American Dynamics
From Tyco Security Products

DMP Intrusion Integration User Guide

v5.2

Revison A0

Notice

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

Under copyright laws, the contents of this manual may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Tyco Security Products. © 2018 Tyco Security Products. All Rights Reserved.

American Dynamics

6600 Congress Avenue

Boca Raton, FL 33487 U.S.A.

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

Windows® is a registered trademark of Microsoft Corporation. PS/2® is a registered trademark of International Business Machines Corporation.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco Security Products will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco Security Products. are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

Introduction

Installation

Administration

Configuration

Operation

Alert Types   49

American Dynamics

Introduction

DMP Integration Overview

DMP security systems integrate seamless with victor, allowing customers to monitor and configure their DMP security system (DMP Intrusion device hardware) and alarms directly from the victor unified client.

This seamless integration between DMP security systems and victor unified systems is brought about by **DMP Intrusion Integration software**.

DMP security system consists of DMP intrusion Panels, one or more keypads, and various sensors and detectors.

The following table lists the supported Panel types:

Panel Type	Firmware version
XR500N	V206, V208, V212
Canadian Version XR500N	V206, V208, V212
XR500E	V208, V212
XR100N	V206, V208, V212
XR150N	V110, V171
XR550N	V111
XR550E	V111, V171

Product Components

- **Unified victor Graphical User Interface**: Used to configure DMP objects and perform manual actions.
- **DMP Objects**: Physical or logical DMP entities in the victor environment. The DMP objects are:

American Dynamics

- Panel
- Partitions
- Zones
- Outputs
- Secondary devices
- User
- User Profiles

- **DMP Server Component**: The center of the integration. The DMP Server Component facilitates and maintains communication with the DMP devices and auto-creates **Partitions**, **Zones**, **Outputs**, **Secondary Devices, User, and User Profiles** based on the Panel capabilities.

Figure 3-1 System Overview: IP Configuration
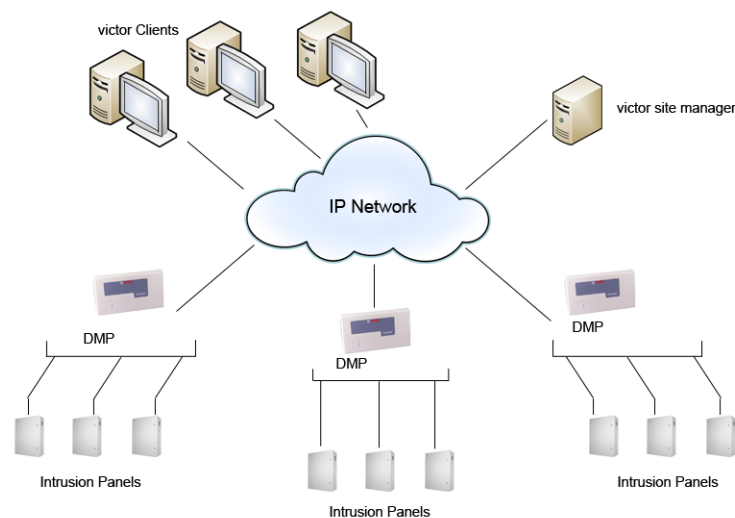
After you install the driver all relevant DMP Object editors are available from the Victor Unified Client Intrusion.

Features

The objective of the DMP Intrusion integration is to provide a standard, single interface between DMP Intrusion devices and American Dynamic's victor Unified Video Management product.

The following features are supported:

- Encryption types 128 and 256 for XR550E Panel for Alarm channel.
- Manual synchronization of the following DMP objects:
    - Partition
    - Zones
    - Output
    - Secondary Zones
    - User
    - User Profiles
- Manual actions to control the DMP objects.
    - Panel: Synchronize, Arm system, Disarm system, Force Arm system, Silence alarm, Reset Sensor.
    - Partition: Arm, Force Arm, or Disarm
    - Zone: Bypass, Reset
    - Output: Activate, Deactivate, Momentary Output, Continuous pulse
- Silence Trouble and Reset Sensor
- Adding of new DMP Panels.
- Editing of DMP objects (Panels, Partitions, Zones, Outputs, Secondary devices, User, and User Profiles)
- Viewing the status and information of configured DMP objects.
- victor role respect.
- Provides integration with victor Object Association.
- Monitors devices on victor Maps and Health dashboard.

American Dynamics

Installation

Minimum Requirements

Hardware

DMP Intrusion integration has the same hardware requirements as victor unified client and victor Application Server. Therefore, if the target computer meets the Unified Server requirements, then it meets the DMP Intrusion Integration requirements.

Prerequisites

Prerequisites to install DMP Intrusion Integration are:

• You must have the appropriate Window's permissions.

• You must be a member of the local Administrators group or have equivalent privileges.

• To install the DMP Intrusion Integration on a corporate network, you must co-ordinate with your corporate network administrator.

• You must have installed victor Application Server and have a license for the following:

> • victor Application Server

> • DMP Integration

Note

Refer to the DMP release notes for the latest software version.

Installation

You must install the DMP Intrusion installer on both the **victor Application Server** and all **victor unified client** machines.

Procedure 4-1 Installing DMP Intrusion Integration to victor

Step	Action

1	Close all programs.
2	Go to http://www.americandynamics.net.
3	Download the appropriate version of the DMP Integration Software Driver for your version of victor.
4	Launch the DMP Integration Software Installer. The **End User License Agreement** window appears.
5	Select **I agree to the license terms and conditions** check box, and then click **Install**. The **Tyco CrossFire Service Alert** dialog box appears.
6	Click **OK** to continue with the installation. The **Welcome to the Integration Setup** wizard appears.
7	Click **Next** to continue with the installation. The **Installation Options** dialog box appears.

Note

For EMC solution, if you want to enable the driver for redundancy, select the **Redundant server installation using supported third party redundancy** check box, enter the Virtual sever (alias) name and then click **Next.**

| **8** | Click **Next**. The **Ready to Install the Integration** dialog box appears. |
| **9** | Click **Install**. **Completed the Integration Setup Wizard** appears. |

Note

If you click **Cancel**, installation is rolled back to clean state.

| **10** | Click **Finish** to complete the installation process. The **Setup Successful** dialog box appears. |
| **11** | Click **Close** to exit the installation.
After the installation is complete, a new group called **Intrusion** is available on the **Setup** tab. |

- End -

Administration

General Hardware Information

Detailed hardware information is available for all configured DMP Intrusion devices in victor.

Accessing Hardware Information

Follow the steps to access the hardware information:

1   On the **Show All** button in the **Intrusion** group, click the required object.

        A new tab opens and all available objects appear.

2   Click on the **Edit** icon and select the object you want to access.

This information is also available if you right-click an object on the Device List and click **Edit**.

victor Integration Information

Roles

victor roles support DMP Intrusion device privileges. All context menu actions that are 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 DMP Intrusion objects. Object Association refers to linking unrelated victor objects with the intent of enabling incident building capability. For more information about Object Associations, refer to the *victor unified client Configuration and User Guide.*

Reports

victor's report selection tool and Find in Journal feature support DMP Intrusion 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 events configuration for DMP Intrusion Objects. For further information on events, refer to the *victor unified client Configuration and User Guide.*

Maps

victor Maps and Find on Map features support DMP Intrusion objects. For more information on Maps and the Find on Map feature, refer to the *victor unified client Configuration and User Guide* available on the American Dynamics website:

www.americandynamics.net

Note

victor editors offer the following save options when creating or editing objects:

• **Save and Close** - Save the current object and close the editor.

• **Save** (Apply) - Save changes and keep the editor open, so that you can make further changes.

• **Save and New** - Save the current object and open a new editor to create a new object with default values populated.

• **Close** - Cancel changes and close the editor without saving.

Configuration

DMP Panel Configuration using DMP Keypad

This section provides instructions to configure the DMP Panel hardware using keypad to communicate with unified server.

The unified Integration supports the following DMP Panel softwares:

- V206
- V208
- V212
- V110 (for XR150N)
- V111(for XR550N and XR550E)
- V171 (for XR150N and XR550E)

The Integration's communication mode is supported by Network (TCP/IP).

Procedure 5-1 Configuring the Account Number in the DMP Panel

An Account Number is used to uniquely identify each Panel. Follow the steps to configure the Account Number:

Step	Action
1	To access the Programmer:
	a Install the reset jumper across the two **J16** reset pins for two seconds.
	b Remove the reset jumper and place it over just one pin for future use.
	c Enter the password to enter the programming mode using the Keypad.
	d Press the **CMD**. **PROGRAMMER** displays.
2	Go to **COMMUNICATION** using **CMD**.
3	Press **SELECT** to go into the **COMMUNICATION** section.
4	In the **COMMUNICATION** section, select the **Account Number** option. This can be configured using **Select** keys and **DATA ENTRY DIGIT** keys.
5	Enter the **Account Number**.
6	Press **CMD** and then ←(Back) to revert to the **Programmer Section**.

7   Press **CMD** until the **STOP** option appears.

8   Press the **Select** key.

The Panel displays a **Saving, Please Wait** message.

> **NOTE**   After configuring the Account Number in the Panel, you must configure the same account number in the Panel Editor.

- End -

Procedure 5-2 Configuring Network parameters in the DMP Panel

Step	Action

1   To access the Programmer:

    a   Install the reset jumper across the two **J16** reset pins for two seconds.

    b   Remove the reset jumper and place it over just one pin for future use.

    c   Enter the password to enter the programming mode using the Keypad.

    d   Press **CMD** button**.**
         PROGRAMMER is displayed.

2   Press the **CMD** button go to **NETWORK OPTIONS**.

3   Press the **SELECT** to go into the **NETWORK OPTIONS** section.

4   In the **NETWORK OPTIONS** section, select the **LOCAL IP ADDRESS** option. This can be configured using **Select** keys and **DATA ENTRY DIGIT** keys.

5   Enter the Local IP Address, Subnet Mask, DNS Server, and Gateway Address.

6   Press **CMD** and then ← (Back) to revert to the **Programmer Section**.

7   Press **CMD** until the **STOP** option appears.

8   Press the **Select** key.
       The Panel displays a **Saving, Please Wait** message.

> **NOTE**
> - After you configure the IP address in the Panel, you must configure the same IP address in the Panel Editor.
> - When you configure the Static IP address in the Panel, ensure you also configure the Gateway Address, Subnet Mask, and the DNS Server. Follow the same procedure to configure the Subnet Mask, the DNS Server, and the Gateway Address.
> - To change the network settings, such as the IP Address, the Gateway Address, and so on, set the DHCP (Dynamic Host Configuration Protocol) option to **NO**. If you set the DHCP option to **YES**, you cannot configure the addresses.

- End -

Procedure 5-3 Configuring the Remote Key in the DMP Panel

Remote Key is used for remote functioning. Follow the steps to configure the Remote Key:

Step	Action

1 To access the Programmer:

    a Install the reset jumper across the two **J16** reset pins for two seconds.

    b Remove the reset jumper and place it over just one pin for future use.

    c Enter the password to enter the programming mode using the Keypad.

    d Press **CMD** button**.**
       PROGRAMMER is displayed.

2 Press the **CMD** button to go to **REMOTE OPTIONS**.

3 Press **SELECT** to go into the **REMOTE OPTIONS** section.

4 In the **REMOTE OPTIONS** section, select the **REMOTE KEY** option. This can be configured using **Select** keys and **DATA ENTRY DIGIT** keys.

5 Enter the remote key**.**

6 Press **CMD** and then ← (Back) to revert to the **Programmer Section**.

7 Press **CMD** until the **STOP** option appears.

8 Press the **Select** Key.
    The Panel displays a **Saving**, **Please Wait** message.

> **NOTE** After you configure the Remote Key in the Panel, you must configure the same Remote Key in the Panel Editor.

- End -

Procedure 5-4 Configuring the Programming Port in the DMP Panel

Programming Port is used to send all heart beats from the driver to the Panel and to send status updates from the Panel to the driver. Follow the steps to configure the Programming Port:

Step	Action

1 To access the Programmer:

    i Install the reset jumper across the two **J16** reset pins for two seconds.

    ii Remove the reset jumper and place it over just one pin for future use.

    iii Enter the password to enter the programming mode using the Keypad.

    iv Press **CMD** button**.**
       PROGRAMMER is displayed.

2 Press the **CMD** button to go to **REMOTE OPTIONS**.

3 Press **SELECT** to go into the **REMOTE OPTIONS** section.

4 In the **REMOTE OPTIONS** section, select the **NETWORK PROG PORT** option. This can be configured using **Select** keys and **DATA ENTRY DIGIT** keys.

American Dynamics

5   Enter **NETWORK PROG PORT.**

6   Press **CMD** and then ←(Back) to revert to **Programmer Section**.

7   Press **CMD** until the **STOP** option appears.

8   Press the **Select** key. The Panel displays a **Saving**, **Please Wait** a message.

| NOTE | After you configure the Programming Port in the Panel, you must configure the same Programming Port in the Panel Editor. Programming port is the command port. |

- End -

Procedure 5-5 To Configure the Date and Time in the DMP Panel

Step	Action

1   Access the **User Menu**.

2   Press **COMMAND** until **TIME** displays. Press the **Select key**.

3   The Panel displays the current **Day and Time**.

4   Press the **COMMAND** key. The Panel displays the current **Date**.

5   Press the **COMMAND** key to make any changes.

6   The Panel displays **TIME DAY DATE**.

7   Select **TIME**, the Panel displays **-: AM** and **PM**. Enter the current time and select **AM** or **PM**.

8   The Panel changes back to **TIME DAY DATE**.

9   Select **DAY**, the Panel displays **SUN MON TUE WED**.

10   Press the **COMMAND** key to display **THU FRI SAT**. Select the correct day. Use the **Back Arrow** key to toggle between the different day of the week.

11   Select **DATE**, the Panel displays **MONTH**:- Enter up to 2 digits for the month.

12   Press **COMMAND,** the Panel displays **DAY**:- Enter up to 2 digits for the day.

13   Press **COMMAND,** the Panel displays **YEAR**:- Enter up to 2 digits for the year.

14   Press **COMMAND**. The display returns to the **TIME DAY DATE**.

15   Press the **Back Arrow** key to exit the User Menu.

Procedure 5-6 Configuring the Receiver Port

Receiver port is used to report all alarms from Panel to victor. The receiver port also displays event messages. Follow the steps to configure the Receiver Port:

Step	Action

1   To access the Programmer:

    a   Install the reset jumper across the two **J16** reset pins for two seconds.

    b   Remove the reset jumper and place it over just one pin for future use.

    c   Enter the password to enter the programming mode using the Keypad.

    d   Press **CMD** button**.**
          PROGRAMMER is displayed.

2   Press the **CMD** button to go to **COMMUNICATION.**

3   Press **SELECT** to go into the **COMMUNICATION** section.

4   In the **COMMUNICATION** section, select the Path option. You can configure this using the Select keys and DATA ENTRY DIGIT keys.

5   Enter **Path =1**.

6   Select PATH 1 NET COMM TYPE=NET.

7   Press CMD until the **PATH 1 NET CHECKIN MINS** option is visible.

8   Enter **PATH 1 NET CHECKIN MINS=3**.

9   Press the **CMD** button.

10   Enter **PATH 1 NET FAIL MINS=240**.

11   Press the **CMD** button until the **Receiver IP** is visible.

12   Enter the Unified Server IP address at which you want to receive the Panel's Event Messages.

13   Press the **CMD** button.

14   Enter the Receiver PORT to the port at which you want to receive the Panel's Event Messages.

15   Press **CMD** and then ← (Back) to revert to Programmer Section.

16   Press **CMD** until **STOP** option appears.

17   Press the **Select** key. The Panel displays a **Saving, Please Wait** message.

> **NOTE**   You must configure the same Receiver Port in the Panel Editor. Receiver port is the Alarm port.

- End -

Procedure 5-7 Enabling Encryption in the Communication Path

This procedure encrypts the network when accessing the DMP controller remotely by enabling encryption in the communication path**.**

Step	Action

1   To Access the Programmer:

    a   Install the reset jumper across the two J16 reset pins for two seconds.

    b   Remove the reset jumper and place it over just one pin for future use.

    c   Enter the password to enter the programming mode using the Keypad.

    d   Press **CMD** button**.**
          PROGRAMMER is displayed.

2   Press the **CMD** to go to **REMOTE OPTIONS**.

3 Press **SELECT** to go into the **REMOTE OPTIONS** section.

4 In the **REMOTE OPTIONS** section. Select the **ENCRYPT NETWORK REMOTE** option. You can use the **Select** keys and **DATA ENTRY DIGIT** keys to configure this.

5 Select **ENCRYPT NETWORK REMOTE = YES**.

6 Press CMD and then ← (Back) to revert to Programmer Section.

7 Press CMD until the **STOP** option appears.

8 Press the **Select** key. The Panel displays a **Saving, Please Wait** message.

9 After enabling encryption on the Panel, select the **Command Port Encryption** check box in the Panel Editor to enable encryption in victor.

> **NOTE** If there is a mismatch in the encryption configuration between the DMP Panel and Panel editor, then the behavior of the driver is not assured.

- End -

Procedure 5-8 Enabling Encryption in Network path

This procedure encrypts the network when accessing the DMP controller remotely by enabling encryption in the network channel.

Step	Action

1 To access the Programmer:

    a Install the reset jumper across the two **J16** reset pins for two seconds.

    b Remove the reset jumper and place it over just one pin for future use.

    c Enter the password to enter the programming mode using the Keypad.

    d Press **CMD** button**.**
        PROGRAMMER is displayed.

2 Press the **CMD** button to go to **COMMUNICATION.**

3 Press **SELECT** to go into the **COMMUNICATION** section.

4 In the COMMUNICATION section select the **Path** option. This can be configured using Select Keys and DATA ENTRY DIGIT keys.

5 Enter Path =1.

6 Select **PATH 1 NET COMM TYPE=NET**.

7 Press the **CMD** button until the **PATH 1 NET ENCRYPT** option is visible.

8 Enter **PATH 1 NET ENCRYPT = Yes**.

Note

For XR550E Panels, you must either select the encryption type 128 or 256.

9 Press the **CMD** button and then ← (Back) to revert to the Programmer Section.

10 Go to **NETWORK OPTIONS** using **CMD**.

11 Press **SELECT** to go into the **NETWORK OPTIONS** section.

12   In the **NETWORK OPTIONS** section, select the **PASSPHRASE** option. This can be configured using select keys and data entry digit keys.

13   Enter the exact eight digit alphanumeric pass phrase. You must configure the same pass phrase on the server.

14   Press the **CMD** button and then ← (Back) to revert to the Programmer Section.

15   Press the **CMD** button until the **STOP** option appears.

16   Press the **Select** key. The Panel displays a **Saving, Please Wait** messages.

17   After enabling encryption on the Panel, go to the Panel Editor in victor, select the **Alarm Port Encryption** check box and enter the same configured Passphrase in the **PassPhrase** box.

NOTE	If there is a mismatch in the encryption configuration between the Panel and Panel Editor, then the behavior of the driver is not assured.

After the communication is established, you must program the required Zones, Outputs, Partitions and other objects in the Panel. See the *LT-0679-Programming-Guide* for more information.

- End -

Changing Configuration Settings

You can change the behavior of all the configured DMP Panels in unified application in a controlled manner using the `DMPConfiguration.xml` file. The file is located in:

`Tyco\CrossFire\ServerComponents\DMPConfiguration.xml`

You can change the following fields in the XML file:

```
<add key="CommandChannelHeartbeatIntervalInSeconds" value="10"/>

<add key="ReconnectIntervalForCommandChannel" value="180"/>

<add key="PanelSynchronizeBatchCount" value="3"/>
```

The following table describes the fields in the XML file:

Field	Description
Command Channel Heartbeat Interval in Seconds	Indicates the time interval between two successive heart beats sent by the DMP driver to the Panel to maintain the TCP communication. Value can range from 5 to 10 seconds.

Reconnect Interval for Command Channel	Indicates the time interval between two successive attempts made by the Integration to reconnect with the Panel, when no response from Panel is received. The minimum value should be 180 seconds.
Bulk Synchronization	Synchronizes the number of Panels simultaneously based on the Bulk Synchronization value. Value can range from 1 to 10 Panels. The default value is 3.

Configuring DMP objects

Adding DMP Panels

Before you add Partitions, Zones, Outputs, User, and User Profiles, you must configure new Panels using the DMP Panel editor.

Procedure 5-9 Adding New DMP Panels

Before you begin to configure the DMP Panel, ensure that you have the following:

- Panel Account Number
- Panel IP Address
- Alarm Port
- Panel type
- Remote key

Step	Action

1   In the **Intrusion** group, click on the **New** icon and then click the **DMP Panel**.

The **New DMP Panel** tab opens.

2   Click **General**. Add the following details in the expanded list:

Property	Description
Name	Enter a unique name for the Panel. The name can have up to 100 characters. **Note** Ensure that the name is unique, else an error message displays.

Description	Enter a description for the Panel. The description can have up to 100 characters.
Enabled	Select the **Enabled** check box to establish the communication between victor and the Panel. **Note** If the DMP Panel is disabled, the communication between victor and the DMP Panel is disabled.

3   Click **Panel Configuration**. Add the following details in the expanded list:

Property	Description
Panel Type	Select a Panel type from the **Panel Type** drop-down. The options available are: • XR500N • XR100N • XR500E • XR150N • XR550N • XR550E
Account Number	Enter the assigned Panel Account Number of the DMP Panel. • Account number is used to uniquely identify the Panel. • The valid range is from 1 to 65535. • If the account number is not unique, an error message is displayed. • The account number must be same as configured in the DMP Panels.
Panel IP Address	Enter the TCP/IP address of the Panel. The IP address must be in IPv4 format and unique within the system network.
Command Port	Enter the command port number. The command port identifies the port used to communicate messages to and from the Panel. Command port number can range from 1025 to 6553 and it can have a maximum of five digits. The default Command Port is 2001.
Host IP Address	Enter the TCP/IP address of the Host machine. The IP address must be in IPv4 format and unique within the system network.

Local Alarm Port	Enter the Local Alarm Port number.
	Local alarm port is used to receive data from the Panel.
	Local Alarm Port number can range from 1025 to 65535 and can have a maximum of five digits. The default value is 2011.
	Note
	If multiple Panels are in use, there must be a unique Alarm port number. If not an error message is displayed.
Remote Key	Enter the Remote Key.
Command Port Encryption	Select the check box to enable the encryption in the command channel.
	This field is enabled only for XR500E and XR550E Panel type.
Alarm Port Encryption	Select the check box to enable the alarm channel encryption.
	This field is enabled only for XR500E and XR550E Panel type.
Passphrase	Enter the Pass Phrase.
	Passphrase is the password used to enable encrypted notification from Panel and provide a secure means for data communications.
	Passphrase must have 8 characters with alphanumeric value.
	This field is enabled only for XR500E and XR550E Panel type.
Encryption Type	Select a type of encryption from the Encryption Type drop-down.
	Supported encryption types are: 128 and 256.
	Note
	Only XR550E Panel supports 128 and 256 type of encryption.

4   Click **Panel Information** to view the following:

Note

The Panel information is displayed after the Panel is synchronized:

Property	Description
Firmware Version	This field is read-only.
	Displays the firmware version of the Panel.
Last Synchronization Time	This field is read-only.
	Displays the date and time the Panel was last synchronized.

MAC Address	This field is read-only.
	Displays the MAC address of the Panel.
Serial Number	This field is read-only.
	Displays the Serial number of the Panel.
Version Date	This field is read-only.
	Displays the date of the application firmware version.

5   Click **Panel Status** to view the following:

Expander	**Information**
Command Channel Status	The options available are: • Online • Offline • Disabled • Unknown
Synchronization Status	The options available are: • Unknown • Synchronizing • Synchronized • Synchronization Failed • Start Synchronization

6   Click **Associations:**

    a   Click to open the **Object Selector**.

    b   From the **Type** list in the **Object Selector**, select an object to associate it with the DMP Panel.

    c   Click **OK**.

7   Click **Save**.

What to do Next

• Synchronize the configured DMP Panel. See .

- End -

Editing DMP Panels

Procedure 5-10 Editing DMP Panels

Use the DMP Panel editor to configure server connection details in victor.

Step	Action
1	In the **Intrusion** group, click on the **Edit** icon and then click the **DMP Panel**. A **DMP Panels** opens and all available DMP Panels are listed.
2	Right-click the Panel that you want to edit and click **Edit.** A new tab opens.
3	Click **General** and edit the required information. For more information, see step 2 of Procedure 5-9.
4	Click **Panel Configuration** and edit the required information. For more information, see step 3 of Procedure 5-9.
5	(Optional) Click **Panel Information** to view the information about the Panel. For more information, see step 4 of Procedure 5-9.
6	(Optional) Click **Panel Status** to view the status of the Panel. For more information, see step 5 of Procedure 5-9.
7	Click **Associations.** Use the Object Selector to associate other hardware devices with the DMP Panel. For more information, see step 6 of Procedure 5-9.
8	Click **Save**.

- End -

Administration

Viewing and Editing DMP Partitions

You cannot create partitions directly from victor. Depending on your victor role assignment, you can view and edit partitions from the Intrusion ribbon.

Procedure 5-11 Viewing and Editing DMP Partitions

Step	Action
1	In the **Intrusion** group, click on the **Show All** icon and click the **DMP Partitions.** The **DMP Partitions** tab opens and all available **DMP Partitions** appear. A new tab opens.
2	Right-click the Partition that you want to modify and click **Edit.**
3	Click **General.** Add the following details in the expanded list:

Property	Description
Name	You can modify the name of the Partition. The name can have up to 100 characters. **Note** Ensure that the name is unique, else an error message is displayed.
Description	You can modify the description for the Partition. The description can have up to 500 characters.
Enabled	Select the **Enabled** check box to establish the communication between victor and the partition. By default, the **Enabled** check box is selected. If you clear the check box, the communication between victor and the partition is disabled.

4	Click **Partition Information.** Add the following details in the expanded list:

Property	Value
Partition Number	Displays the partition number. The partition number is used to uniquely identify a Partition. The partition number is assigned as configured in the Panel when the Panel is synchronized. This field is read-only.
Account Number	Displays the account number of the Panel. The account number is assigned as configured in the Panel when the Panel is synchronized. This field is read-only.

5 Click **Partition Zone Mapping** to view the following:

Property	Description
Zone Name	Displays the name of the Zone that is mapped to the Partition. Zone name is assigned as configured in the Panel when the Panel is synchronized. This field is read-only.
Zone Number	Displays the zone number that is mapped to the Partition. Zone number is assigned as configured in the Panel when the Panel is synchronized. This field is read-only.
Zone Type	Displays the zone type that is mapped to the Partition. Zone type is assigned as configured in the Panel when the Panel is synchronized. This field is read-only.
Board	Displays the Interface board to which this zone is connected. Board is assigned as configured in the Panel when the Panel is synchronized. This field is read-only.

6 Click **Partition Status** to view the following:

Property	Description
Armed Status	The options available are: • Armed • Disarmed
Late Status	The options available are: • No Abnormal Condition • Late to Close
Schedule Status	The options available are: • In Schedule • Not In Schedule

7 Click **Associations:**

a Click to open the **Object Selector**.

b From the **Type** list in the **Object Selector**, select an object to associate it with the DMP Partition.

c Click **OK**.

8 Click **Save**.

- End -

Viewing and Editing DMP Zones

You cannot create Zones directly from victor. Depending on your victor role assignment, you can view and edit Zones from the Intrusion ribbon.

Procedure 5-12 Viewing and Editing Zones

Step	Action

1   In the **Intrusion** group, click on the **Show All** icon and then click the **DMP Zones**.

The **DMP Zone** tab opens and all available DMP Zones appear.

2   Right-click the Zone that you want to edit and click **Edit**.

A new tab opens.

3   Click **General**. Add the following details in the expanded list:

Property	Description
Name	You can modify the name of the Zone. The name must be unique and can have up to 100 characters. **Note**: If the name is not unique, an error message is displayed.
Description	You can modify the description for the Zone.
Enable	Select the **Enabled** check box to establish the communication between victor and the Zone. By default, the **Enabled** check box is selected. If you clear the check box, you cannot perform the manual actions on the Zones and status updates are not reported.

4   Click **Zone Information** to view the following:

Property	Value
Zone Number	Zone number is used to uniquely identify a Zone. It is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Zone Type	Displays the type of the Zone. Zone type is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Board	Displays the interface board to which the Zone is connected. Board is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.

Send State Changes to Activity Viewer	Select the check box to send the state change message to the Activity Viewer.
	After you select this check box, **Send State Changes to Journal** check box is selected automatically.
Send State Changes to Journal	Select this check box to journal the state changes.

5   Click **Zone Status** to view the following:

Property	Value
Active Status	The options available are:
	• Active
	• Inactive
Hardware Status	The options available are:
	• Open
	• Short
	• Inactive
	• Active
Supervision Status	The options available are:
	• Normal
	• Open
	• Bypassed
	• Short
	• Low Battery
	• Missing
	• Trouble
	• Uninitialized

6   Click **Associations:**

a   Click ⊕ to open the **Object Selector**.

b   From the **Type** list in the **Object Selector**, select an object to associate it with the DMP Zone.

c   Click **OK**.

7   Click **Save**.

- End -

View and Edit DMP Outputs

You cannot create Outputs directly from victor. Depending on your victor role assignment, you can view and edit Outputs from the Intrusion ribbon.

Procedure 5-13 Viewing and Editing DMP Outputs

Step	Action

1   In the **Intrusion** group, click on the **Show All** icon and then click the **DMP Output**.

The **DMP Outputs** tab opens and all available DMP Outputs appear.

2   Right-click the Output that you want to modify and click **Edit**.

A new tab opens.

3   Click **General** to modify the following:

Property	Description
Name	You can modify the name of the Output. The name must be unique and can have up to 100 characters. **Note**: If the name is not unique an error message is displayed.
Description	You can modify the description for the Output. The description can have up to 100 characters.
Enabled	Select the **Enabled** check box to establish the communication between victor and the output. By default, the **Enable** check box is selected. If you clear the check box, you cannot perform manual actions.

4   Click **Output Information** to view the following:

Property	Value
Output Number	Output Number is used to uniquely identify an Output. It is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Output Type	Displays the type of the output. Output type is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Board	Displays the interface board to which this output is connected. Board is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Send State Changes to Activity Viewer	Select the check box to send the state change message to the Activity Viewer. After you select this check box, the **Send State Changes to Journal** check box is selected automatically.
Send State Changes to Journal	Select the check box to journal the state changes.

5   Click **Status** to view if the Output is active or inactive.

6   Click **Associations:**

   a   Click to open the **Object Selector**.

   b   From the **Type** list in the **Object Selector**, select an object to associate it with the DMP Partition.

   c   Click **OK**.

7   Click **Save**.

- End -

Viewing and Editing DMP Secondary Devices

You cannot create secondary devices directly from victor. Depending on your victor role assignment, you can view and edit secondary devices from the Intrusion ribbon.

Procedure 5-14 Viewing and Editing DMP Secondary Devices

Step	Action

1   In the **Intrusion** group, click on the **Show All** icon and then click the **DMP Secondary Device**.

A **DMP Secondary Devices** tab opens and all available secondary devices appear.

2   Right-click the secondary device that you want to modify and click **Edit.**

A new tab opens.

3   Click **General** to modify the following:

Property	Description
Name	You can modify the name of the secondary devices. The name must be unique and can have up to 100 characters. **Note**: If the name is not unique an error message is displayed.
Description	You can modify the description for the secondary devices. The description can have up to 100 characters.
Enabled	Select the **Enabled** check box to establish the communication between victor and the secondary device.

4   Click **Secondary Device Information** to view the following:

Property	Value
Device Number	Device Number is use to uniquely identify secondary devices. It is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Device Type	Displays the type of device. It is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.

5 Click **Secondary Devices Zones** to view the Zone information:

Property	Value
Zone Name	Displays the name of the zone that is associated with the secondary device. Zone name is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Zone Number	Displays the zone number that is associated with the secondary device. Zone number is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Zone Type	Displays the type of Zone that is associated with the secondary device. Zone type is assigned as configured in Panel when Panel synchronization is performed. This field is read-only.
Board	Displays the interface board to which this output is connected. Assigned as configured in Panel when Panel synchronization is performed. This field is read-only.

6 Click **Secondary Devices Output** to view the output information:

Property	Value
Output Name	Displays the name of the output that is associated with the secondary device.
Output Number	Displays the output number that is associated with the secondary device.
Output Type	Displays the type of the output that is associated with the secondary device.
Board	Displays the interface board to which this output is connected. It is assigned as configured in Panel when Panel synchronization is performed This field is read-only.

7 Click **Associations:**

    a Click to open the **Object Selector**.

    b From the **Type** list in the **Object Selector**, select an object.

    c Click **OK**.

8 Click **Save**.

- End -

American Dynamics

Viewing and Editing DMP User Profiles

You cannot create profiles directly from victor. Depending on your victor role assignment, you can view and edit profiles from the Intrusion ribbon.

Procedure 5-15 Viewing DMP User Profiles

Step	Action

1   In the **Intrusion** group, click the **Show All Item** button.

2   Select **DMP Profile**.

A list of available user profiles displays.

Procedure 5-16 Editing DMP User Profiles

Step	Action

1   In the **Intrusion** group, click the **Edit Existing Item** button.

2   Select **DMP Profile**.

A list of available user profiles displays.

3   Right-click on the **User Profile** to edit and select **Edit**.

4   Expand the **General** section to make the changes to the profile name and description.

Note

All controls except for **Name** and **Description** are read-only and cannot be modified.

Field	Description
Name	The Name of the DMP Profile. The name should be unique and can be up to 100 characters long. **Note** Ensure that the name is unique, otherwise an error message is displayed.

Description	The description for the profiles. The description can be up to 100 characters long.
Enabled	This check box must be selected to apply the configuration.

5 Expand the **User Profile information** section to view the user profile details.

Note

All controls except for **Name** and **Description** are read-only and cannot be modified.

Field	Description
Controller	Displays the name of the Controller.
Profile Number	Each profile is assigned with a unique number from 1 to 99.
Re-arm Delay	Allows the entry of 0 to 250 minutes to be used to delay automatic re-arming when the user disarms an area outside of the schedule. If zero is selected, the re-arming occurs based on permanent programming in the controller.

Re-arm Delay is also used to delay a late-to-close message to the Central Station when the Controller does not use automatic arming. |
| **Permission** | |
| Arm/Disarm | All areas are listed. The Armed areas are selected. |

6   Click the **Menu** option tab to view user profile options.

Note

All check boxes except for Name and Description are read-only and cannot be modified.

7   Click the **Shifts** tab to view read-only status information about the DMP User Profile.

Note

All fields except for Name and Description are read-only and cannot be modified.

8   Click the **Personnel** tab to view all DMP users that belong to the particular user profile. If the user is linked to Personnel, then the corresponding DMP User-Personnel mapping is shown.

Note

All fields except for Name and Description are read-only and cannot be modified.

- End -

Viewing and Editing DMP Users

You cannot create a user directly from victor. Depending on your victor role assignment, you can view and edit profiles from the Intrusion ribbon.

Procedure 5-17 Viewing DMP Users

Step	Action

1   Click on **Show All Item** button and navigate to the **Intrusion** group.

2   Select **DMP User**.

A list of available users displays.

Procedure 5-18 Editing DMP Users

Step	Action

1   Click on **Edit Existing Item** button and navigate to the **Intrusion** group.

2   Select **DMP User**.

A list of available users displays.

3 Right-click on the **DMP User** to edit and select **Edit**.

4 Expand the **General** section to make the changes to the profile name and description.

Field	Description
Name	Used to modify the name of the DMP Profiles. The name can be up to 100 characters long. **Note** Ensure that the name is unique, otherwise an error message is displayed.
Description	Used to modify the description for the profiles. The description can be up to 100 characters long.

5 Expand the **DMP User information** section to view the details.

Field	Description
User Info	

User Number	Each User has a number. The numbered is 1 through 9999. This number identifies the user to the system and is transmitted to the Central Station when the user arms or disarms ares.
Temp Date	When Temp Code is enabled for a user, the Temp Expire Date/Temp Date becomes unavailable. This is the date the profile expires.
Personnel	The personnel name linked to the DMP User.

6   Click the **User Profile Name** tab.

Field	Description
Name	Displays the name of the DMP User.
Description	A general description of the DMP User.
User Identification	
First User Profile name	Displays the name of the First User Profile name assigned to the DMP User.
Second User Profile name	Displays the name of the Second User Profile name assigned to the DMP User.
Third User Profile name	Displays the name of the Third User Profile name assigned to the DMP User.
Fourth User Profile name	Displays the name of the Fourth User Profile name assigned to the DMP User.

Configuring DMP Actions

You can schedule actions for the following DMP objects:

- DMP Panel
- DMP Partition
- DMP Zone
- DMP Outputs

Procedure 5-19 Configuring a DMP Action

Step	Action

1   Click on the **New** icon in the **Intrusion** group, and click the **DMP Actions**.

         The **New DMP Action** tab opens.

2   Click **General**. Enter a name (mandatory) and description (optional) in respective fields.

3   Click **Action.**

      a   Click ⊕ , the Object Selector opens.

      b   Select an object from the **Type** List, select an action from the **Name** list and click **OK**.

         Repeat as required.

4   Select the same type of object in the Device field.

5   Select the desired action from the **Device Action** drop-down list.

> **Note**
>
> If you want to remove a Device, select the check box of the device to be removed and click ⊗ .

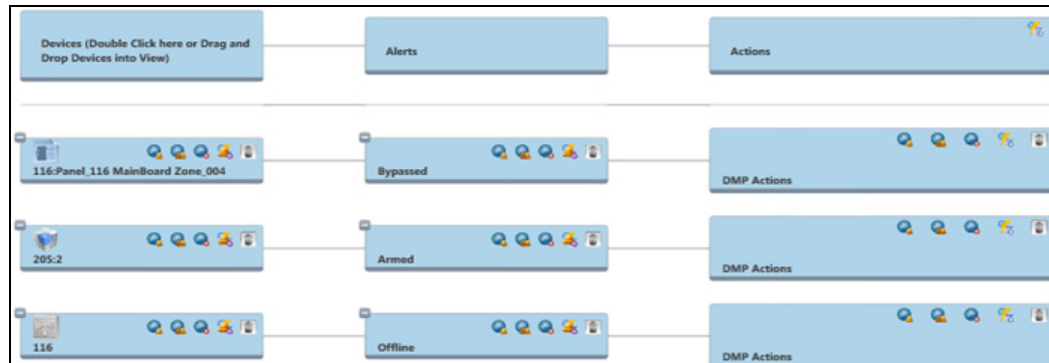**6**   Click **Save and Close**.

- End -

American Dynamics

35

Configuring DMP Alerts

Use the **Event Setup** editor to configure alerts.

The **Events/Schedule** setup editor provides a dynamic, visual method of linking Devices, Alerts and Actions.
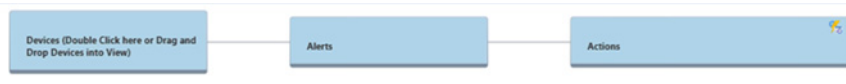Refer to *victor unified Client User Manual* to configure Alerts.

Refer to [Alert Types](#) on page 49 for a full list of victor support alert types.

Configuring Schedule Actions for DMP

Procedure 5-20 .Configuring Schedule Actions for DMP

Step	Action
1	Select **Event/Schedule Setup** from the **Build** tab.
2	Double-click the Device node and use the object selector and select type as **Schedules.**

Step	Action
3	Select the required schedule from the list.

Note

You should have created the schedule to select it. Refer to the v*ictor Unified Client User Manual* for more information on Creating Schedule.

Step	Action
4	Selected Schedule is displayed in the Device node.
5	Select [icon] 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 [icon] in the **Alerts** node to add actions.
9	Select **DMP Action** from the object selector. You should have created DMP Action to select it. See [Panel Synchronization](#) on page 40.

10   Repeat as required.

11   Click **Save and Close**.

- End -

Operation
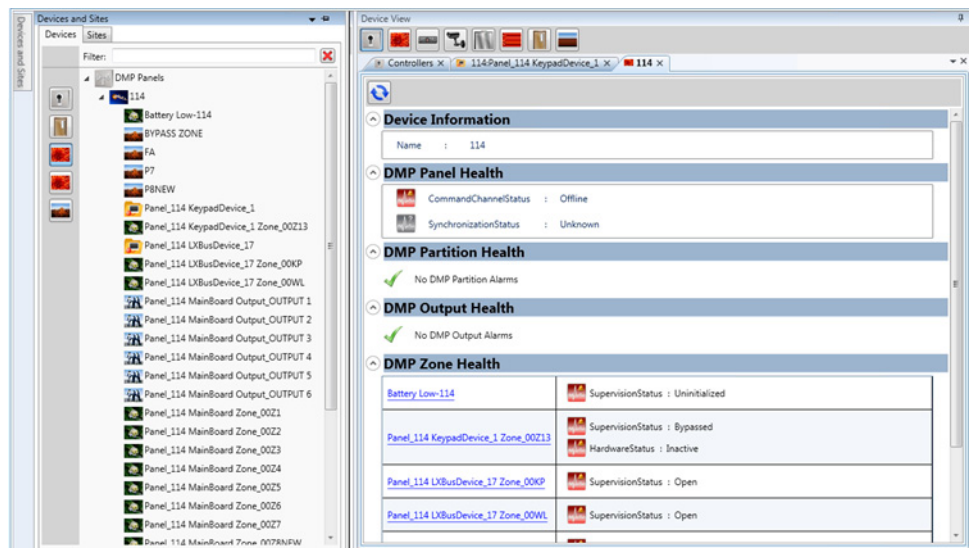
Health Dashboard

Health status of all DMP objects is displayed in the Health Dashboard.
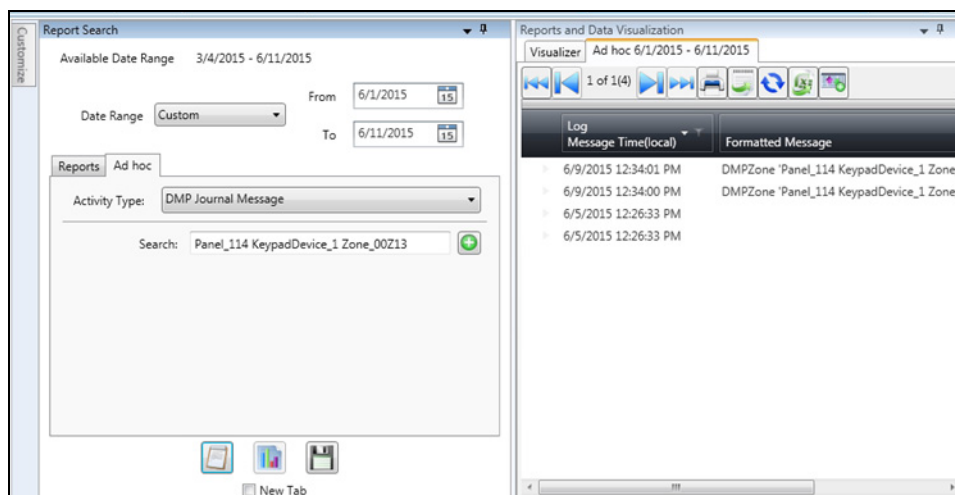

Refer to [Appendix B:](#)on page 51 for a full list of supported health statuses.

Reports

Use the victor journaling type, DMP Journal Message to search for reports related to DMP, as shown in the following figure

Figure 6-1 victor unified client DMP Integration Reports

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

Dynamic Views

All configured DMP Panels, Zones, Partition, Outputs and Secondary devices can display in **Dynamic Views** tab. You can perform manual actions on configured objects.

Manual Actions

You can perform the following manual actions from the victor client:

Panel Synchronization

You can Synchronize DMP Panels directly from the victor device list. For more information about accessing the Device List, refer to the *victor Unified Client Operation Guide.*

Before you synchronize the DMP Panel, ensure the following:

• The DMP Driver is up and running.

• The Panel is online.

• The communication status of the Command channel is online.

Procedure 6-1 .Synchronizing the DMP Panel

Step	Action
1	Open the **Device List**.
2	Expand the **DMP Panel** object type.
3	Right-click the Panel that you want to synchronize and select **Synchronize from Panel**
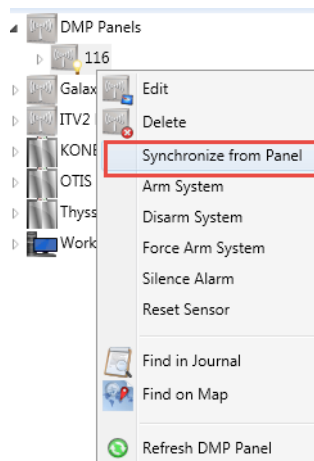
4 Verify the status of the Panel in the **Activity Viewer**.
The status of the Panel changes from **Start Synchronization**, then to **Synchronizing,**
and then to **Synchronized**.

NOTE	The context menu is visible if the associated DMP Panel is online.

Troubleshooting Tips

• If the synchronization has stopped or failed:

  • Ensure that the DMP Panel has been configured in accordance with Changing
  Configuration Settings. You must perform these configuration steps exactly as
  instructed, else the DMP Panel will fail to synchronize reliably. You can use the
  DMP keypad or the DMP Remote Link software application to configure the
  DMP Panel.

  • From the server, perform a continuous PING to the DMP Panel and ensure that
  it consistently replies successfully to each PING.

  • When a new Panel is installed, run the initialization function –Com/RMT. This
  will initialize all configurations in Communication and Remote options in the
 Panel. Then, reconfigure these sections to bring the Panel online. See DMP

American Dynamics

Panel Configuration using DMP Keypad on page 9 to reconfigure Communication and Remote options in the Panel.

- • If multiple communication paths are configured, validate if victor is configured as the primary path. For victor to function properly with the DMP integration, you must configure victor as the primary path.

- • If synchronization occurs immediately after configuration and modification of Panel, it may fail.Panels may take time to initialize and stabilize communication with Unified Server. Try re-synchronization after communication is stable.

Arming and Disarming the DMP Panel

Procedure 6-2 Arming the DMP Panel

Step	Action

1	Open the **Device List**.
2	Expand the **DMP Panel** object type.
3	Right-click the Panel you want to arm and select **Arm System.**
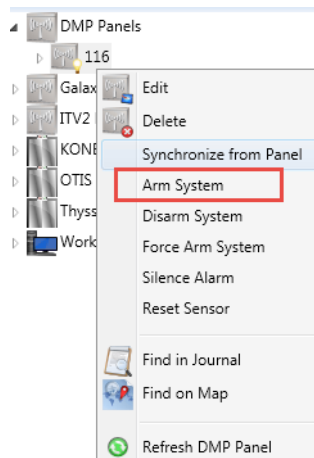
| **4** | Verify the status of the partition in the Panel. |

The status changes to Armed.

- End -

Procedure 6-3 Disarming the DMP Panel

Step	Action

| **1** | Open the **Device List** tab. |

The device list displays.

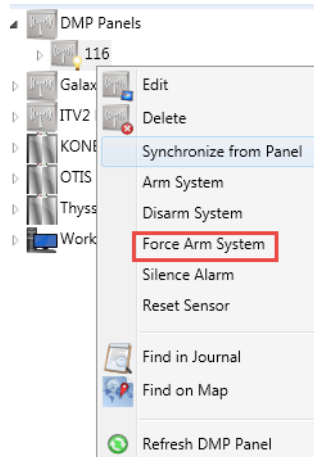| **2** | Expand the DMP Panel object type. |
| **3** | Right-click the Panel that you want to disarm. |

4   Select **Disarm System.**

5   Verify the status of the partition in the Panel.

The status changes to Disarmed.

NOTE	The context menu is visible if the associated DMP Panel is online.

Force Arm the Partition in the Panel

Procedure 6-4 Force Arming the Partition in the Panel

Step	Action

1   Open the **Device List** tab.

The device list displays.

2   Expand the DMP Panel object type.

3   Right-click the Panel you want to Force Arm.

4   Select **Force Arm System**.

5   Verify the status of the partition in the Panel.

The status is changed to Armed.

| NOTE	The context menu is visible if the associated DMP Panel is online.

Silence Alarm

Use the **Silence Alarm** option to silence the alarm bell or siren.

Procedure 6-5 Silencing an Alarm

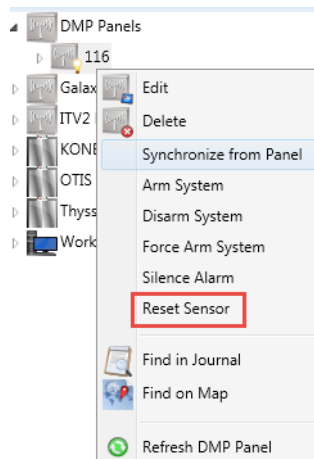| Step	Action
1	Open the **Device List** tab.
	The device list displays.
2	Expand the DMP Panel object type.
3	Right-click the Panel whose alarm you want to silence.
4	Select **Silence Alarm**.
	The alarm bell or siren is silenced.
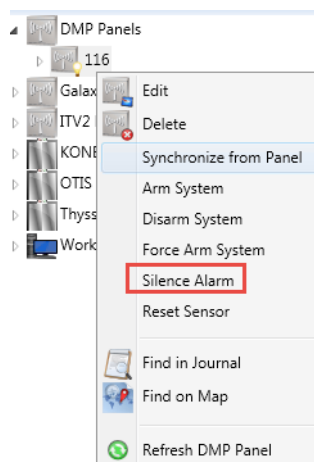
Reset Sensor

Use the **Reset Sensor** option to reset the sensor that has latched due to an alarm condition, for example, smoke or glass break detectors.

Procedure 6-6 Reseting the Sensor

Step	Action
1	Open the **Device List** tab.
	The device list is displayed.
2	Expand the DMP Panel object type.
3	Right-click the Panel whose sensor you want to reset.
4	Select **Reset Sensor.**
	The sensor is reset.

- End -

Bypass and Reseting Zones

You can bypass and reset zones directly from the victor device list.

Procedure 6-7 Bypassing a Zone

Step	Action

1   Open the **Device List** tab.

The device list is displayed.

2   Expand the **DMP Panel** object type.

3   Expand the **DMP Panel**.

4   Expand the **DMP Zone** folder.

5   Right-click the DMP Zone that you want to bypass.

6   Click **Bypass**.

The status of the DMP Zone changes to Bypassed.

- End -

Procedure 6-8 Reseting a Zone

Step	Action

1   Open the **Device List** tab.

The device list is displayed.

2   Expand the **DMP Panel** object type.

3   Expand the **DMP Panel**.

American Dynamics

4   Expand the **DMP Zone** folder.

5   Right-click the DMP Zone that you want to reset.

6   Click **Reset.**

The status of the zone changes to **Normal**.

NOTE	• The context menu is visible if the associated DMP Panel is online.
	• You can bypass the 24 Hrs Zones from the victor application. DMP 'Remote Link' application supports this operation. This operation is not supported from the DMP keypad hardware.
	• You can bypass the Zones assigned to Armed Partition from the victor application. DMP 'Remote Link' application supports this operation. This operation is not supported from the DMP keypad hardware.

- End -

Activate and Deactivate Outputs

You can activate and deactivate outputs directly from the victor device list.

Procedure 6-9 Activating and Deactivating Outputs

Step	Action

1   Open the **Device List** tab.

The device list is displayed.

2   Expand the **DMP Panel** object type.

3   Expand the **DMP Panel**.

4   Expand the **DMP Outputs** folder.

5   Right-click the **Panel** whose output you want to change.

- To activate the output select **Active**.

- To deactivate the output, select **Inactive.**

- To trigger a continuous pulse, select **Continuous Pulse.**

- To trigger a momentary output, select **Momentary Output.**
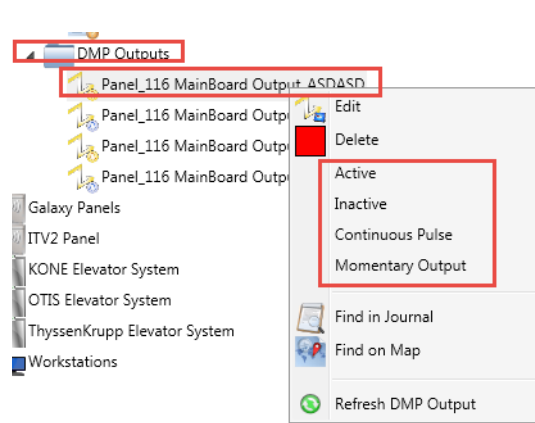
| **NOTE** | The context menu is only visible if the associated DMP Panel is online. |

Appendix A: Alert Types

The Event Configuration editor is used to configure alerts for DMP objects. The following tables detail the **Alert Types** supported for DMP Objects in victor.

Table 7-1 Alert Types for DMP Panels

Panel Alert Type	Options Available
Command Channel Status	• Online • Offline • Disabled
Synchronization Status	• Start Synchronization • Synchronizing • Synchronized • Synchronization Failed
Armed Status	• Armed System • Disarmed System • Partially Armed System

Table 7-2 Alert Types for DMP Partitions

Partition Alert Type	Value
Armed State	• Armed • Disarmed • Forced Arm
Late Status	• No Abnormal Condition • Late to Close
Schedule Status	• In Schedule • Not In Schedule

Table 7-3 Alert Types for DMP Zones

Zone Alert Type	Value
Supervision Status	• Normal • Open • Short • Bypassed • Low Battery • Missing • Trouble • Uninitialized
Active Status	• Active • Inactive
Hardware Status	• Active • Inactive • Short • Open

NOTE   victor alerts for DMP Zones will work only if the **Send State Changes to Journal** check box is selected in the DMP Zone editor.

Appendix B: Health Status

Supported Health status depictions for DMP object type are as follows

Table 8-1 Health status for DMP Panels

Property	Panel Status	Health Status
Command Channel Status	Online	Normal
	Off-line	Device Alert
	Disabled/Unknown	Unknown
Synchronization status	Start Synchronizing	Normal
	Synchronizing	Normal
	Synchronizing failed	Device Alert
	Synchronized	Normal
Panel Status	Battery Low	Device Alert
	Tamper	Device Alert
	Power Fail	At Risk
	Alert	Device Alert
	Alarm	Device Alert
	Trouble	At Risk

Table 8-2 Health status for DMP Partitions

Property	Partition Status	Health Status
Armed status	Armed System	Normal
	Disarmed System	
	Forced Alarmed System	
	Partially Armed System	
Late Status	No Abnormal Condition	Normal
	Late to Close	Device Alert

Table 8-3 Health status for DMP Zones

Property	Zone Status	Value
Active Status	• Inactive	Normal
	• Active	Normal
Input HW Status	• Open	Device Alert
	• Short	Device Alert
	• Inactive	Normal
	• Active	At Risk
Supervision Status	• Normal	Green/NORMAL
	• Open	Device Alert
	• Short	Device Alert
	• Low Battery	Device Alert
	• Trouble	At Risk
	• Missing	Device Alert

Table 8-4 Health status for DMP Outputs

Property	Output Status	Value
Active Status	• Active	Normal
	• Inactive	
	• Pulsed	