exist the subsection and section.

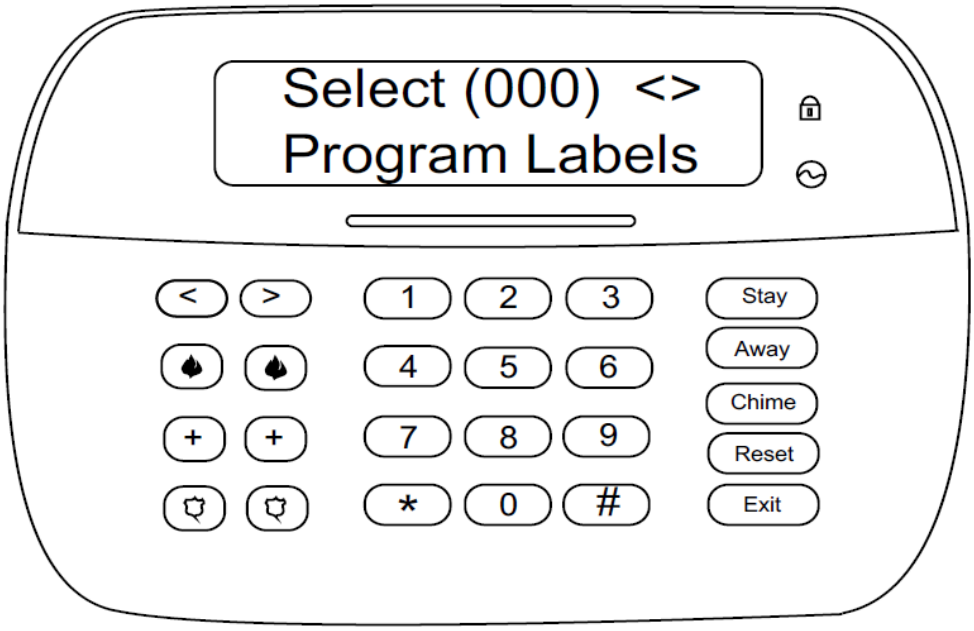
## Procedure - Configuring the Communicator

1. Press [*] [**8**].



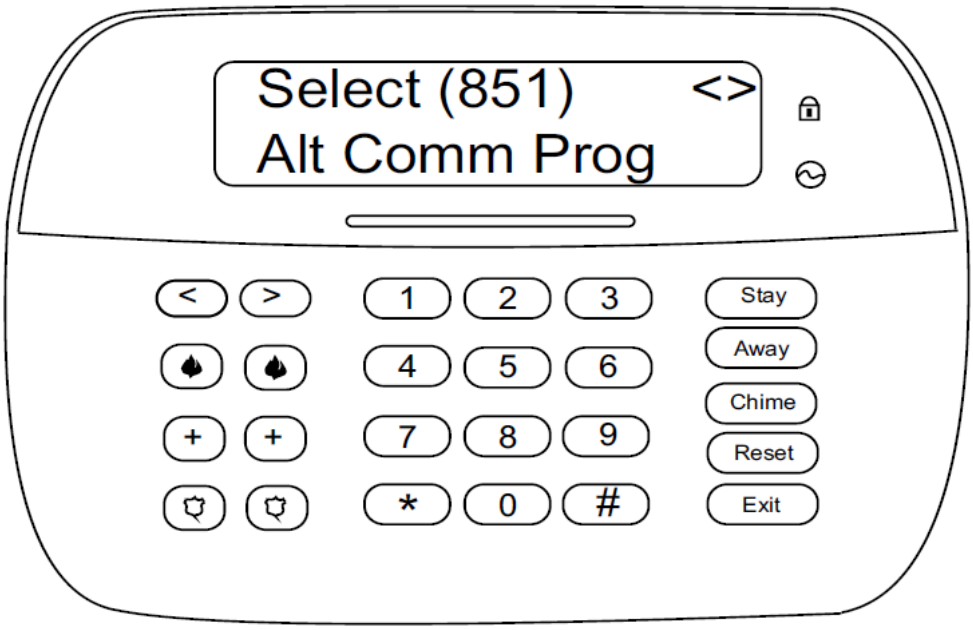

2. Enter the Installer Code. Default Installer code is **5555**.

   **Select <000> Program Labels** message appears, as shown in the following figure:

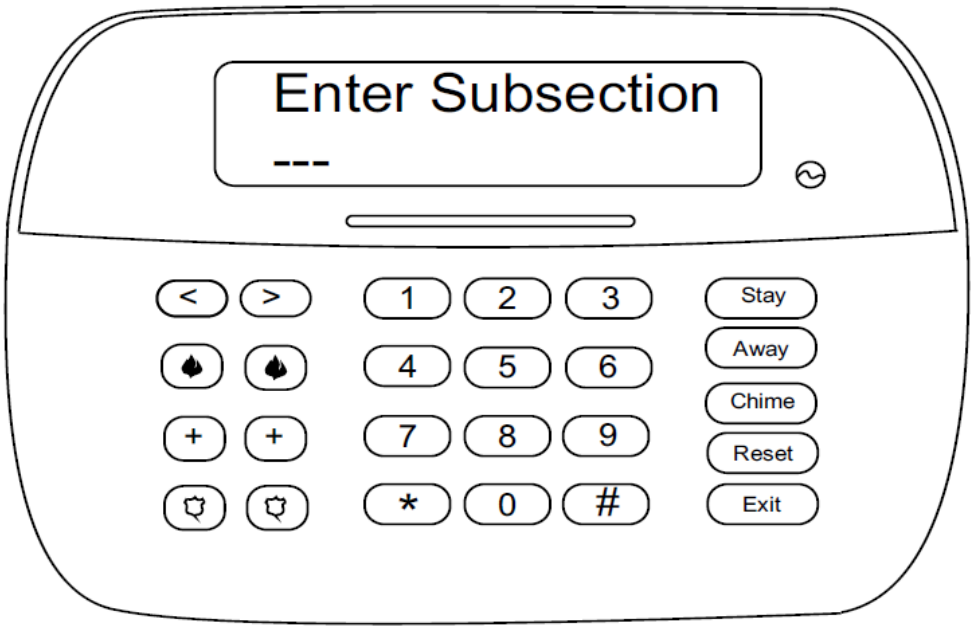



3. Press [851]

   **Select <851> Alt Comm Prog** message appears, as shown in the following figure:




4. Press # to exit the subsection. The **Enter Subsection** message appears:




### Procedure - Viewing the Panel Account Number (subsection 651)

The Panel account number is the local panel encryption key of the panel. The first 8 digits of this code are used as a Remote Encryption Key in the integration.

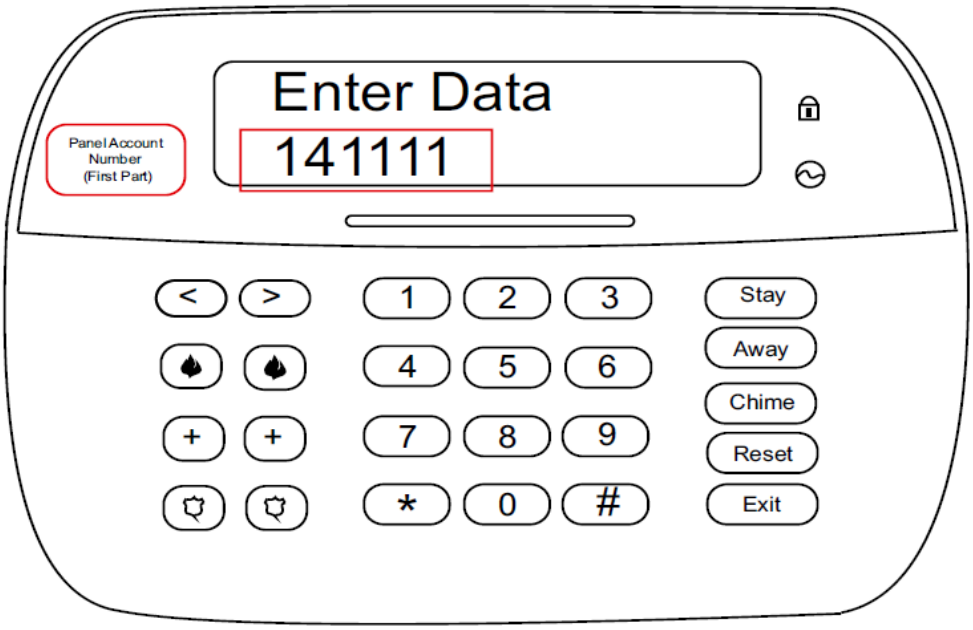
The account number is a 12 digit number which is unique to the panel and cannot be modified.

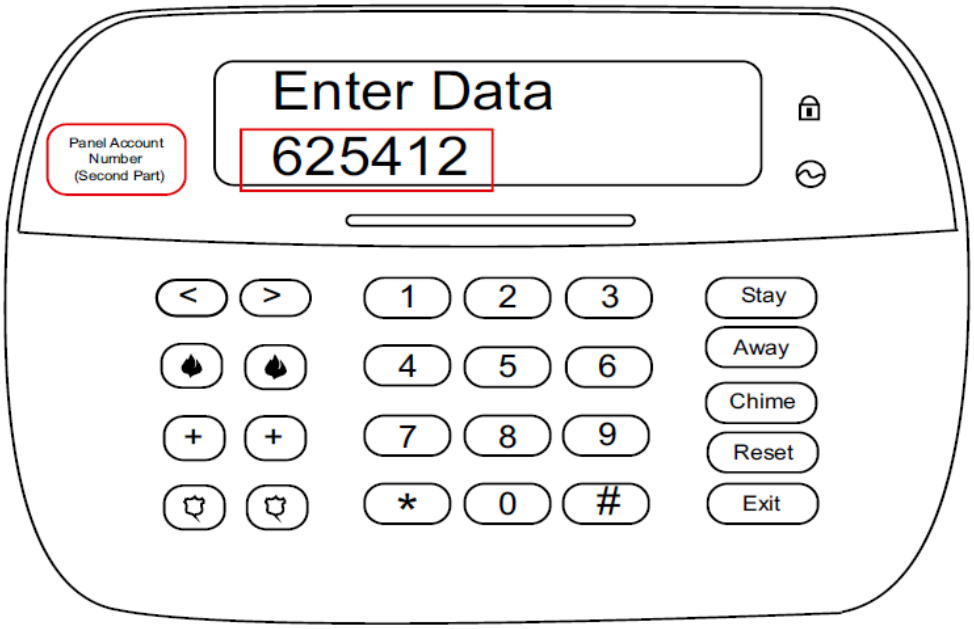
To view the Panel account number, continue from Step 4 of "Configuring the Communicator" on page 13. and then perform the following procedure.

1. Press subsection **[651]** using the keypad.

**NOTE** If using communicator firmware version 5.xx, then press subsection [**422**].

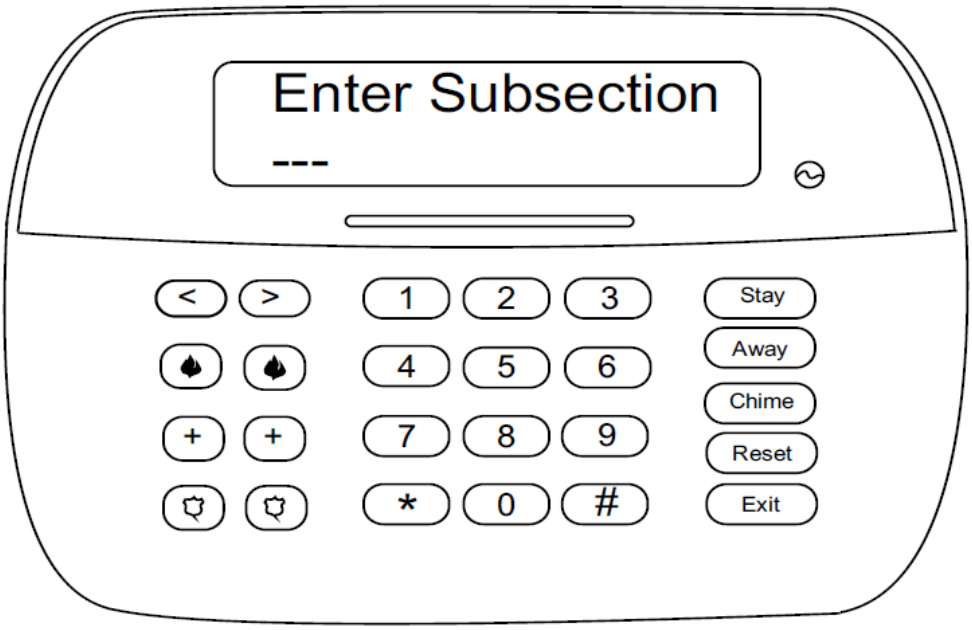
2. The first 6 digits of the panel account number appears on the keypad. Scroll using the (>) button to view the complete panel account number.




3. Press (#) to exit the subsection.

**Enter Subsection** message appears, as shown in the following figure:

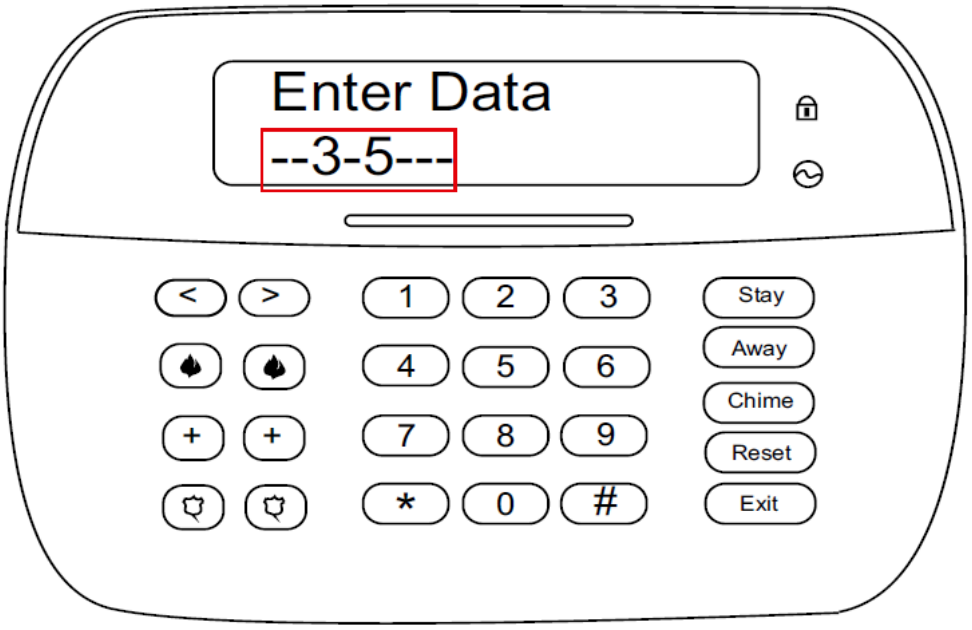



### Procedure - Enabling the DSC PowerSeries Neo or Pro Panel over Ethernet (subsection 663)

1. Press subsection [**663**].

**NOTE** If using communicator firmware version 5.xx, then press subsection [**425**].

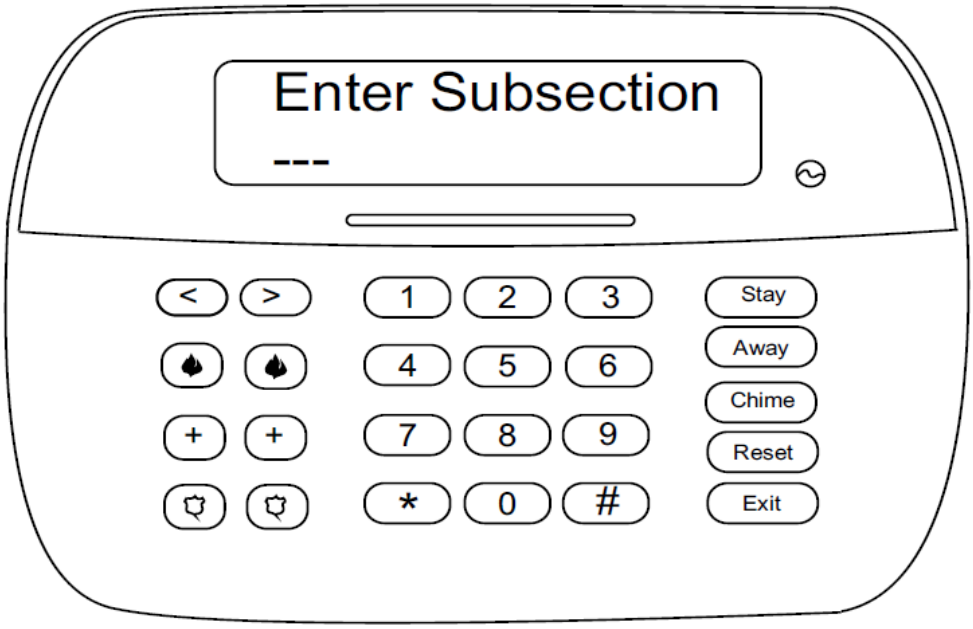
2. Verify if bit 3 and 5 are enabled. Options 3 and 5 need to be enabled for the DSC PowerSeries Neo or Pro Panel over Ethernet.




3. If not enabled, press 3 and 5 once.

**NOTE** When you press 3, the bit is **ON**, and if you press 3 again it is **OFF**. All other bits need to be OFF.

4. Press # to exit the subsection.



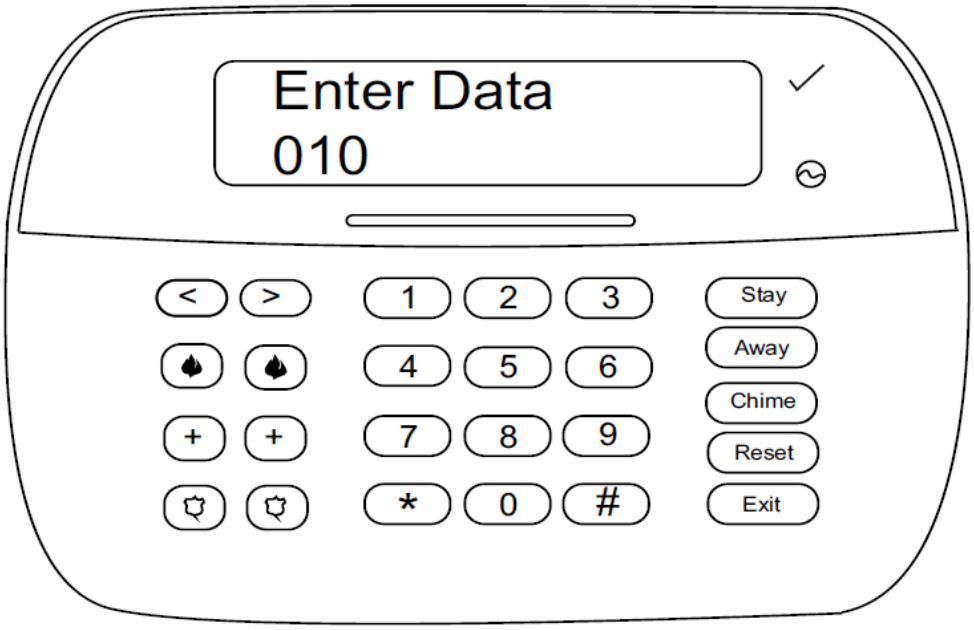

## Procedure - Configuring the ITv2 Server IP Address (subsection 693)

1. Press subsection [693].

**NOTE** If using communicator firmware version 5.xx, then press subsection [**428**].

2. Enter the IP Address.

   For example, if the IP address is 10.2.3.4, enter 010 002 003 004. In the following figure, only 010 is shown:




3. Press # to exit the subsection.

## Procedure - Configuring the Port Number (subsection 694)

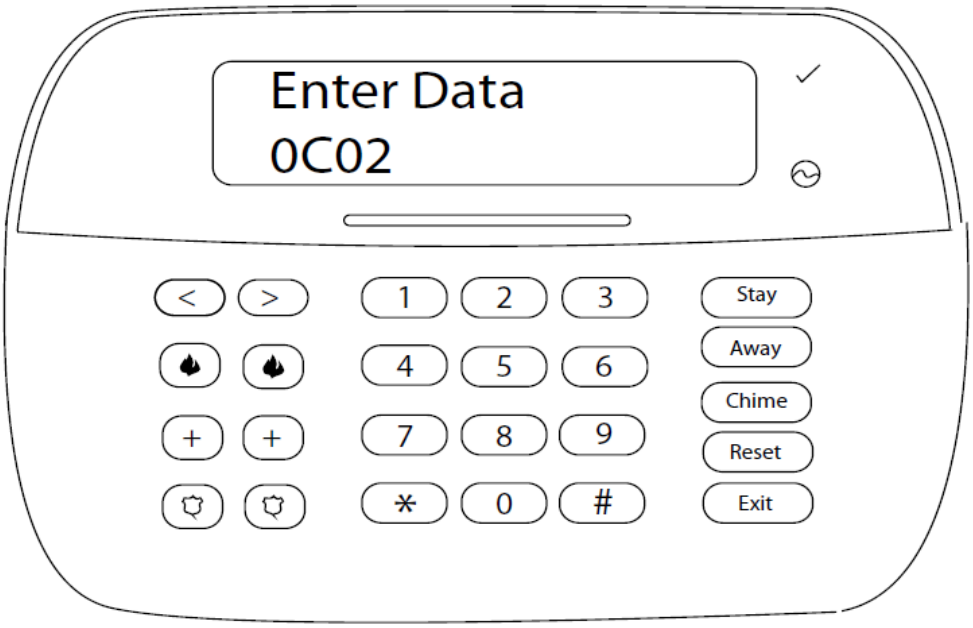
The configured port is used as the alarm port for ITv2 Integration. The port number starts from 3072 equivalent to 0C00 in hexadecimal value.

**NOTE** To enter the hexadecimal value, press [*] to use keypad as alphabet and again press [*] to use as number. For example, to enter 0C12: press 0 [*] 3 [*] 2

1. Press subsection [694].

**NOTE** If using communicator firmware version 5.xx, then press subsection [429].

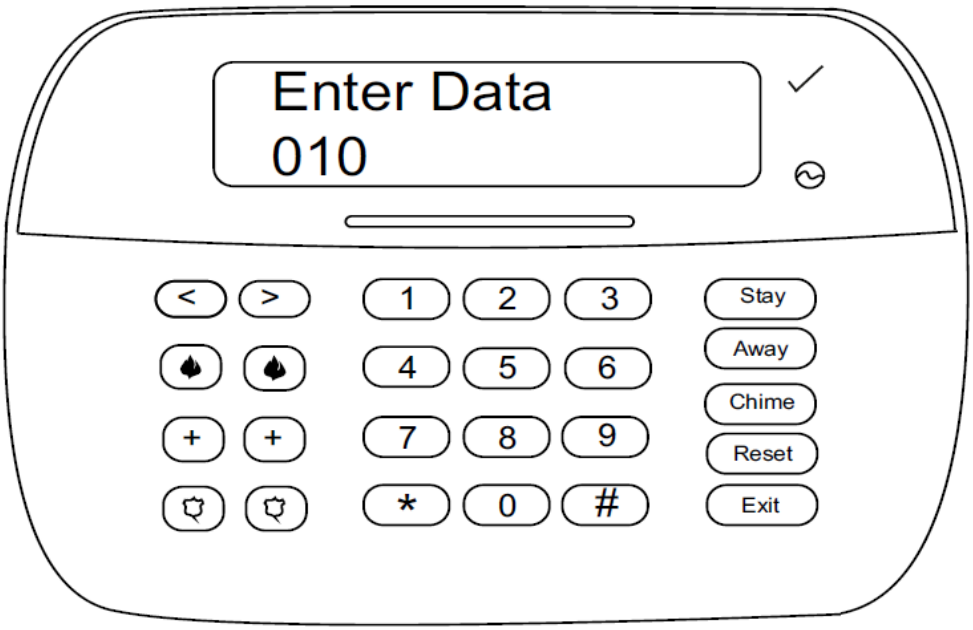
2. Enter the port number in the hexadecimal format.




3. Press # to exit the subsection.

### Procedure - Configuring the Panel IP Address (subsection 992)

1. Press subsection [**992**].




2. Enter the IP Address. For example, if the IP address is 10.2.3.4 enter 010 002 003 004. This is the IP Address of the panel.
3. Press # to exit the subsection.

**NOTE**

- In the instance of a DHCP, the IP address will automatically be allocated in sub-section 992.
- Power recycle the panel after network reconfiguration and installation.

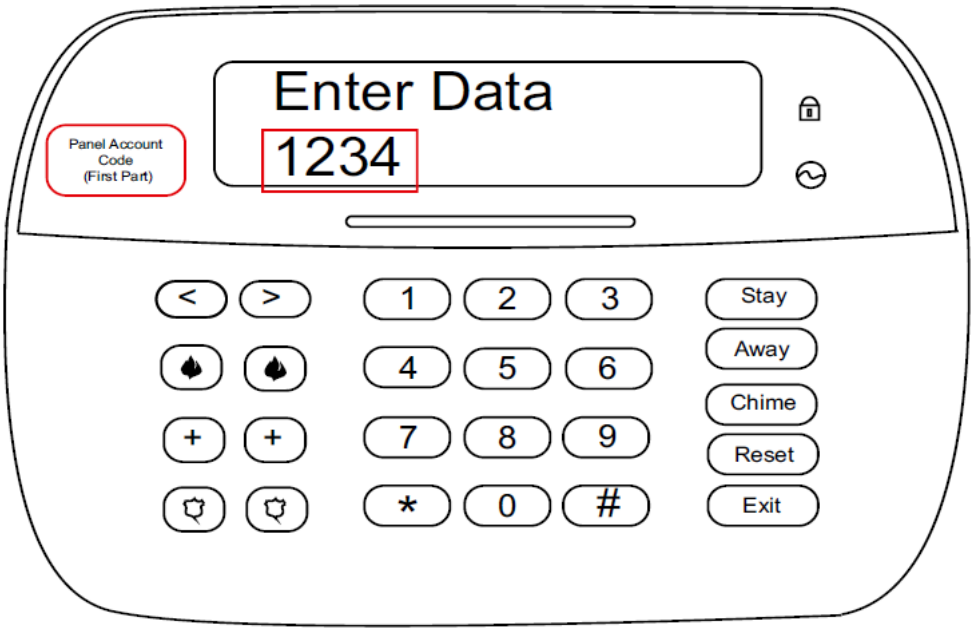
### Procedure - Viewing the Remote Panel Account Code (subsection 652)

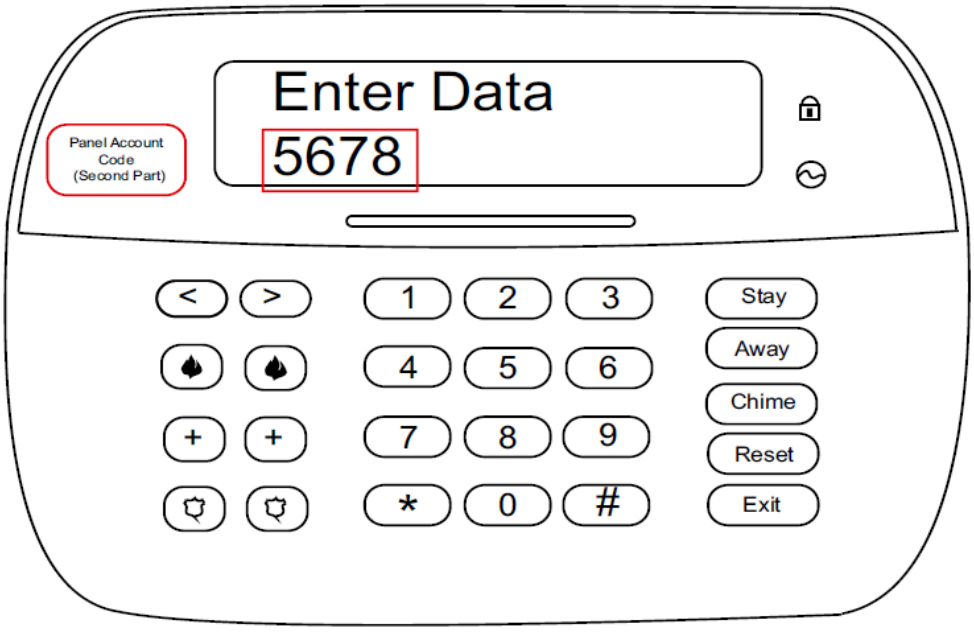
The remote account code is the remote encryption key of the panel. The code is used as the local encryption key for the integration and cannot be modified.

1. Enter the subsection [652] using the keypad.

**NOTE** If using communicator firmware version 5.xx, then press subsection [423].

2. The first 4 digits of the remote account code appears. Scroll using the button to view the complete the panel account number.



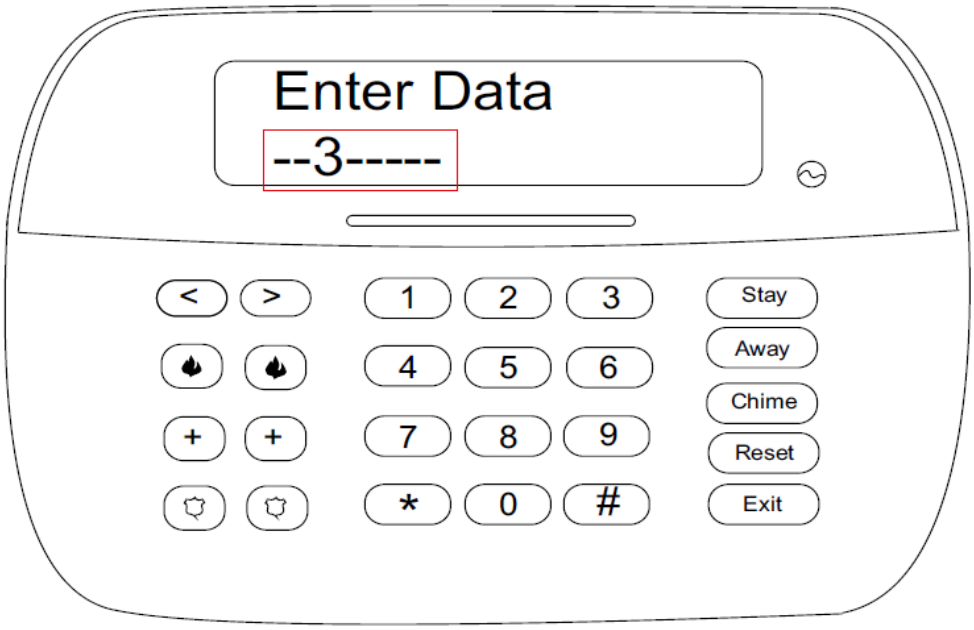
3. Press # to exit subsection and section.

## Procedure - Enabling TCP Communication (subsection 664)

1. Press subsection [**664**].

**NOTE** If using communicator firmware version 5.xx, then press subsection [426].

2. Verify if bit 3 is enabled. Option 3 needs to be enabled for TCP Communication.




3. If not enabled, press 3.

**NOTE** When you press 3, the bit is **ON**, and if you press 3 once again it is **OFF**. All other bits need to be **OFF**.

4. Press # to exit subsection and section.

## Procedure - Adding ITv2 Panels

**NOTE** **Panel Account Number**, **Encryption Key**, **Access Code**, and **Installer Code** are assigned and provided with the DSC Neo or Pro Panel hardware.

1. Select **New**, search for ITv2 Panel and click on it. A New ITv2 Panel window displays.
2. Enter the details in the ITv2 Panel. For more information, see Fields of the ITv2 Panel Editor.
3. Click **Save and Close**.

After adding the ITv2 panel you must synchronize the panels. For more information, see Procedure - Synchronizing from the Panel.

**Figure 2:** Neo Panel Editor

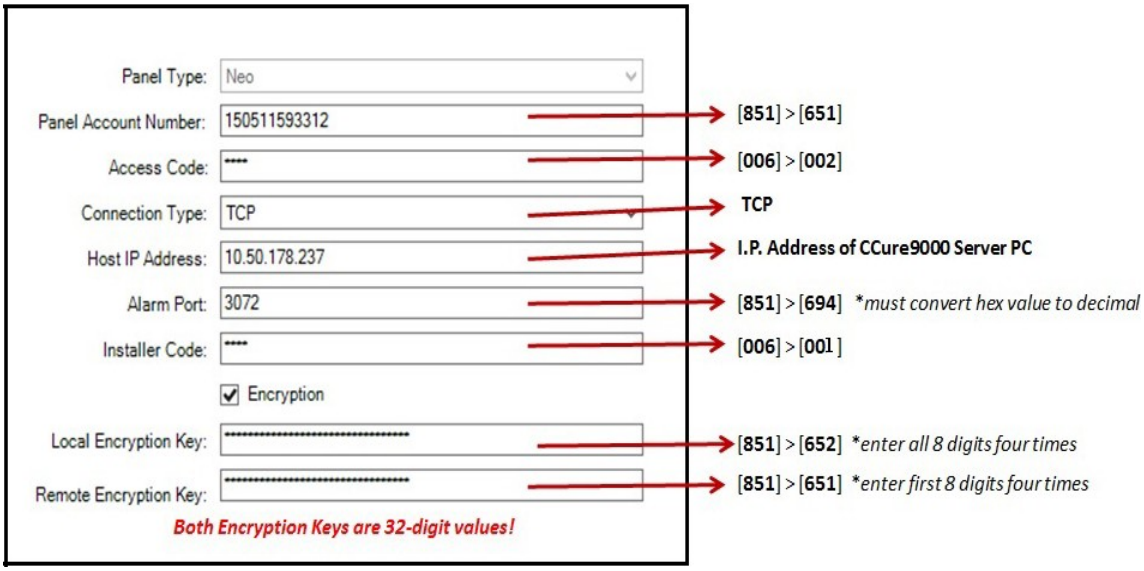
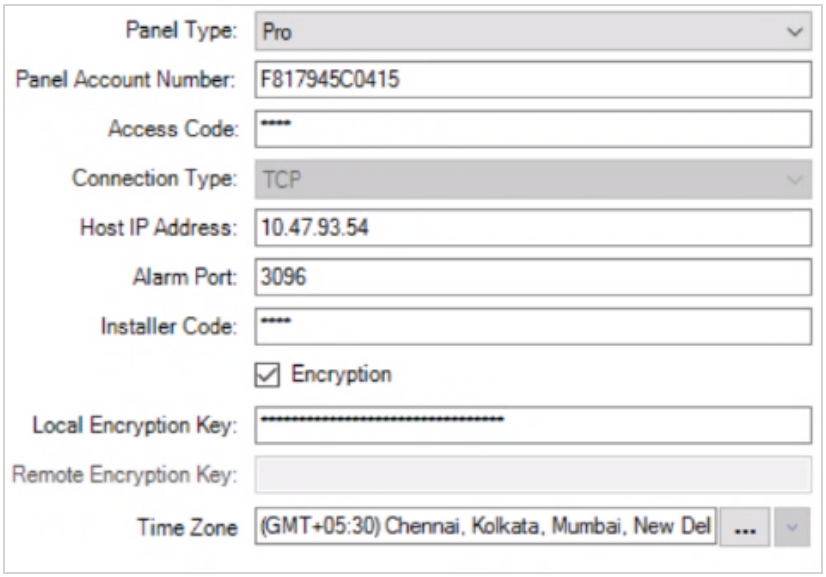



**Figure 3:** Pro Panel Editor



## Fields of the ITv2 Panel Editor

**Table 5:** General Section

| Property | Description |
|---|---|
| Name | Enter a unique name to identify the ITv2 Panel.<br>The name of the panel can be alphanumeric and up to 100 characters long.<br>Ensure that the name is unique, else an error message is displayed. |
| Description | (Optional) Enter a description for the panel. |
| Enabled | Select the check box to establish the communication between the victor and the ITv2 Panel.<br>If the Panel is disabled, the communication between victor and the Panel is disabled. |

**Table 6:** Configuration Section

| Property | Description |
|---|---|
| Panel Type | Select a panel type from the available options:<br>• Neo (default)<br>• Pro |
| Panel account number | Enter the assigned account number of the DSC Neo or Pro Panel.<br>Panel account number is unique to a panel and provided with the DSC Neo or Pro Panel hardware.<br>The account number must be 12 characters and numeric only, else an error message is displayed.<br>For more information on how to view the Panel account number, see Configuring DSC PowerSeries Neo and Pro Panel Hardware using the Keypad. |
| Access code | Enter the access code.<br>The access code is the master code of the panel used to authenticate operations in the panel, such as: User Level tasks, Event Level tasks, and System Level tasks.<br>The access code is assigned and provided with the Panel hardware. You can modify the Access code in the panel keypad only. For more information on how to modify the access code, see Configuring DSC PowerSeries Neo and Pro Panel Hardware using the Keypad.<br>The Access code must have only numeric values and can be four, six or eight digits long.<br>**Note:** If you modify the access code in the DSC Neo or Pro Panel, the same should be configured in victor or else the events and schedule actions will fail to work, as expected. |
| Connection Type | The connection type used to select the mode of communication. By default, the connection type is TCP. |
| Host IP Address | Enter the TCP/IP address of the unified server.<br>The IP address must be in the IPv4 format. For example, 191.2.3.4 |
| Alarm Port | Enter the port number used for communication.<br>The Alarm Port is used for communication between the Unified server and the DSC Neo or Pro panel.<br>The port number can be four, six or eight digits long.<br>**Note:** If multiple Panels are in use, there should be an unique Alarm port number for each panel, else an error message is displayed. |

| Property | Description |
|---|---|
| Installer Code | Enter the Installer Code of the panel, which is assigned and provided with the Panel hardware.<br>The Installer Code is used to authenticate the panel configuration tasks performed in the programing mode.<br>You can modify the Installer Code in the panel using keypad only. For more information on how to modify the installer code, see Configuring DSC PowerSeries Neo and Pro Panel Hardware using the Keypad. |
| Encryption | Select the check box to enable the encryption.<br>The encryption key is used to authenticate the handshake between the panel and the unified server.<br>The encryption key is assigned and provided with the DSC PowerSeries Neo or Pro Panel hardware.<br>For more information on how to modify the encryption key, see Configuring DSC PowerSeries Neo and Pro Panel Hardware using the Keypad. |
| Local Encryption Key | This field is enabled only if the Encryption check box is enabled. Enter the local encryption key.<br>The local encryption key is 8 characters code, which is configured in the DSC PowerSeries Neo or Peo Panel.<br>Enter the eight character code four times.<br>For more information on how to modify the Local Encryption key in the DSC Neo or Pro Panel, see Configuring DSC PowerSeries Neo and Pro Panel Hardware using the Keypad. |
| Remote Encryption Key | This field is only enabled if the Encryption check box is selected. Enter the remote encryption key.<br>**Note:** If you select the Pro panel type, the remote encryption key is disabled. If you select the Neo panel type, the remote encryption key is enabled.<br>The remote encryption key is the first 8 digit of the Panel Account number.<br>Enter the first eight digit of the account number four times.<br>For example, if the account code is 123456789012, you have to enter the first eight digit (12345678) four times.<br>To view the account number, see Configuring DSC PowerSeries Neo and Pro Panel Hardware using the Keypad. |
| Time Zone | Click  to display the Object Selector. Select a time zone from the Object Selector window and click OK. The panel synchronizes based on the selected time zone. |

**NOTE** Ensure that the installer code and access code set in the configuration tab is same as that mentioned in the Panel section [006]. If they are not same, the Panel is locked after performing the number of tries configured in the Panel section [012].

**Table 7:** Late to Open Control Section

| Property | Description |
|---|---|
| Late to Open Control | Late to Open Control is used to schedule the monitoring period.<br>Select this check box to enable the Late to Open Control. |
| Hour (Sunday to Saturday) | Enter the time in hour when the panel should be disarmed This field is enabled, if Late to Open Control is enabled.<br>The valid range is from 00:00 – 23:59 hours.<br>For example - 16.00 |
| Minute (Sunday to Saturday) | Enter the time in minute when the panel should be disarmed. This field is enabled, if Late to Open Control is enabled.<br>The valid range is from 00 – 59 minutes.<br>For example - 00.15 |

**Table 8:** Panel Information Section

| Expander | Information |
|---|---|
| Panel Information | • Device software version<br>• Protocol Version<br>• Last Synced time<br>• Max Zones<br>• Max Users<br>• Max Partitions<br>• Max Outputs<br>• Enable Panel Event Buffer |

**Table 9:** Status Section

| Property | Description |
|---|---|
| Online Status | Indicates the online status of the Panel. |
| Synchronization Status | Indicates the synchronization status of the Panel. |
| System Trouble | Indicates the system trouble status of the Panel. |
| Communication Trouble | Indicates the communication trouble status of the Panel. |
| Wireless Device Trouble | Indicates the wireless device trouble status of the Panel. |
| Wired Module Trouble | Indicates the wired module trouble status of the Panel. |

**Table 10:** User Section

| Property | Description |
|---|---|
| User Index | Indicates the number to identify the user. The number is incremental when you create a new row in the table and cannot be modified. |
| User Name | Click  to display the Object Selector. Select a user from the Object Selector window and click **OK**. The selected user is mapped to a panel.<br>See Procedure - Mapping Personnel to ITv2 User and Procedure - Removing a ITv2 User mapping from personnel for information regarding users and panels. |

**Table 11:** Virtual Zone Configuration Section

| Property | Description |
|---|---|
| Virtual Zone Index | Indicates the number to identify the virtual zone. The number is incremental when you create a new row in the table and cannot be modified. |
| Zone Name | Click  to display the Object Selector. Select a zone from the Object Selector window and click **OK**. The selected zone is mapped to a virtual zone. |

## Associations Section

Use the Object Selector in this section to associate other hardware devices with the ITv2 Panel (maximum of 5).

**NOTE**

- Ensure the following before performing Write Assignment operation:
  - Partition is not in an Alarm or Armed state.
  - Keypad is not in programming mode.
- Ensure you Save and Close after every Write Assignment operation.
- After performing a Write Assignment operation if the message - Function unavailable/Panel is busy appears, perform Sync to Panel. This ensures that the configuration communicates to the Panel.
- The sync status of the panel changes to Synchronizing-Synchronized after every write operation.
- The user in Index 1 is the Master User in the Panel, therefore the modification of the Primary User is not allowed through the integration.
- In the User tab, Index 1 will be reserved for the Primary User, which cannot be edited or removed.

## Troubleshooting

If the Panel does not come online and cannot establish a connection, verify the following areas are operational:

- Verify the physical connection between the Panel and the server is working by performing the following:
  - Ping the IP Address of the Panel configured in section [851] - [001] and/or [851]- [992]. Verify the IP Address is pinging on the network.
  - Use ‘netstat’ to check the connection is established with the alarm port.
  - Any other application such as DLS should not be connected to the Panel.
- Verify if CrossFire services, the server, and the ITv2 driver are running.
- Verify if Panel Account number, Alarm port, Access code, Installer code, Encryption key, and Host IP Address is entered correctly.
- Verify the configuration of the DSC Neo or Pro Panel hardware.

**NOTE**

Verify the Installer Code and the Access Code are the same as the Panel section [006]. If this is set differently, it will lock the Panel after X number of attempts for Y duration that was configured in Panel section [012].

After adding the ITv2 panels you must synchronize the panel. For more information, see Procedure - Synchronizing from the Panel.

## Editing ITv2 Panels

You can make the following changes:

| Task | Link |
|---|---|
| Modify Parameters in ITv2 Panel | Procedure - Modifying Parameters in ITv2 Panel |
| Map Users to Panel | Procedure - Mapping Personnel to ITv2 User |
| Remove a User from a Panel | Procedure - Removing a ITv2 User mapping from personnel |
| Configure a Virtual Zone | Procedure - Configuring a Virtual Zone |
| Remove a Virtual Zone | Procedure - Removing a Virtual Zone |

### Procedure - Modifying Parameters in ITv2 Panel

1. Select **Show All**, search for ITv2 Panel and click on it. A list displays all available ITv2 Panels.
2. Right-click the panel you want to edit.
3. Select **Edit** and make the required changes.
4. Click **Save and Close**.

For information about fields in the ITv2 panel, see Fields of the ITv2 Panel Editor.

### Procedure - Mapping Personnel to ITv2 User

1. Select the ITv2 Panel you want to edit, and click the **Users** tab.
2. Click  to map a ITv2 User to Personnel. The Object Selector appears listing all the personnel in it.
3. Select the Personnel to map to ITv2 user and click **OK**.
4. Click  to save and close the Panel editor.

**NOTE**

- The user in Index 1 is the Master User in the Panel and thus the modification of the Primary User is not allowed through the integration.
- Do not delete the User while sync is in progress.

### Procedure - Removing a ITv2 User mapping from personnel

1. Select the ITv2 Panel you want to edit and click the **Users** drop-down menu.
2. Select a User row that you want to remove and erase the personnel entry by removing the content from personnel column.

3. Click  to save and close the Panel editor.

### Procedure - Configuring a Virtual Zone

1. Select the ITv2 Panel you want to edit, then click the Virtual Zone Configuration drop- down menu.
2. Click  to add a new virtual zone. A new row is created and the Virtual Zone Index is incremented by 1.
3. Click  on the newly created blank row under the Virtual Zones column. The Object Selector appears.
4. Select the virtual zone you want to associate with the Panel and then click OK.
5. Click  and wait until the status of the panel has changed from Synchronizing to Synchronized.
6. Click  to save and close the Panel editor. The zone is mapped to the Virtual Zone and appears in the Device List. The normal zone is changed to a virtual zone.

### Procedure - Removing a Virtual Zone

1. Select the ITv2 Panel you want to edit, then click the Virtual Zone Configuration drop- down list.
2. Select the row corresponding to the virtual zone you want to remove and click  .
3. Click  and wait until the status of the panel has changed from **Synchronizing** to **Synchronized**.

**NOTE** The virtual zone row is removed and the virtual zone is changed to a normal zone only when the user clicks  after clicking  , also the virtual zone will be removed from the panel and the database.

4. Click  to save and close the Panel editor.

## Viewing and Editing ITv2 Partitions

You cannot create Partitions directly from victor. Depending on your victor role assignment, you can view or edit partitions from the Setup tab.

### Procedure - Viewing and Editing ITv2 Partitions

1. Select **Show All**, search for ITv2 Partition and click on it. A list displays all available partitions.
2. Right-click the Partition and select **Edit**.
3. Click **Save and Close** after completion of edits.

**NOTE** During synchronization, you cannot modify the details in the ITv2 Panel editor.

## Fields of the Partition Editor

The following sections are used to edit different portions of the ITv2 Partition:

### General Section

**Table 12:** General Section

| Property | Value |
|---|---|
| Partition Number | Displays the Partition number of the Panel and is auto-generated during Panel synchronization. (Read only) |
| Account Number | Displays the Account code of the Partition and is auto-generated during Panel synchronization. (Read only) |
| Account Code | You can modify the account code of the partition used for authenticating the partition manual actions.<br>The account code can be 1 to 4 digits long. For example, 1234. |
| Entry Delay 1 | Enter the entry delay time in seconds.<br>The maximum delay can be up to 999 seconds.<br>An entry delay is the amount of time the security system waits before triggering the alarm when certain doors are opened. |
| Entry Delay 2 | If you want to have additional exit delay, enter the entry delay time in seconds.<br>The maximum delay can be up to 999 seconds. |
| Exit Delay 1 | Enter the exit delay time in seconds.<br>The maximum delay can be up to 999 seconds.<br>The time duration that exists, after the code is entered till the system begins to monitor is called an exit delay. This delay is set to give time to exit from the building after arming the system from inside. |

### Zone Assignment Section

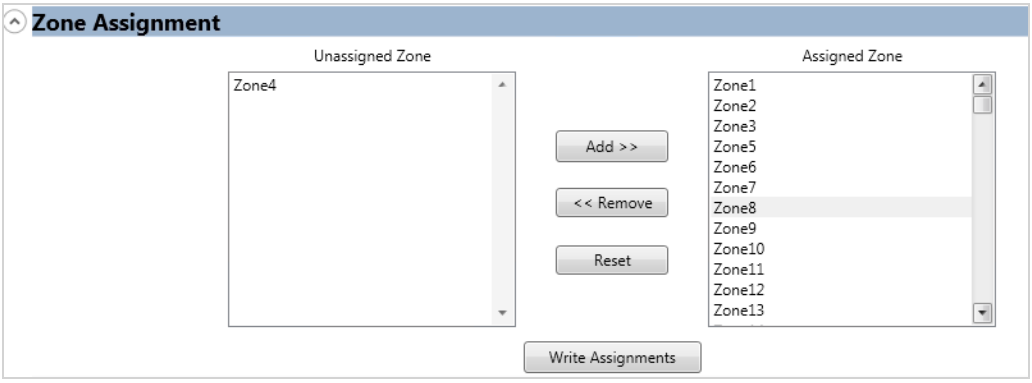


**Table 13:** Zone Assignment Section

| Property | Value |
|---|---|
| Unassigned Zone | Lists all unassigned zones. |
| Assigned Zone | Lists all assigned zones. |
| Add | Used to add unassigned zones to assigned zones. |
| Remove | Used to move assigned zones back to the unassigned list. |
| Reset | Resets assignments to the default value. |
| Write Assignments | Reflects the changes in the ITv2 panel hardware. |

### Output Assignment Section

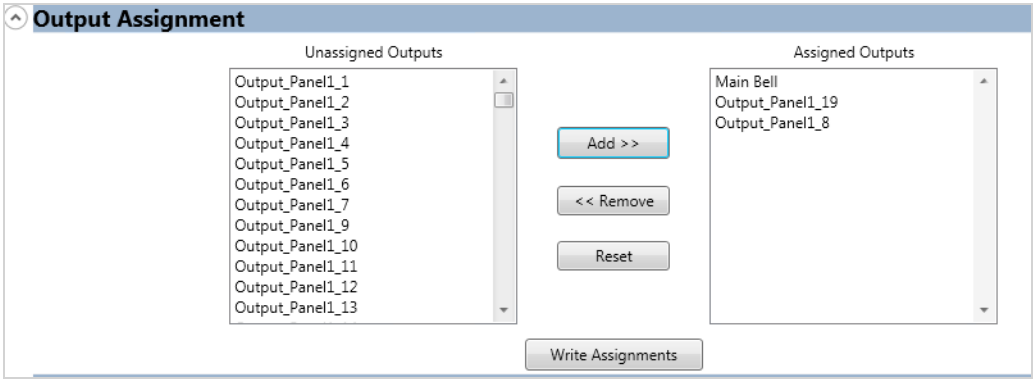



**Table 14:** Output Assignment Section

| Property | Value |
|---|---|
| Property | Value |
| Unassigned Outputs | Lists all unassigned outputs. |
| Assigned Outputs | Lists all assigned outputs. |
| Add | Used to add unassigned outputs to assigned outputs. |
| Remove | Used to move assigned outputs back to the unassigned list. |
| Reset | Resets assignments to the default value. |
| Write Assignments | Reflects the changes in the ITv2 panel hardware. |

**User Assignment Section**

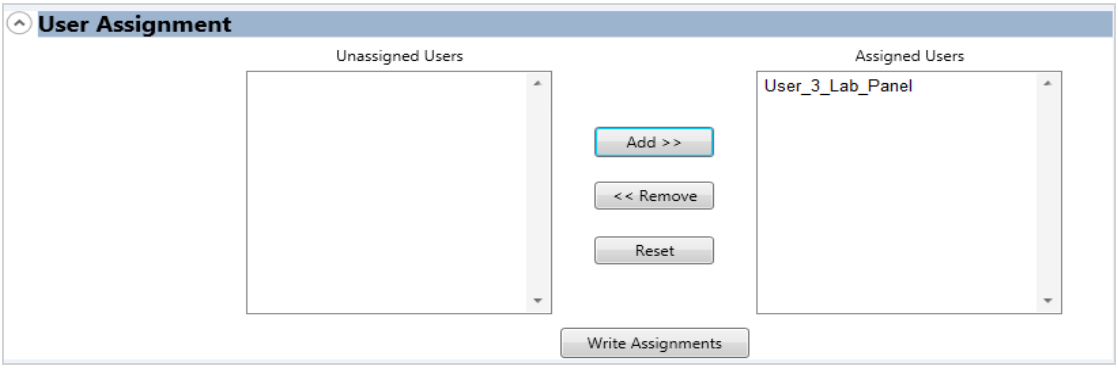



**Table 15:** User Assignment Section

| Property | Value |
|---|---|
| Unassigned Users | Lists all unassigned users. |
| Assigned Users | Lists all assigned users. |
| Add | Used to add unassigned users to assigned users. |
| Remove | Used to move assigned users back to the unassigned list. |
| Reset | Resets assignments to the default value. |
| Write Assignments | Reflects the changes in the ITv2 panel hardware. |

**NOTE**

Ensure the following before performing Write Assignment operation:

- The Partition is not in an Alarm or Armed state.
- The keypad is not in programming mode.
- Ensure you Save and Close after every Write Assignment operation.
- After a Write Assignment operation, if 'Function unavailable/Panel is busy' message appears, perform Sync to Panel. This ensures that the configuration is saved in the Panel.
- The sync status of the panel changes to Synchronizing-Synchronized after every write operation.

**Status Section**

**Table 16:** Status Section

| Property | Value |
|---|---|
| Armed State | Indicates the arm state of the partition. Following options are available:<br>■ Disarmed<br>■ Stay Armed<br>■ Away arm with No Entry Delay<br>■ Night Armed<br>■ Quick Armed<br>■ User Armed<br>■ Instant Stay Armed<br>■ Stay Armed with No Entry Delay<br>■ Global Stay Armed<br>■ Global Away Armed<br>■ Customized Armed<br>■ Away Armed With No Entry delay<br>■ Night Armed with No Entry Delay |
| Ready State | Indicates if the partition is ready for arming or not. Following options are available:<br>■ Ready<br>■ Not Ready |
| Alarm in Memory Status | Indicates if the alarms are in memory or not. Following options are available:<br>■ Alarm in Memory<br>■ No Alarms in Memory |

**Associations Section**

Use the Object Selector in this section to associate other hardware devices with the ITv2 Panel.

## Viewing and Editing ITv2 Zones

You can create zones only in the Panel. Depending on your victor role assignment, you can view or edit zones from the Intrusion ribbon on the Setup tab.

### Procedure - Viewing and Editing ITv2 Zones

1. Select **Show All**, search for ITv2 Zone and click on it. A list displays all available Zones.
2. If you need to edit a zone, right-click the zone and click **Edit**.
3. Click **Save and Close** to save your changes.

## Fields of the ITv2 Zone Editor

### General Section

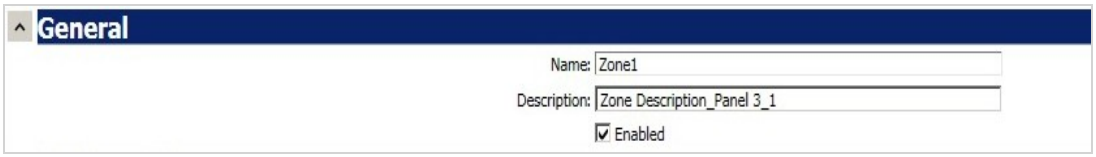



**Table 17:** General Section

| Property | Value |
|---|---|
| Name | Enter a unique name to identify the ITv2 Zone. If the name is not unique, an error message is displayed. The name of the panel can be alphanumeric and can have a maximum of 100 characters. |
| Description | Enter a description for the zone. |
| Enabled | Select the check box to establish the communication between the victor and the ITv2 Zone. If the Zone is disabled, the communication between victor and the Zone is disabled. |

### Configuration Section

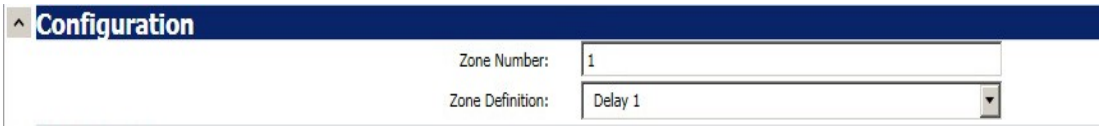



**Table 18:** Configuration Section

| Property | Value |
|---|---|
| Zone number | The Zone number is auto-generated during Panel synchronization. |
| Zone Definition | You can modify the zone type after you pull the zones from the Panel to victor. |

**Attributes Section**

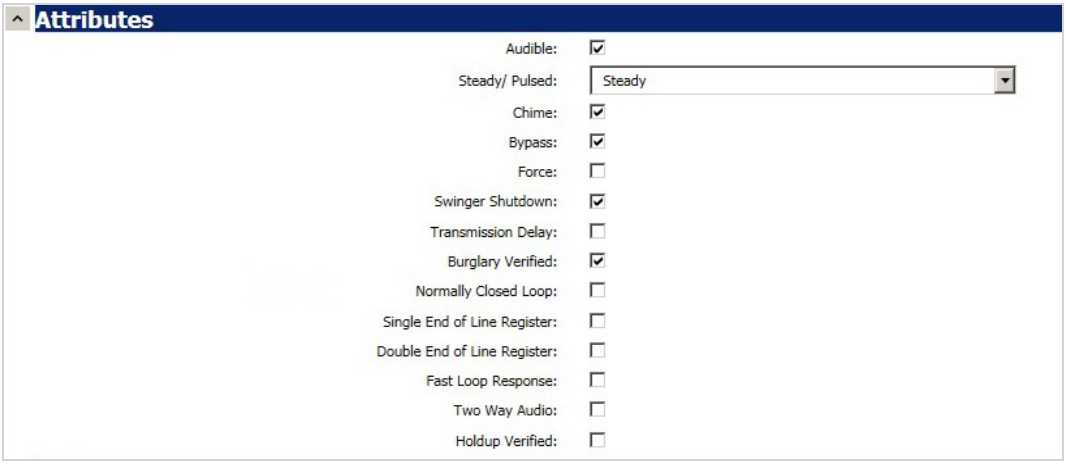



**Table 19:** Attributes Section

| Attribute | Description |
|---|---|
| Audible | Select to enable the audio of the panel. |
| Steady/Pulsed | Use to select a type of beep. Following options are available:<br>■ Steady<br>■ Pulsed |
| Chime | Select to enable the chime.<br>Chime indicates the user to open the zone with a beep or other configured sound, instead of alarm when the partition is not armed. |
| Bypass | Select to enable the bypass. |
| Force | Select to enable the force.<br>Force is used for arming a partition even if zone is having trouble and not ready for arm. |
| Swinger Shutdown | Used to set the number of alerts per day. All alerts after the set limit are suppressed |
| Transmission delay | Select to enable the transmission delay.<br>This is used to delay in transmitting the alert to the monitoring station. |
| Burglary Verified | Select to enable Burglary alarm verification. |
| Normally Closed Loop | Select to enable the normally closed loop connection type. |
| Single End of Line Register | Select to enable the single end of line register connection type. |
| Double End of Line Register | Select to enable the double end of line register connection type. |
| Fast Loop Response | Select to enable the fast loop response.<br>This is used for loop response time for mail panel zones. |

| Attribute | Description |
|---|---|
| Two Way Audio | Select to enable the two way audio.<br>If the central station is capable, the system (provided that it has an audio module) will allow audio verification to occur.<br>This can be one or two way conversation with the any user in the site. |
| Holdup Verified | Select to enable the hold up verified option.<br>Hold-up is used to alarm for the panic situation. Hold-up zone can be bypassed only through Master access code. |

**Status Section**

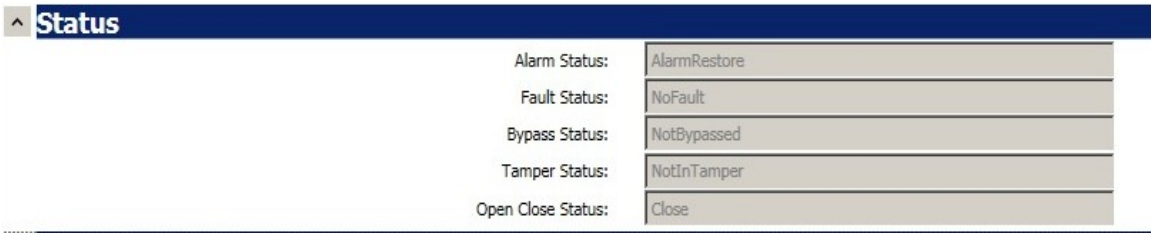



**Table 20:** Status Section

| Property | Value |
|---|---|
| Alarm Status | Indicates the status of the alarm in the Zone. Possible values are:<br>■ Alarm<br>■ Normal<br>■ Unknown |
| Fault Status | Indicates whether the zone is faulty or not. Possible values are:<br>■ Fault<br>■ No Fault |
| Bypass Status | Indicates whether the zone is bypassed or not. Possible values are:<br>■ Bypassed<br>■ Not Bypassed |
| Tamper Status | Indicates whether the zone is tampered or not. Possible values are:<br>■ Tamper<br>■ Not in Tamper |
| Open Close Status | Indicates whether the zone is opened or closed. Possible values are:<br>■ Open<br>■ Close |

#### Associations Section

Use the Object Selector in this section to associate other hardware devices with the ITv2 (maximum of 5).

**NOTE** Bypass/Reset of the zones does not work if any partition is in Arm/Alarm on the panel.

## Viewing and Editing Virtual Zones

Virtual zones are used by the third party hardware devices such as the iSTAR, apC, etc. to report alarms to central Activity Viewer using DSC Neo or Pro Panels. The DSC Neo or Pro Panel supports up to 32 virtual zones.

**NOTE** You should map one virtual zone with only one device action, but one device action can be mapped to multiple virtual zones. For example, Camera 1 is mapped to Virtual Zone 1 and Virtual Zone 2.

Virtual zones are configured in section [560] in the programming mode of the panel.

The ITv2 Virtual Zone editor is used to configure details such as: name, description, definition, and attributes. You can also view the Open Close status of the zone from this editor.

### Procedure - Accessing and Editing the ITv2 Virtual Zone in a Dynamic View

- Select **Show All**, search for ITv2 Virtual Zone and click on it. A list displays all configured Virtual Zones.
- Right-click the virtual zone you want to access and click Edit. The ITv2 Virtual Zone editor opens. See Configuration Section and Attributes Section for more information.

## Viewing and Editing ITv2 Outputs

You cannot create outputs directly from victor. Depending on your victor role assignment, you can view or edit outputs from the Intrusion ribbon on the Setup tab.

### Procedure - Viewing and Editing ITv2 Outputs

1. Select **Show All**, search for ITv2 Output and click on it. A list displays all available outputs.
2. Right-click the panel and click **Edit**.
3. Click **Save and Close** to save your changes.

## Fields of ITv2 Output Editor

#### General Section

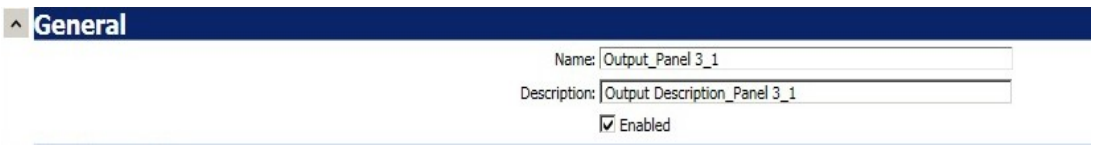


**Table 21:** General Section

| Property | Value |
|---|---|
| Name | Enter a unique name to identify the ITv2 Output. If the name is not unique, an error message is displayed.<br>The name of the panel can be alphanumeric and can have a maximum of 100 characters. |
| Description | Enter a description for the output. |
| Enabled | Select the check box to establish the communication between the victor and the ITv2 Panel.<br>If the Output is disabled, the communication between victor and the Output is disabled. |

### Configuration Section

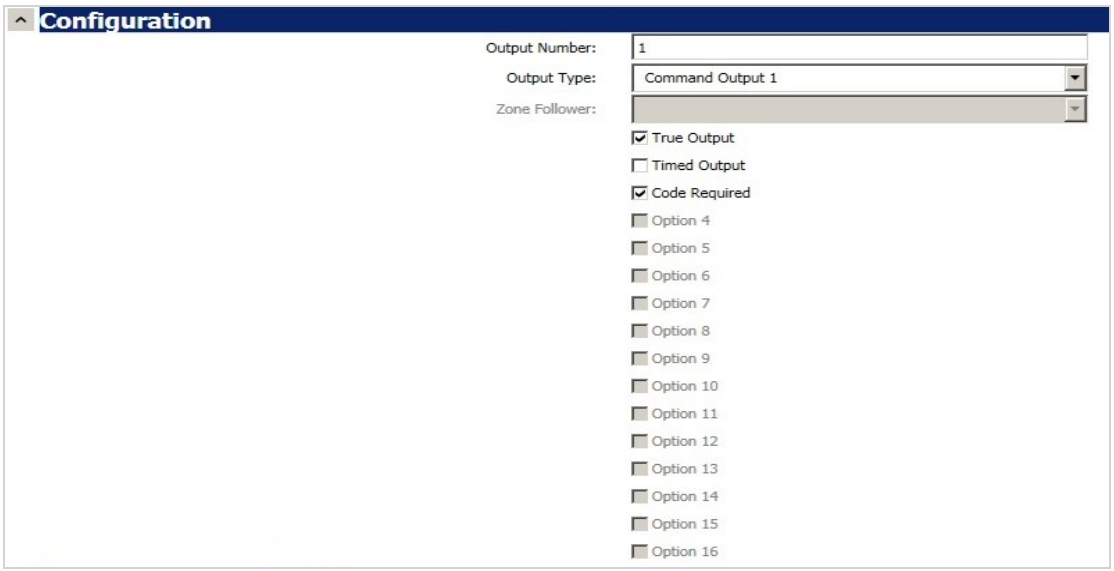



**Table 22:** Configuration Section

| Property | Value |
|---|---|
| Output Number | Displays the number assigned to the Output that is used to identify the Output.<br>The Output number is auto-generated during Panel synchronization and cannot be modified. |
| Output Type | Displays the type of Output.<br>The output type is auto-generated during Panel synchronization and can be modified.<br>Based on the output type, the attributes are displayed. |
| Zone Follower | This field is enabled only if the output type is Zone Follower. Select the zone from the list.<br>Use this option to monitor a specific zone. |
| Attributes | Attributes are displayed based on the output type. Select an attribute to enable it.<br>For more information on available attributes for each output type, refer to the DSC ITv2 Panel User Manual. |

**NOTE** Output name changes will not reflect in panel.

**Status Section**

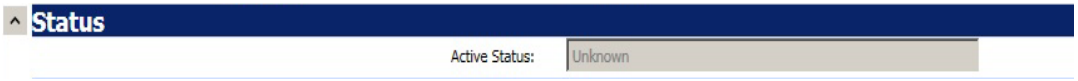



**Table 23:** Status Section

| Property | Value |
|---|---|
| Active Status | Indicates whether the output is Active or Inactive |

**Associations Section**

Use the Object Selector in this section to associate other hardware devices with the ITv2 Panel (maximum of 5).

## ITv2 Alarm Filter

The **Alarm Filter** is used to filter certain group of alarms for assigned panels. Refer Figure 4 on Page 42 for the Alarm Filter Editor.

The Filter categories listed under the **Filter Configuration** section of the **Alarm Assignment** Tab are the available Alarm/Event filters list for the ITv2 Panel.

When you select one or more Alarms/Events listed under the left column of **Filter Configuration** section under **Alarm Assignment** Tab and click **Add**, then the selected Alarms/Events are moved to the right column of **Filter Configuration** section under **Alarm Assignment** Tab.

When you enable the check boxes **Send To Monitoring Station** and **Send to Journal** under the **Options** section of **Alarm Assignment**Tab, then the filter applied sends the Alarms/Events notification to the Monitoring Station and the Journal for both the Alarms/Event filter categories listed **Filter Configuration** section.

When you disable the check boxes **Send To Monitoring Station** and **Send to Journal** under the **Options** section of **Alarm Assignment** Tab, then the filter applied does not send the Alarms/Events notification to Monitoring Station and Journal for the Alarms/Event filter categories listed under **Filter Configuration** section, thereby filters the Alarms/Events of the ITv2 panel in sending it to the Monitoring station and the Journal.

### Configuring the Alarm Filter

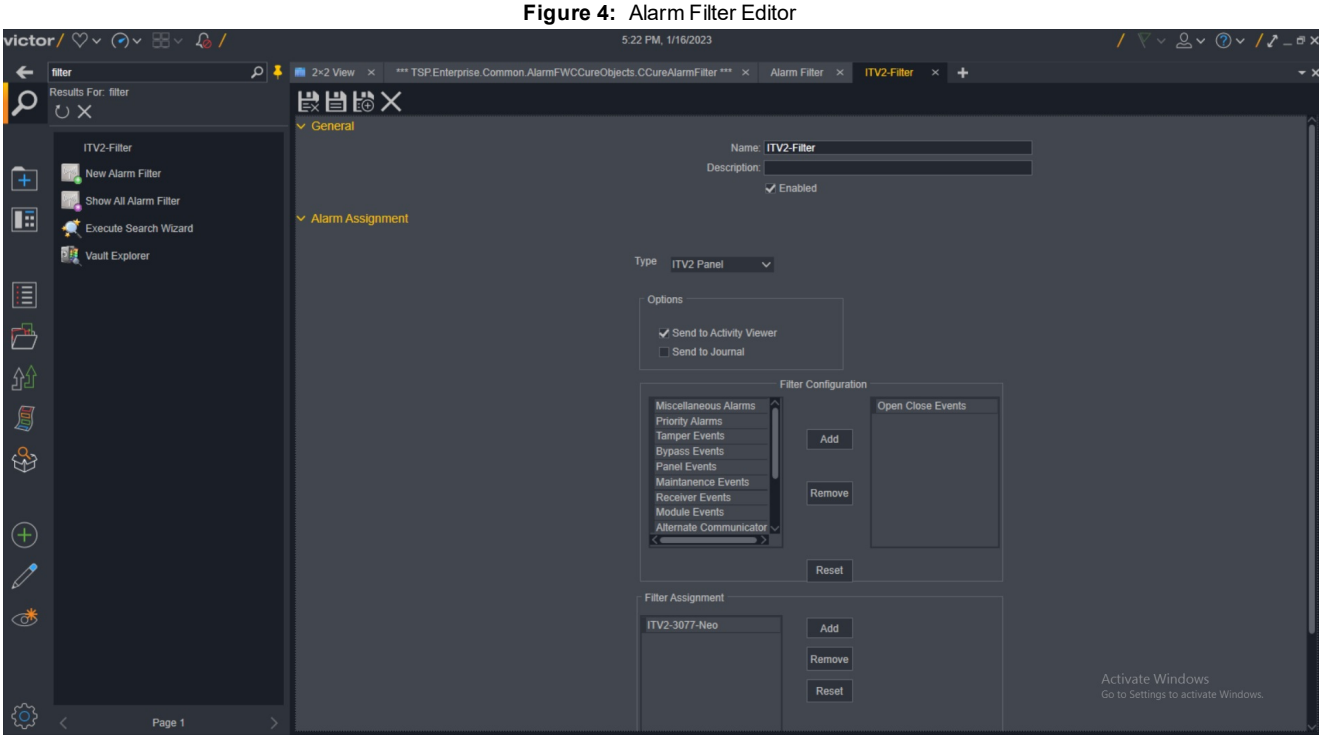
Alarm Filter is used to filter certain group of alarms for assigned panels.

#### Procedure - Configuring the Alarm Filter

1. Launch victor Client application.

2. In the search area, enter string as Filter and click on Search icon.
3. Click **New Alarm Filter** option listed under the searched results.
4. The **New Alarm Filter editor** window appears in the victor client application, refer Figure 4 on Page 42.

**Figure 4:** Alarm Filter Editor




5. Enter the Alarm Filter name and description in the **Name** and **Description** field under the **General** tab respectively.
6. Select the **Enabled** check-box under the **General** tab to enable the Alarm Filter.
7. Click the **Alarm Assignment** Tab.
8. Click the drop-down in **Type** filed under **Alarm Assignment** Tab and select panel type as **ITv2 Panel**.
9. (Optional) Select the check-boxes **Send To Monitoring Station** and **Send to Journal** under the **Options** section of **Alarm Assignment**Tab to send the alarm message to the Monitoring Station and to journal the message respectively.
10. Select one or more Alarms/Events listed under the left column of **Filter Configuration** section under the **Alarm Assignment** Tab and click **Add** Add, then the selected Alarms/Events are moved to the right column of **Filter Configuration** section.
11. Click **Save and Close**.

## Procedure - Removing the Alarm Filter

1. Select the Alarms from the right column of **Filter Configuration** section under the **Alarm Assignment** Tab field and click **Remove** Remove.

   The selected Alarms are removed and appears in the left column of **Filter Configuration** section.
2. Click **Save and Close**.

### Procedure - Resetting the Alarm Filter

1. Click **Reset**  under the **Filter Configuration**section of **Alarm Assignment** Tab.

   The Alarms are reset to the default settings.
2. Click **Save and Close**.

### Procedure - Assigning the Panel to the ITv2 Alarm Filter

1. Click **Add**  under the **Filter Assignment**section of **Alarm Assignment** Tab.
2. Select the Panel from the new window popped up with the configured ITv2 panels list and click **OK**  .
3. Click **Save and Close** to save and exit.

### Procedure - Removing the Panel to the ITv2 Alarm Filter

1. Select the ITv2 Panel from the left column of **Filter Assignment**section under the **Alarm Assignment** Tab and click Remove  .

   The selected Panels are removed and appears in the left column of **Filter Assignment** section.
2. Click **Save and Close** to save and exit.

### Procedure - Resetting the Panel to the ITv2 Alarm Filter

1. Click **Reset**  under the **Filter Assignment**section of **Alarm Assignment** Tab.

   The Panels are reset to the default settings.
2. Click **Save and Close**.

## Fields of the Alarm Filter Editor

#### General Section

**Table 24:** General Section

| Property | Value |
|---|---|
| Name | Enter the name of the Alarm Filter. |
| Description | Enter the description about the Alarm Filter. |
| Enabled | Select the check box to enable the Alarm Filter. |

#### Alarm Assignment Section

**Table 25:** Alarm Assignment Section

| Property | Value |
|---|---|
| Type | Select ITv2 Panel from the list. |
| Options | If required, select the following in the Option section:<br>■ Check-box **Send to Activity Viewer**, if you want to send the alarm message to the Activity Viewer, if the alarm exists.<br>■ Check-box **Send to Journal**, if you want to journal the message, if the alarm exists. |
| **Filter Configuration** | |
| Left Column | Available Alarm list in ITv2. |
| Right Column | Lists the configured Alarms. |
| Add | Click to add the Alarm.<br>Select the Alarm from the left column and click **Add**. The selected Alarm is configured to the right column. |
| Remove | Click to remove the configured Alarm.<br>Select the Alarm from the right column and click **Remove**. The selected Alarm is removed from the right column and appears in the Alarms list (left column). |
| Reset | Click to rest the Alarms. |
| **Filter Assignment** | |
| Add | Click to add a Panel.<br>Select a Panel from the list. The selected Panel is assigned to the alarm filter (listed in the left column). |
| Remove | Click to remove the assigned Panel.<br>Select a panel from the Assigned section (left column) and click **Remove**. The selected panel is removed from the Assigned list (left column). |
| Reset | Click to reset the Panels |

## Alarm Group by Filter

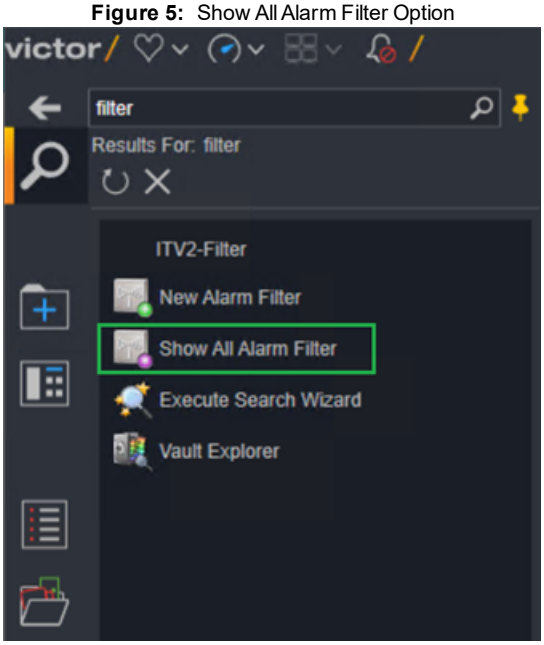
**Table 26:** Alarm Group by Filter

| | Alarm Group | Alarm Filter |
|---|---|---|
| Zone Status | PriorityAlarm | Alarm<br>Fault |
| | Open Close Events | Open Close |
| | BypassEvents | Bypass |
| | Tamper Events | Tamper |
| Partition Status | PriorityAlarm | Arm/Disarm Notification<br>Alarm in Memory |
| | MiscellaneousAlarms | Trouble Status<br>Ready<br>Entry Delay and Exit Delay |
| Panel Status | Maintenance Events | Device Low Battery<br>PanelTrouble |
| | Module Events | Module Trouble<br>Wireless/Keypad Fault |
| | PanelEvents | Log OnlyEvents |

## Procedure - Accessing the Alarm Filter in victor Client

1. Launch victor Client application.
2. In the search area, enter string as Filter and click on Search icon.
3. Click **Show All Alarm Filter** option listed under the searched results.

**Figure 5:** Show All Alarm Filter Option

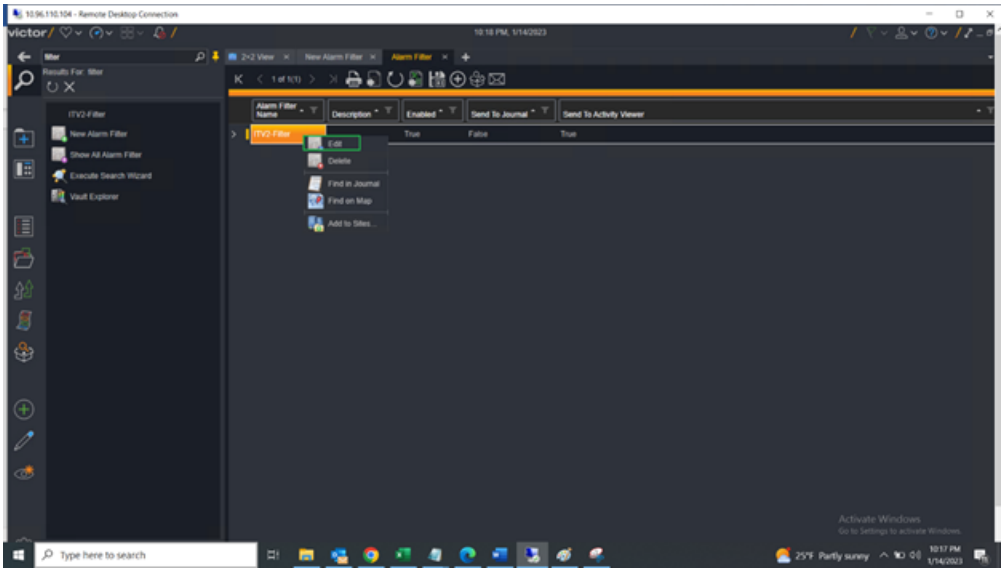



4. The **Alarm Filter** window appears in the victor client application with all the list of configured Alarm Filters.

### Procedure - Editing the Alarm Filter Configuration

1. In the search area, enter string as Filter and click on Search icon.
2. Click **Show All Alarm Filter** option listed under the searched results.
3. The **Alarm Filter** window appears in the victor client application with all the list of configured Alarm Filters.

4. Right-click the **Alarm Filter** that you want to access and select **Edit**.



### Procedure - Deleting the Alarm Filter Configuration

1. In the search area, enter string as Filter and click on Search icon.
2. Click **Show All Alarm Filter** option listed under the searched results.
3. The **Alarm Filter** window appears in the victor client application with all the list of configured Alarm Filters.
4. Right-click the **Alarm Filter** that you want to access and select **Delete**.
5. A Confirmation message is displayed. Enter **Yes** to delete or **No** to cancel.

## Configuring ITv2 Actions

ITv2 Integration Actions are available for the following objects:

- ITv2 Panel
- ITv2 Partition
- ITv2 Zone
- ITv2 Output
- ITv2 Virtual Zone

### Procedure - Configuring ITv2 Actions

1. Select **ITv2 Action** from the **New** icon on the left side of the panel.
2. Enter **Name** and **Description** for the ITv2 Integration Action.
3. In the ITv2 Device field, select to add device. The Object Selector displays.
4. Select desired object and click **OK**.
5. Repeat steps 1 to 5 as required.
6. Select desired action from the ITv2 Device Action drop-down list.
7. Click **Save and Close**.

**NOTE** If you want to remove the device, select the device check box to be removed and click

## Configuring ITv2 Alerts

The Event Setup editor can be used to configure alerts.

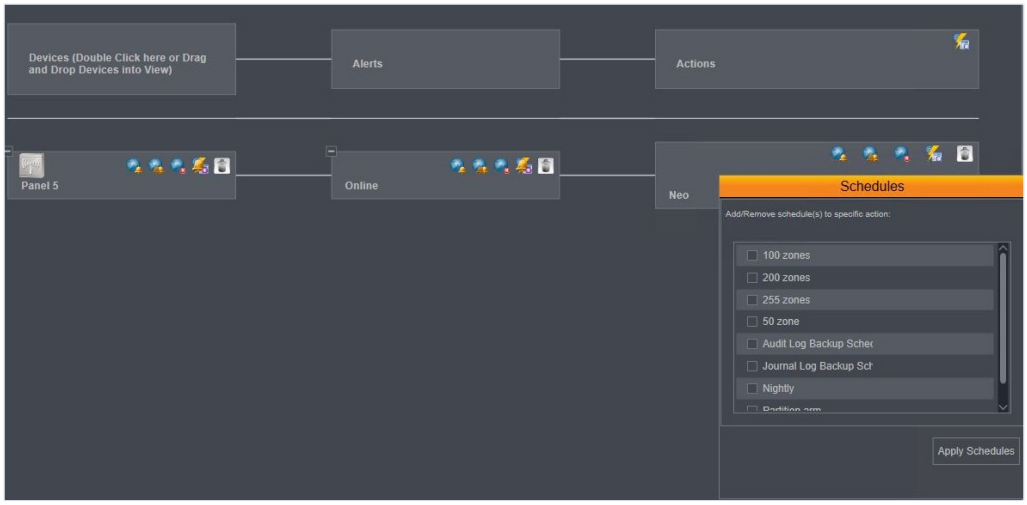
For further information on Events, refer to the *victor Administration and Configuration Guide*.


See Appendix A: Alert Types to view a complete list of Alert Types supported by victor.

### Procedure - Configuring Schedule Actions for ITv2

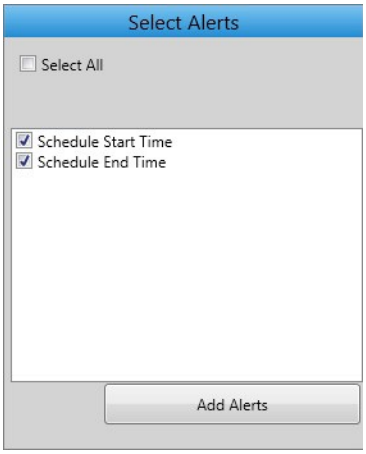
1. Select **Event/Schedule Setup** from the New icon on the left side of the panel. The Event/Schedule Setup page opens.
2. Double-click the Device node and use the object selector and select Type as **Schedules**.


3. Select the required Schedule from the list. You must have created the schedule to select it. Refer to the *victor Administration and Configuration Guide* for more information about Creating Schedules.

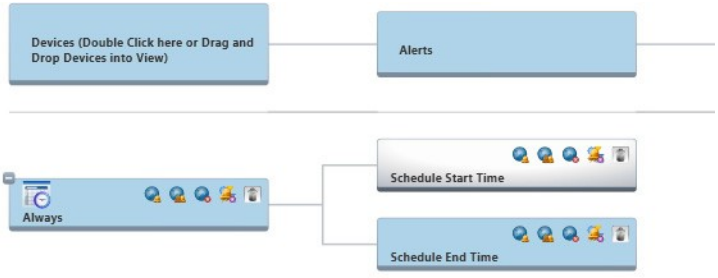



4. Selected **Schedule** is displayed in the Device node.


5. Select  in Device node to add **Alerts**.
6. Select **Schedule Start Time** and **Schedule End Time** check box from the **Select Alert** window.




7. Click **Add Alerts**. The Schedule Start Time and Schedule End Time is displayed in the **Alerts** node.



8. Select in the **Alerts** node to add actions.
9. Select ITv2 Action from the object selector. You should have already created ITv2 Integration Action to select it. See Configuring ITv2 Actions for more information.

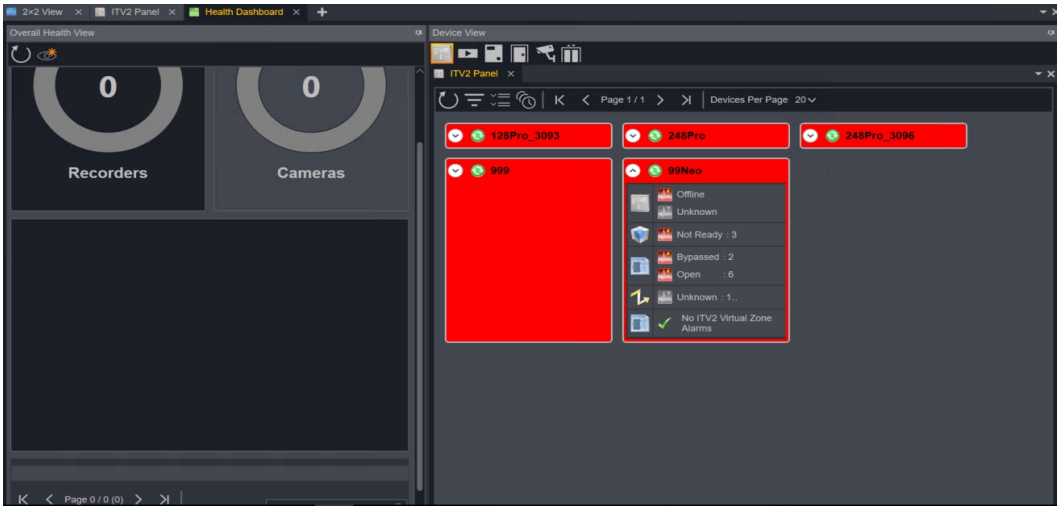

10. Repeat as required.
11. Click **Save and Close**.

**NOTE** Partitions disabled in the Panel will not update any status in C•CURE 9000.

# Operation

## Health Dashboard

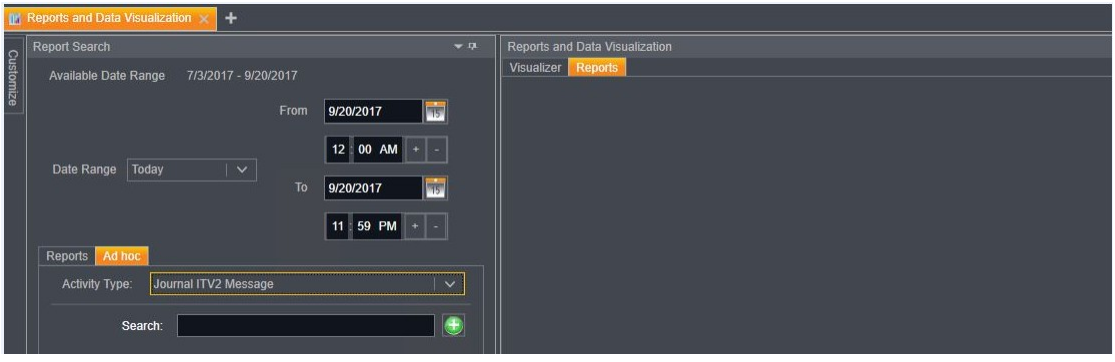
Health status of all ITv2 objects is annunciated in victor's Health Dashboard as follows:




Refer to Health Status for a full list of supported health statuses.

## Reports

Gives information of all the ITv2 actions performed during a selected time interval. To view the Reports, click Reports and data visualization and then click New. Go to the Ad hoc tab and select Journal ITv2 Messages from the Activity Type drop-down.




For more information on reporting within victor, refer to the victor Unified Client Configuration and Administration Guide.

## Dynamics Views

All configured ITv2 Panels, Zones, Areas and Outputs are displayed in victor's object list views (dynamic views), you can right-click an object and perform manual actions on configured objects.

## Manual Actions

The following message appears in the monitoring station if any partition is in alarm and armed:


You can perform the following manual actions from victor client:

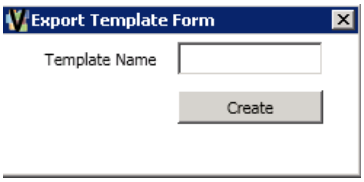
| Manual Actions | Manual Actions |
|---|---|
| Creating and Applying Template | Procedure - Creating a Template<br>Procedure - Applying a Template |
| Synchronizing the Panel | Procedure - Synchronizing from the Panel<br>Procedure - Synchronizing to the Panel |
| Manual Actions Performed Using Virtual Keypad | Procedure - Arming the Partition Using Virtual Keypad<br>Procedure - Disarming the Partition Using Virtual Keypad<br>Procedure - Bypassing the Zone Using Virtual Keypad<br>Procedure - Resetting the Zone Using Virtual Keypad<br>Procedure - Activating the Command Output Using Virtual Keypad<br>Procedure - Deactivating the Command Output Using Virtual Keypad<br>Procedure - Viewing Troubles in the Panel Using Virtual Keypad<br>Procedure - Viewing Alarms in the Panel Using Virtual Keypad |
| Global Arming or Disarming Partitions in the Panel | Procedure - Performing ITv2 Panel Manual Actions<br>Global Away Arm<br>Global Stay Arm<br>Global Disarm<br>Procedure - Enable Open/Close notification<br>Procedure - Disable Open/Close notification |
| Arming and Disarm Partitions | Procedure - Arming and Disarming Partitions: |
| Performing System Tests in the ITv2 Partition | Performing System Tests in the ITv2 Partition |
| Bypassing and Resetting Zones | Procedure - Bypassing the Zone<br>Procedure - Resetting the Zone |
| Activating and Deactivating Command Outputs | Procedure - Activating the Command Output<br>Procedure - Deactivating the Command Output |

## Creating and Applying Template

### Procedure - Creating a Template

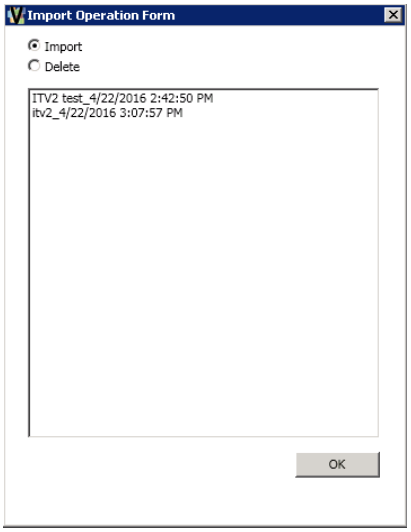
Creating a template saves time because you do not have to re-enter the same information again. Follow the steps to create a template:

1. From the **Navigation bar**, click the **Show All** icon, and then click **ITv2 Panel**.
2. The ITv2 Panel tab appears. Right-click the ITv2 Panel and select **Create Template**.
3. **Export Template Form** window appears. Enter a template name and click **Create**.




### Procedure - Applying a Template

1. Select **Show All** icon, and search for ITv2 Panel and click on it.
2. The **ITv2 Panel** tab appears. Right-click the ITv2 Panel and select **Apply Template**.
3. **Import Operation** window appears. Select **Import**, select a template and then click **OK**.




The configurations are applied to the Panel.

**NOTE**

- Only if the Personnel exists, the user code and attribute, and the user partition assignment is written to the Panel.
- Do not apply the template in ITv2 Panel which was created with ITV2 Panel.

## Synchronizing the Panel

### Procedure - Synchronizing from the Panel

1. Right -click the panel and select **Synchronize from Panel**.

**NOTE** During synchronization, User cannot modify the panel editor.

### Procedure - Synchronizing to the Panel

1. Open the victor device list in the victor Unified Client application.
2. Right-click the panel and select **Synchronize to Panel**.

### Troubleshooting Tips

If the synchronization has stopped or failed:

- Check the physical connection between the panel and the server:
  - In the command prompt, type “ping <IP address>” (for example “ping 191.20.4.5”) and verify the connection.
  - Telnet to the command port number and the IP address.
  - Utilize the ‘netstat’ command to find problems in the network.
- Ensure the user is not inside programming mode while the driver is attempting to write to the panel.
- Verify if the ITv2 driver and the server is up and running.
- Verify if the alternate communication is enabled in the DSC Neo or Pro Panel by using the section number 382 and option 5 and section 407 and option 7.
- Verify if any faulty hardware is connected to the panel.

### Manual Actions Performed Using Virtual Keypad

ITv2 Virtual Keypad allows you to view the list of Partitions, Zones, Output, Troubles, and Alarms in the DSC Neo or Pro Panel. Ensure the panel is online and synchronized prior to accessing the virtual keypad. It is recommended that you open only one Virtual Keypad at a time.

**NOTE** The ITv2 objects in the virtual keypad are displayed in alphabetical order.

The following actions can be completed using the Virtual Keypad:

- Arm or Disarm a partition
- Bypass or Reset a Zone
- Activate or Deactivate an output

#### Procedure - Arming the Partition Using Virtual Keypad

Ensure that the status of the partition is Ready. You cannot arm the partition if the status is Not Ready or Unknown.

1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Partitions**. All available Partitions appear.
3. Select the partition that you want to arm. Use the up and down arrow to move up and down.
4. Click **Arm**. The status of the partition is updated in the panel and is displayed in the Activity Viewer.
5. Click ✕ to exit.

**NOTE** You cannot arm the partition when the zones of the partition are in trouble.

### Procedure - Disarming the Partition Using Virtual Keypad

1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Partitions**. All available Partitions appear.
3. Select the partition that you want to disarm. Use the up and down arrow to move up and down.
4. Click **Disarm**. The status of the partition is updated in the panel and is displayed in the Activity Viewer.
5. Click ✕ to exit.

### Procedure - Bypassing the Zone Using Virtual Keypad

1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Zones**. All available Zones are listed.
3. Select the zone that you want to bypass. Use the up and down arrow to move up and down.
4. Click **Bypass**. The status of the zone is updated in the panel and is displayed in the Activity Viewer.
5. Click ✕ to exit.

### Procedure - Resetting the Zone Using Virtual Keypad

1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Zones**. All available zones appear.
3. Select the zone that you want to reset. Use the up and down arrow to move up and down.
4. Click **Reset**. The status of the zone is updated in the panel and is displayed in the Activity Viewer.
5. Click ✕ to exit.

### Procedure - Activating the Command Output Using Virtual Keypad

1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Output**. All available command outputs appear.
3. Select the command output that you want to activate. Use the up and down arrow to move up and down.
4. Click **Activate**. The status of the command output is updated in the panel and is displayed in the Activity Viewer.
5. Click ✕ to exit.

### Procedure - Deactivating the Command Output Using Virtual Keypad

1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Output**. All available command outputs appear.

3. Select the command output that you want to deactivate. Use the up and down arrow to move up and down.
4. Click **Deactivate**. The status of the command output is updated in the panel and is displayed in the Activity Viewer.
5. Click to exit.

### Procedure - Viewing Troubles in the Panel Using Virtual Keypad

1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Troubles** . All available troubles in the panel appear.
3. Click to exit.

### Procedure - Viewing Alarms in the Panel Using Virtual Keypad

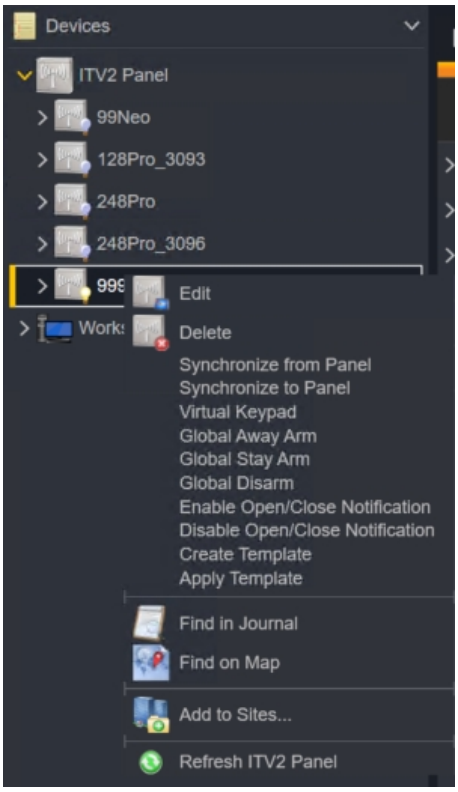
1. Right-click the Panel and select **Virtual Keypad**.
2. In the Virtual Keypad, click **Alarms**. All available troubles in the panel appear.
3. Click to exit.

**NOTE** Partitions disabled in the panel will not update any status in victor.

## Global Arming and Disarming Partitions in the Panel

You can arm or disarm all the partitions together from the panel. You can perform the following manual actions from the ITv2 Panel:

- **Global Away Arm:** Arms all the Partitions in the panel. This option is used to arm all the sensors associated to a panel. For example; the motion sensors, doors, and windows associated to a panel will be armed.
- **Global Stay Arm:** Arms only the perimeter of the system in the panel. This option is used to bypass the interior motion sensors and arms only the perimeter associated to a panel. For example, the doors and windows will be armed bypassing interior sensors.
- **Global Disarm:** Disarms all the partition in a Panel.




Ensure the following, before performing the global arm or disarm actions:

- The ITv2 is Online.
- Partitions are ready with no trouble and no alarm.
- Zones are closed with no fault, no alarm and no tamper.

**NOTE**

- You cannot arm a partition when the status of the zones of the partition are in Trouble.
- Unsuccessful command response reporting depends upon the number of retries for the same command.

### Procedure - Performing ITv2 Panel Manual Actions

1. Right-click the ITv2 Panel you want to perform the manual action.
2. Choose one of the manual actions:

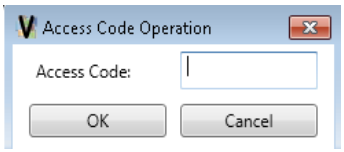
- Global Away Arm

  If you want to arm all the partitions in the panel select **Global Away Arm**.
- Global Stay Arm

  If you want to arm all the partitions, except for the interior sensors in the panel, select **Global Stay Arm**.
- Global Disarm

  If you want to disarm all the partitions in the panel select **Global Disarm**.

3. The **Access Code Operations** dialog box appears. Enter the Access Code and click **OK**.




The status of the Partition in the Panel changes to the manual action performed.

### Procedure - Enable Open/Close notification

1. Right click on the Panel and from the context menu, select **Enable Open/Close Notification**.

   On selecting this action all the Zones Status Change reporting will be enabled on the panel.

### Procedure - Disable Open/Close notification

1. Right click on the Panel and from the context menu, select **Disable Open/Close Notification**.

   On selecting this action all the Zones Status Change reporting will be Disabled on the panel.

### Arming and Disarming Partitions

You can arm and disarm individual partitions from the ITv2 Partition.

- **Arm:** Arms the selected Partition.
- **Disarm:** Disarms the selected Partition.

The following table lists all the available arm types:

**Table 27:** Arm Types for ITv2

| Arm Type | Description |
|---|---|
| Stay Arm | Select this check box to enable Stay Arm option.<br>Stay Arm option is used to arm only the doors, windows and bypass the interiors. For example; motion detectors.<br>If this option is enabled, all motion sensors are disabled and the entry and exit delay is enabled. |
| User Arm | Select this check box to enable User Arm option. |
| Away Arm with No Entry Delay | Select this check box to enable Away Arm with No Entry Delay option.<br>Away Arm with No Entry Delay option is used to arm the Partition without any entry delay. |
| Quick Arm | Select this check box to enable Quick Arm option<br>Quick Arm option is used when you want to exit the armed zone, to avoid disarming and then re-arming the zone. |
| Night Arm | Select this check box to enable Night Arm option.<br>Night Arm option is used to arm the zones except for the devices that is set as Night zone. |
| Stay Arm with No Entry Delay | Select this check box to enable Stay Arm with No Entry Delay option.<br>Stay Arm with No Entry Delay option is used to arm the zones, except the motion detectors, without any entry delay.<br>If this option is enabled, all motion sensors are disabled and the entry and exit delay is disabled. |
| Away Arm | Select this check box to enable away Arm option.<br>Away Arm option is used to arm the zones, except the motion detectors, without any entry delay.<br>If this option is enabled, all motion sensors are disabled and the entry and exit delay is disabled. |

| Arm Type | Description |
|---|---|
| Instant Stay Arm | Select this check box to enable instant stay Arm option.<br>Instant Stay Arm option is used to instantly arm the zones, except the interiors. |
| Disarm | Select this check box to enable disarm option. Disarm option is used to disarm the Partition. |

**NOTE**

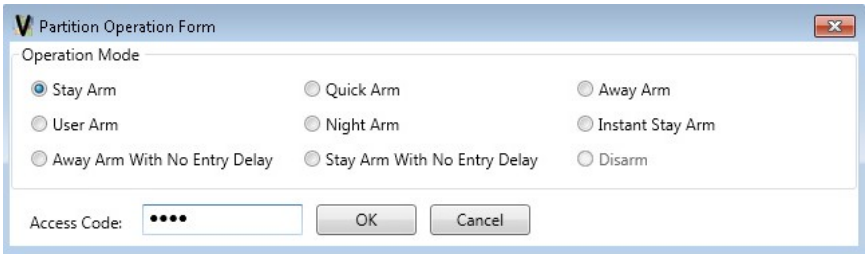
You cannot arm the Partition when the Zones of the Partition are in trouble. For instance, if you arm a partition and do not receive any notification of the arms status, then there may be a zone associated with that partition that is in trouble.

Ensure the following, before performing the manual actions:

- The ITv2 is Online.
- The ITv2 has Synchronized successfully.
- The Partition is in the Ready status to be armed.
- The user should not be in Programming Mode through the keypad.

### Procedure - Arming and Disarming Partitions:

1. Right-click the partition and select **Arm/Disarm**.
2. The **Partition Operation Form** window opens, select an **Operation Mode**, enter the **Access Code** and then click **OK**:




Access Code is mandatory for User Arm, Away Arm with No Entry Delay, and Stay Arm With No Entry Delay.

- For **Arm**, the status is changed to **Armed** and if there is any alarm in the partition, the beep is silenced in the partition.
- For **Disarm** the status is changed to **Disarmed**.

**NOTE**

- For reporting purposes, arming without a user Access Code will be displayed as Special User.
- The Partition should not be in alarm or armed state.
- Stay Arm, Quick Arm, Night Arm, Instant Stay Arm, and Away Arm do not a require access code to operate. It will always appear as Armed by Special User in the Monitoring Station even if you enter the access code.
- Access Code is mandatory for User Arm, Away Arm with No Entry Delay, and Stay Arm with No Entry Delay.
- The user should not be in Programming Mode through the keypad.

## Performing System Tests in the ITv2 Partition

System tests are performed to ensure that the system is functioning as intended. The System Test option tests the following:

- System Bell Output
- Keypad lights
- Panel standby battery

Ensure the ITv2 is online before performing the manual actions.

### Procedure - Performing System Test

1. Right-click the Partition object and then click **System Test**.
2. Enter the **Access Code** and click **OK**.

During the System Test all keypad sounders and sirens are activated for two seconds. All keypad lights are turned ON, and the Ready, Armed, and Trouble LEDs flash.

## Bypassing and Resetting Zones

You can bypass and reset Zones directly from the victor Device List.

### Procedure - Bypassing the Zone

1. Right-click the zone object and select **Bypass**.
2. The selected Zone is bypassed and the status changes to **Bypassed**.

### Procedure - Resetting the Zone

1. Right-click the zone object and select **Reset**.
2. The selected zone is reset and the status changes to Not Bypassed.

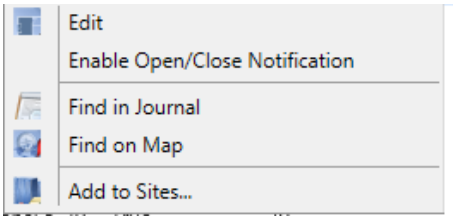
**NOTE** Bypassing or Resetting of zones does not work if a Partition is in Arm on the Panel.

### Procedure - Enable Open/Close status

1. Right-click on the Zone Context Menu and select **Enable Open/Close** notification from the context menu.

   This will start the Zone Status notification.

**NOTE** User can select multiple panels and do the above action.

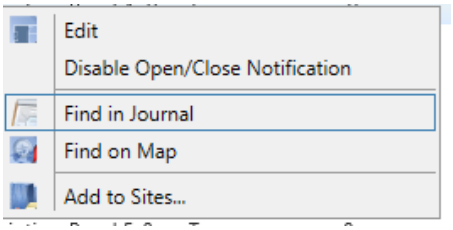



### Disable Open/Close status

1. Right click on the Zone context menu and select **Disable Open/Close** notification from the context menu.

   This will stop the zone status notification.

**NOTE** User can select multiple panels and do the above action.




## Activating and Deactivating Command Outputs

Command outputs are activated and deactivated directly from the victor Device List.

### Procedure - Activating the Command Output

1. Right-click the command output object and select **Activate Command Output**.
2. Enter the Access Code and click **OK**. The selected command output is active and the status changes to **Active**.

### Procedure - Deactivating the Command Output

1. Right-click the command output object and select **Deactivate Command Output**.
2. Enter the Access Code and click **OK**. The selected command output is deactivated and the status changes to **Inactive**.

# Troubleshooting

This section provides troubleshooting information for issues that may occur in the ITv2 Integration.

**Problem:**

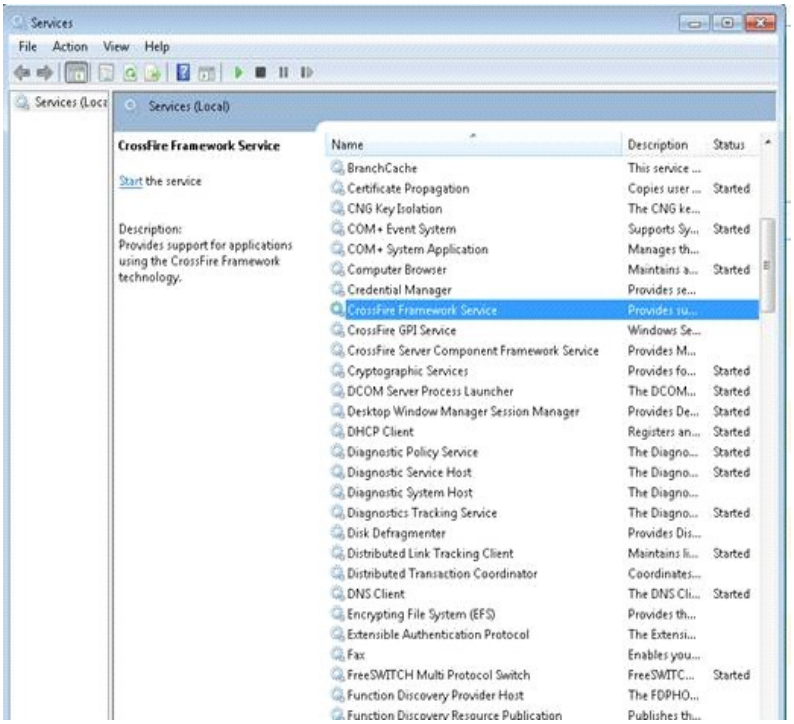
Sometimes the installation may fail if the CrossFire service does not stop on time and throws a time out error.

**Solution:**

Ensure that you have completed the following steps:

- Check if the CrossFire service is stopped from services panel in case of installation failure. Refer to the image below.
- Wait till the CrossFire service is stopped and then trigger the installation again. This will work fine as the service is stopped already.

**Figure 6:** Figure 7-1 CrossFire Services



# Appendix A: Alert Types

The Event Configuration editor is used to configure Alerts for ITv2 objects. The following tables detail the supported Alert Types supported for ITv2 Objects within victor:

**Table 28:** Alert Types for ITv2 Panels

| Panel Alert Type | Value |
|---|---|
| Online Status | Online<br>Offline<br>Disabled<br>Unknown |
| Synchronization Status | Synchronizing<br>Synchronized<br>Synchronization Failed |
| System Trouble | Fire Trouble<br>AC Loss<br>Configuration Trouble<br>Module Battery Charger Trouble<br>Module Battery Missing Trouble<br>Module Low Battery Trouble<br>Module Supervisory Trouble<br>Module Bus Low Voltage<br>Module Aux Trouble<br>Ground Fault<br>Module Tamper<br>Output Fault<br>Device Delinquency<br>Density Low Sensitivity<br>Device Internal Fault<br>Service Request Trouble<br>Time Date Trouble<br>System Trouble<br>Device Tamper<br>Normal<br>Carbon Monoxide Trouble<br>Device Fault |

| Panel Alert Type | Value |
|---|---|
| Communication Trouble | Communication Trouble<br>Fail to Communicate<br>Ethernet Trouble<br>GSM Trouble<br>Printer Offline<br>Telephone Line Monitoring Trouble<br>GSIP Receiving Trouble<br>SIM Lock Trouble<br>All Receiver Not Available Status<br>All Receiver Supervision Trouble |
| Sensor Trouble | RF Jam Trouble<br>RF transmitter Low Battery |
| Relay Trouble | Bell Trouble<br>Normal |

**Table 29:** Alert Types for ITv2 Partitions

| Partition Alert Type | Value |
|---|---|
| Armed State | Away Armed with No Entry Delay<br>Away Armed<br>Disarmed<br>Night Armed<br>Night Armed with No Entry Delay<br>Quick Armed<br>Stay Armed<br>Stay Armed with No Entry Delay<br>User Armed<br>Unknown |
| Ready State | Ready<br>Not Ready<br>Unknown |
| Alarm in Memory State | Alarms in Memory<br>No Alarms in Memory<br>Unknown |
| Trouble State | Troubles Present<br>No Trouble Present<br>Unknown |

| Partition Alert Type | Value |
|---|---|
| Zone Bypassed State | Zone Bypassed<br>No Zone Bypassed<br>Unknown |

**Table 30:** Alert Types for ITv2 Zones

| Partition Alert Type | Value |
|---|---|
| Bypass State | Bypassed<br>Not Bypassed<br>Unknown |
| Fault State | Fault<br>No Fault<br>Unknown |
| Open Close State | Open<br>Close<br>Unknown |
| Tamper State | Tamper<br>Not in Tamper<br>Unknown |

# Appendix B: Health Status

Supported Health status annunciations for each ITv2 object type are as follows:

**Table 31:** Health status for ITv2 Panels

| Panel Status | Health Status |
|---|---|
| Online<br>Disabled<br>Synchronizing<br>Synchronized<br>Start Synchronization | Normal |
| Offline<br>Synchronization Failed | Device Alert |
| Unknown | Unknown |

**Table 32:** Health status for ITv2 Partitions

| Partition Status | Health Status |
|---|---|
| Arm/Disarm<br>No Alarm in Memory<br>No Alarm<br>Ready<br>No Trouble<br>No Zone Bypassed | Normal |
| Alarm in Memory<br>Alarm<br>Not Ready<br>Trouble<br>Zone Bypassed | Device Alert |
| Unknown | Unknown |

**Table 33:** Health status for ITv2 Zones

| Zone Status | Value |
|---|---|
| No Fault<br>Reset<br>No Tamper<br>Alarm Restore<br>Close | Normal |
| Bypass<br>Fault<br>Tamper<br>Alarm<br>Open | Device Alert |

**Table 34:** Health status for ITv2 Outputs

| Output Status | Value |
|---|---|
| Active<br>Inactive | Normal |