

Release Notes for victor v5.2 DMP Intrusion Integration v3.60.43.0

Document Version A0
March 2018

This document provides important information about the integration software for the victor DMP Intrusion Integration. Read this document before installing the product.

Product: Unified DMP Intrusion Integration

- Integration Software Version: 3.60.43.0

This driver release is qualified with victor when installed on:

- victor Unified Systems v3.60 (C•CURE v2.61 and victor v5.0), or
- victor Unified Systems v3.65 (C•CURE v2.61 and victor v5.1), or
- victor Unified Systems v3.70 (C•CURE v2.70 and victor v5.2).

Contents

1. [Overview](#)
2. [Qualified Hardware and Firmware](#)
3. [Software Requirements](#)
4. [Contents of the Installation Package](#)
5. [Supported Installation Types](#)
6. [Pre-Installation](#)
7. [Installation](#)
8. [Post-Installation](#)
9. [Upgrading the DMP Integration](#)
10. [Scalability](#)
11. [Language Support](#)
12. [Compatibility Matrix](#)
13. [Known Issues and Limitations](#)
14. [Defects Fixed](#)
15. [End of Release Notes](#)

1. Overview

The victor platform provides seamless integration with the DMP Intrusion Security System, allowing customers to monitor their important intrusion system devices from victor. The software also monitors: the Intrusion Panel status, Arming or Disarming Partitions, Activating or De-activating Outputs and Bypass or Reset Zones.

2. Qualified Hardware and Firmware

The victor DMP Intrusion Integration supports the following hardware and firmware:

Table 1: DMP Intrusion Hardware and Firmware

| DMP Panel Model | DMP Panel Firmware |
|-------------------------|--------------------|
| XR500N | V206, V208, V212 |
| Canadian Version XR500N | V208, V206, V212 |
| XR500E | V212, V208 |
| XR100N | V206,V208, V212 |
| XR150N | V110, V171 |
| XR550N | V111 |
| XR550E | V111, V171 |

3. Software Requirements

The DMP Intrusion Integration requires the following software versions:

- victor Unified Client: v5.0/v5.1/v5.2.

4. Contents of the Installation Package

The table below lists the contents of the DMP Intrusion Integration installation package:

Table 2: DMP Installation Package

| File | Description |
|--|--|
| Unified_DMP-Integration.exe | DMP Unified Integration software setup file |
| victor-v5-2-dmp-integration_um_ra0_lt_en.pdf | Unified victor Integration Software for DMP Intrusion User Guide |
| victor-v5-2-dmp-integration_rn_ra0_lt_en.pdf | Release Notes for Unified DMP Intrusion Integration |

5. Supported Installation Types

Following installation types are supported for victor DMP Intrusion Integration:

- Unified Standalone
- victor Standalone
- Unified Enterprise
- victor Enterprise

6. Pre-Installation

Prerequisites to install DMP Intrusion Integration on the victor Application Server:

- You must be a member of the local Administrators group or have equivalent privileges.
- victor Application Server must be installed and licensed with the DMP Integration.

Prerequisites to install DMP Intrusion Integration on the clients:

- You must be a member of the local Administrators group or have equivalent privileges.
- You must install victor client.

7. Installation

Note: Ensure you stop all applications to avoid problems during installation.

Run the **Unified_DMP-Integration.exe** to install the DMP Integration on the victor Application Server or remote client.

For detailed instructions about installing the DMP Intrusion Integration, see the *victor unified client DMP Integration User Manual*.

Note: You cannot install the DMP Integration server components on a victor Application Server MAS.

8. Post Installation

Perform the following steps after installation:

1. Launch the **Server Configuration Application**:
 - a. On the taskbar, click the **Start** button and then click **All Programs**.
 - b. Click **Tyco**, right-click the **Server Configuration** and then click **Run as Administrator**. **Server Configuration Application** page opens.
2. Start **DMP Services**:
 - a. On the **Server Configuration Application** page, click the **Services** tab.

- b. Ensure that both Crossfire Framework Service and Crossfire Server Component Framework Service are **running**.
 - c. In the **Extension Services** area, locate the **DMP Driver Service**. Select the **Enabled** check box and then click the Start button. The status of the DMP Driver Service changes to **Running**.
3. Launch the victor client:
 - a. On the taskbar, click the **Start** button and then click **All Programs**.
 - b. Click **victor**.

9. Upgrading the DMP Integration

Caution:

If you have made any changes in the configuration file - DMPDriverService.exe, ensure you back up the file before upgrading. The configuration file is located at Tyco\CrossFire\ServerComponents.

Follow the steps to upgrade the DMP Integration:

- Upgrade victor v4.8 SP1/v4.8.1/v4.9 to victor v5.2, and then install the DMP Integration.
- Upgrade victor v4.9.1 to victor v5.2, and then install the DMP Integration.
- Upgrade victor v5.0/v5.1 to victor v5.2, and then install the DMP Integration.

10. Scalability

This driver supports 150 panels per server.

11. Language Support

This driver supports the English (US) language.

12. Compatibility Matrix

The table below lists the Compatibility Matrix of DMP Intrusion Integration:

| Table 3: DMP Compatibility Matrix | |
|-------------------------------------|--|
| victor versions v5.0, v5.1 and v5.2 | |
| Partner | DMP |
| Partner Product | Canadian XR500N, XR500N, XR500E, XR100N, XR150N, XR550N and XR550E |
| Partner Product version | Firmware -206, 208, 212, 110, 111, 171 |
| Integration driver version | 3.60.43.0 |
| victor License option | ADVC-DMP |
| Enterprise certified | Yes |
| Redundancy certified | Yes (everRun MX) |
| Supported Server OS | All OS supported by victor Server |
| Supported Client OS | All OS supported by victor Client |
| Supported SQL | All SQL Server supported by victor |

13. Known Issues and Limitations

This section describes the DMP Intrusion known limitations.

- The following features are not supported in this release:
 - DMP Partition Trigger for Forced Arm
 - Key fob zones
 - Migration of a standalone machine with a DMP Driver to SAS
 - Journaling of system activity messages
 - The DMP Main Board Device objects
 - Non-supervised Zones, and Zone Groups that have non-supervised zones are listed in Events (Bypass Zone, Reset Zone Actions).
- When the DMP Partition is disarmed, the DMP Zone that was in a bypassed state displays the supervision status as **Bypass** instead of **Open**. This is due to panel limitations.
- DMP panels comes online irrespective of Panel Type selected in the DMP Controller Configuration window.
- DMP output status is not reported by the panel. Output status is only updated during synchronization.
- Messages for activities performed during the offline state of a panel are reported with the current Timestamp.
- DMP Hardware with the Canadian version does not support remote Arm.
- Occasionally, multiple device activity messages are logged in the victor Activity Viewer.
- To upgrade the driver to the current version, you must use the User Account that was used to install the earlier version of DMP Integration.
- First time configuration of a “Blank” type zone shows as “Unknown” for Hardware, Supervision and Active State.
- After disarming an armed Partition, the status of the associated bad state zones continue to display as 'Bypassed'.
- Partition schedule status is only updated after synchronization. Since the panel does not notify the schedule status changes through the Alarm Channel, partition schedule status changes are not reported.
 - **Workaround:** Use the Reset option to manually reset the associated bad zones in victor.
- After upgrading to the current driver, the DMP panel should be synchronized again for DMP user and DMP Profile.

14. Defects Fixed

The table below lists the defects fixed in this version of the software:

Table 4: General Fixes

| Category | SPAR Number | SPAR Description |
|------------|-------------|--|
| DMP Driver | 515588 | Resolved an issue of installation failure occurring in DMP driver 3.60.33.0. |

15. End of Release Notes

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.

© 2018 Tyco Security Products.
All rights reserved.