ADPRO® Video Central Platinum

Product Release Notes V3.06.00

March 2022
Doc. 29578_05

Honeywell

Disclaimer

The contents of this document are provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

This document includes registered and unregistered trademarks. All trademarks displayed are the trademarks of their respective owners. Your use of this document does not constitute or create a license or any other right to use the name and/or trademark and/or label. This document is subject to copyright owned by Xtralis. You agree not to copy, communicate to the public, adapt, distribute, transfer, sell, modify, or publish any contents of this document without the express prior written consent of Xtralis.

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Xtralis. All proper health and safety precautions must be taken during the installation, commissioning, and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Xtralis is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Xtralis accredited training course can install, test and maintain the system.

Liability

You agree to install, configure, and use the products strictly in accordance with the User Manual and product documents available from Xtralis.

Xtralis is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits, or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation, or advice given by or on behalf of Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis in relation to the products is limited to:
(i) in the case of services, the cost of having the services supplied again; or
(ii) in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Xtralis harmless for any claim, cost, demand, or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

Trade Name Statement

ADPRO, Xchange, FastTrace, iFT, eFT, iFT-E, iFT Gateway, IntrusionTrace, LoiterTrace, XO, iTrace, iCommand, iCommission, iPIR, and FMST are trademarks and/or registered trademarks of Honeywell and/or its subsidiaries in the United States and/or other countries. Other brand names mentioned herein are for identification purposes only and may be trademarks of their respective holder(s). Your use of this document does not constitute or create a licence or any other right to use the name and/or trademark and/or label.

Document Conventions

The following typographic conventions are used in this document.

Convention	Description
Bold	Used to denote: emphasis Used for names of menus, menu options, toolbar buttons
Italics	Used to denote: references to other parts of this document or other documents. Used for the result of an action

The following icons are used in this document.

Icon	Description
	Note. This icon indicates information of special interest that will help the reader make full use of the product, optimise performance, etc. Failure to read the note will not result in physical harm to the reader, or damage to equipment or data.
	Caution! This icon indicates danger to equipment. The danger can be loss of data, physical damage to the equipment, or permanent corruption of configuration details.
	Warning! This icon indicates danger of physical harm to the reader. Not following instructions may lead to death or permanent injury.
	Warning! This icon indicates danger of electric shock. This may lead to death or permanent injury.
	Warning! This icon indicates that there is a danger of inhaling dangerous substances. This may lead to death or permanent injury.

https://www.security.honeywell.com

Contents

1 Product Release 5

2 New Features and Enhancements 6

2.1 User Interface 6
2.2 Events and Alarms 6
2.3 Site Overview 6
2.4 Configuration 6
2.5 Database 7
2.6 Data Conversion 8
2.7 Secure Viewer 8
2.8 General 8
2.9 Video Wall 8
2.10 P2P Support 8
2.11 Secure streaming 9
2.12 Upgrade to SQL Server 2019 9

3 Removed Features 10

4 Known Issues and Limitations 11

4.1 Known Issues 11

5 Software and Hardware Requirements 12

5.1 Client User Interface PC 12
5.2 Server/Database PC 12
5.3 Hard Drive Specification Guidelines 13
5.4 Video Wall PC 13
5.5 Peripherals 13
5.6 System Specifications 14
5.7 Data Compatibility 14

1 Product Release

These release notes list the changes for the Video Central Platinum software from version C3.05 to version V3.06.03.02.

Furthermore, this document contains a list of known issues and workarounds (if available), and information on limitations of the software.

Finally, this document lists all system requirements for hardware and software, and compatibility requirements.

2 New Features and Enhancements

2.1 User Interface

- Added the polish language.
- The camera I/O status page has been redesigned, allowing to isolate individual camera points.
- Improved error notification in case archiving fails due to insufficient disk space.
- In VCP UI Live Mode, if an audio error occurs, an error message is displayed, and now the user is prompted to restart the unit's audio server.

2.2 Events and Alarms

- Added support for the new NetIO digital tamper events that are available on XO 4.2.
- In the VCP Event Viewer, which is launched via Event Search, the Next or Previous button used for cycling through alarm images, are disabled if there are no subsequent images to show.
- Added a column to the Event Search dialog, showing the cameras associated with the event.
- Added a new search option in the Event Search dialog, to search for events linked with a specific camera.
- The VCP Event Viewer now automatically shows, as first camera, the camera where the event originates from. The VCP Event Quad Viewer now indicates the camera event source.
- For the SITE CONNECT, SITE SELECT, SITE RELEASE, SITE DISCONNECT and SITE ACKNOWLEDGEMENT events, the Events list now contains the user name in the Detector Text column.

2.3 Site Overview

- The Site Armed/Disarmed status on the Site Overview page is now updated on the fly, upon receiving a "SYSTEM ARMED" event from the unit. Prerequisite for this to work properly, is to use an alarm profile where the "End of alarm tx" checkbox is ticked, on the unit. If required, the "SYSTEM ARMED" event can be hidden from the ASL, using Sensor Monitoring.

2.4 Configuration

- VCP related configuration files have been moved to the "ADPRO VCP" folder under the common application data folder. E.g. "C:\ProgramData\ADPRO VCP". The configuration files include vcp_bi.ini, VCPClientConfig.xml, VCPAppLauncherConfig.xml, ADPROSW.config and GPSMapsSettings.xml.
- Temporary, backup and log files are moved to subfolders under the "ADPRO VCP" folder. The "ADPRO VCP" folder resides under the common application data folder.

  The following folders are now used by VCP:

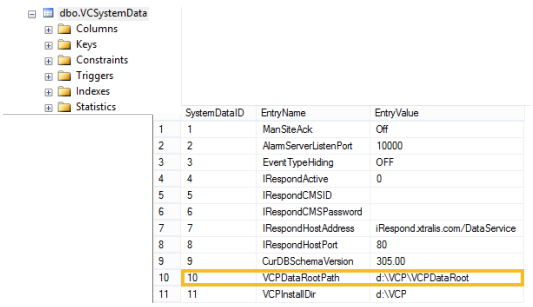
<CommmonApplicationData folder>\ADPRO VCP
Used for storing VCP configuration files, and other files that do not belong in any of the subfolders.
<CommmonApplicationData folder>\ADPRO VCP\Temp
Used for temporary files, i.e. files that are supposed to be cleaned up by VCP.
<CommmonApplicationData folder>\ADPRO VCP\Temp\SavedAlarms
Used by the XO Alarm Server SDK for temporary caching alarm information.

<CommmonApplicationData folder>\ADPRO VCP\Backup
Used by VCP for storing backups of config files, etc.
<CommmonApplicationData folder>\ADPRO VCP\Logs\Server
Contains VCP Server rolling log.
<CommmonApplicationData folder>\ADPRO VCP\Logs\Client
Contains VCP UI rolling log.
<CommmonApplicationData folder>\ADPRO VCP\Logs\VideoWall
Contains VCP VW rolling log.
<CommmonApplicationData folder>\ADPRO VCP\Logs\GlobalMaps
Contains Global Maps application rolling log

- Improved the appearance of the IP Configuration window that is displayed if the VCP UI is launched with a misconfigured bind-to-IP address. It was not clear that the window originated from the VCP UI. The window now clearly indicates that it relates to VCP.
- Added ability to configure .NET remoting client socket (bind-to-address and client port) for VCP VideoWall, Global Maps application, and the ADPRO Media Server. This provides the ability to better finetune these applications to the needs of an environment where network communication is more restricted.

2.5 Database

- VCP setup now comes with SQL Server 2014 Express with Advanced Services. On the setup wizard's prerequisites page, the setup provides the ability to install SQL Server 2014 Express with Advanced Services, if the user did not select a valid existing SQL Server instance.
- Installation of the SQL Server instance, that is required for installing the VCP related databases, has been separated from the VCP setup. The VCP setup no longer integrates installation of SQL server into the VCP setup process. The wizard still does provide a link on the prerequisites page, which allows to run the setup for SQL Server 2014 Express with Advanced Services. SQL Server setup then runs with default configuration settings. But setup of SQL Server will not be fully automated. The user must take action to proceed through the SQL Server setup wizard and is allowed to make changes to the configuration. The user is not forced to use "XTRALIS_CYCLOPS" as the name of the SQL Server instance. VCP now supports custom instance names. This allows to install the VCP databases on existing SQL Server instances.
- Added support for SQL Server 2014, SQL Server 2016.
- Added support for setting the path to the EventExtraData folder in the SystemData table.



	SystemDataID	EntryName	EntryValue
1	1	ManSiteAck	Off
2	2	AlarmServerListenPort	10000
3	3	EventTypeHiding	OFF
4	4	IRespondActive	0
5	5	IRespondCMSID	
6	6	IRespondCMSPassword	
7	7	IRespondHostAddress	iRespond.xtralis.com/DataService
8	8	IRespondHostPort	80
9	9	CurDBSchemaVersion	305.00
10	10	VCPDataRootPath	d:\VCP\VCPDataRoot
11	11	VCPInstallDir	d:\VCP

2.6 Data Conversion

- The tool now shows wait cursor whilst the conversion is busy.

2.7 Secure Viewer

- Added extra logging to the Secure Viewer Extractor post-extract process, to allow for better error handling.

2.8 General

- VCP is supported on Windows 10 and Windows Server 2012, Windows Server 2016.

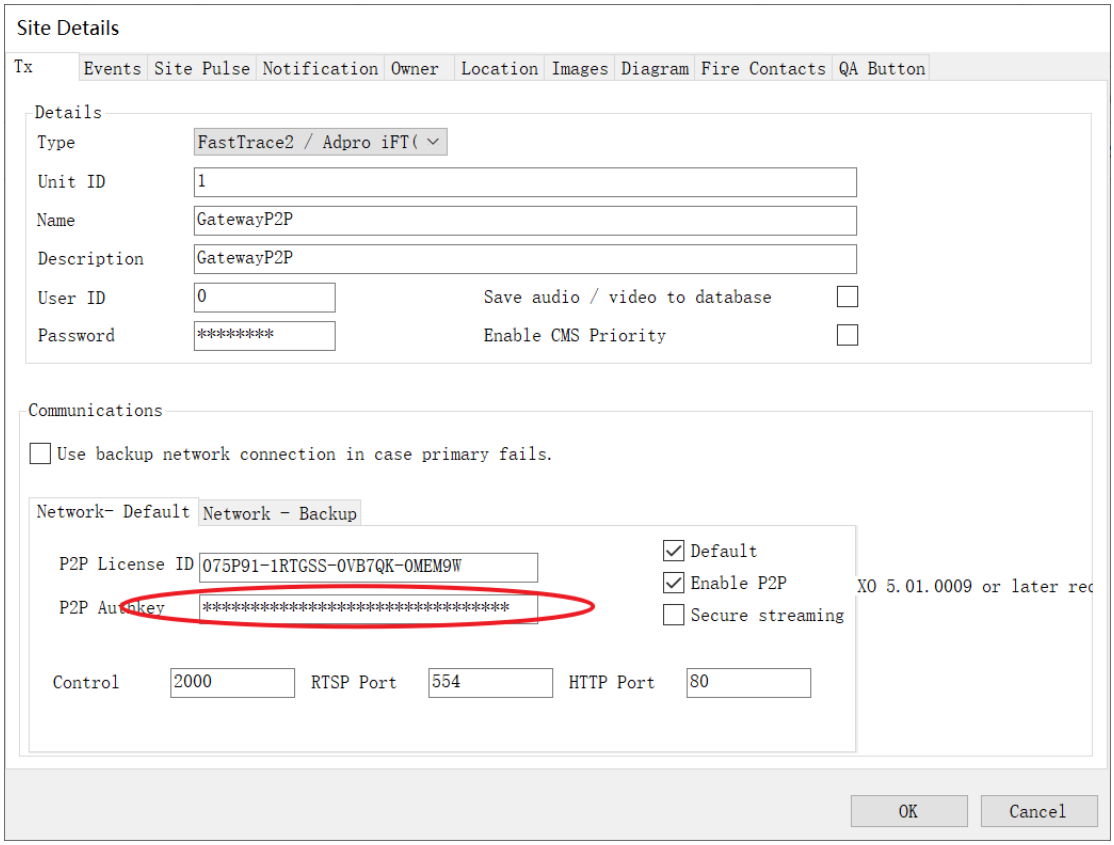
2.9 Video Wall

- VCP Video Wall can now be configured not to require a ping reply from VCP Server before it attempts to connect to the Server. By default, the Video Wall does not connect to the Server if it doesn't receive a ping reply.
  - ➢ The setting, PING_SERVER, is configurable in the AdproSW.config file.

2.10 P2P Support

Note: The devices with XO5 firmware support P2P connections. To get the P2P license key, add the XO device to Xchange2 and click **Activate your P2P license** on the **Manage Products** page for the device to get the TUTK license code. Copy it to the clipboard by clicking the text icon and use it for device connection in VCP. For more details, see *Xchange2 User Guide*.

V3.06 has the option to enable a P2P connection from the **Site Details** (Tools > Administration > Sites) page. The IP Address and Host Name fields disappear when the **Enable P2P** option is selected, and the **P2P License ID** and **P2P Authkey** fields will appear. The P2P Authkey is obtained from the XO client. For more details, see *P2P Setup Guide*.



2.11 Secure streaming

V3.06 also supports enabling encrypted streaming through the **Secure streaming** option on the **Site Details** page.

2.12 Upgrade to SQL Server 2019

VCP installs SQL Server 2019 Express and SQL Report Server 2019 Express (SQL Server Reporting Services-SSRS) for 64-bit operating systems (if there is no previous SQL Server installation). Install the Reporting Server only after installing the SQL Server. There is no change in the installation procedure for 32-bit operating systems, and VCP will install SQL Server 2014 in this case (for backward compatibility).

3 Removed Features

- To avoid confusion with the colour of bounding boxes, colour configuration for quad alarm bounding has been removed.
- Removed the iRespond functionality from the application.
  The settings in the database are preserved.
- Removing the VCP feedback tool from setup.

4 Known Issues and Limitations

4.1 Known Issues

Video and Private Wall:

- Older FastTrace 2 units may have difficulty connecting to the Video and Private Wall.

VCP Server:

- The VCP Server will not shut down if an archive is in progress.

Review:

- Review mode may export a larger time frame than expected causing the export to take a very long time. To the operator it looks like it has stopped working. This is due to the time/date selection range not matching the slider time/date range. Workaround is to use the slider.
- Export Review Data – progress dialog does not show 100% before it is closed.

User Permissions:

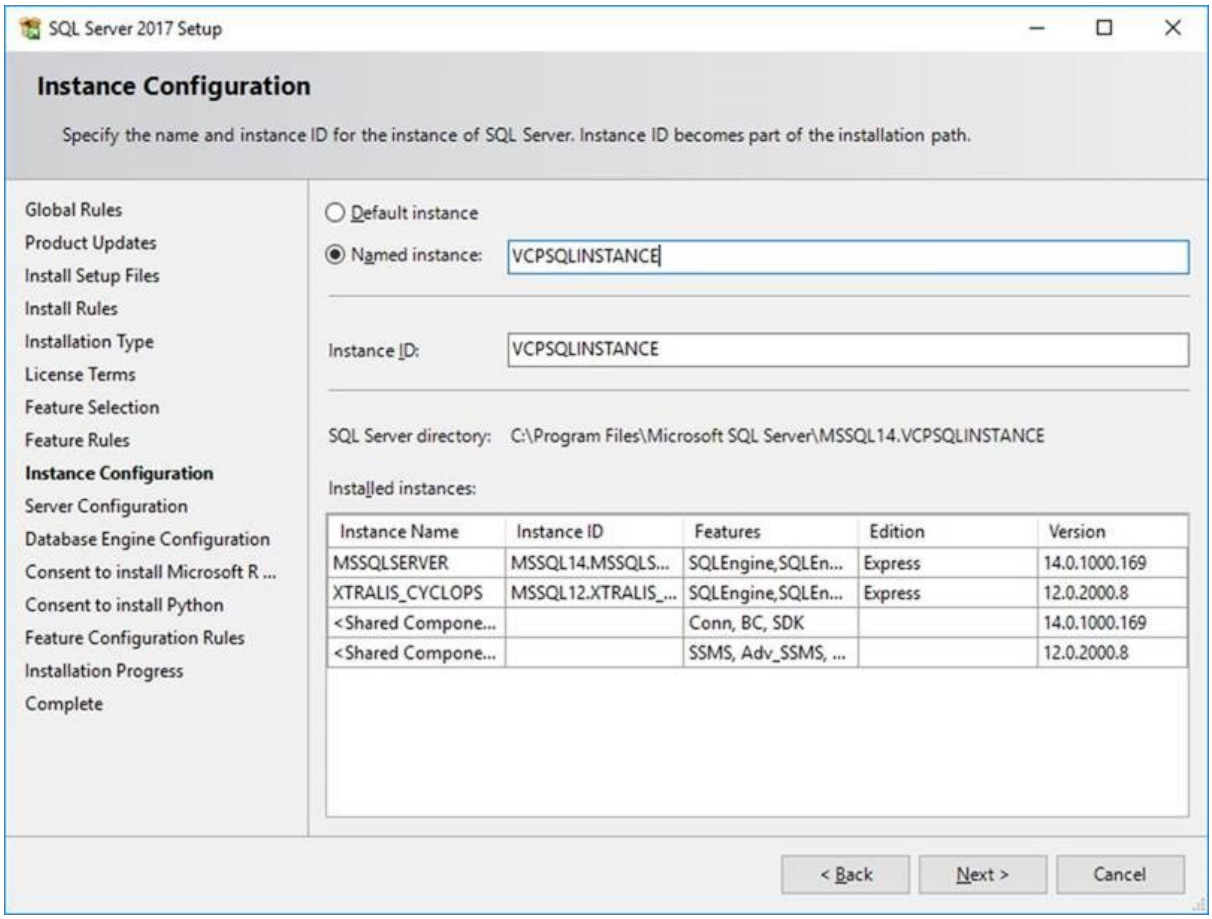
- Users with no access to acknowledge alarms can still do so due to mandatory site acknowledge option.

Hidden Alarms:

- Hidden alarms for FT2 should be identified as a text alarm type as we do not get images.

SQL Server Instance:

- Choose a named SQL server instance on the Instance Configuration page of the SQL Server setup when you are installing the SQL server instance to be used with VCP. VCP 3.6.0 does not support the default SQL Server instance. The installation fails if default SQL Server instance is used.



5 Software and Hardware Requirements

5.1 Client User Interface PC

- Operating System:
  - Windows 10 professional 32 bit
  - Windows 10 Professional 64 bit (recommended)
  - Windows 10 Enterprise 32 bit
  - Windows 10 Enterprise 64 bit
- 3.6 GHz Quad Core processor or better (recommended: i7-7700 CPU)
- 8 GB RAM (minimum), 16 GB (recommended)
- Discrete 512 MB video card, Nvidia Series 9 or better, with 1280 x 720 minimum resolution.
  1680 x 1050 as a minimum resolution provides the ability to view all columns within the Active Sites List without the need for scroll bars.
- 2 TB, 7200 rpm hard drive
- 1000BASE-T network card
- 1000BASE-T network backbone
- Internet Explorer 11 (recommended).

5.2 Server/Database PC

- Operating System:
  - Windows Server 2008
  - Windows Server 2012 R2 STD 64 bit.
  - Windows Server 2016 64 bit. (recommended)
- Supported SQL Server Editions
  - SQL 2014 Express with Advanced services
  - SQL 2016 Express
- Video Central Platinum comes with SQL Server 2014 Express out of the box. This version limits the maximum database size to 10 GB, use of one CPU core, and 1 GB of memory usage. For medium to large Central Monitoring Stations it is recommended to upgrade SQL Server to Standard or better editions.
  - Note: Video Central Platinum continues to work with SQL Server 2008 R2 express instances.
- 3.6 GHz Quad Core processor or better (recommended: i7-7700 CPU)
- 8 GB RAM (minimum), 16 GB (recommended)
- Discrete 256 MB video card with 1280 x 720 minimum resolution
- Hard drives for operating system and VCP (see the *Hard Drive Specification Guidelines* on page 13):
  - Using standard 7200 rpm hard drives: minimum 2 TB is recommended.
  - Using SSDs: minimum 500 GB is recommended.
- Minimum of 2 TB, 7200 rpm hard drive for backup and archives
- 1000BASE-T network card
- 1000BASE-T network backbone
- Internet Explorer 11 (recommended).

5.3 Hard Drive Specification Guidelines

For best performance and to enable a level of redundancy:

- System with fewer than 500 alarms per day: one standard 7200 rpm drive (minimum spec, no redundancy).
- System with between 500 and 5000 alarms per day:
  - minimum of two standard 7200 rpm drives in RAID 0 (no redundancy)
  - minimum of four standard 7200 rpm drives in RAID 10 (with redundancy).
- System with more than 5000 alarms per day:
  - Minimum of two Solid State Drives (SSD) in RAID 0 (no redundancy)
  - Minimum of four Solid State Drives (SSD) in RAID 10 (with redundancy).

Notes:

- You can add more drives in a RAID 10 configuration. However, it is recommended they are added in even numbers. For example: 4, 6, or 8 drives.
- Most modern motherboards support RAID 10. Alternatively, you can use a plug-in controller.
- SATA3 drives are typically faster than SATA2 if supported by the motherboard.
- 15,000 rpm drives are typically faster than 7,200 rpm drives.
- Use the above specification for the drives hosting the Windows operating system and all VCP components, including SQL Server 2008/SQL Server 2014. You can install alternative drives for backup purposes.
- RAID 10 redundancy is not a replacement for frequent database backups.
- This information is offered as a guideline. SQL Server 2008/SQL Server 2014 can be a heavy disk user. The load depends on alarm load, alarm load within a given period of time (as the above spec assumes an average load), quantity of sites, quantity of users, and use of other features such as database backup or reporting. ADPRO recommends that you discuss your specific circumstances with ADPRO technical support staff before you purchase hardware.
- SSDs will supply the best performance for all usage patterns listed above.

5.4 Video Wall PC

- Operating System:
  - Windows 10 professional 32 bit
  - Windows 10 Professional 64 bit (recommended)
  - Windows 10 Enterprise 32 bit
  - Windows 10 Enterprise 64 bit
  - Windows Server 2008
  - Windows Server 2012 R2 STD 64 bit
  - Windows Server 2016 64 bit
- 3.6 GHz Quad Core processor or better (recommended: i7-7700 CPU)
- 8 GB RAM (minimum), 16 GB (recommended)
- Discrete 512 MB video card, NVidia Series 9 or better, with 1280 x 720 minimum resolution
- 2 TB, 7200 rpm hard drive
- 1000BASE-T network card
- 1000BASE-T network backbone.

5.5 Peripherals

- DVD-ROM, industry standard device (10 x speed or higher)
- Mouse/keyboard/joystick (for PTZ).
- Sound card/speakers/microphone (required for audio capability).

5.6 System Specifications

- Limit of 255 simultaneous connections to ADPRO FastTrace 2 Series/iFT Series/eFT devices
- Limit of 10 simultaneous HeiTel connections with live video only
- Limit of 5 simultaneous HeiTel connections with alarms
- Limit of 16 user interfaces
- Limit of 60,000 alarms per day
- One license required for the Video Central Platinum server (license is free since the V03.06 version)
- Limit of 4 Video Wall application servers each with 4 monitors for a total of 80 video streams per Video Wall application server, or 320 video streams system wide.

5.7 Data Compatibility

Video Central Platinum version V3.06.00 requires ADPRO FastTrace 2 Series/iFT Series firmware version V2.11.0024 or above.

https://www.security.honeywell.com

UK and Europe +44 1442 242 330 **D-A-CH** +49 431 23284 1 **The Americas** +1 781 740 2223
Middle East +962 6 588 5622 **Asia** +86 21 5240 0077 **Australia and New Zealand** +61 3 9936 7000

A *Disclaimer* about this document, statements about *Intellectual Property, Copyrights*, and *Liability*, as well as a *General Warning* are available in an earlier section of this document.

Doc. 29578_05

Honeywell