IQSIGHT

VRM 4.80 - Release notes

Date:
9 June 2026

Introduction

Product:	Video Recording Manager
Version:	4.80
Compatible BVMS version:	14.0

This document contains latest information about the Video Recording Manager (VRM) release 4.80. This version is designed to be used in a BVMS 14.0 environment. Product boundaries are also described in the datasheet which can be found on the IQSIGHT web page.
The latest version of the Release Notes is always available on the IQSIGHT Product catalog. The VRM is included in the BVMS installation package.

General

VRM Video Recording Manager is a key part of BVMS ecosystem, providing a Distributed Network Video Recorder solution, eliminating the need for dedicated NVRs. VRM supports iSCSI-based storage systems and the Bosch/IQSIGHT IP devices (IP cameras and IP video servers).

VRM Video Recording Manager comprises the following software packages:

- VRM Server including VRM Monitor
- VRM eXporter Tool

Please note: For VRM Video Recording Manager the BVMS Viewer can be used as standalone replay client. For playback of unencrypted video data exported by VRM eXport Wizard, BVMS has to be used.

VRM offers system-wide recording monitoring and management of Bosch/IQSIGHT iSCSI storage, video IP encoder and IP cameras. VRM software supports Bosch/IQSIGHT H.264/H.265 and MPEG-4 IP video devices.

Supported storage subsystems are the Bosch/IQSIGHT DSA and DLA disk array systems (iSCSI-based DVA storage systems still will work). iSCSI disk arrays are not attached directly to VRM, but instead can be attached anywhere on a standard IP network via a 1 GbE uplink as well depending on iSCSI storage model via 10 GbE (e.g. DSA E-Series E2700 or E2800).

New functionality

Build	ID	Description
4.80.0029	500036	Prepared for Remote Portal Single Sign-on authentication for VideoView+ for DIVAR IP **Note:** This feature will be released at later point with planned Remote Portal and Video Security app upgrade

Resolved issues

Build	ID	Description
4.80.0029	500154	(FIXED) VSC authentication failure after VRM server restart
4.80.0029	502515	(FIXED) Optimized thumbnail handling for multiple Video Security clients connected
4.80.0029	502223	(FIXED) RTSP streaming from VRM might not work properly for CPP14 cameras
4.80.0029	502408	(FIXED) VRM might crash when opening VRM Monitor pages
4.80.0029	504447	(FIXED) Improved stability

Restrictions and known issues

Installation, Upgrade, Downgrade

- VRM 4.80 is the only version fully compatible with BVMS 14.0 - if older VRM version is used with BVMS 14.0, Video Security client connection will not work properly.
- VRM 3.82 or higher is available as 64 bit version only (no 32 bit version available). When upgrading from a VRM 32 bit version to a 64 bit version SSL certificates will be removed and have to be added manually to the system. Exception: self-signed certificates will be replaced automatically.
- **Important Note:** Downgrade from version 4.00 or higher to an earlier version is not possible.
- For VRM-managed cameras the replace functionality is supported since BVMS 9.0 using Configuration Client. The Configuration Manager does not support any device replacement of VRM managed cameras.
  (Note: In case the device replace is not performed via BVMS Configuration Client and to grant access to the recordings of a defective VRM-managed camera, keep the camera's IP address as offline camera. Once the minimum retention time has expired, the IP address is free to use.

The camera replacement has to be added as new device to the VRM system.)
For non-VRM-managed cameras, a replace function is available in the Configuration Manager.

- To swap to existing IP cameras in their physical installation location including the swap of their IP addresses while keeping the recording footage linked to the original IP address is not supported. Customers in the need to perform such a swap of two operational cameras, are requested to contact the local IQSIGHT technical support.
- When upgrading an existing VRM server installation a message might be shown that the “rms service” could not be stopped. Enter “retry” in the message box and the installation routine will properly be continued.
- Up to 128 replay sessions tunneled through VRM are supported. Same applies for the failover VRM, if exists. Bandwidth limits of network and storage must not be exceeded. 10Gb Ethernet is highly recommended.
- Separate replay sessions are established for:
  - Each Operator Client in playback mode (for timeline handling, etc)
  - Each camera/cameo with an active playback
  - Each live camera in VSC displayed through DIVAR IP, BVMS or VRM connection

Storage

- “LUN Size”: Size of a single LUN may not exceed 64 TB. If LUN-size exceeds 2000 GB, the pool needs to be configured properly in Configuration Manager.
  Note: VRM uses a virtualization layer and manages 1GB blocks out of all LUNs.
  Thus, for the functionality it makes no difference how many LUNs are configured within one storage subsystem as long as the maximum of 4.000.000 blocks (4PB storage) is not exceeded for the total VRM system.
- Maximum number of 120 iSCSI targets
- Maximum number of 254 LUNs per target
- Restrictions for LUNs larger than 2000 GB:
  - Requires camera firmware version 6.30 or later; usage of Firmware 6.44 or later is recommended due to improved Firmware security.
- Changing IP-Addresses for iSCSI-storage on the fly is not supported. Please refer to the Security Knowledge Base or consult your local support for manual alternatives.
- Recording file structure on SD card shall not be modified manually.

Recording

- When using recording encryption the VSG has to be installed on a separate hardware than the VRM. Otherwise, neither failover VRM nor a redundancy key will be able to decrypt encrypted recordings.
- Switching recording encryption on/off multiple times frequently may lead to wrong state on current recording block.
- The new recording encryption format introduced with camera firmware 7.60 is supported by VRM 3.82.0049 or higher
- Recording encryption is supported for camera firmware 7.10 and higher.
- Bosch cameras produced before January 2014 may not able to encrypt their recordings. The VSG can encrypt the recordings for these cameras if this is required.
- Bosch cameras produced before January 2014 may not able to encrypt their multicast traffic.
- For recording encryption a redundancy key is mandatory. The redundancy key is the only way to decrypt encrypted recordings in case of loss of the VRM decryption certificate with its private key.

- Short enabling (for a few moments) and disabling of encrypted recording leads to the effect that the current recording block may be only in a consistent state after being released by the IP camera.
- Encryption is supported on all DIVAR IP systems except for DIVAR IP 2000
- The current version of the VRM exporter tool does not support export of encrypted video in native format. But it is possible to convert encrypted video from VRM into MP4 files. Exporting encrypted recordings directly from an SD card is not possible.
- H.265 encoded video recording and playback is supported
- Time Server: VRM expects a Windows Time Server running. For the BVIP cameras/encoders and the VRM a common time server must be configured to ensure an application-wide, uniform time-base. The VRM Server must synchronize with the same Time Server used for all VRM managed BVIP cameras/encoders.
- "Prioritization Live Viewing vs. Recording": Recording and live viewing are independent processes and do not have a prioritization. The number of replay sessions started may influence the recording, i.e. system resources of storage array may be getting low and unrecognized by the VRM.
  Note: Recording must be manually configured in a way to allow for the required recording sessions and/or replay sessions.
- “Automatic/Failover”: On failure of the primary storage and switching to the failover storage a recording gap of multiple seconds will occur.
- Alarm recording: sometimes an active pre-alarm recording will be shown twice in the recording list.
- Firmware 5.0 and higher: Prealarm may be set to a minimum value of 1s and post alarm to 5s. Firmware versions prior to 5.0 pre- and postalarm recording: the minimum time that can be configured for prealarm recording is 15 seconds and 5 seconds for postalarm recording.
- Failover: switching the primary and secondary iSCSI target may result in a span list with incorrect quota
- Failover (Backup) server must not execute “format” jobs
- Recording Migration: Recordings that were created in a direct iSCSI environment with FW 3.52 cannot be migrated directly to a VRM solution but recordings will be ignored. Local recordings of BVIP devices with Firmware 4.10 or higher may be migrated to VRM environments.
- Changing devices from M2 to M4 mode:
  Due to the additional channels in M4 mode the recordings from encoder input 3 that were accessible under channel 2 in M2 mode are now accessible under channel 3. Old recordings of channel 3 created in M2 mode are still accessible under channel 2.
- Changing devices from M4 to M2 mode:
  Recordings from channel 3 and 4 in M4 mode will not be accessible anymore in M2 mode. Please backup any relevant data before switching from M4 to M2. Once the device has been set to M2 mode data of channel 3 and 4 will be deleted.
- FTP Export of Recording: If FTP export for local recording of a BVIP device has been configured this must be deactivated manually before the camera/encoder is moved to a VRM environment
- Authenticity check is not available if ANR is enabled.
- During alarm recording, authenticity check is only available within the recordings.
- In case function “Secondary target usage” in a storage pool is enabled, this consumes blocks from other storages in that pool. Each IP camera and IP encoder gets extra blocks from one additional storage system assigned for usage in case primary is not reachable. By default this function is disabled (off) at each new pool. For each camera channel 2x 1GB blocks are reserved/assigned to the block list when having this feature enabled. E.g. VIP X1600 XFM4 would get 2x4 = 8 blocks form secondary storage. 16-channel encoder would get 32 blocks assigned. As the situation that the VRM and a complete storage go offline at the same time is seen on low risk, the secondary target usage is by default set to “off” and can be enabled if desired anyhow.

- Restrict video functionality not supported for cameras/encoders based on platform CPP3 or older.

Configuration

- “GUI”: Device tabs block on some PCs when camera privileges are modified and a device of different type is selected without saving the changes.
  Note: Workaround and privilege changes should be saved before selecting a device of another type.
- Mass operations might not work reliably when more than 200 devices are selected.

Troubleshooting

- To avoid high CPU loads while zipping system log files in case of trouble shooting the zipping process is running with lowest priority and may take a while.
- If extended logging is activated and disk space is running below 1 GB free space, VRM automatically deactivates extended logging.
- RCP+ logging must not be activated for more than 2000 devices. In this case extended logging must be turned off.

IntuiKey

- “Replay”: IntuiKey can't start replay of media files stored on local PC
- “UI Display”: IntuiKey user interface displays ISO-Latin1 characters only

Network Configuration

- After licensing VRM no changes on the network links from different adapters should be done else VRM might encounter problems with license and/or block management
- Assigning multiple IP addresses to one ethernet interface is not supported.
- Web-based live-/playback only works for H.264 streams
- RTSP access for remote clients is only possible in interleaved mode