VIDEO INTELLIGENCE PLATFORM™

3VR VISIONPOINT™

INSTALLATION AND CONFIGURATION GUIDE

3VR VisionPoint™ VMS and Enterprise Software Version 8.1.x

DRAFT

3VR, Inc
814 Mission Street, Suite 400
San Francisco, CA 94103
www.3VR.com

Tele: 415.495.5790
Sales: 415.513.4611
Fax: 415.495.5797
Email: info@3VR.com

DRAFT

3VR VIDEO INTELLIGENCE PLATFORM™

VISIONPOINT™ INSTALLATION AND CONFIGURATION GUIDE

DRAFT

DRAFT

CHAPTER 1

3VR APPLIANCE INSTALLATION

1. INSTALLATION PREREQUISITES 21
   - 1.1 System Requirements 21
   - 1.2 Download Client Applications Package from 3VR Support Portal 21
   - 1.3 Obtain System License Key (If Applicable) 21
   - 1.4 Bring Required Items to Installation Location 22
   - 1.5 Install 3VR Client Applications (If Connecting With a Laptop) 22
2. ITEMS IN THE SHIPPING CONTAINER 23
   - 2.1 1000-Series 23
   - 2.2 2000-Series 23
   - 2.3 2100-Series 24
   - 2.4 3000-Series 24
   - 2.5 4000-Series 25
   - 2.6 4000-Series Enterprise 25
   - 2.7 5500-Series 26
3. PRODUCT DIAGRAMS 27
   - 3.1 1000-Series 27
   - 3.2 2000-Series 28
   - 3.3 2100-Series 29
   - 3.4 3000-Series 30
   - 3.5 4000-Series and 4000-Series Enterprise 31
   - 3.6 5500-Series 32
4. PHYSICAL INSTALLATION 33
   - 4.1 3VR System Environmental Conditions 33
   - 4.2 1000-Series 33
   - 4.3 2000-Series 33
   - 4.4 2100-Series 34
   - 4.5 3000-Series 34
   - 4.6 4000-Series, 5500-Series 34
5. CONNECT TO THE APPLIANCE 35
   - 5.1 Connecting with a Monitor, Mouse, and Keyboard 35
   - 5.2 Connecting with a Laptop 36
6. ACCEPT EULA 38
   - 6.1 Connected with Monitor, Mouse, and Keyboard 38
   - 6.2 Connected with a Laptop 38
7. RUN THE 3VR APPLIANCE CONFIGURATION TOOL 40

DRAFT

CHAPTER 2

VMS/ENTERPRISE SERVER SOFTWARE INSTALLATION

1. INSTALLATION PREREQUISITES 47
   - 1.1 Installation Restrictions 47
   - 1.2 System Requirements 47
   - 1.3 Obtain System License Key (If Applicable) 47
   - 1.4 Bring Required Items to Installation Location 48
2. INSTALL MICROSOFT .NET FRAMEWORK 4.X 48
3. INSTALL AND CONFIGURE MYSQL OR MSSQL 50
   - 3.1 Download MySQL 50
   - 3.2 Install MySQL 50
   - 3.3 Enable .NET Framework 4.x 54
   - 3.4 Install SQL Server 2012 56
   - 3.5 Configure SQL Server 2012 59
4. INSTALL 3VR VISIONPOINT™ VMS SERVER/ENTERPRISE SERVER SOFTWARE 61

CHAPTER 3

BASIC SYSTEM MANAGER CONFIGURATION

1. CONFIGURE BASIC SETTINGS IN 3VR SYSTEM MANAGER 65
   - 1.1 Launch System Manager (Users Connected to a 3VR Appliance) 65
   - 1.2 Log in to System Manager (Users Connected to Third-Party Hardware) 65
   - 1.3 Edit VMS Server Display Name 66
   - 1.4 Edit Local Language Settings 67
   - 1.5 Configure Keyboard Input 67
   - 1.6 Enter System License Key (Optional) 68
   - 1.7 Edit Network Settings 69
   - 1.8 Edit Known Host Setting 70
2. CONFIGURE OUTGOING EMAIL SETTINGS 70
3. CONFIGURE EVENT AND VIDEO STORAGE SETTINGS 72
4. CONFIGURE SCHEDULES 73
   - 4.1 Recording Settings Schedule 73
   - 4.2 Peak and Off-Peak Bandwidth Use Schedule 74
5. INSTALL PLUG-INS 76
6. SET CERTIFICATION DATE 77

DRAFT

7. RUN THE 3VR INSTALLATION REPORT 77
7.1 Searching for VMS Servers on an Enterprise Server 80
8. UPDATING DATE AND TIME SETTINGS 82
8.1 Edit the Time Zone 82
8.2 Edit the NTP Server 82
8.3 Edit the System Date and Time 83
9. NEXT STEPS 83

CHAPTER 4

ENTERPRISE SERVERS, REGIONS, AND USER ACCOUNTS

1. MANAGING VMS SERVERS ON AN ENTERPRISE 87
1.1 Adding a VMS Server 87
1.2 Renaming a VMS Server 88
1.3 Changing the Network Settings of a VMS Server Already on the Enterprise 88
1.4 Removing a VMS Server from the Enterprise 91
2. MANAGING REGIONS ON AN ENTERPRISE 92
2.1 Adding a Region 92
2.2 Renaming a Region 92
2.3 Removing a Region 93
2.4 Moving a VMS Server to a Different Region 93
2.5 Removing a VMS Server from a Region 94
3. WORKING WITH USER ACCOUNTS 95
3.1 Creating a New User Account 95
3.2 Editing a User Account 96
3.3 Disabling a User Account with Password Expiration 96
3.4 Re-Enabling a Disabled User Account 97
3.5 Resetting a User's Password 97
3.6 Deleting an Account 98
4. USER ROLES 98
4.1 User Role Basics 98
4.2 Viewing User Role Details 98
4.3 Assigning Roles to User Accounts 99
4.4 About the Default User Roles 99
4.5 Creating Custom User Roles 101
4.6 Sample Custom User Roles 102
5. ACCOUNT SECURITY 104
5.1 User Password Constraints 104
5.2 Unlocking a Suspended User Account 106

DRAFT

6. ACCOUNT ADMINISTRATION 106
6.1 Exporting the User List 106
6.2 Viewing Connected Users 107
6.3 Auditing User Accounts (Fall Release-2015 (8.1.x and above) only) 108
7. ENTERPRISE USER MANAGEMENT 109
7.1 Syncing Users with the Enterprise 109
7.2 Synchronizing with LDAP Servers 110

CHAPTER 5

GENERAL CAMERA CONFIGURATION

1. VIEWING CAMERAS IN SYSTEM MANAGER 121
1.1 Watch Video on VMS Server 121
1.2 Image Snapshot 121
2. BASIC CAMERA SETTINGS 122
2.1 Viewing Camera Settings 122
2.2 Camera Name 122
2.3 Camera Type 123
2.4 Camera Visibility 123
3. MOTION RECORDING SETTINGS 124
3.1 Motion Sensitivity Settings 124
3.2 Motion-Based vs. Continuous Recording 125
3.3 Other Motion Settings 126
3.4 Using Camera-Based Motion Detection (Fall Release-2015 (8.1.x and above) only) 127
4. FACE FINDING SETTINGS 133
4.1 Enabling or Disabling Face Finding 133
4.2 Measuring Eye Distance 133
4.3 Configuring Face Exclusion Zones 134
5. EVENT VIDEO AND IMAGE SETTINGS 134
5.1 Event Image Size 134
5.2 Event Data Overlays 135
5.3 Event Video and Image Buffering Settings 135
6. CAMERA DISPLAY SETTINGS 136
6.1 Overlay Date and Time 136
6.2 Mask Video in Region 137
6.3 Enable Alarm for Video Loss 137

DRAFT

7. INTERACTING WITH CAMERAS 138
7.1 Resetting a Camera to Default Settings 138
7.2 Copying Camera Configuration 138
7.3 Enabling or Disabling Cameras 139
7.4 Adding a Camera 139
7.5 Deleting a Camera 139

CHAPTER 6

ANALOG CAMERA CONFIGURATION

1. CONNECT ANALOG CAMERAS 143
1.1 1000-Series 143
1.2 3000-Series 143
1.3 4000-Series 143
1.4 5500-Series 144
2. VERIFY VIDEO QUALITY OF ANALOG CAMERAS 144
3. ANALOG CAMERA BASICS 145
3.1 Camera Type 145
3.2 Analog Video Input ID 145
3.3 Supported Cameras 145
4. H.264 RECORDING SETTINGS 146
4.1 H.264 Video Resolution 146
4.2 H.264 Video Frame Rate 146
4.3 H.264 Video Quality 147
5. CONTINUOUS RECORDING SETTINGS 147
5.1 Continuous Recording Video Frame Rate 147
5.2 Continuous Recording Video Quality 148
6. ANALOG CAMERA COLOR SETTINGS 148

CHAPTER 7

ANALOG PTZ CAMERA CONFIGURATION

1. PTZ CAMERA BASICS 151
2. PTZ INTERFACES 151
2.1 COM2 Serial Port 151

DRAFT

3. CONNECTING MULTIPLE PTZ CAMERAS 153
3.1 Wire Splicing 153
3.2 Daisy Chaining 153
3.3 Coaxitron Translator 154
4. PTZ CAMERA CONFIGURATION 157
4.1 Select the PTZ Camera Driver 157
4.2 Configure PTZ Settings 157

CHAPTER 8

IP CAMERA CONFIGURATION

1. OVERVIEW 161
1.1 Supported Cameras 161
1.2 IP Camera Connection Methods 161
2. CONFIGURE CAMERA NETWORK SETTINGS 161
3. CONNECT CAMERA(S) 162
4. CONFIGURE SECONDARY NIC (CLOSED NETWORK SETUP ONLY) 163
5. ENTER SYSTEM LICENSE KEY (HYBRID APPLIANCES ONLY) 163
6. CONFIGURE IP CAMERAS 164
6.1 Manual Camera Configuration 164
6.2 Discover Network/IP Cameras 165
6.3 Export Settings to CSV 167
6.4 Universal Drivers 167
7. IP CAMERA SETTINGS 169
7.1 Select Video Mode 170
7.2 Configure Video Recording Settings for MJPEG Video 171
7.3 Configure Video Recording Settings for MPEG-4 Video 172
7.4 Configure Video Recording Settings for H.264 Video 174
7.5 Configure 360-Degree Panomorph Camera Settings (Fall Release-2015 (8.1.x and above) only) 175
7.6 Smart Streaming 178
7.7 Camera-Specific Settings When Smart Streaming is set to YES 179
7.8 Hardware Rendering 179

DRAFT

8. USING THE GENERIC IP CAMERA DRIVER 180
8.1 Identifying the URL Path 180
8.2 Configuring a Generic IP Camera 180
9. IP CAMERA TROUBLESHOOTING 181
9.1 IP Camera Fails To Load 181
9.2 Generic IP Camera Driver Troubleshooting 183
10. CONFIGURING IP CAMERA VIRTUAL REGIONS 183
10.1 About Virtual Regions 183
10.2 Configuring Virtual Regions 183
11. CONFIGURING MULTIPLE PIPELINE MANAGER 186

CHAPTER 9

CONFIGURATION WITH TEMPLATES

1. TEMPLATES OVERVIEW 191
1.1 About Templates 191
1.2 Templatable System Settings 191
1.3 Templatable Camera Settings 192
2. CREATING TEMPLATES 195
2.1 Defining a New Template 195
3. APPLYING A TEMPLATE TO A VMS SERVER 197
3.1 Applying a Template from a File 197
3.2 Applying a Template Saved on the Enterprise 199
3.3 Renaming a Template 202
4. MANAGING TEMPLATES ON THE ENTERPRISE 203
4.1 Deleting a Template 203
4.2 Exporting a Template 204
4.3 Importing a Template 205

DRAFT

CHAPTER 10

AUDIO CONFIGURATION

1. AUDIO OVERVIEW 209
2. CONNECT ANALOG AUDIO CABLES (IF APPLICABLE) 209
   - 2.1 1000-Series 209
   - 2.2 3000-Series 209
   - 2.3 4000-Series 210
   - 2.4 5500-Series 210
3. ENABLE AUDIO RECORDING (IF APPLICABLE) 210
4. CONFIGURE AUDIO CAMERAS 211
5. AUDIO SETTINGS REFERENCE 212

CHAPTER 11

SPOT MONITOR

1. PHYSICAL SETUP 215
   - 1.1 1000-Series 215
   - 1.2 2000-Series 215
   - 1.3 2100-Series 215
   - 1.4 3000-Series 215
   - 1.5 4000-Series 216
   - 1.6 5500-Series 216
2. CONFIGURING SPOT MONITOR 216
   - 2.1 Configuring Spot Monitor from the Local Console 216
   - 2.2 Configuring Spot Monitor from System Manager 217
   - 2.3 Spot Monitor Display Settings 217
   - 2.4 Starting Spot Monitor 220
   - 2.5 Stopping Spot Monitor 221
3. DUAL SPOT MONITORS 222
   - 3.1 About Dual Spot Monitors 222
   - 3.2 Physical Setup 222
   - 3.3 Enabling Dual Spot Monitors 223
   - 3.4 Configuring Dual Spot Monitors from the Local Console 224
   - 3.5 Configuring Dual Spot Monitors from System Manager 225

DRAFT

CHAPTER 12

HEALTH MONITORING AND MAINTENANCE

1. HEALTH MONITORING 229
   - 1.1 Filtering Health Alerts 229
   - 1.2 Acknowledging Health Alerts 231
   - 1.3 Exporting Health Alerts 232
   - 1.4 Configuring Email Notification of Health Alerts 233
   - 1.5 Enabling or Disabling Health Alert Notifications 235
   - 1.6 Customizing Health Alert Thresholds 235
   - 1.7 Health Alerts Reference 237
2. DIAGNOSTIC AND SUPPORT TOOLS 240
   - 2.1 System Status Indicator (Not Applicable to All Models) 240
   - 2.2 RAID/Disk Settings (3VR Appliance Only) 240
   - 2.3 Test Appliance Connectivity 241
   - 2.4 Uninterruptible Power Supply Settings 242
   - 2.5 License Settings and Resource Units 244
3. SYSTEM STORAGE 245
   - 3.1 System Storage: Two Approaches 246
   - 3.2 Best Practices for Smart Storage Consumption 246
   - 3.3 Monitoring Storage Consumption 247
   - 3.4 Storage Upgrades 247
4. ENTERPRISE HEALTH CHECK 248
5. TROUBLESHOOTING 249
   - 5.1 Troubleshooting Resources 249
   - 5.2 Exporting Logs 249
   - 5.3 Exporting System Diagnostics 252
   - 5.4 System Information (Fall Release-2015 (version 8.1.x and above) only) 254

CHAPTER 13

UPDATING SOFTWARE

1. UPDATING A SINGLE VMS SERVER 259
   - 1.1 Send Update Package 259
   - 1.2 Update VMS Server 260
   - 1.3 Update Client Applications 260

DRAFT

2. UPDATING AN ENTERPRISE - LIVE UPDATE 261
2.1 Update Enterprise Server 261
2.2 Update Your Client Applications 261
2.3 Send Update Package to VMS Servers 262
2.4 Update VMS Servers 263
2.5 Update All Other Client Applications 264
3. UPDATING AN ENTERPRISE - SCHEDULED UPDATE 264
3.1 Schedule Enterprise Update 264
3.2 Schedule VMS Server Update 266
3.3 Update Client Applications 267
4. UPDATING AN ENTERPRISE - MANAGING SCHEDULED UPDATES 267
5. UPDATING AN ENTERPRISE - MANAGING UPDATE PACKAGES 269
6. UPDATING PLUG-INS 271

CHAPTER 14

FIELD UPGRADEABLE STORAGE

1. OVERVIEW 275
2. LIMITATIONS 275
3. BACKING UP SETTINGS 275
4. IDENTIFYING HARDWARE AND STORAGE TYPE 276
5. PLAN FOR RECORDING INTERRUPTION 277
6. BASIC PHYSICAL INSTALLATION 277
7. MODIFYING STORAGE 279
7.1 5500-Series RAID - Adding a New Volume 279
7.2 4000-Series and 5500-Series RAID - Replacing Existing Disks 280
7.3 5500-Series Non-RAID - Adding New Disks 281
7.4 4000-Series and 5500-Series Non-RAID – Replacing Existing Disks 283

DRAFT

CHAPTER 15

EXTENDED STORAGE SERVER

1. FUNCTIONAL OVERVIEW OF EXTENDED STORAGE SERVER 287
   - 1.1 About ESS 287
   - 1.2 Requirements 288
2. HOW TO CONFIGURE ESS 288
   - 2.1 Server-Side Configuration 288
   - 2.2 Client Configuration 290
   - 2.3 Health Alert 291
3. ESS INTEGRATION WITH OPCENTER AND ENTERPRISE SERVER 292
   - 3.1 OpCenter via Enterprise Server connecting to an Unavailable Appliance 292
   - 3.2 OpCenter via Enterprise Server Connecting to an Available Appliance 293
4. ESS ERROR CONDITIONS 294
   - 4.1 Error Conditions 294

CHAPTER 16

3VR APPLIANCE-SPECIFIC FEATURES

1. 3VR APPLIANCE-SPECIFIC FEATURES 299
2. ALARM INTEGRATION 299
   - 2.1 Alarm Inputs 299
   - 2.2 Alarm Outputs 300
3. PHYSICAL CONNECTIONS 300
   - 3.1 4000-Series and 5500-Series 300
   - 3.2 External Adapters 301
4. ALARM INPUTS 302
   - 4.1 Configure Alarm Inputs 302
   - 4.2 Generate Test Alarm Input Event 303
5. ALARM OUTPUTS 304
   - 5.1 Configure Alarm Outputs 304
   - 5.2 Test Output Connection with External Alarm Alert Action 305
6. TROUBLESHOOTING ALARM INTEGRATION 306
   - 6.1 Review Physical Setup 306
   - 6.2 Check System Manager Configuration 306
   - 6.3 If Alarm Test Fails for All Terminal Pairs 306

DRAFT

7. HDMI-TO-CVBS CONVERTER 307
7.1 Items in Shipping Container 307
7.2 Product Diagram 307
7.3 Converter Installation 307

APPENDIX A

IMAGE GUIDELINES FOR FACIAL SURVEILLANCE

1. THE IMPORTANCE OF IMAGE QUALITY 311
1.1 Key Elements in Optimizing Images for Facial Surveillance 311
2. IMAGING BACKGROUND 311
2.1 Resolution 312
2.2 Field of View 312
3. CAMERA PLACEMENT FOR FACIAL ANALYSIS - FOUR FACTORS 313
3.1 Field of View Determines Size and Resolution of Face 313
3.2 Horizontal Angle 315
3.3 Vertical Angle 315
3.4 Lighting Level 316
3.5 Additional Considerations for Megapixel Cameras 317
4. IMAGE USE AND OPTIMIZATION FOR FACIAL ANALYSIS 318
4.1 Imported Images 318
4.2 CCTV Video 319
5. CONCLUSION 323

DRAFT

3VR Inc. (hereinafter "3VR") provides this manual "AS IS," for informational use only, without warranty of any kind, expressed or implied, including but not limited to representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. 3VR reserves the right to revise this manual and to make changes in its content without obligation to notify any person or organization of such revision or change. In no event shall 3VR, Inc., its Directors, Officers, or Employees be liable for any indirect, special, incidental, or consequential damages (including damages for loss of profits, loss of business, loss of use or data, interruption of business and the like), even if 3VR has been advised of the possibility of such damages arising from any defect or error in this manual or product.

3VR Inc., 3VR, and the 3VR logo are trademarks of 3VR. 3VR may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license from 3VR, the furnishing of this document does not give you any license to these patents, patent applications, trademarks, copyrights, or other intellectual property. Other products, trademarks or names appearing in this document may or may not be trademarks, licensees, or copyrights of their respective owners and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

The persons depicted in this document are, to the best of 3VR's knowledge, employees of 3VR or casual passers-by, and are neither suspected of any crime nor have they been convicted of any crime. The incidents portrayed and the names used in this document are fictitious and any resemblance to the names, character, or history of any actual person, living or deceased, is coincidental and unintentional.

DRAFT

Warning

This product contains an internal battery. There is danger of explosion if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Contact Technical Support

If you are having trouble with a 3VR system or application, contact 3VR Technical Support by phone at 415-513-4572 or email support@3VR.com Monday through Friday, 5 a.m. to 6 p.m. Pacific Time (8 a.m. to 9 p.m. Eastern Time) for assistance.

3VR Support Portal

Download the latest client and system software, plug-ins, and documentation from the 3VR Support Portal at http://partners.3VR.com.

3VR VisionPoint™ VMS Installation and Configuration Guide

© 2004 - 2016 3VR, Inc.

Last modified: June, 2016

DRAFT

CHAPTER 1
3VR Appliance Installation

1. INSTALLATION PREREQUISITES 21
   - 1.1 System Requirements 21
   - 1.2 Download Client Applications Package from 3VR Support Portal 21
   - 1.3 Obtain System License Key (If Applicable) 21
   - 1.4 Bring Required Items to Installation Location 22
   - 1.5 Install 3VR Client Applications (If Connecting With a Laptop) 22
2. ITEMS IN THE SHIPPING CONTAINER 23
   - 2.1 1000-Series 23
   - 2.2 2000-Series 23
   - 2.3 2100-Series 24
   - 2.4 3000-Series 24
   - 2.5 4000-Series 25
   - 2.6 4000-Series Enterprise 25
   - 2.7 5500-Series 26
3. PRODUCT DIAGRAMS 27
   - 3.1 1000-Series 27
   - 3.2 2000-Series 28
   - 3.3 2100-Series 29
   - 3.4 3000-Series 30
   - 3.5 4000-Series and 4000-Series Enterprise 31
   - 3.6 5500-Series 32
4. PHYSICAL INSTALLATION 33
   - 4.1 3VR System Environmental Conditions 33
   - 4.2 1000-Series 33
   - 4.3 2000-Series 33
   - 4.4 2100-Series 34
   - 4.5 3000-Series 34
   - 4.6 4000-Series, 5500-Series 34
5. CONNECT TO THE APPLIANCE 35
   - 5.1 Connecting with a Monitor, Mouse, and Keyboard 35
   - 5.2 Connecting with a Laptop 36
6. ACCEPT EULA 38
   - 6.1 Connected with Monitor, Mouse, and Keyboard 38
   - 6.2 Connected with a Laptop 38
7. RUN THE 3VR APPLIANCE CONFIGURATION TOOL 40

DRAFT

DRAFT

1. INSTALLATION PREREQUISITES

Important
This guide describes installation and configuration of VisionPoint VMS on 3VR appliances, VMS servers, and 3VR Enterprise servers. Differences regarding these platforms are pointed out in the text.

Important
This chapter describes how to install and configure VisionPoint™ VMS on 3VR appliances. If you are installing a VisionPoint™ VMS server on third-party hardware, including Enterprise servers, the installation procedure is different. Please skip this chapter and proceed to chapter 2 of this guide for installation instructions.

Appliance Compatibility:
VisionPoint™ VMS version 8.1.x is compatible with 5500-Series, X-Series, and Server Class appliances. It is not compatible with E-Series appliances.

1.1 System Requirements

Go to the 3VR Partners Support Portal and review the *Supported Operating Systems* document for information regarding the system requirements for using 3VR VisionPoint™ VMS.

DRAFT

1.2 Download Client Applications Package from 3VR Support Portal

Prior to heading to the installation site, you must download the 3VR VisionPoint™ Client Applications from the 3VR Support Portal. This package contains client software, and documentation that you need to complete the installation.

1. Go to the 3VR Support Portal (http://partners.3VR.com) and sign in with your company's portal login.
2. Once signed in, mouse over the **Software** link in the left sidebar and then over **8.1.x (where "8.1.x" represents the current release)**. Then select the **8.1.x VisionPoint™ VMS Installation Package for 3VR Appliances**.
3. Click the Software Link for the **8.1.x Client Applications**. The software package is downloaded to your computer.
4. After the 3VR Client Applications .zip file has downloaded, unzip it using WinzZip or a similar utility.

1.3 Obtain System License Key (If Applicable)

If you plan to install facial surveillance or other advanced features on the appliance, you must enter the system license key that was provided to you at the time of purchase before you can enable these features. If you do not have access to the order confirmation email, you can obtain the Appliance Serial number in System Manager or from the device itself. Otherwise, you can look up the license key by serial number on the 3VR Support Portal:

1. Go to the 3VR Support Portal (http://partners.3VR.com) and sign in with your company's Support Portal login.
2. Once signed in, click the 3VR License Lookup link. (Alternatively, you can go directly to the key retrieval page with this link: http://3VR.com/license. You can use most web-enabled phones to access this page.)
3. Click the **3VR License Lookup Form** link.
4. Enter the requested information, including the system serial number, and then click the **Find System License** button.

1.4 Bring Required Items to Installation Location

The following items are required for installation:

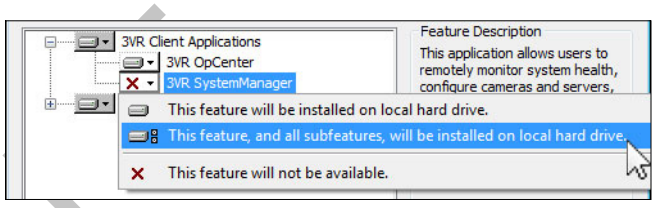
1. 3VR shipping container with all of the standard accessories and peripherals.
2. One of the following sets of items, used to log in to the system for configuration:
   - Monitor, mouse, and keyboard

     OR

   - Laptop running Windows XP, Vista, or Windows 7, and a D-Link USB network adapter or network cable.
3. 3VR VisionPoint™ Client Applications Package downloaded in step 1.1.

1.5 Install 3VR Client Applications (If Connecting With a Laptop)

1. On your laptop, load the 3VR Resource DVD included in the shipping box.
2. From the auto-start page, click the **Install Software** button.
3. Follow the prompts in the installation wizard. When you get to the **Setup Type** screen, select **Custom**, and then click **Next >**.
4. Click the red X next to 3VR System Manager and select **This feature, and all subfeatures, will be installed on local hard drive**. Make sure to also select 3VR OpCenter.
5. Click **Next >** and then follow the prompts to finish the installation.



Details

See the document *Installing and Upgrading 3VR Client Applications*, available on the Installation and Resource DVD, for more detailed instructions on installing 3VR System Manager, OpCenter, and other applications.

DRAFT

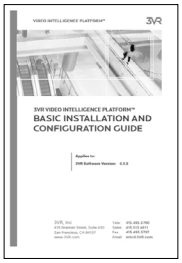
2. ITEMS IN THE SHIPPING CONTAINER

The photos below show the contents of the shipping containers for the 3VR appliances.

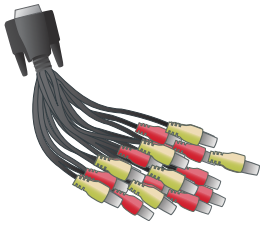
2.1 1000-Series

1000-Series unit

3VR Video Intelligence Platform™ Basic Installation and Configuration Guide



Audio/video cables



Power cable

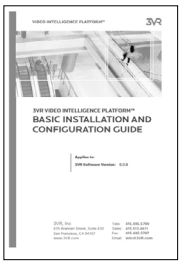
Power adapter

2.2 2000-Series

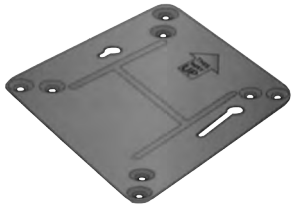
2000-Series unit

Wall-mount screws

3VR Video Intelligence Platform™ Basic Installation and Configuration Guide



Wall-mount bracket



Power adapter

Power cable

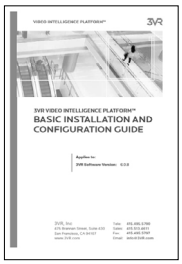
DRAFT

2.3 2100-Series

2100-Series unit

Wall-mount screws

3VR Video Intelligence Platform™ Basic Installation and Configuration Guide



Power adapter

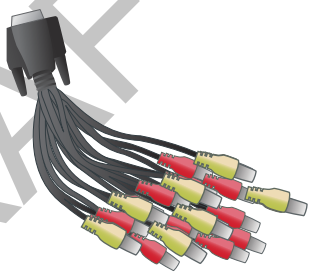
Power cable

Wall-mount brackets

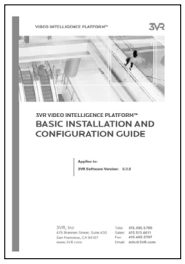
2.4 3000-Series

3000-Series unit

Audio/video cables



3VR Video Intelligence Platform™ Basic Installation and Configuration Guide



Power cable

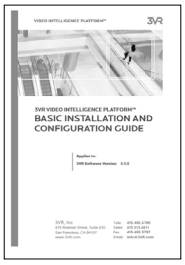
Power adapter

DRAFT

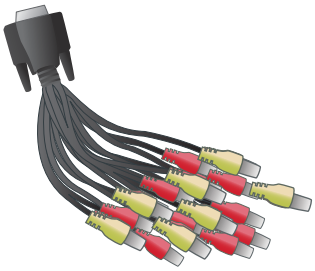
2.5 4000-Series

4000-Series unit

3VR Video Intelligence Platform™ Basic Installation and Configuration Guide

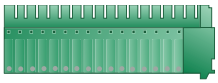


Audio/video cables



Power cable

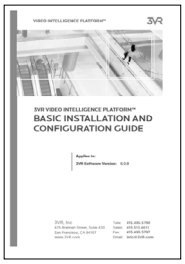
Alarm adapter



2.6 4000-Series Enterprise

4000-Series unit

3VR Video Intelligence Platform™ Basic Installation and Configuration Guide



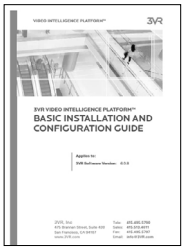
Power cable

DRAFT

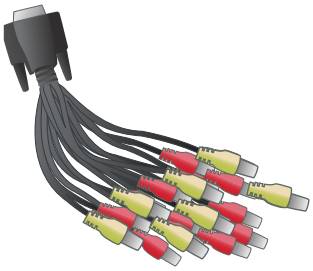
2.7 5500-Series

5500-Series Unit

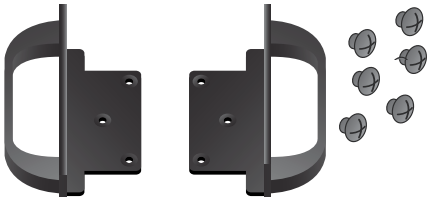
3VR Video Intelligence Platform™ Basic Installation and Configuration Guide



Audio/video cables



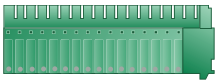
2 rack-mount ears and 6 screws



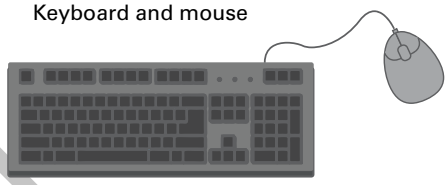
Power cable

2 case keys

Alarm adapter



Keyboard and mouse



*Video and audio cables are not included with NVR units.

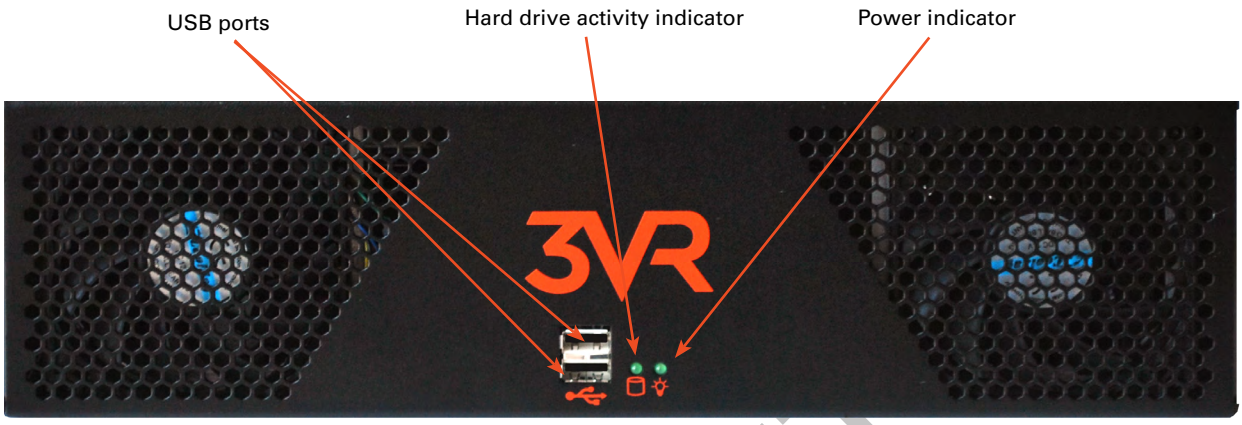
DRAFT

3. PRODUCT DIAGRAMS

The photos below call out the indicators and connectors on the 3VR appliances.

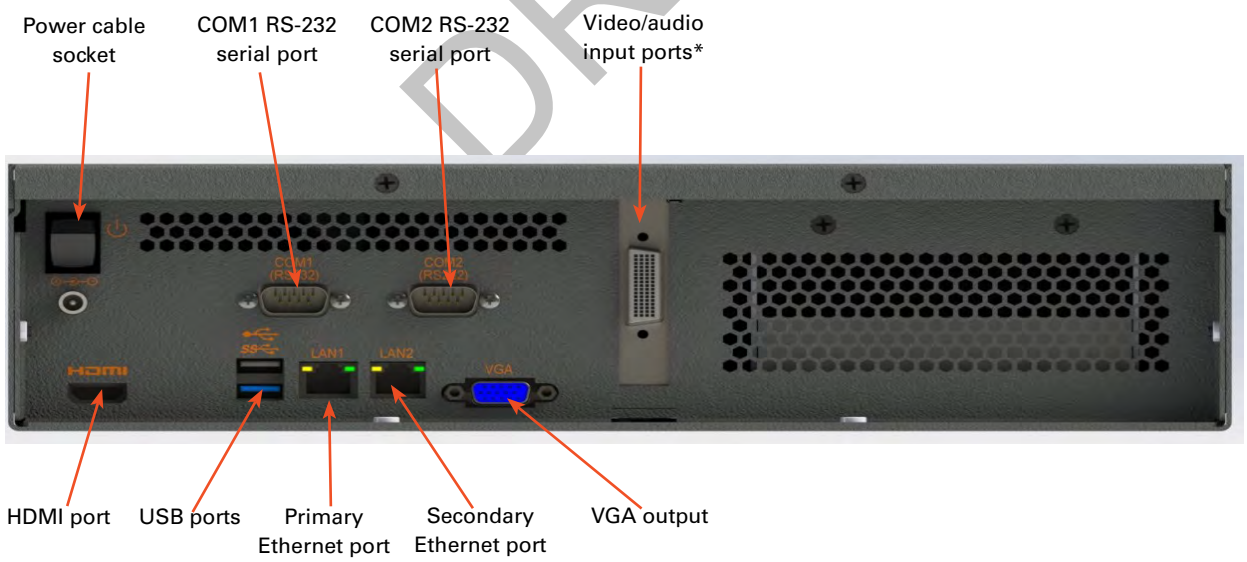
3.1 1000-Series

Front View



Rear View

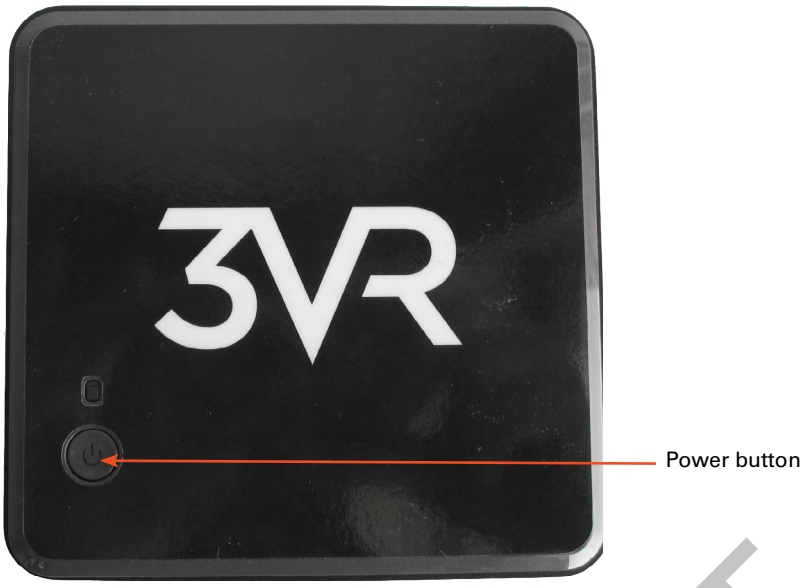
*NVR units do not have audio/video input ports.



DRAFT

3.2 2000-Series

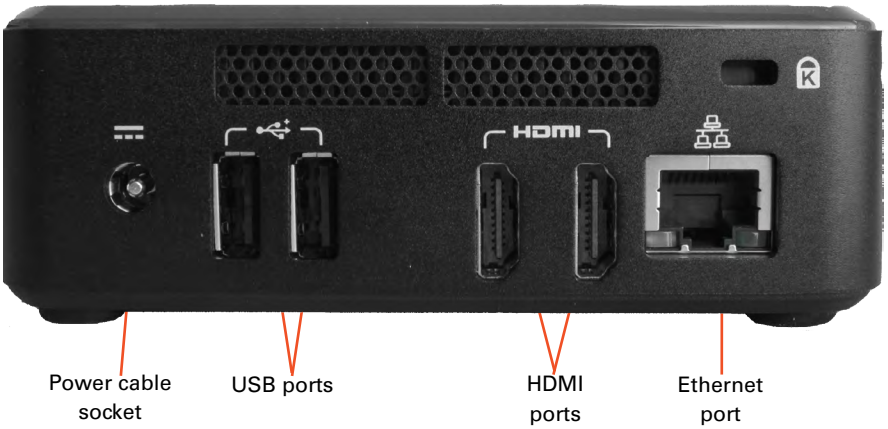
Top View



Front View

DRAFT

Rear View



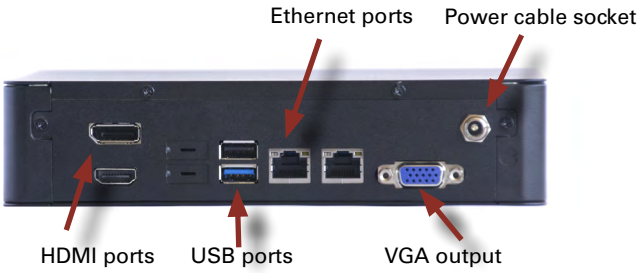
*The 2000-Series is an NVR and is not capable of connecting directly to analog cameras.

**The 2000-Series does not support USB Alarm I/O devices.

3.3 2100-Series

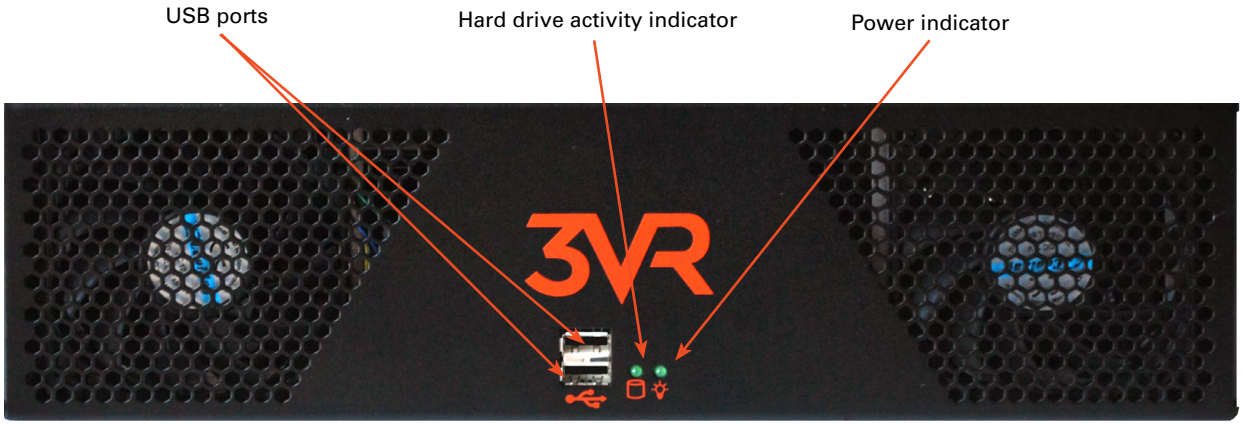
Top View

Rear View

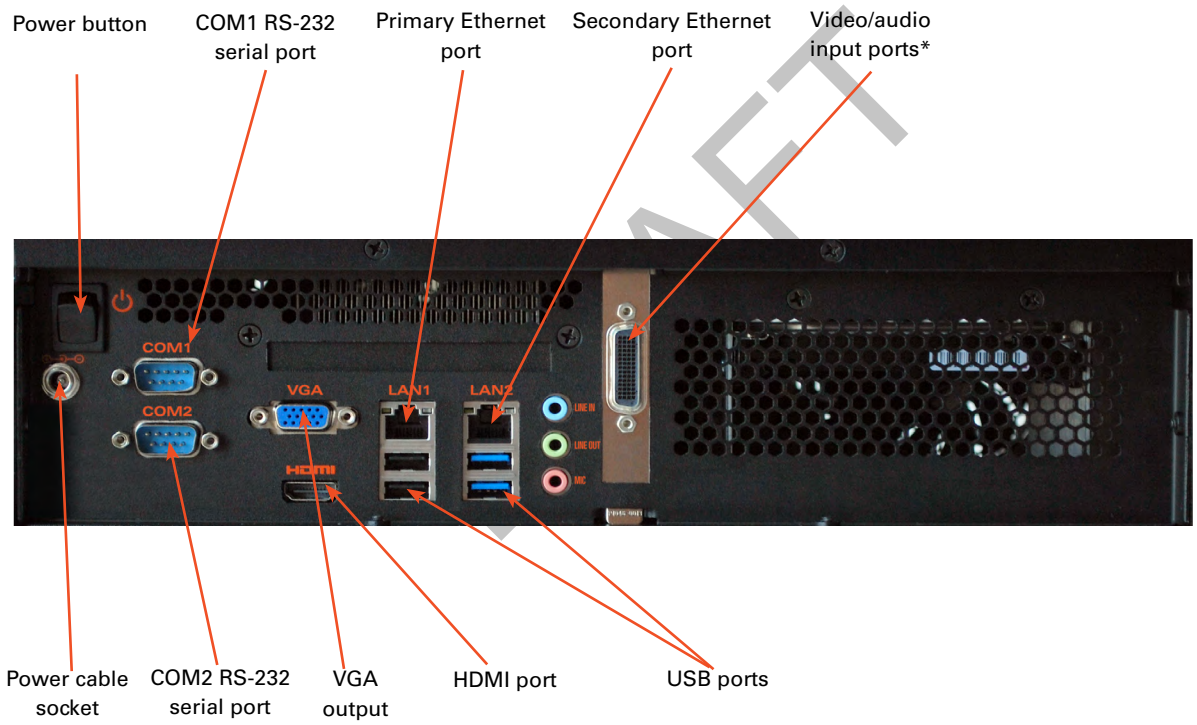


3.4 3000-Series

Front View



Rear View

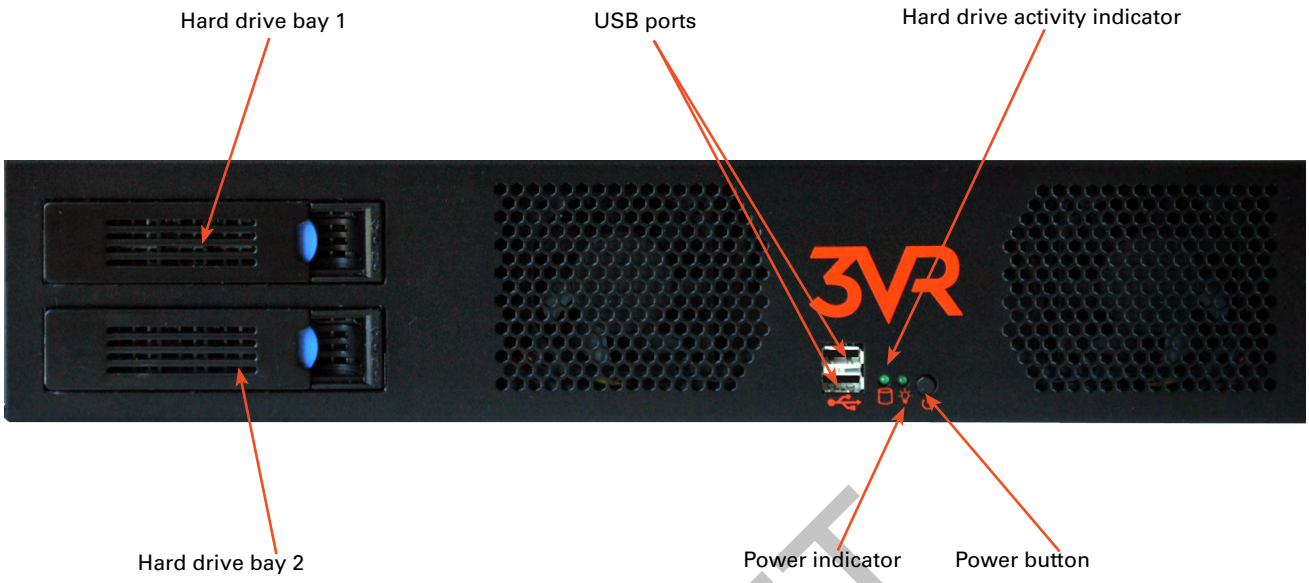


*NVR units do not have audio/video input ports.

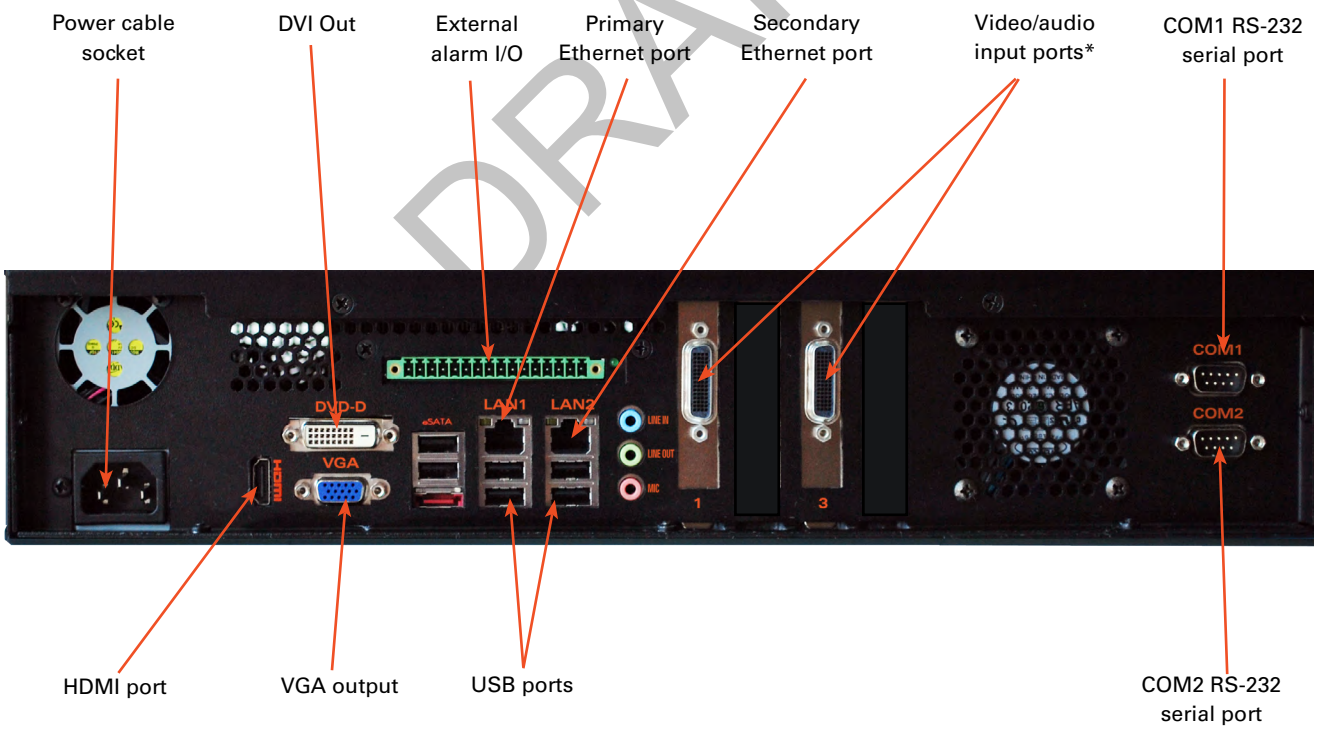
** COM1 is configurable through BIOS to RS-422/485.

3.5 4000-Series and 4000-Series Enterprise

Front View



Rear View



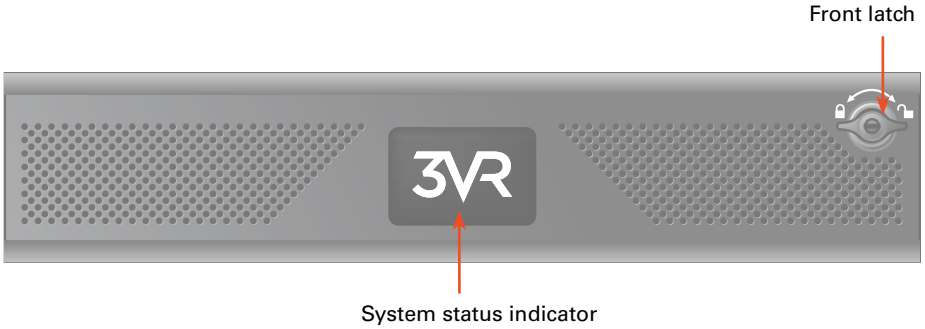
*NVR units do not have audio/video input ports.

**4000-Series Enterprise does not have video input ports.

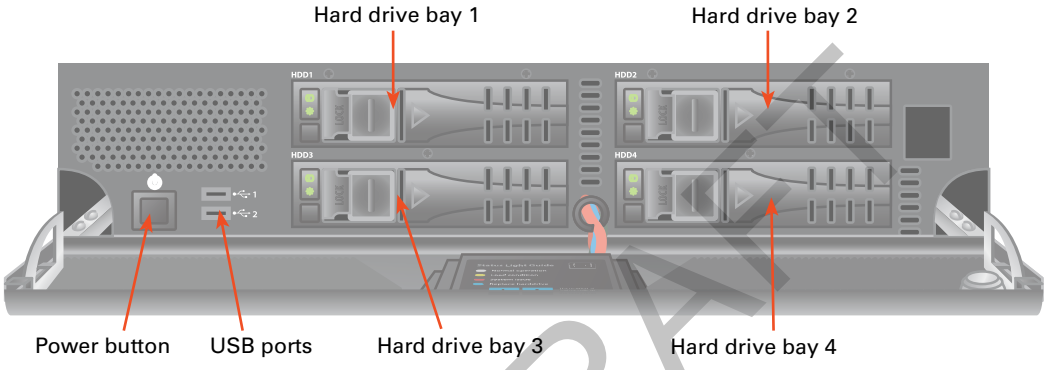
DRAFT

3.6 5500-Series

Front View

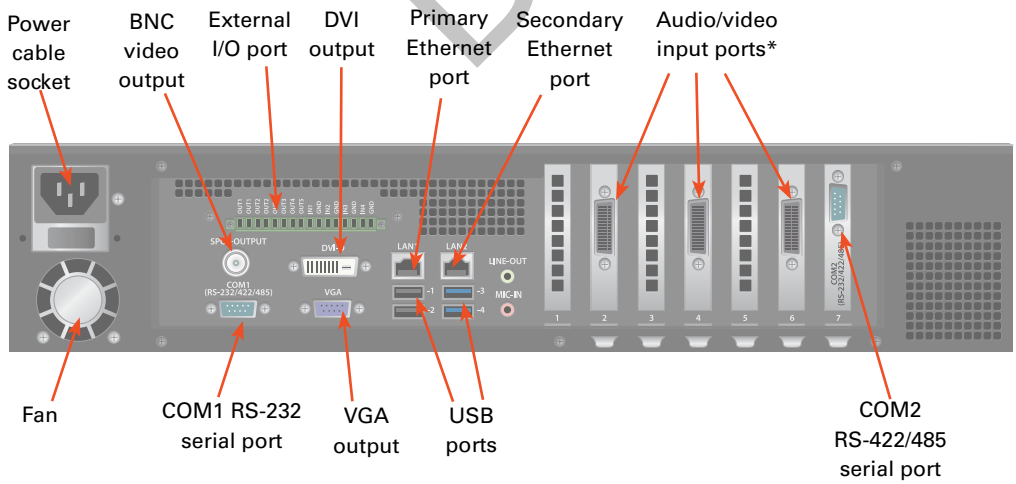


Front Interior View



DRAFT

Rear View



*Depending on configuration, 5500-Series appliances may have 0, 1, 2, or 3 audio/video input ports.

4. PHYSICAL INSTALLATION

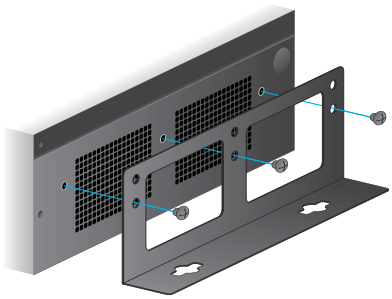
This section describes how to physically install an appliance.

4.1 3VR System Environmental Conditions

The below table represents the ideal environmental conditions for the 1000, 2000, 2100, 3000, 4000, and 5500 Series. Inspect the site to determine the appropriate location for the installation. Ensure that the environmental conditions listed below are satisfied; installing the unit in a location that exceeds the conditions listed below voids its warranty.

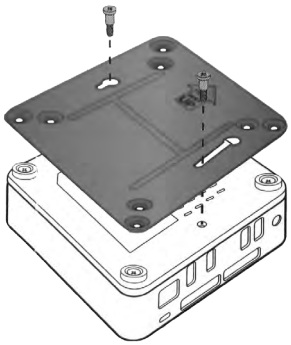
3VR Appliance Environmental Conditions	
Operating Temperature	5° to 35°C (41° to 95°F)
Heat Dissipation	1200 BTU/Hour
Humidity	5% to 95% RH (non-condensing)
Storage Conditions	-10° to 60°C (14° to 140°F)
Clearance	A minimum of 4″ clearance in both front and rear of unit.
Power Requirements	100–240 VAC; 7–3.5 A, 60/50 Hz. Consumption 350 W (max)

4.2 1000-Series



Install the wall-mount brackets for the 1000-Series on the underside of the appliance, as shown in the image above.

4.3 2000-Series

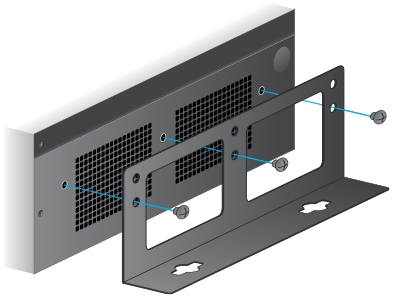


Install the wall-mount brackets for the 2000-Series on the underside of the appliance, as shown in the image above.

DRAFT

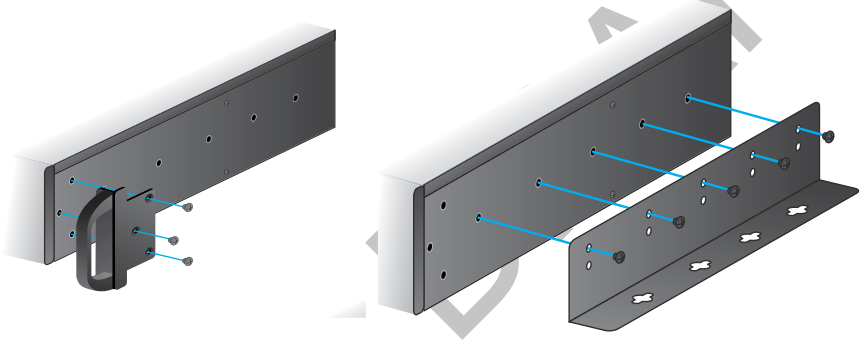
4.4 2100-Series

4.5 3000-Series



Install the wall-mount brackets for the 3000-Series on the right and left side of the appliance, as shown in the image above.

4.6 4000-Series, 5500-Series



Install the wall-mount brackets and rack ears for the 4000-Series on the right and left side of the appliance, as shown in the image above.

DRAFT

5. CONNECT TO THE APPLIANCE

There are two ways to connect to a 3VR appliance during installation and configuration:

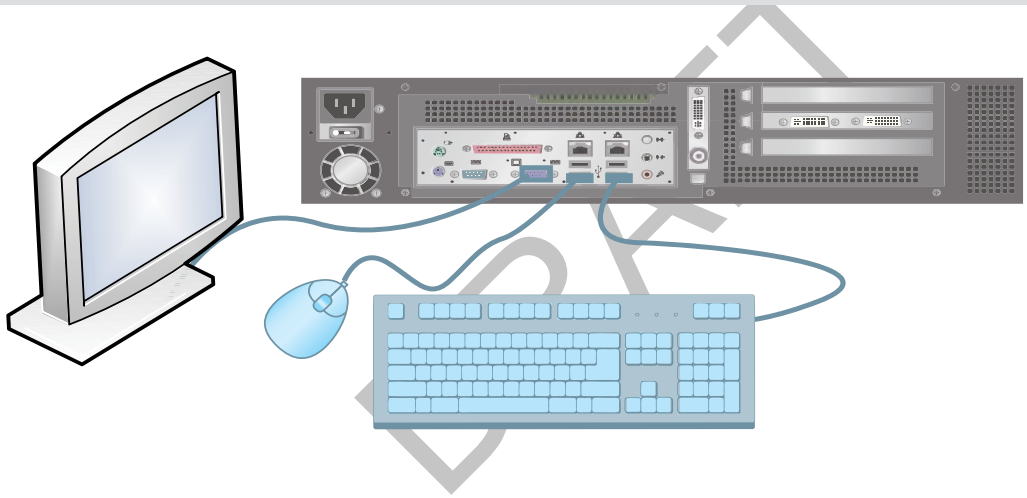
- **5.1 Connecting with a Monitor, Mouse, and Keyboard** page 35
- **5.2 Connecting with a Laptop** page 36

5.1 Connecting with a Monitor, Mouse, and Keyboard

1. Connect the monitor, mouse, and keyboard to the back of the appliance.
   - Ensure that the monitor is capable of the minimum supported resolution: 1024x768.
   - The mouse and keyboard must be a wired USB or PS/2 model that does not require special drivers*.

*** Notes**

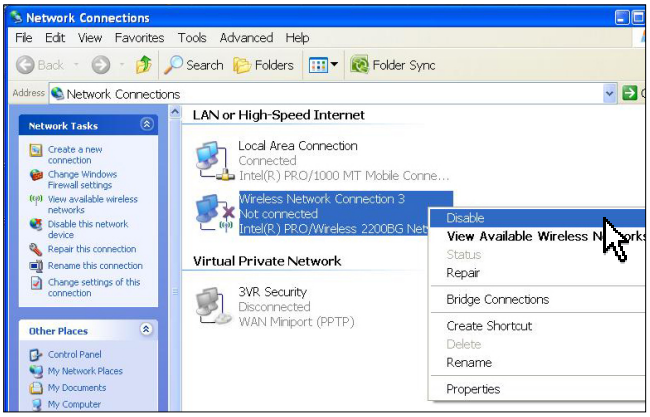
1) You must connect PS/2 peripherals before the appliance boots up to function properly. If a PS/2 mouse and/or keyboard is not responding, restart the system.
2) The 2000-Series, 2100-Series, 3000-Series, 4000-Series, and 5500-Series support USB peripherals only.
3) The 2000-Series support monitors with HDMI outputs.



DRAFT

5.2 Connecting with a Laptop

The following options all entail creating a local network between the 3VR Appliance and your laptop. In order to log in to the system with a laptop, you need to first install the 3VR Client Applications System Manager and OpCenter. See the *VisionPoint VMS User Manual* for information on installing OpCenter.



Step 1. Prepare Laptop

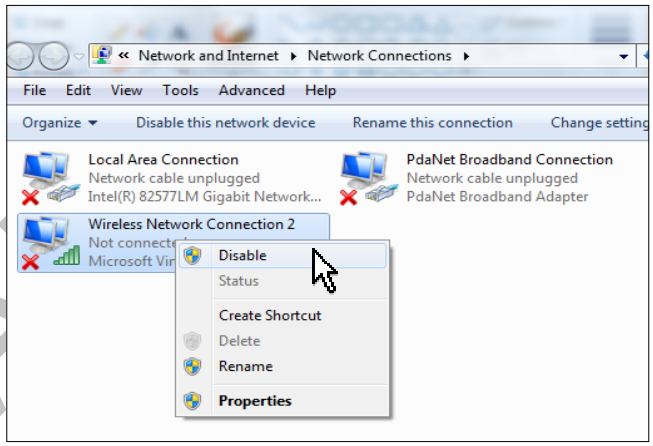
Windows 7

1) Launch the **Network and Internet** dialog box from the Windows Control Panel.

2) Click **Network and Sharing Center**.

3) Click **Change adapter settings**.

4) Right-click the wireless connection and select **Disable**.



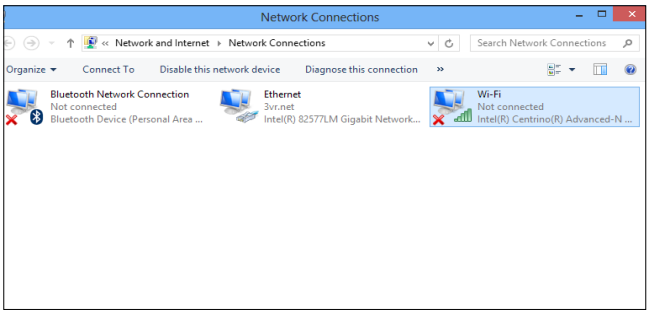
Windows 8

1) Tap Search. Enter **Control Panel**. The Control Panel appears.

2) Double-click **Network and Sharing Center**.

3) Click **Change adapter settings**.

4) Right-click the wireless connection and select **Disable**.



DRA

2. Verify that the laptop is set to DHCP:

   Windows 7/8

   1) Right-click the network icon and then select **Open Network and Sharing Center**.

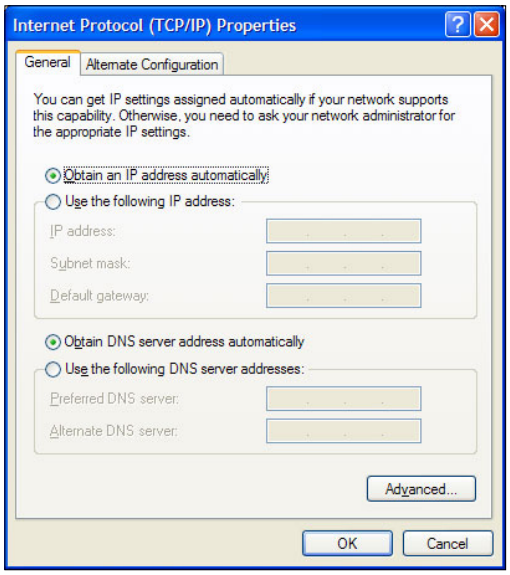
   2) Click **Change adapter settings**.

   3) Right-click the Local Area Connection and select **Properties**.

   4) In the **Local Area Connection Properties** window, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

   5) Make sure that **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected.

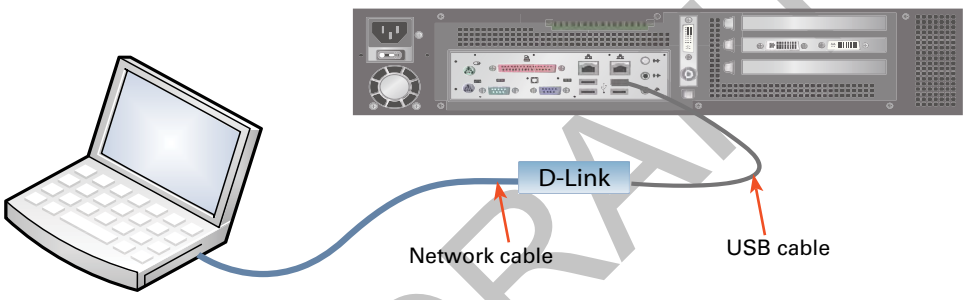
3. Disable any firewalls and all virus, ad ware, or spyware detection software running on the laptop.



Step 2. Connect Laptop to 3VR Appliance

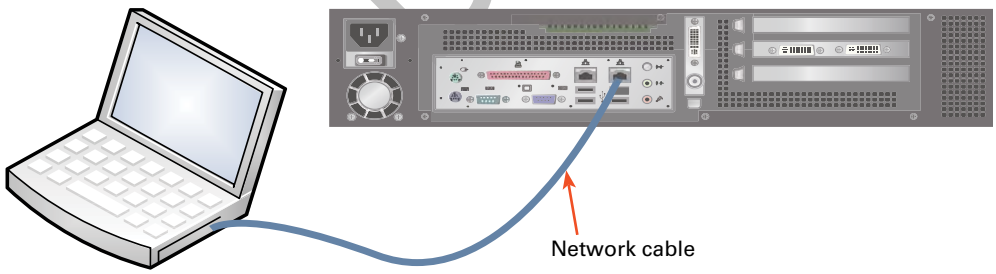
1. Connect your laptop to the 3VR appliance using one of the following methods:

   Laptop and D-Link Network Adapter



DRAFT

   Laptop and Network Cable Connected to Secondary Ethernet Port



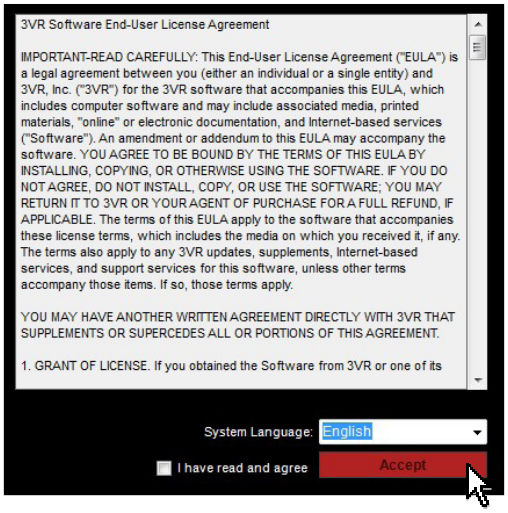
   Note: By default, the secondary Ethernet port is the right-hand port.

2. When the local network connection is recognized, the **Local Area Connection** icon in the laptop system tray displays a yellow triangle with an exclamation mark, reading **Limited/No Connectivity**. This means you have successfully connected.

6. ACCEPT EULA

6.1 Connected with Monitor, Mouse, and Keyboard

After the VMS Server restarts, the **End User License Agreement (EULA)** appears.



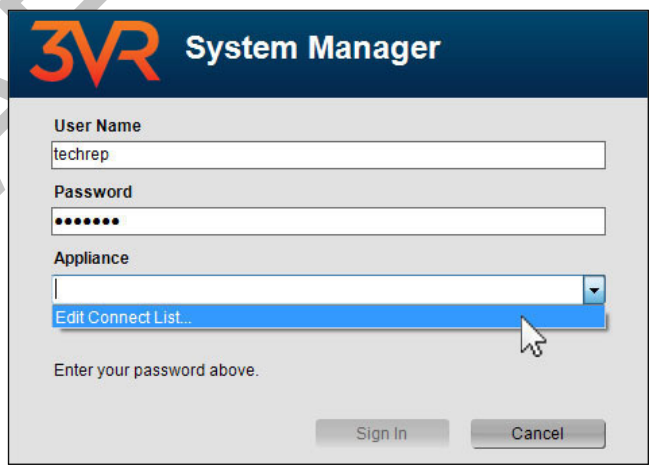
4. **For the 2000, 3000, 4000, and 5500-Series appliances only:** VisionPoint™ VMS is currently localized in English, Simplified Chinese, Latin American Spanish, Japanese, and Korean. Select the language you would like this system to use locally on the appliance from the drop-down menu.

> **Note**
> 1) Localization on the appliance itself is currently supported on all 3VR appliances.
> 2) You can also change the local language settings of a 3VR system in System Manager after initial installation. See chapter 3 for more information.
> 3) 3VR also localized remote client applications in above-named languages. The client applications automatically launch in a supported language based on the language settings of your PC.

5. **For all appliances:** Read the agreement carefully, and then check the box next to **I have read and agree** and click **Accept** to continue.

DRAFT

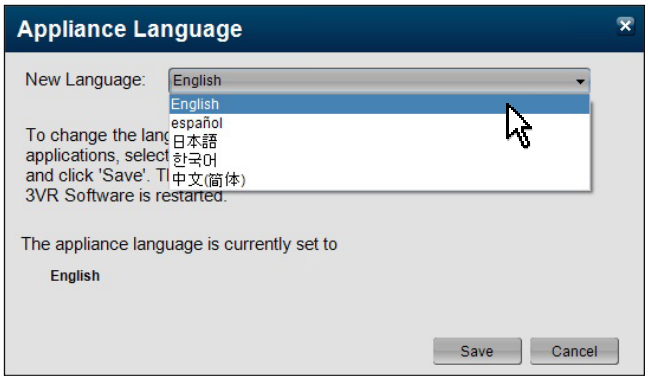
6.2 Connected with a Laptop



1. On the laptop, launch the System Manager client application (double-click the desktop shortcut or click **Start** > **Programs** > **3VR Client Software 8.1.x** > **3VR System Manager**).

2. At the sign-in screen, type the default technician user name and password:

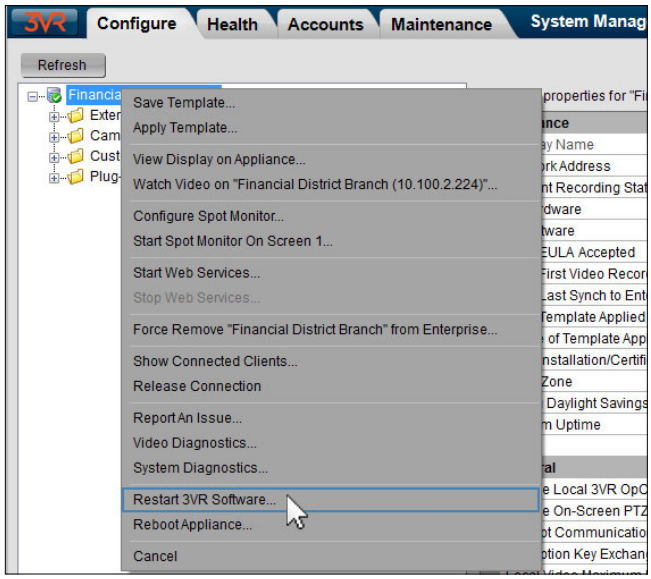
   - User Name: **techrep**
   - Password: **3MeDeee**



3. Click the drop-down arrow next to the **Appliance** box and select **Edit Connect List**.

4. In the **Appliance Language** dialog box, select the desired language from the drop-down menu and click **Save**.

5. For the settings change to take effect, you must restart the 3VR software. To do this, right-click on the system name, and then select **Restart 3VR Software**.



6. If you would like to use a different keyboard layout, see chapter 3.

7. In the **Edit Connect List** window, click the **Find Local Appliance** button.

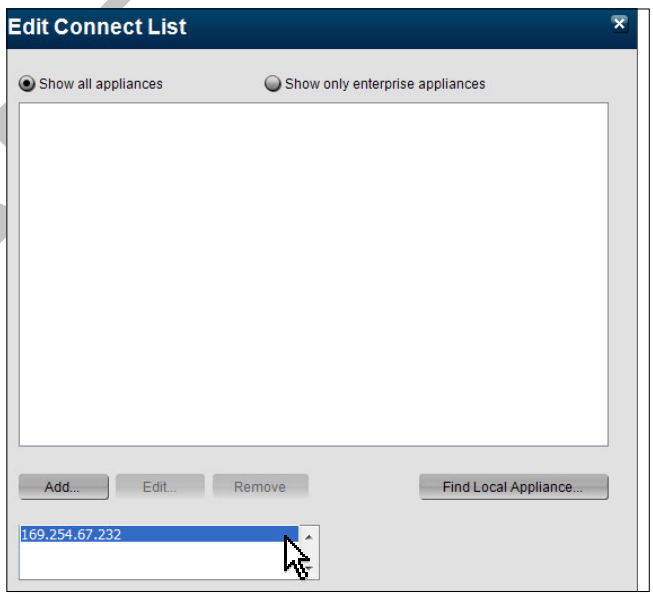
8. Wait 1-2 minutes. When the laptop recognizes the 3VR unit, the lower box populates with a single IP address in the format **169.254.xxx.xxx**. Click the IP address to highlight it.

9. Click the **Connect** button to sign in. The **End User License Agreement** appears.

10. Read the agreement carefully, and then check the box next to **I have read and agree.**

11. **1000, 2000, 2100, 3000, 4000, and 5500-Series appliances only:** VisionPoint™ VMS has been localized in English, Korean, Simplified Chinese, Japanese, and Latin American Spanish. Select a language for this appliance to use locally from the drop-down menu.

12. Click **Accept** to continue. You can change language settings in System Manager after initial installation.



DRAFT

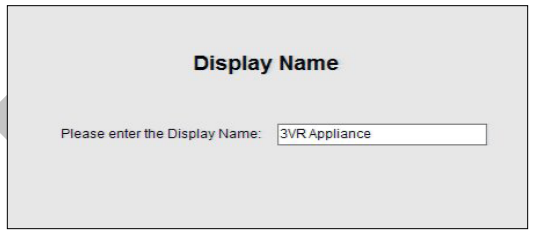
7. RUN THE 3VR APPLIANCE CONFIGURATION TOOL

After you accept the EULA, the appliance displays the 3VR Initial System Setup wizard. The wizard guides you through some basic system configuration tasks.

- Set the system display name.
- Configure network settings.
- Set the system time, date, and time zone.
- Enter the license key.
- Configure analog and IP cameras.
- Configure email settings.
- View the installation report.

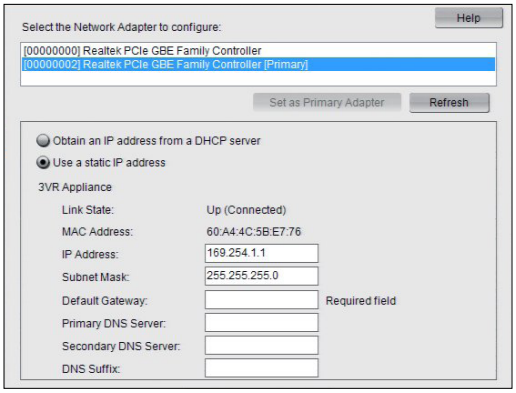
*** You must click Apply in each window to save settings before moving forward to the next screen.**

Step 1. Set the Display Name:



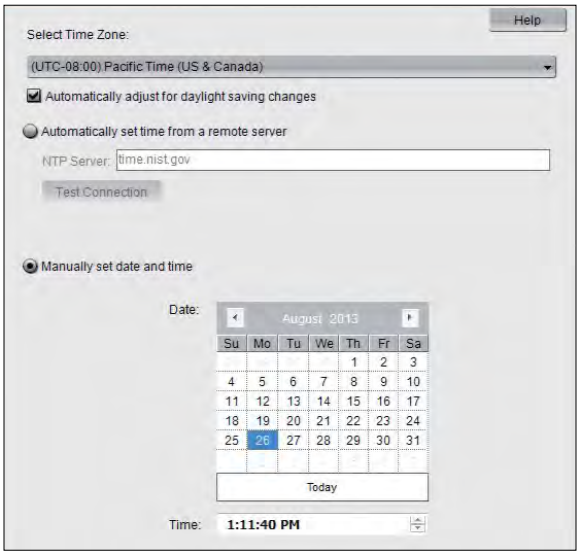
1. Enter the name of the 3VR Appliance as you would like it displayed within System Manager and OpCenter.
2. Click **Apply** and then **Next**.

Step 2. Configure Network Settings:



1. Select the network adapter labeled as Primary.
2. Enter the IP address, subnet mask, and default gateway as defined by your IT team.
3. Click **Apply** and then **Next**.

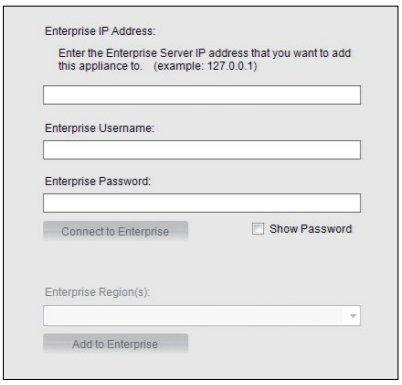
Step 3. Set Time Zone, Date, and Time:



1. Select the time zone where this appliance is installed from the drop-down list.
2. If applicable for the selected time zone, verify that automatically adjust the clock for Daylight Saving Time is selected.
3. If using an NTP server, select the radio button next to **Automatically set time from a remote server** and enter the NTP server in the **Server Address** text box.
4. If not using an NTP server, set the date and time.
5. Click **Apply** and then **Next**.

DRAFT

Step 4. Add System to Enterprise (Optional):



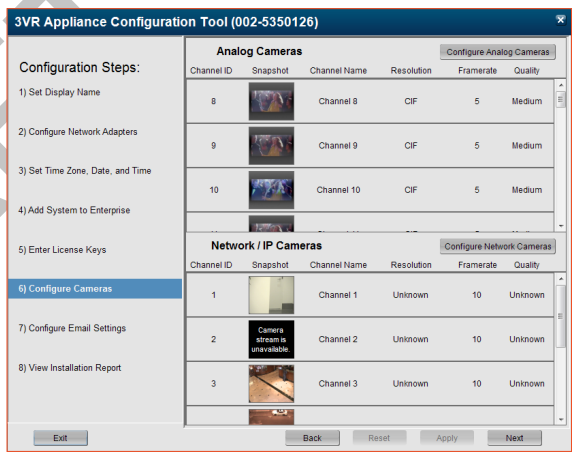
1. Enter the network address of the Enterprise you wish to connect to.
2. Enter the username.
3. Enter the password and select **Connect to Enterprise**.
4. Select the region this appliance should belong to (optional) and click the **Add to Enterprise** button.
5. Click **Apply** and then **Next**.

Step 5. Enter the License Key:

1. Add the license key for this unit.
2. Click **Apply** and then **Next**.

Step 6. Configure Cameras:

The Configure Cameras screen allows you to configure both network and analog cameras.

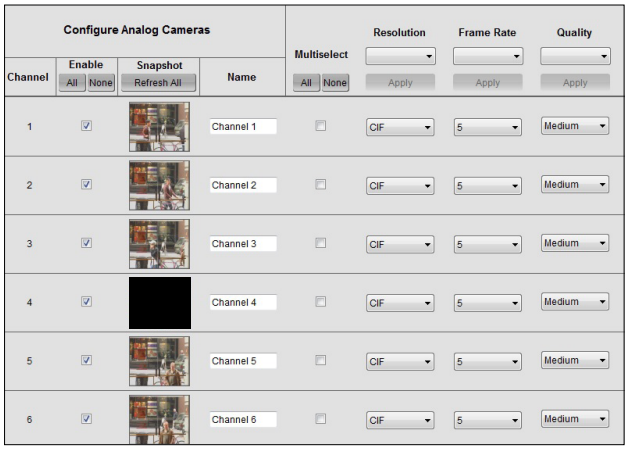


1. To configure analog cameras, click the **Configure Analog Cameras** button.
2. To configure network cameras, click the **Configure Network Cameras** button.

DRAFT

Configure Analog Cameras

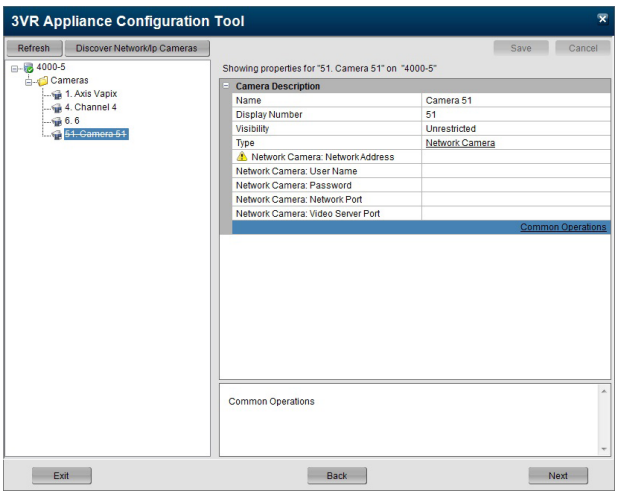
If the system is an NVR, there will be no analog cameras listed. A black box next to a camera indicates the system is not receiving a feed from the camera or camera settings need adjusting. Check all camera connections.



1. Enable cameras by selecting the check box or selecting the **All** button under **Enable**
2. Enter the display name of the camera.
3. Adjust resolution
4. Adjust frame rate
5. Adjust video/image quality
6. Click **Apply** and then **Next**.

Configure Network Cameras

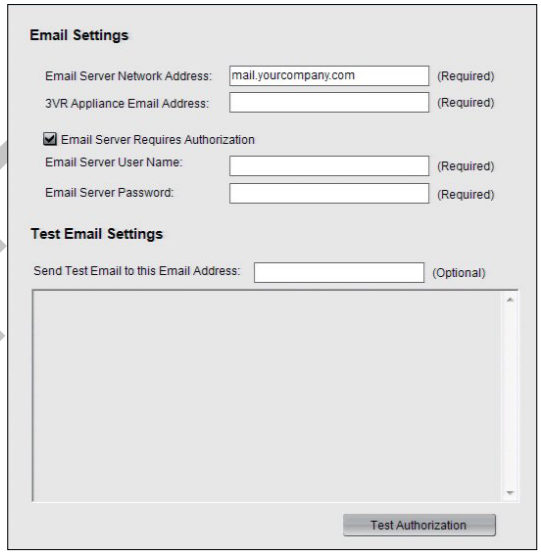
1. Click **Discover Network/IP Cameras** to have the 3VR Appliance look for available network/IP cameras. Please refer to Chapter 5, Section 6.2 for instructions on how to use this feature.



> **Note**
>
> After you complete the configuration, you can manually add a camera.
>
> - Right-click the camera folder and choose **Add Camera**. This will add a new, unconfigured camera channel to the list.
> - Select the new channel to configure the camera.

Step 7. Configure Email Settings

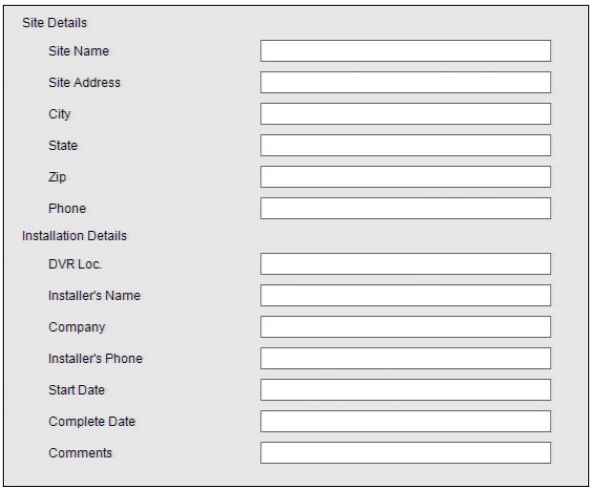
1. Enter the address of the email server to be used.
2. Enter the email address for the Appliance
3. (Optional)Check the box If your email server requires authentication.
4. Enter the email username.
5. Enter the email password.
6. (Optional) Enter the email address for a recipient of test email and then click **Test Authentication**.
7. Click **Apply** and then **Next**.



DRAFT

Step 8. View Installation Report

In addition to displaying the final setup information from the previous steps, you can use the Installation Report to label that information with specifics, such as site name and address, when the system was installed, where the DVR is physically located, installation date, and physical location of the 3VR Appliance. This step is optional.



Step 9. Successful Configuration and 3VR Appliance Reboot

Upon successfully completing configuration, a Congratulations message appears and indicates the software has been configured correctly. At this time, you need to restart the 3VR Appliance to commit these settings.

1. Click **Save** and **Restart System** to begin the reboot process. A message pops up warning that the system is about to be rebooted.

2. Click the **Reboot** button to move forward with restarting the system.

DRAFT

DRAFT

CHAPTER 2

VMS/Enterprise Server Software Installation

1. INSTALLATION PREREQUISITES 47
   - 1.1 Installation Restrictions 47
   - 1.2 System Requirements 47
   - 1.3 Obtain System License Key (If Applicable) 47
   - 1.4 Bring Required Items to Installation Location 48
2. INSTALL MICROSOFT .NET FRAMEWORK 4.X 48
3. INSTALL AND CONFIGURE MYSQL OR MSSQL 50
   - 3.1 Download MySQL 50
   - 3.2 Install MySQL 50
   - 3.3 Enable .NET Framework 4.x 54
   - 3.4 Install SQL Server 2012 56
   - 3.5 Configure SQL Server 2012 59
4. INSTALL 3VR VISIONPOINT™ VMS SERVER/ENTERPRISE SERVER SOFTWARE 61

DRAFT

DRAFT

1. INSTALLATION PREREQUISITES

Reference
This chapter describes how to install and configure VisionPoint™ VMS server and Enterprise server on third-party hardware **only**. If you are installing a 3VR appliance, please refer to chapter 1 of this guide.

1.1 Installation Restrictions

- For 3VR VisionPoint™ VMS to operate successfully, install only one instance of VisionPoint™ VMS on any one Windows system.
- A "sleeping" or "hibernating" Windows system cannot record video. Be sure to disable sleep and/or hibernation power options on your system for consistent recording. Please see your Windows documentation for more information about power options.
- System updates to Windows or to third-party applications can cause system reboots and downtime. These reboots interrupt video recording. Consider adjusting your system update settings to minimize these interruptions.

1.2 System Requirements

Go to the 3VR Partners Support Portal and review the *Supported Operating Systems* document for information regarding the system requirements for using 3VR VisionPoint™ VMS.

http://partners.3vr.com/

In order for VisionPoint™ VMS to function, you will first need to install Microsoft .NET Framework 4.x and MySQL Version 5.6 or MSSQL 2012 or later. Prior to heading to the installation site, ensure that either the server already has these pieces of software installed or you will be able to download the correct installation files on-site. If you will not have Internet access on the server at the installation site, download the correct versions and bring them with you. You will find instructions for downloading and installing the proper versions of Microsoft .NET Framework 4.x and MySQL Version 5.6 or MSSQL 2012 in the sections below.

Note
3VR VisionPoint™ VMS Server 8.1.x is not supported on X-Series appliances.

DRAFT

1.3 Obtain System License Key (If Applicable)

At the time of purchase, you will be issued a license key to enable IP cameras, facial surveillance, and any other advanced features on the VMS server. You must enter this system license key before you can configure these features. If you do not have access to the order confirmation email, you can look up the license key by serial number on the 3VR Support Portal:

1. Go to the 3VR Support Portal (http://partners.3VR.com) and sign in with your company's Support Portal login.
2. Once signed in, click **Obtain System License Key**. (Alternatively, you can go directly to the key retrieval page with this link: http://3VR.com/license. This page can be accessed by most web-enabled phones.)
3. Enter the requested information, including the system serial number, then click the **Find System License** button.

1.4 Bring Required Items to Installation Location

The following items are required for installation:

1. A Windows system meeting the server requirements listed in section 1.2 above
2. Monitor, mouse, and keyboard (Note that you can also install VisionPoint™ VMS by logging into the server using remote desktop. Please refer to your remote desktop software's documentation for more information about this process.)
3. Serial Number and License Key for the system. (See section 1.3 for more information about License Keys. You can also enter the key in System Manager after initial setup, if necessary. See chapter 3 for information about entering a license key after installation.)
4. 3VR VisionPoint™ VMS Installer Package (If you will have Internet access at the installation site, you can download this directly onto the server on-site. Otherwise, please download it from the 3VR Partner Support Portal ahead of time and bring it with you.)
5. Microsoft .NET Framework 4.x and MySQL version 5.6 or MSSQL 2012 or later. (Please refer to "Install Microsoft .NET Framework 4.x" on page 48 and "Install and Configure MySQL or MSSql" on page 50 of this chapter for more information about how to download these free pieces of software. If you will not have Internet access on the VMS server at the installation site, remember to download these necessary programs beforehand.)

2. INSTALL MICROSOFT .NET FRAMEWORK 4.X

Both 3VR VisionPoint™ VMS and MySQL (which is necessary to run VisionPoint™ VMS) require the Microsoft .NET Framework 4.x to function properly.

Note
To check if Microsoft .NET Framework 4.x is installed on your Windows system, select *Programs and Features* from the *Control Panel* and verify that *Microsoft .NET Framework 4 Extended* and *Microsoft .NET Framework 4 ClientProfile* entries are listed.

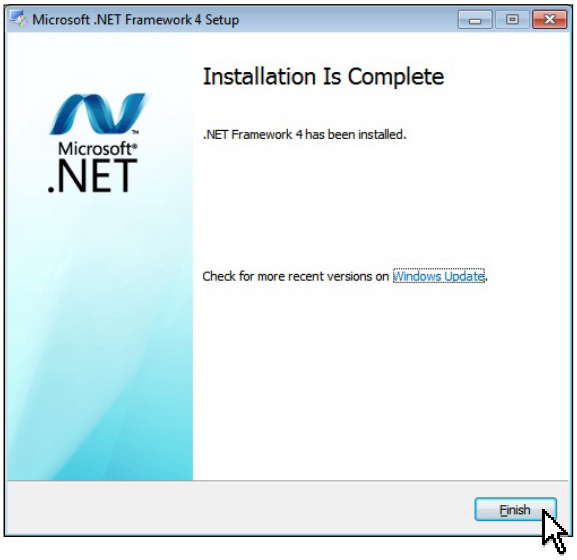
If Microsoft .NET Framework 4.x is not present on the VisionPoint™ VMS server, you must download and install it before proceeding. Begin by connecting to the server either with a monitor, mouse, and keyboard, or using Remote Desktop, then:

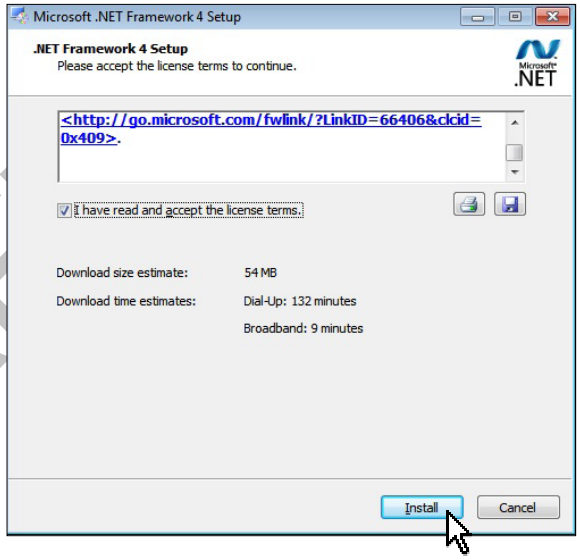
1. Open a web browser and go to the Microsoft .NET 4.x download page: http://www.microsoft.com/en-us/download/details.aspx?id=17851.
2. Click **Download**.
3. When the download completes, double-click **dotNetFx40_Full_setup.exe** to run the installation wizard.
4. Read the .NET license agreement and click the check box next to "I have read and accept the license terms" to accept the terms.
5. Click **Install**.

DRAFT

6. Wait while .NET is installed. This process may take up to 5 minutes.

7. When the installation is complete, click **Finish**.





DRAFT

3. INSTALL AND CONFIGURE MYSQL OR MSSQL

You will need to install either MySQL or MSSQL on your server to run VisionPoint™ VMS. The following sections detail the process for installing MYSQL or MSSQL, and also describe how to configure the database. Note that neither MySQL or MSSQL will function without Microsoft .NET Framework 4.x, so you must complete the installation of Microsoft .NET Framework 4.x as described in section 2 above before continuing with this section.

3.1 Download MySQL

1. Open a web browser and go to the MySQL download page: http://www.mysql.com/downloads/installer/.

2. Download the latest version of MySQL Community Server 5.6.x.

> **Note**
> To check if MySQL is installed on your Windows system, select *Programs and Features* from the *Control Panel* and verify that *MySQL Server 5.6* is listed.
>
> The minimum supported MySQL Server version is 5.6. The instructions and screenshots in this document are based on version 5.5.29.

3.2 Install MySQL

Follow these steps to install MySQL on the VisionPoint™ VMS server.

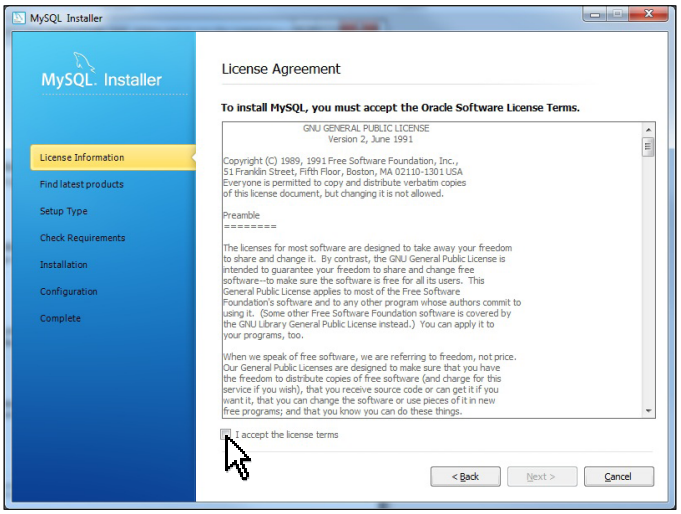
1. Double-click **mysql-installer-community-5.6.xx.x.msi** to begin the installation process.

2. At the **Welcome** screen, click **Install MySQL Products**.

DRAFT

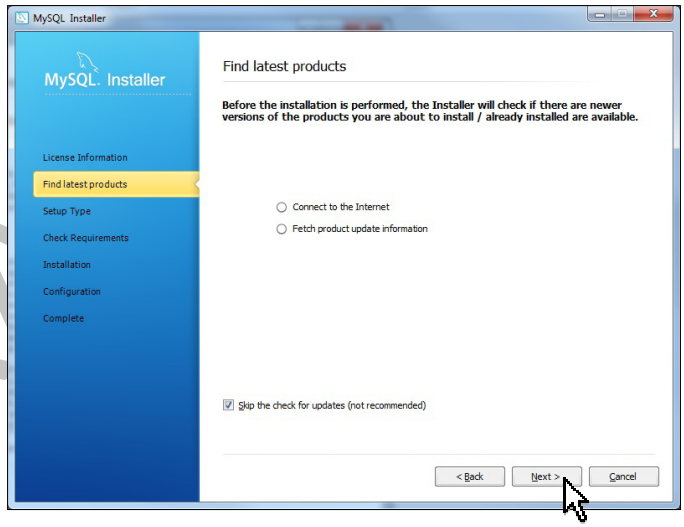
3. The wizard displays the MySQL **License Agreement.** Read the agreement, and then click **I accept the license terms.**

4. Click **Next.**



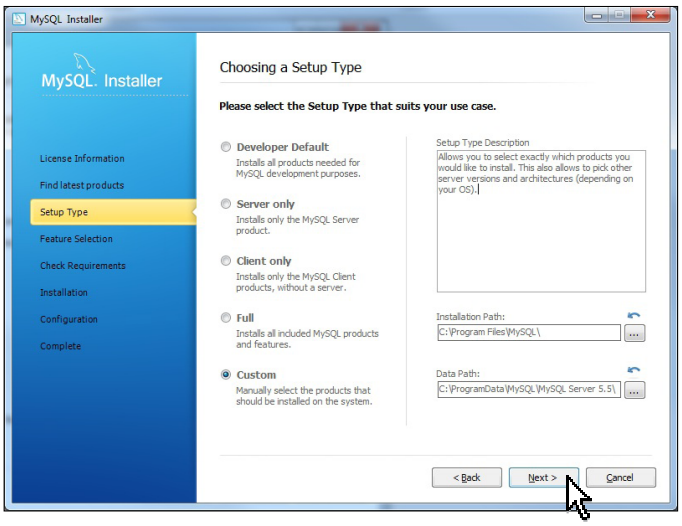
5. In the **Find Latest Products** screen, click **Skip the check for updates**.

6. Click **Next.**



7. Select the **Custom** setup type.

8. Click **Next.**



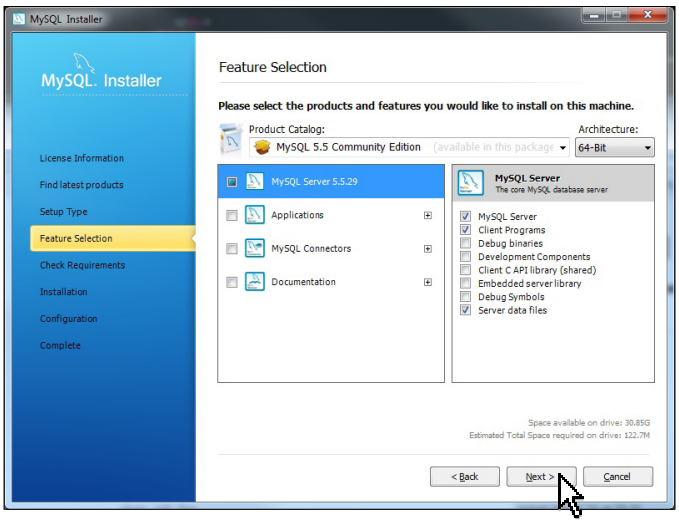
DRA

9. By default, all of the options are selected in the **Custom Setup** screen.

   In the **MySQL Server 5.6.XX** tab, deselect **Debug binaries**, **Development Components**, and **Debug Symbols**.

   Click the check box next to **Applications**, **MySQL Connectors**, and **Documentation** to deselect all items in those tabs.

10. Click **Next**.

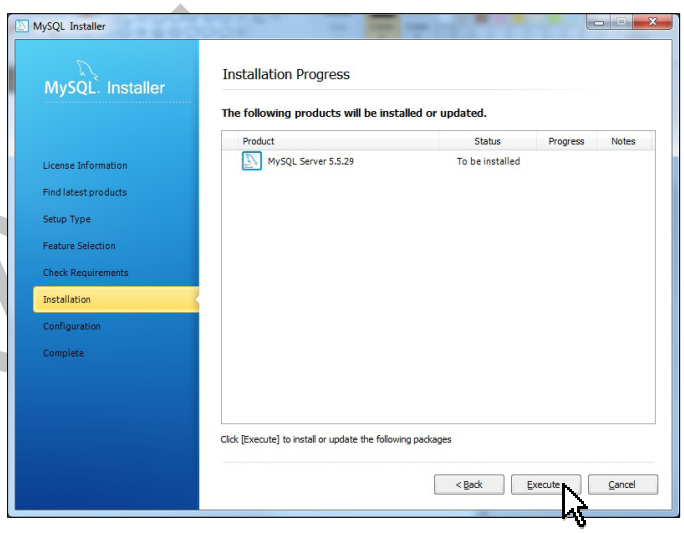


11. At the **Check Requirements** screen, click **Next**.

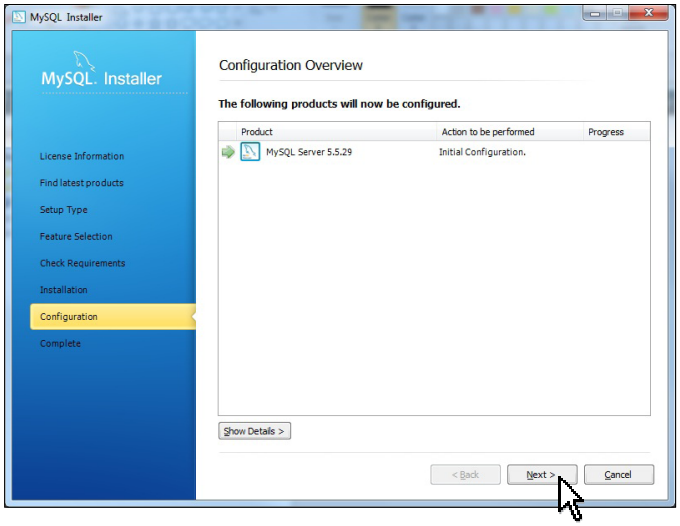
12. Click **Execute** to begin the installation.

13. Wait while MySQL server is installed.

14. When the installation is complete, click **Next**.



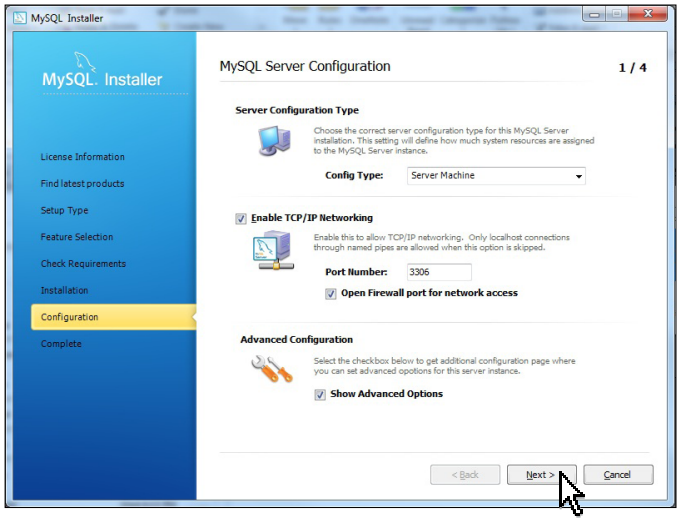
15. The **Configuration Overview** screen shows the software you just installed. Click **Next** to proceed with the configuration.



16. In the **MySQL Server Configuration** screens:

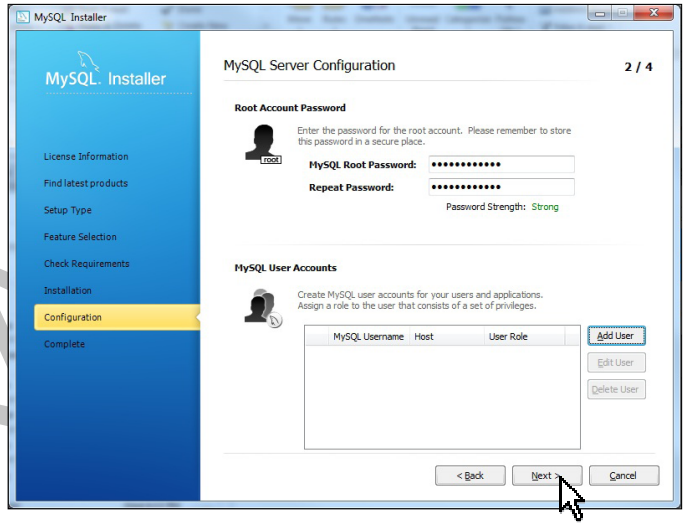
    - Open the **Config Type** drop-down menu and select **Server Machine**.
    - Leave **Enable TCP/IP Networking** checked.
    - Leave **Open Firewall port for network access** checked.
    - Check **Show Advanced Options**.

17. Click **Next**.

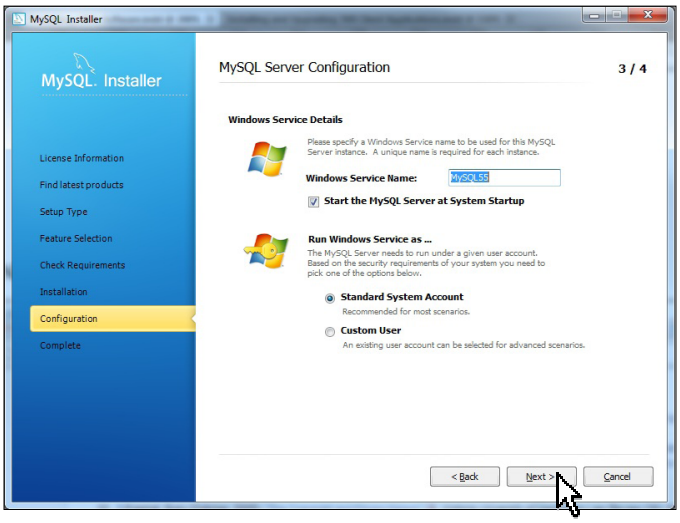


18. In the following screen, create a secure **MySQL Root Password**.

19. Click **Next**.



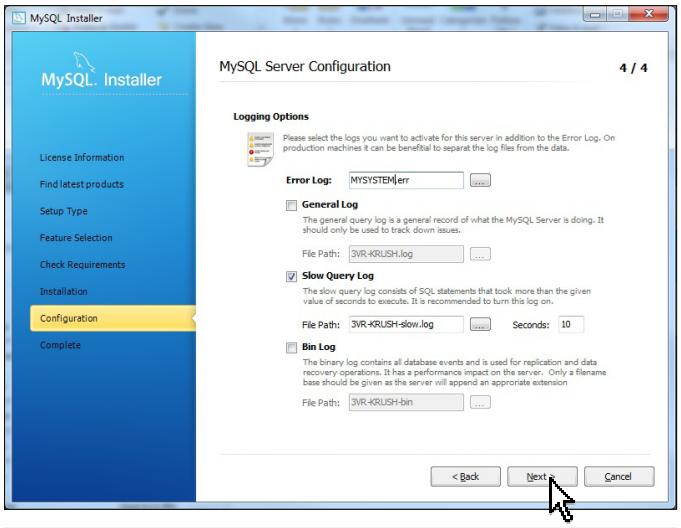
20. Click **Next** to accept the default Windows service settings.



DRA

21. Leave the **Logging Options** at their default values.

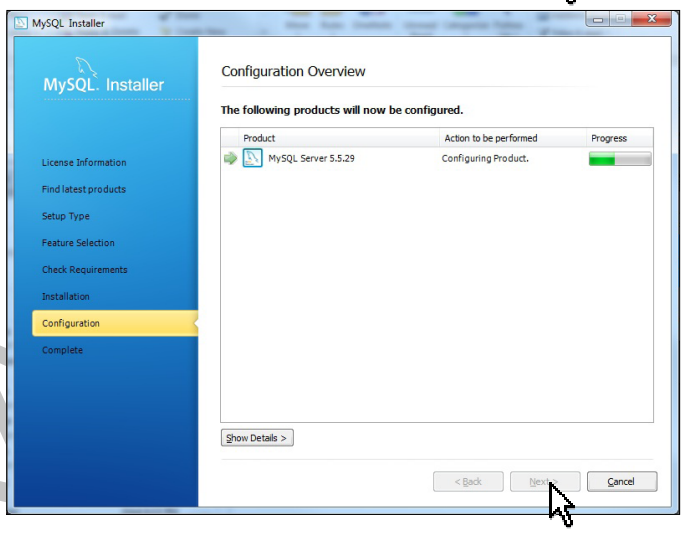
22. Click **Next**.



23. Wait while MySQL is configured.

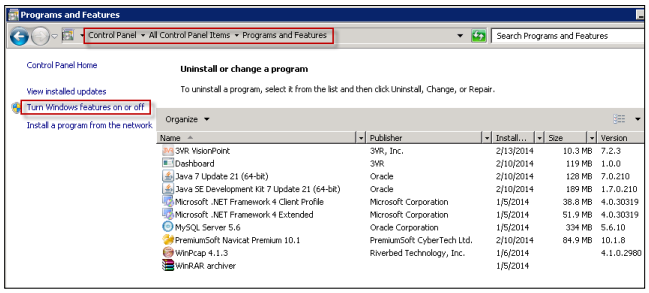
24. When the configuration is complete, click **Next**.

25. In the following screen, click **Finish** to close the wizard.



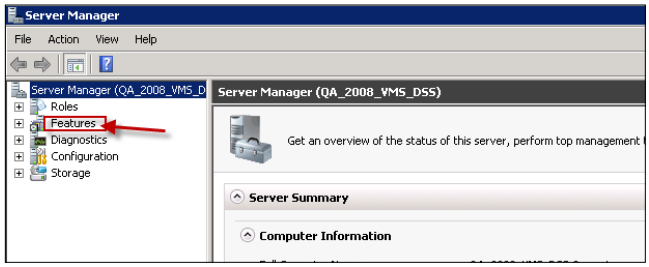
3.3 Enable .NET Framework 4.x

1. Go to **Control Panel** and open **Program and Features**, and then click **Turn Windows features on or off**.



DRA

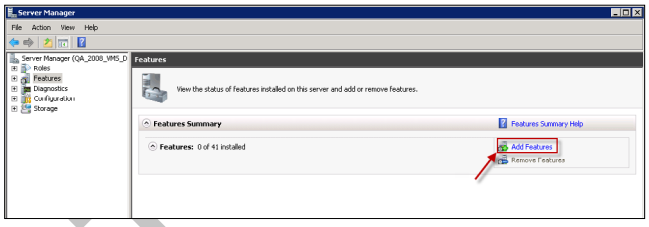
2. At the **Server Manager** screen, click **Features**.



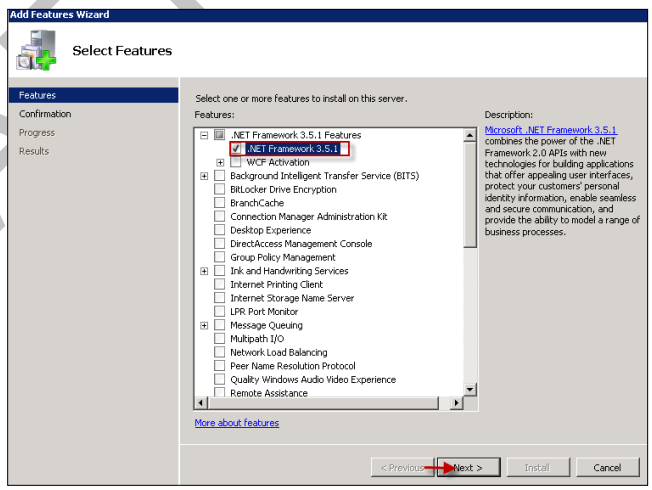
Note

.NET Framework 4.0 is a prerequisite on Window Server 2012. Please follow the steps below to enable it before starting the SQL Server 2012 installation. (If .NET Framework 4.x is installed/enabled, you can skip the rest of this section and go to "Install SQL Server 2012" on page 56.)

3. Click **Add Feature**.

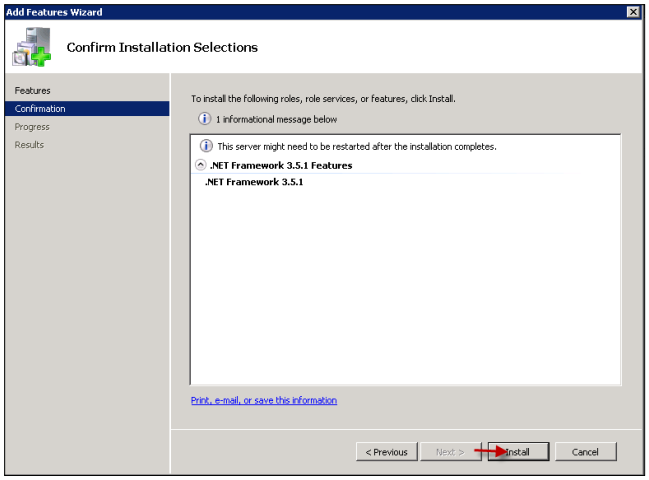


4. Expand **.NET Framework 4.x Features** and select **.NET Framework 4.x**, then click the **Next** button.



5. Click the **Install** button in the Confirm Installation Selections screen.

6. When installation is completed, click the **Close** button.



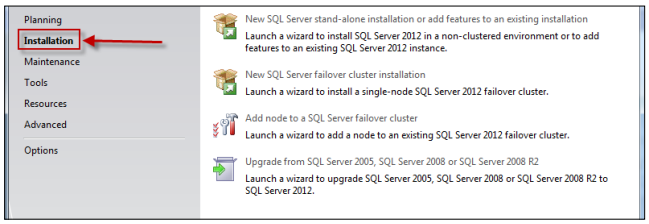
DRAFT

3.4 Install SQL Server 2012

Follow these steps to install SQL Server 2012 on the VMS server.

1. Double-click on the SQL DVD auto run or run the **setup.exe** file on the root of the DVD or **iso** image.

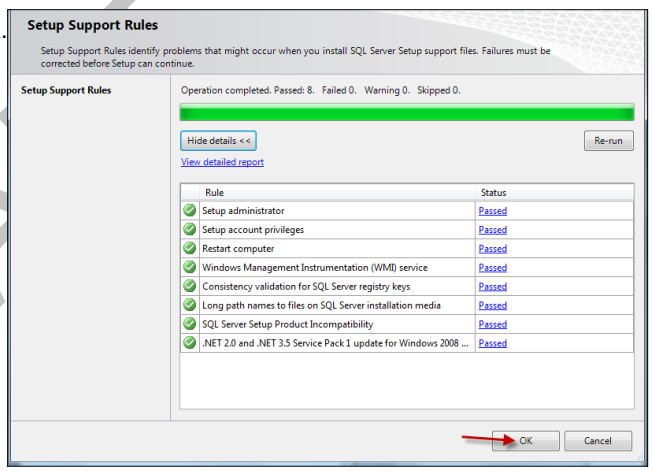
2. When the menu appears, click on **Installation**.



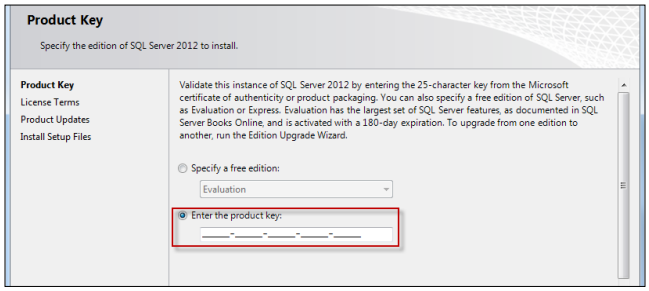
3. Click on **New SQL Server stand-alone installation or add features to an existing installation**.

   - Note: The second option is for configuring a failover-cluster. In our case, we are focusing on setting up a replication model.

4. SQL Server 2012 Setup checks the Setup Support Rules. Click **OK**.

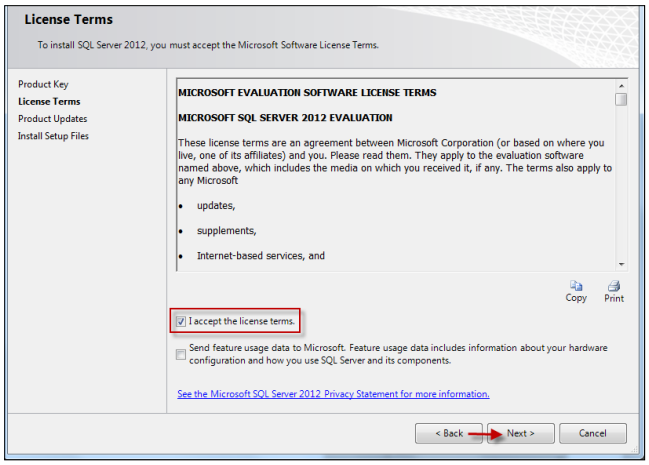


5. Enter your **Product Key** (if not pre-populated) and click **Next**.

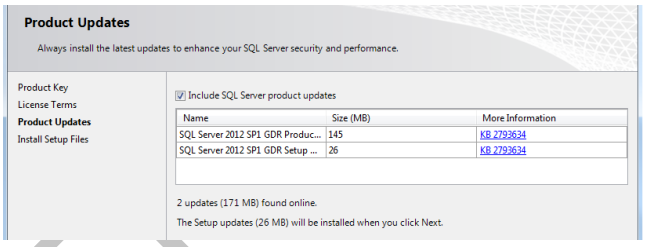


DRAFT

6. Check **I accept the license terms** and click **Next**.

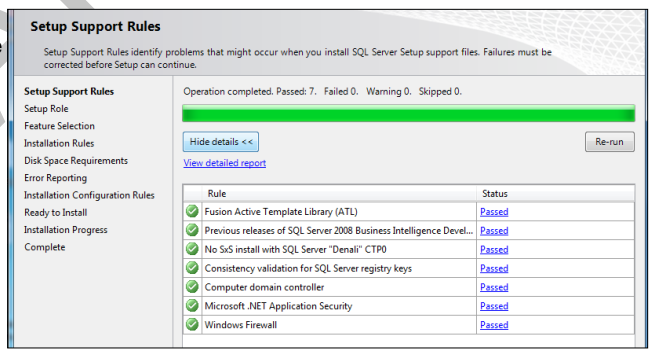


7. Setup identifies additional product updates, this depends on available updates during the time this procedure is executed. Click **Next** to continue.



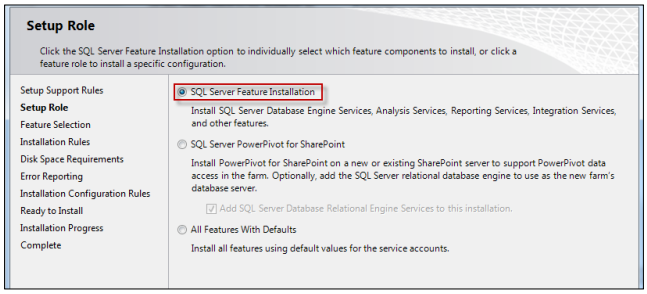
8. The setup downloads the updates. Once complete, click on **Install**.

9. At the **Setup Support Rules** screen, most of the items should be marked as Passed, but it is not uncommon for you to receive a warning about the Windows Firewall. Click **Next** to proceed.



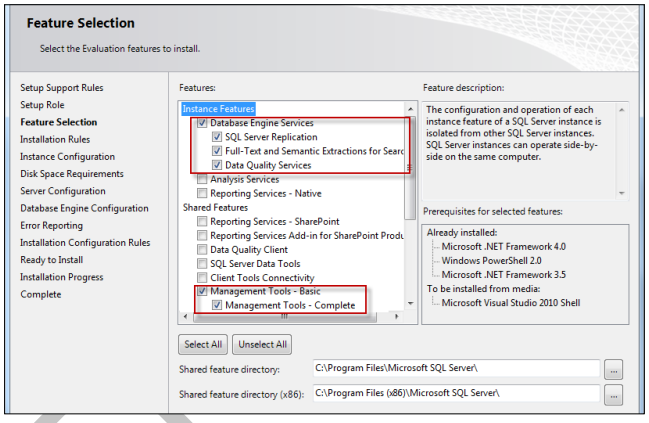
DRAFT

10. Select the **SQL Server Feature Installation** option and click **Next**.

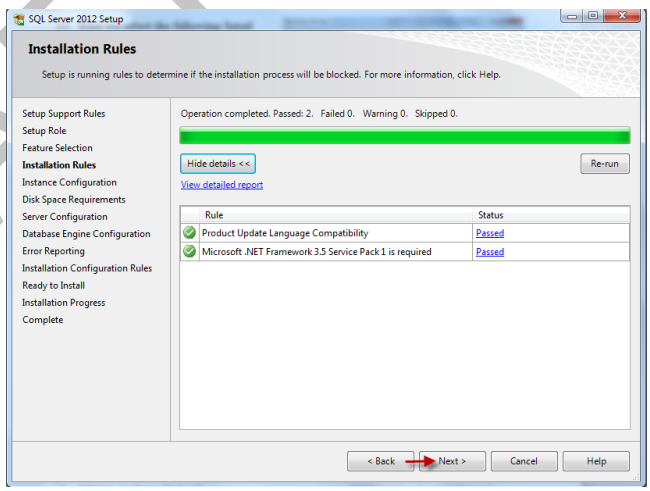


11. Select the following listed features. You can always select additional features if required or re-run the SQL setup to add additional options.

- **Database Engine Services**
- **SQL Server Replication**
- **Full-Text and Semantic Extractions for Search**
- **Data Quality Services**
- **Management Tools – Basic**
- **Management Tools – Complete**



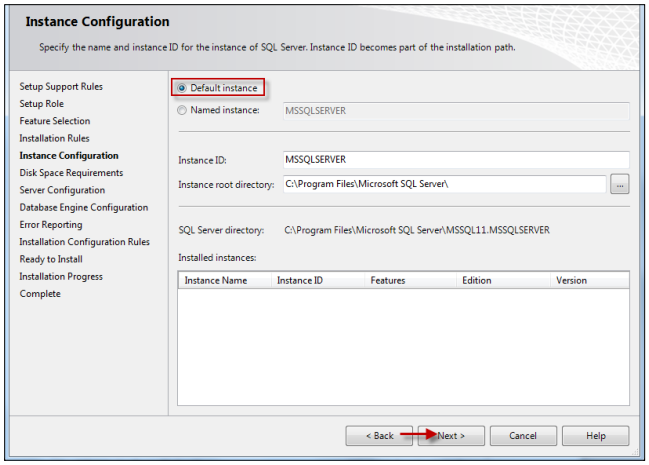
12. Click **Next** once the Installation Rules step is completed.



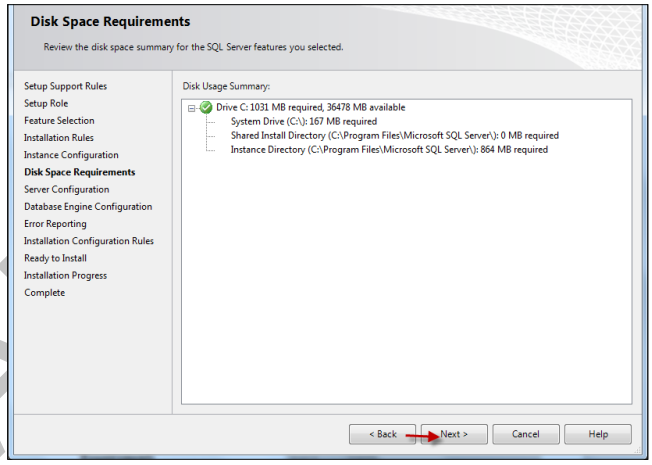
DRAFT

3.5 Configure SQL Server 2012

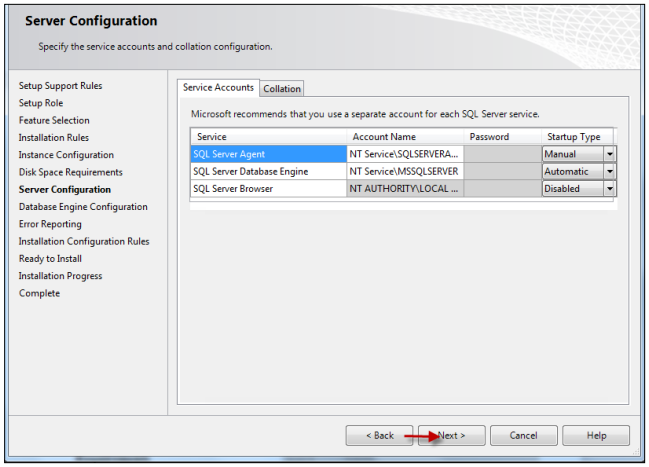
1. Select the **Default instance** and click **Next**.



2. At the **Disk Space Requirements**, click **Next**.

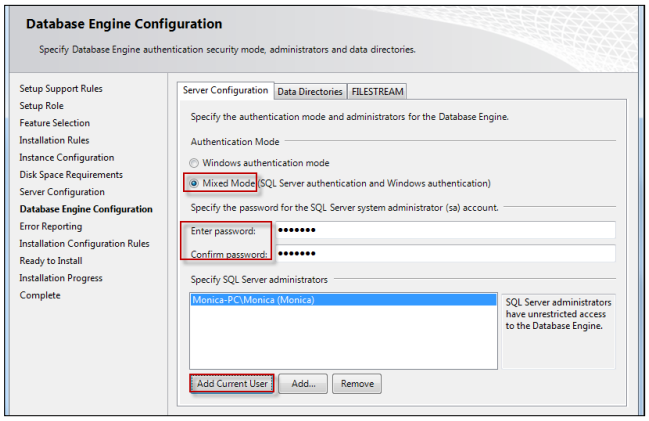


3. At the **Server Configuration**, click **Next**.

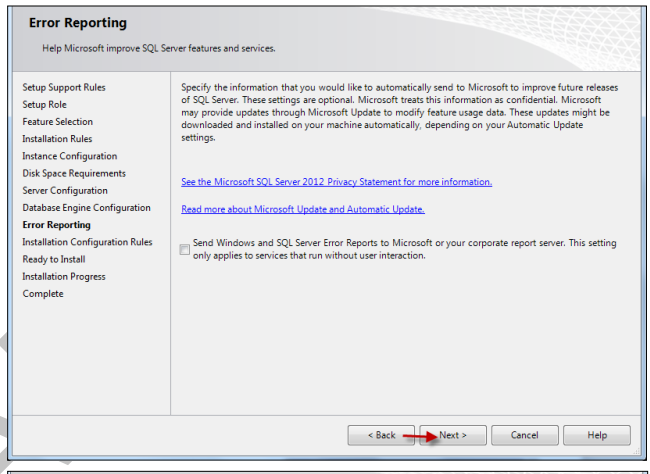


DRA

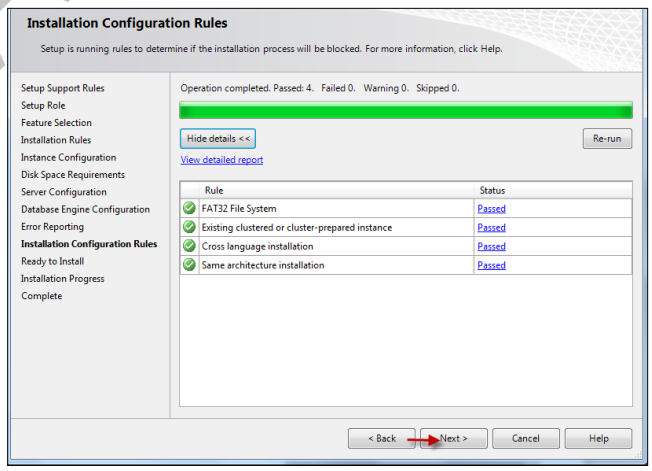
4. Select **Mixed Mode**, enter "**Password**" and "**Confirm Password**" for the "**sa**" account, click on **Add Current User** and click **Next**.



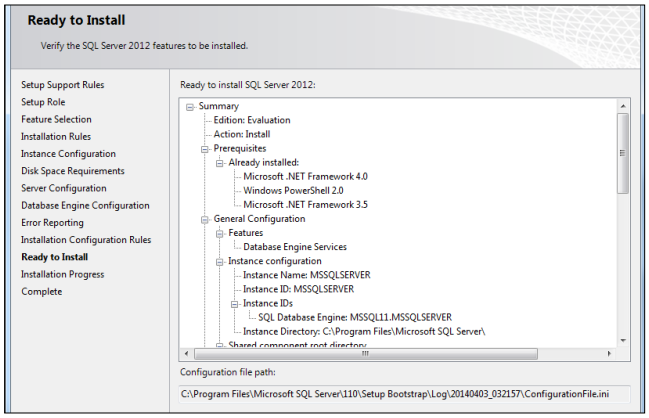
5. Check if you wish to **Send Windows and SQL Server Error Reports to Microsoft** and click **Next**.



6. At the **Installation Configuration Rules**, click **Next**.

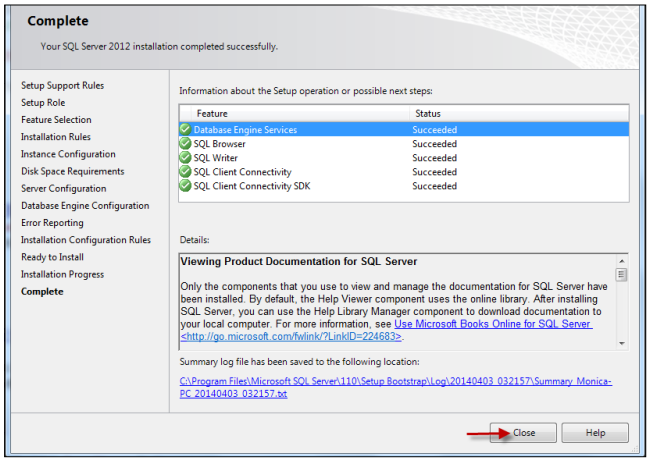


7. At the **Ready to Install** step, click **Install**.



DRA

8. When everything is installed, the wizard displays the status message **Succeeded** for each feature. Click **Close** and follow with a reboot (optional).



4. INSTALL 3VR VISIONPOINT™ VMS SERVER/ENTERPRISE SERVER SOFTWARE

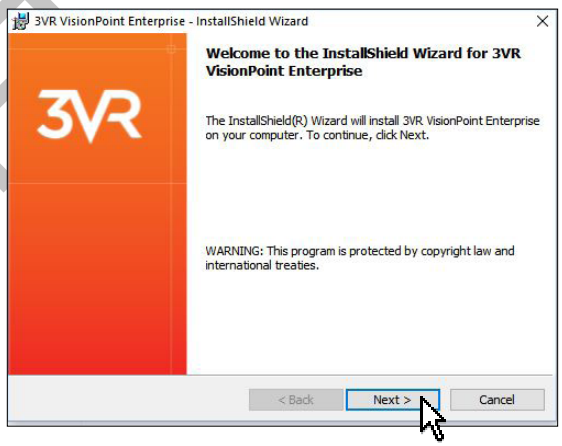
DRAFT

Follow these steps to install 3VR VisionPoint™ VMS server software, including Enterprise servers, on third-party hardware.

1. Double-click the VisionPoint installer .exe to run it. The VisionPoint installer is different for Enterprise servers and VMS servers. Be sure to use the correct installer:

   - VMS Servers: **Installer-VisionPoint-8.1.x.xxxxx.exe**
   - Enterprise Servers: **Installer-VisionPointEnterprise-8.1.x.xxxxx.exe**

2. At the InstallShield Wizard Welcome screen, click **Next**.

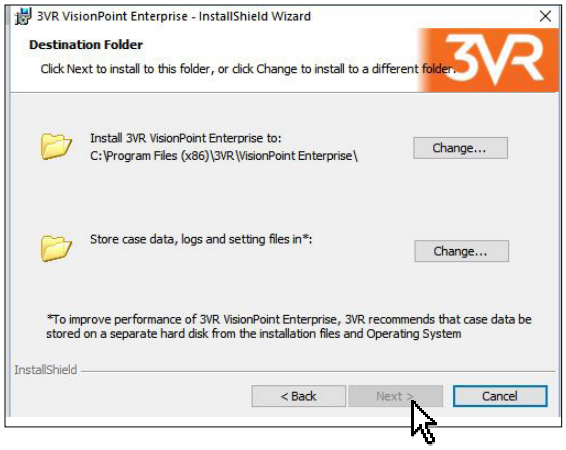


3. The InstallShield Wizard displays the **3VR Software End User License Agreement**.

   Read the agreement carefully, and then click **I accept the terms in the license agreement**.

4. Click **Next**.

5. In the **Destination Folder** screen:



- Specify the directory where the VisionPoint™ software should be installed, or leave at the default (**C:\Program Files\3VR**).
- Specify where video (for standalone VMS servers), case data, logs, and setting files should be installed. For best performance, 3VR recommends selecting a different drive or partition to host these files than the one hosting the software.

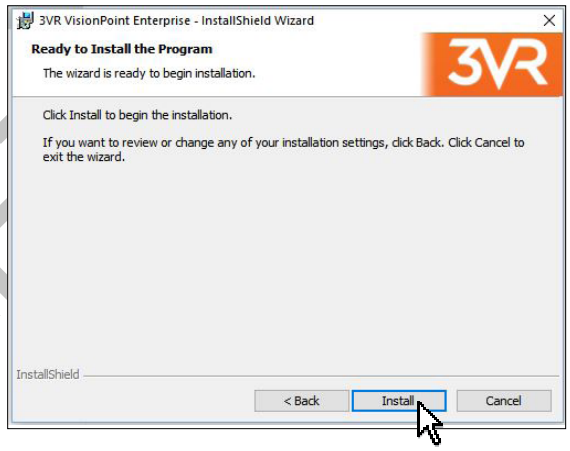
  VisionPoint™ supports using a mapped network drive for video storage. To use a network drive ensure:

  - All applicable machines are part of the same domain/workgroup with sharing enabled
  - The applicable system has full access to the network drive

  For more information about setting up and using network drives, please see your Windows documentation.

- Click **Next**.

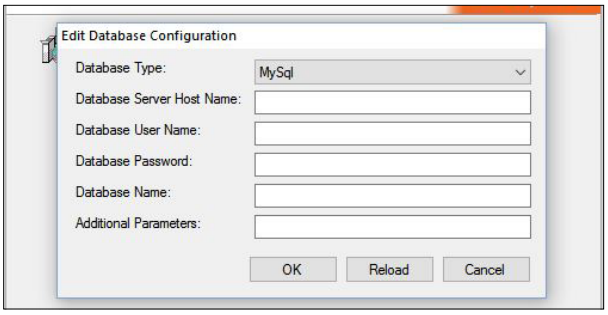
6. Click **Install** to begin the installation.



DRAFT

7. When the **Edit Database Configuration** prompt appears, configure the connection settings for the database:

   - **Database Server Host Name**: type the IP address of the MySQL server (if installed on the same machine, enter "localhost").
   - **Database User Name**: set this to "root"
   - **Database Password**: password you created in the previous section
   - **Database Name**: enter a name for the database, such as "3vrdb". Please note that databases on the same instance of a MySQL installation must have a unique database name.



8. Click **OK**.

9. When installation is complete, click **Finish** to exit the wizard.

Shortcuts for *3VR System Manager* and *3VR OpCenter* should be available on the desktop after installation.

Note

To connect to the 3VR VisionPoint™ VMS server using client applications locally on the system, specify **localhost** for the appliance, rather than using the IP address of the VMS server. When connecting remotely from another Windows system, continue to use the IP address of the VMS server as normal.

CHAPTER 3
Basic System Manager Configuration

1. CONFIGURE BASIC SETTINGS IN 3VR SYSTEM MANAGER 65
   - 1.1 Launch System Manager (Users Connected to a 3VR Appliance) 65
   - 1.2 Log in to System Manager (Users Connected to Third-Party Hardware) 65
   - 1.3 Edit VMS Server Display Name 66
   - 1.4 Edit Local Language Settings 67
   - 1.5 Configure Keyboard Input 67
   - 1.6 Enter System License Key (Optional) 68
   - 1.7 Edit Network Settings 69
   - 1.8 Edit Known Host Setting 70
2. CONFIGURE OUTGOING EMAIL SETTINGS 70
3. CONFIGURE EVENT AND VIDEO STORAGE SETTINGS 72
4. CONFIGURE SCHEDULES 73
   - 4.1 Recording Settings Schedule 73
   - 4.2 Peak and Off-Peak Bandwidth Use Schedule 74
5. INSTALL PLUG-INS 76
6. SET CERTIFICATION DATE 77
7. RUN THE 3VR INSTALLATION REPORT 77
   - 7.1 Searching for VMS Servers on an Enterprise Server 80
8. UPDATING DATE AND TIME SETTINGS 82
   - 8.1 Edit the Time Zone 82
   - 8.2 Edit the NTP Server 82
   - 8.3 Edit the System Date and Time 83
9. NEXT STEPS 83

DRAFT

DRAFT

1. CONFIGURE BASIC SETTINGS IN 3VR SYSTEM MANAGER

To complete initial system setup, you must log into System Manager 3VR's system configuration and maintenance application). Use System Manager to configure basic settings like VMS server display name, local language settings, and keyboard input.

1.1 Launch System Manager (Users Connected to a 3VR Appliance)

When the **Initial System Setup** wizard exits, users connected with a monitor, mouse, and keyboard will see the local sign-in screen.

> **Note**
> Users connected to a 3VR appliance with a laptop and network cable or D-Link network adapter may disregard this step, as System Manager launches immediately after you exit from the Initial System Setup wizard.

1. At the sign-in screen, type the default technician user name and password:
   - User Name: **techrep**
   - Password: **3MeDeee**

DRAFT

1.2 Log in to System Manager (Users Connected to Third-Party Hardware)

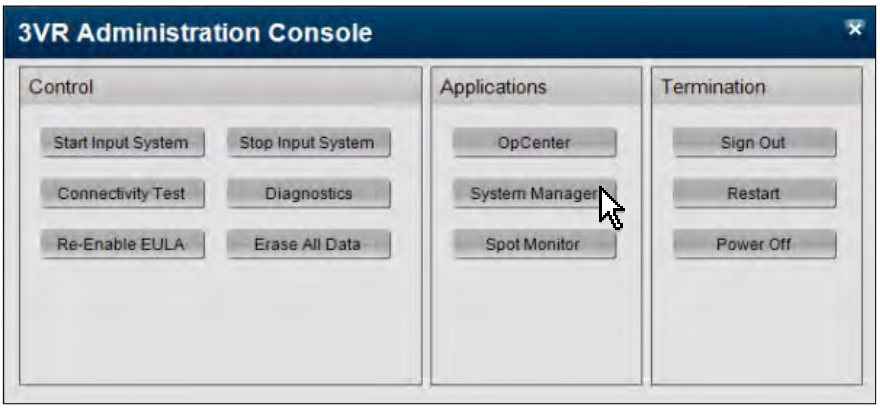
The steps outlined in this section must be performed locally on the VMS server itself. After you enter the VMS server's serial number, you may also choose to log in remotely using the client applications by entering the VMS server's IP address in the **Appliance** field instead of "localhost."

1. Double click on the shortcut on the desktop to launch System Manager.
2. At the local sign in screen, type the default technician user name and password:
   - User Name: **techrep**
   - Password: **3MeDeee**
3. Enter **localhost** for the appliance.
4. Click **Sign In**.

5. When prompted, enter the system's serial number and license key.

6. Click **OK**.

7. After signing in, the 3VR Administration Console appears.

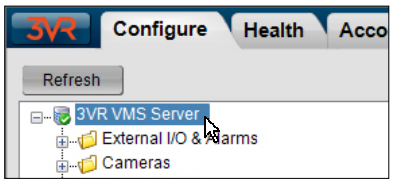


Click the **System Manager** button to launch System Manager.

1.3 Edit VMS Server Display Name

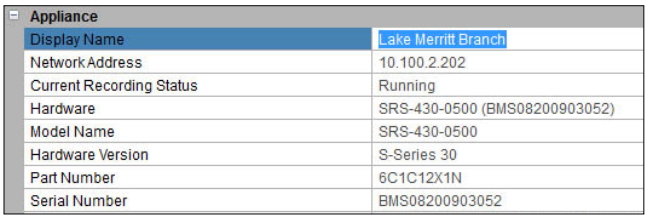
The **Display Name** of a VMS server appears in many places in OpCenter and System Manager. By default, the **Display Name** of a VMS server running on a 3VR appliance is set to "3VR VMS Server." Use the following steps to edit the display name of the server to reflect the customer name or location:

1. In the **Configure** panel of System Manager, click the system name in the left-hand panel. The system settings appear to the right.



2. Click the **Display Name** box.

3. Type a new name for the VMS server.



4. Click the **Save** button.

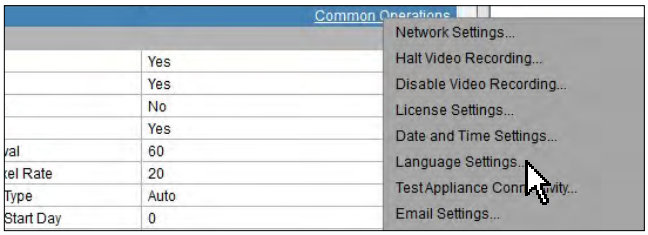
DRAFT

1.4 Edit Local Language Settings

All VMS servers can be configured to use English, Latin American Spanish, Korean, Japanese, or Simplified Chinese as the local language. To change this setting in System Manager:

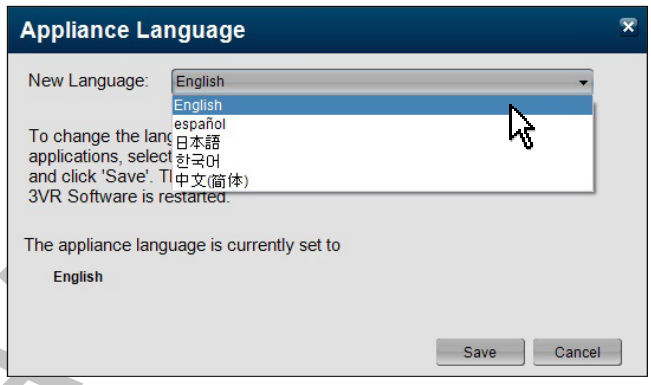
1. In the **Configure** panel of System Manager, click the system name in the left-hand panel to view the system settings. .

2. Click Common Operations, and then click **Language Settings**.



3. In the **Appliance Language** dialog box, select the desired language from the drop-down menu and click **Save**.

4. Restart the 3VR software



1.5 Configure Keyboard Input

If you have configured the system to use a language other than English, you can change the keyboard input mode to accommodate a different keyboard layout.

1. After restarting the system software, log back into System Manager. In the **Configure** panel, right-click the name of the VMS server and select **Reboot Appliance**.

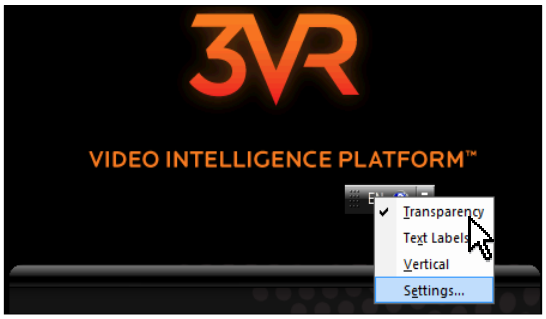
2. When the system starts up after the reboot, the Windows Language Bar appears. 3VR systems are pre-loaded with the following keyboard inputs:

   - Spanish
   - Japanese
   - Chinese, Simplified (PRC) - Microsoft Pinyin ABC input style
   - Chinese, Simplified (PRC) - Microsoft Pinyin New Experience input style
   - Korean

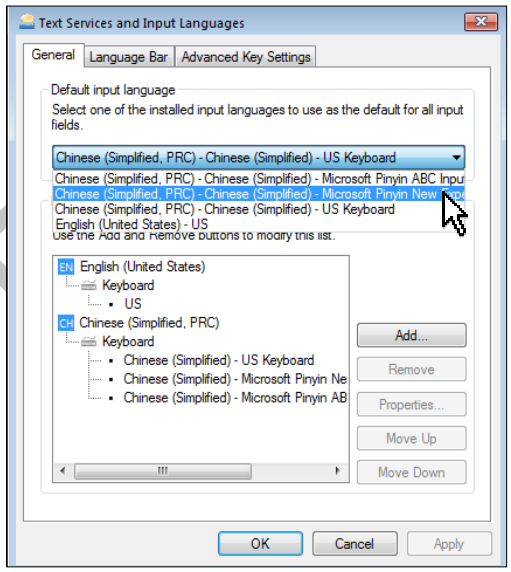
DRAFT

After completing the reboot in step one, the English keyboard input and the input corresponding to the currently selected local language are visible in the Windows Language Bar. You can add more keyboard inputs using the **Language Bar** settings dialog box. 3VR strongly recommends visiting Microsoft's support page for more information about keyboard settings.

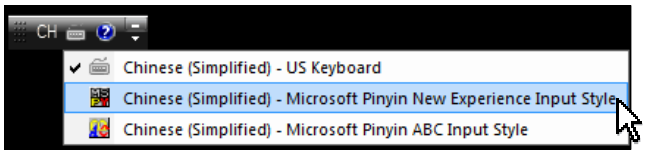
3. To change the keyboard input, right-click the **Language Bar** and then click **Settings**.



4. Select the preferred input language from the menu, and then click **OK**.



5. On the **Language Bar**, you can toggle between English and the selected alternate input style using your mouse.



1.6 Enter System License Key (Optional)

Certain features of 3VR's VisionPoint™ VMS require licenses before you can enable them. The list of licensed features includes:

Analytics: Facial Surveillance, Advanced Object Tracking, License Plate Recognition (after initial license capacity is exceeded), People Counting, etc.

- **IP Camera Expansion:** Enabling IP cameras on a 3VR appliance. HVR's have several IP channels included that do not need an additional license. IP cameras on NVR systems do not require a license key unless you add cameras beyond the initial camera count, for example, adding camera #17 on a 16-channel NVR.

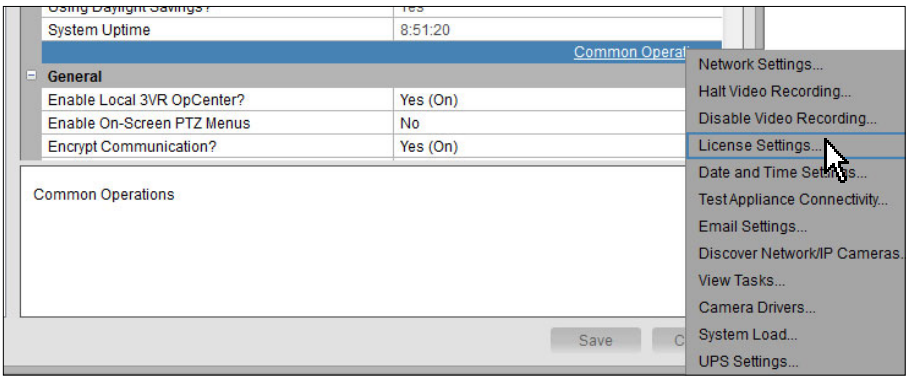
You received a system-specific license key at the time you purchased a licensed feature. If you do not have access to the original order confirmation email, you can look up the license key by serial number on the 3VR Support Portal (go to http://partners.3VR.com, sign in with your company's Support Portal login, and then click the **Obtain System License Key** link).

DRAFT

After you obtain the license key, enter it in the **License Settings** dialog box in System Manager by performing these steps:

1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

2. Click Common Operations, and then click **License Settings**.

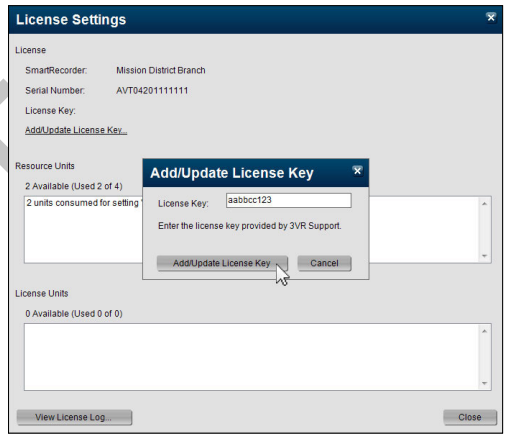


3. In the **License Settings** dialog box, click Add/Update License Key.

4. Type the license key in the pop-up box.

5. Click the **Add/Update License Key** button. The **License Settings** window updates to reflect that a license key was applied.

6. Click **Close** to return to the **Configure** panel.

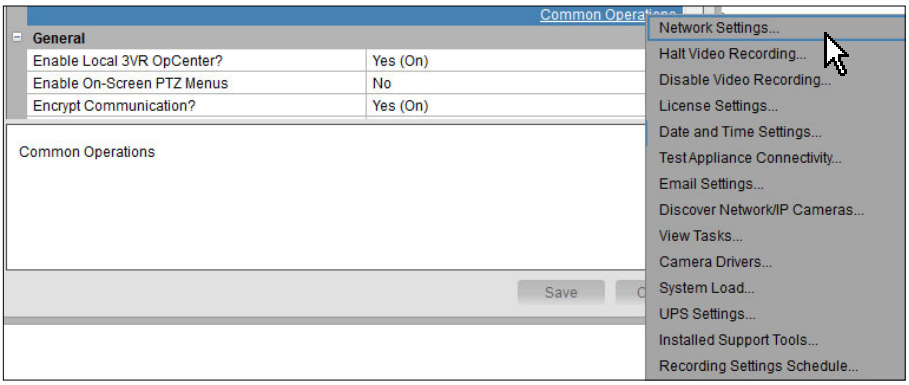


DRAFT

1.7 Edit Network Settings

1. In the **Configure** panel of System Manager, click the VMS server name in the left-hand panel to view the system settings.

2. Under the **Appliance** category heading, click Common Operations, and then click **Network Settings**.



3. The network adapters listed in the Network Settings dialog box will vary depending on the specific hardware. If there are multiple network adapters, select the adapter identified as [Primary] from the list. If there are two network adapters, select the adapter identified as **[Primary]** from the list.*

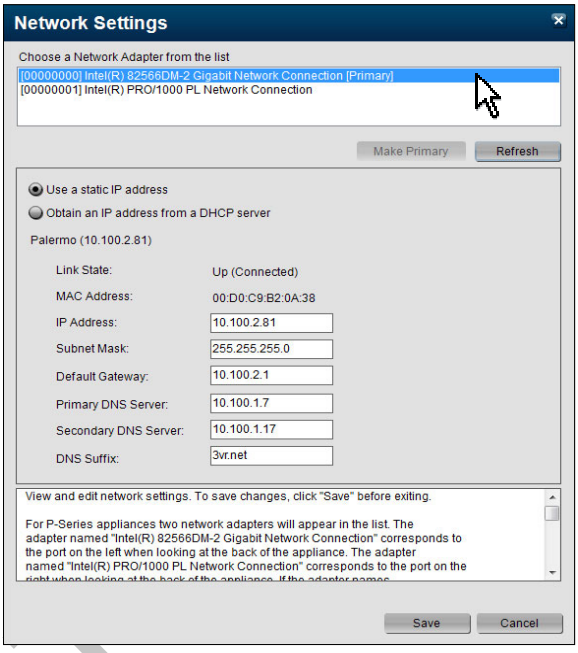
4. If the customer's network uses DHCP, click **Obtain an IP address from a DHCP server**.

   Otherwise, click **Use a static IP address** and type the IP address, subnet mask, and default gateway assigned to the VMS server in the appropriate boxes.

5. If applicable for the installation, type the primary DNS server address, secondary DNS server address, and DNS suffix in the appropriate boxes.

6. Click **Save**.

7. Click **Change Network Settings** to confirm. System Manager closes. Wait about 1 minute for the system software to restart before re-launching System Manager.



***Details**
3VR appliances, 1000, 3000, 4000, 5500, and all NVR systems have two network cards. Refer to the product diagrams in chapter 1 for more information.

1.8 Edit Known Host Setting

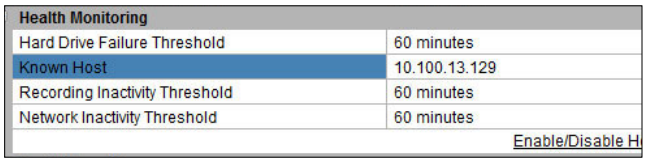
The **Known Host** is the IP address or hostname of a reliable server on the network that can serve as the basis for testing network connectivity. If the VMS server is unable to successfully ping the known host for a period of time, a health alert is generated.

Perform the following steps to configure the known host:

1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

2. Type the IP address of the known host server in the **Known Host** box.

3. Click **Save**.



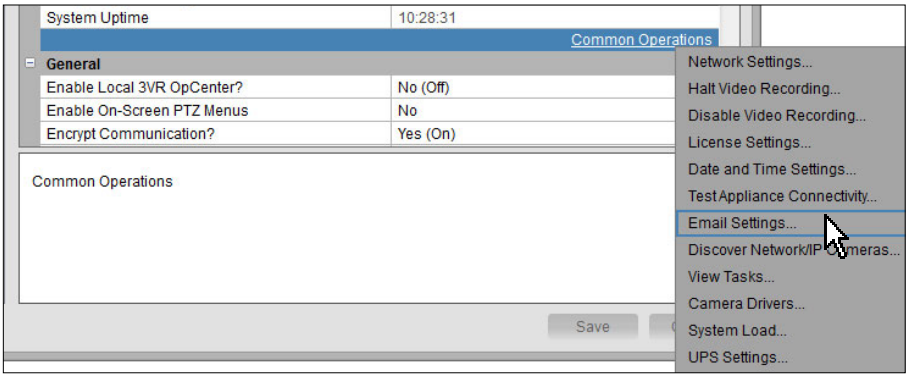
2. CONFIGURE OUTGOING EMAIL SETTINGS

If an email server is accessible on the network and you would like the VMS server to be able to send outgoing email (for example, health alerts or emailed video and events), edit the **Email Settings** in System Manager by performing the following steps:

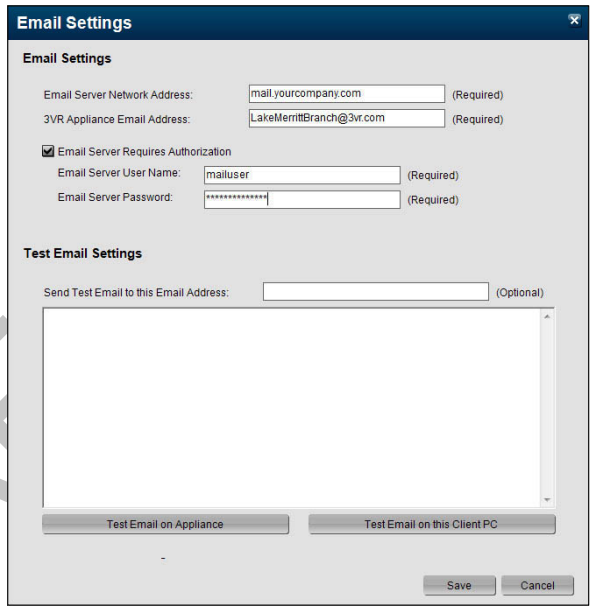
1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

2. Under the **Appliance** category heading, click Common Operations, and then click **Email Settings**.

DRAFT



3. In the **Email Settings** window, type the network address of the email server in the **Email Server Network Address** box.



4. In the **3VR Appliance Email Address** box, type the email address you'd like to appear as the "From" address of all outgoing messages.

   Use your organization's domain name and the correct email address format (for example, companyname@yourdomain.com, or companyname_Email@yourdomain.net).

   3VR strongly recommends that your organization's IT or Network Administrator create an actual email address for 3VR on your mail server, and set it up to forward to members of the security staff.

   If you choose not to create an email address, security settings on your mail server may prevent 3VR messages from reaching external recipients, and replies to messages sent from the VMS server will be undeliverable.

5. If the email server requires a user name and password, check the box next to **Email Server Requires Authorization** and fill out the user name and password fields.

6. Click **Save**.

7. If desired, send a test message to verify the email server configuration is correct:

   - Enter an email address in the **Send Test Email to this Email Address** box.
   - Click **Test Email on Appliance**. A log message indicates whether the email was sent successfully.

DRAFT

3. CONFIGURE EVENT AND VIDEO STORAGE SETTINGS

The VMS server can retain the still images and details from events for extended periods of time even after the event video clip has been deleted from the system due to space constraints.

Events and video associated with an event type are deleted from the system after the number of days specified for each event type has passed.

To access the event storage settings, click the name of the VMS server in the **Configure** panel to display the system settings and scroll down to the **Smart Storage** settings category.

Important
Setting **[Event Type] System Storage** and **Minimum Days of Video** to 0 disables Smart Storage, causing the VMS server to use simple space-based trimming.

[Event Type] System Storage

Default: **90 days**
Range: **0 - 730 days**

Motion Event Storage (Days)	90
Face Event Storage (Days)	90
Imported Image Event Storage (Days)	90
Ext. Input/Alarm Storage (Days)	90
Advanced Object Storage (Days)	90
Advanced Object Storage (Days)	90

These settings define the storage duration for events generated on the VMS server. All events are deleted after the duration specified for each event type.

If system storage is insufficient to retain events for the specified duration, these values may be overridden.

Notes
1) An event added to cases in OpCenter **Cases** panel is retained indefinitely, and its video is not trimmed unless the event is removed from the case.
2) Imported image events are never deleted.

DRAFT

4. CONFIGURE SCHEDULES

You can configure recording settings to record during peak and off-peak hours.

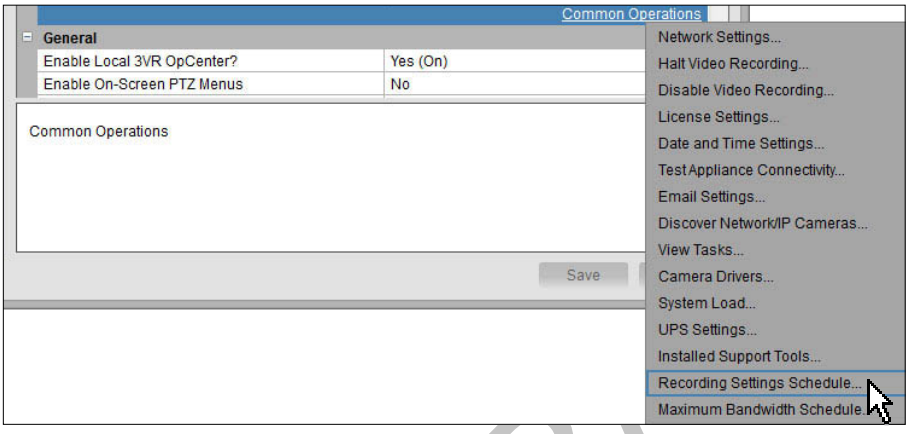
4.1 Recording Settings Schedule

You can configure video frame rate, video quality, video resolution, and continuous recording settings to record with different values during peak and off-peak hours.

To define peak and off-peak hours for recording settings:

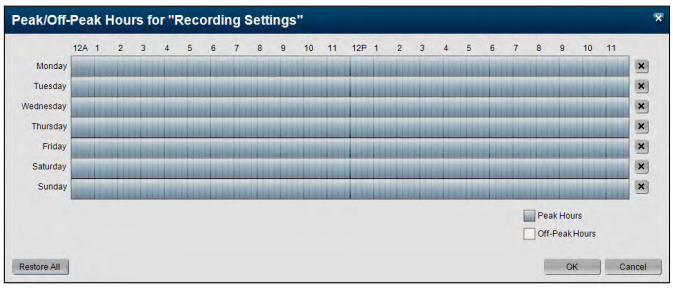
1. In the **Configure** panel of System Manager, click the VMS server name in the left-hand panel to view the system settings.

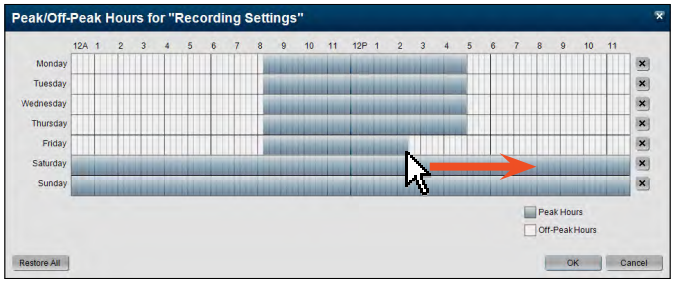
2. Under the **Appliance** category heading, click Common Operations, and then click **Recording Settings Schedule**.



3. To define peak hours for each day, click the box representing the start time, drag the mouse to the right and release when the continuously highlighted region represents the full range of peak hours.

   - The unselected time range represents off-peak hours.
   - To restore the previously stored settings, click **Restore All**.
   - To clear the selection for a single day of the week, click the X button to the right of the schedule for that day.





DRAFT

4. Repeat the above steps for each day of the week.

5. Click **OK** to save the **Peak/Off-Peak Hours for Recording Settings** configuration.

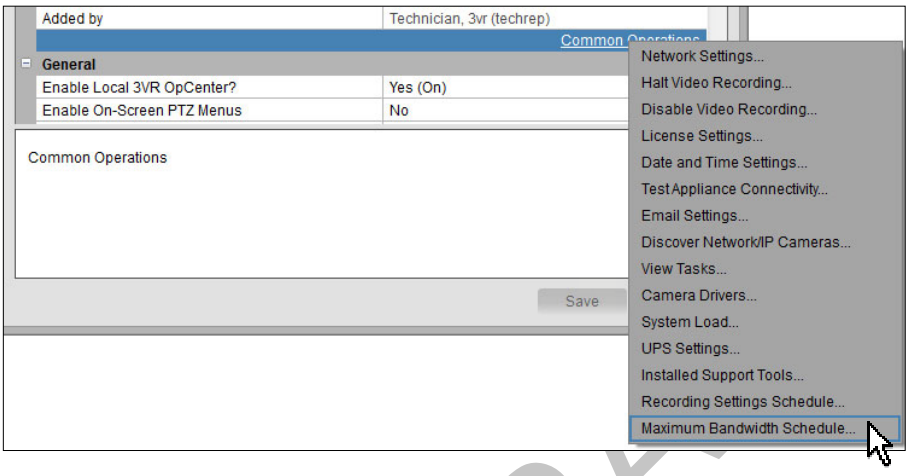
4.2 Peak and Off-Peak Bandwidth Use Schedule

You can configure the VMS server to adhere to different bandwidth consumption constraints during peak and off-peak hours.

To define peak and off-peak hours for bandwidth control:

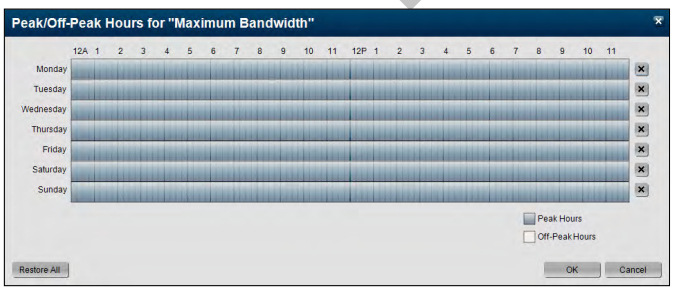
1. In the **Configure** panel of System Manager, click the VMS server name in the left-hand panel to view the system settings.

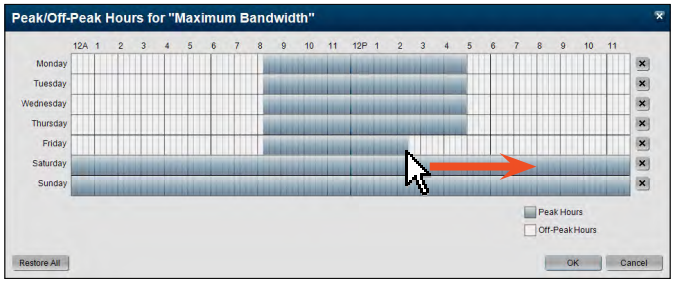
2. Under the **Appliance** category heading, click Common Operations, and then click **Maximum Bandwidth Schedule**.



3. To define the peak hours for maximum bandwidth, click the box representing the start time, drag the mouse to the right and release when the continuously highlighted region represents the full range of peak hours.

   - The unselected time range represents off-peak hours.
   - To revert to the previously stored settings, click **Restore All**.
   - To clear the selection for a single day of the week, click the X button to the right of the schedule for that day.





4. Repeat for each day of the week.

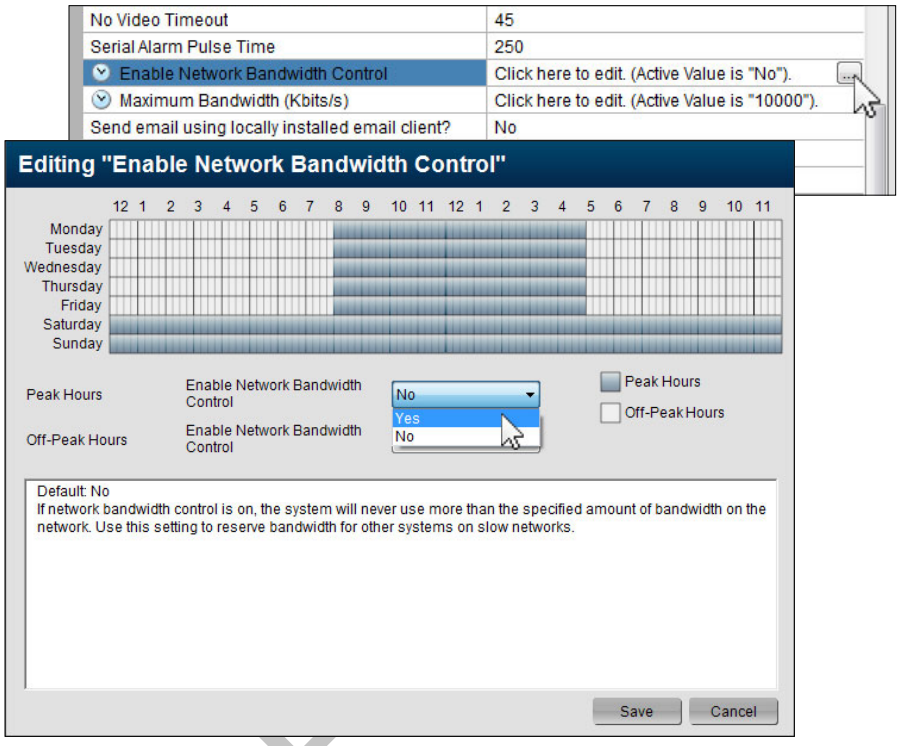
DRAFT

5. Click **OK** to save the **Peak/Off-Peak Hours for Maximum Bandwidth** configuration and return to the **Configure** panel.

6. Scroll down to the **General** settings category, and then click the ellipsis **(...)** button next to **Enable Network Bandwidth Control**.

7. To enable bandwidth control for **Peak** or **Off-Peak** hours, select **Yes** from the corresponding drop-down menu.

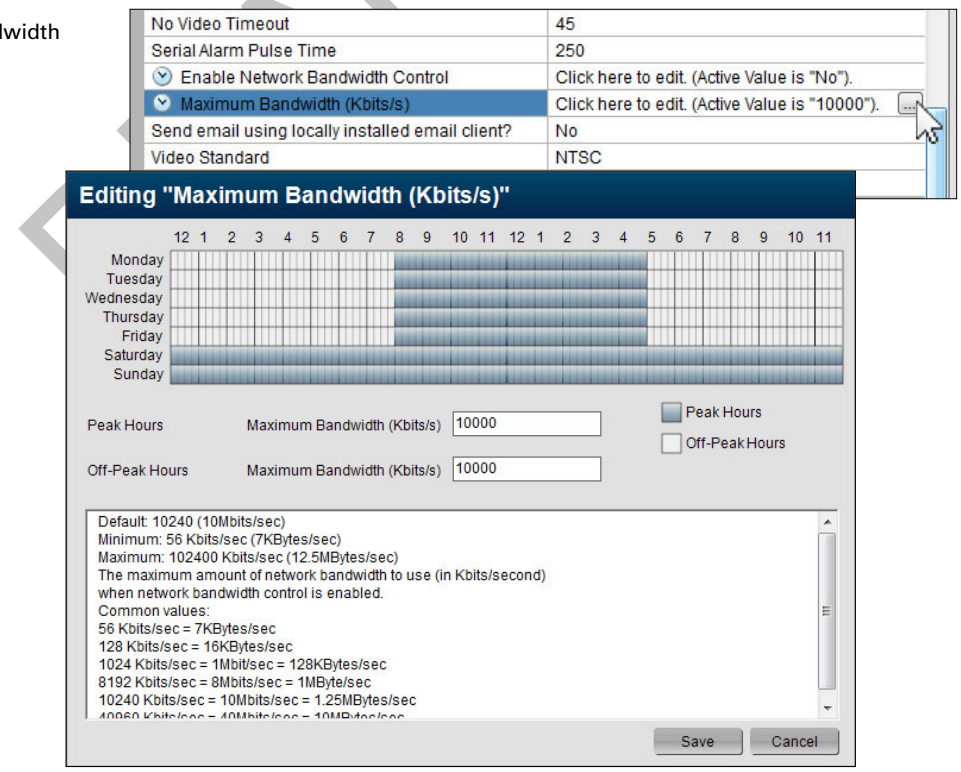
8. Click **Save** to save your changes.



9. To configure maximum bandwidth values, click the ellipsis **(...)** button next to **Maximum Bandwidth**.

10. Enter the maximum allowed bandwidth for **Peak** and **Off-Peak** hours.

11. Click **Save** to save your changes.



Note

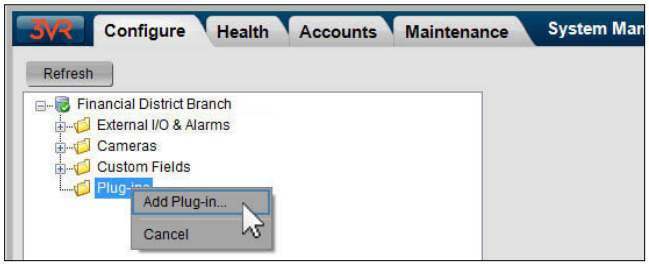
The schedule for bandwidth control and the value for the **Maximum Bandwidth** setting only take effect when **Network Bandwidth Control** is enabled.

5. INSTALL PLUG-INS

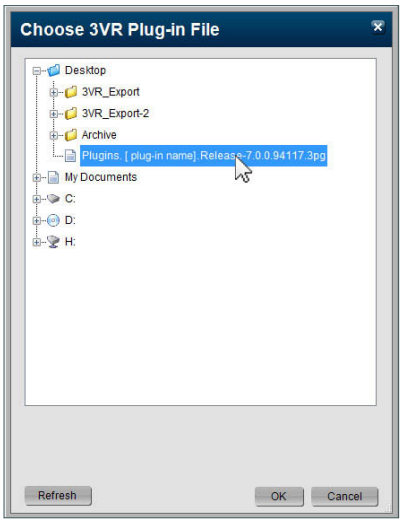
Plug-in Software and Documentation

A link to download the plug-in file and installation documentation was provided to you at the time of purchase. If you do not have access to the original order confirmation email, contact 3VR Technical Support and provide the P.O. number to obtain the download link.

Perform the following steps to install a plug-in on a VMS server:



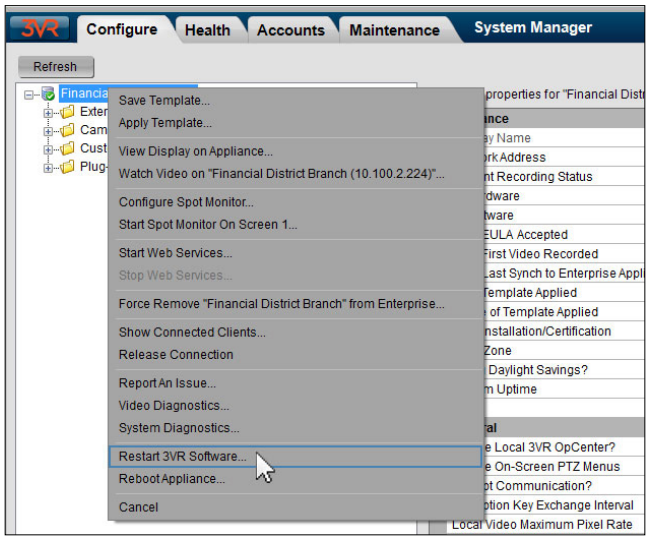
1. In the **Configure** panel of System Manager, click the plus sign beside the system name to display the list of configuration options.
2. Right-click the **Plug-ins** folder and select **Add Plug-in**.
3. In the resulting **Confirm** dialog box, click **Install** to proceed.
4. Navigate to the folder containing the plug-in file.



5. Select the file and click **OK**. The plug-in begins installing. When the plug-in has been installed, it appears below the **Plug-ins** folder.
6. Select the plug-in to display its settings. Configure the settings according to the plug-in's documentation.
7. Click **Save** to save the updated plug-in configuration.

DRAFT

8. You must restart the system software after installing a plug-in or making any changes. Restart the system software by right-clicking the system display name and selecting **Restart 3VR Software**.
9. In the **Confirm** dialog box, click **Restart** to initiate the software restart.
10. Close System Manager and wait 1-2 minutes for the software restart to complete before proceeding.

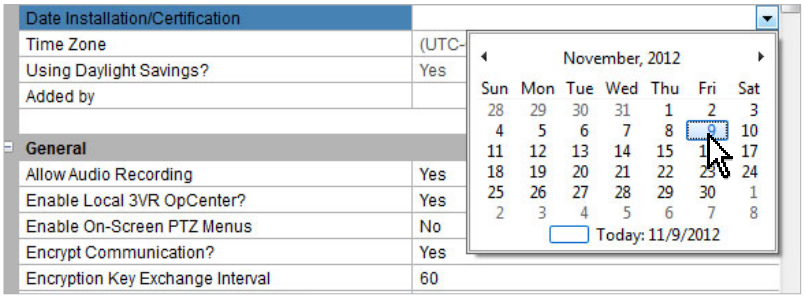


6. SET CERTIFICATION DATE

After you have completed all installation steps, set the **Install/Certification Date** in System Manager to today's date:

1. In the **Configure** panel of System Manager, click the VMS server name in the left-hand panel to view the system settings.

2. Under the **Appliance** category heading, locate the **Date: Install/Certification** setting.
3. Click next to the setting to display a drop-down calendar control.
4. Click today's date.
5. Click **Save**.



7. RUN THE 3VR INSTALLATION REPORT

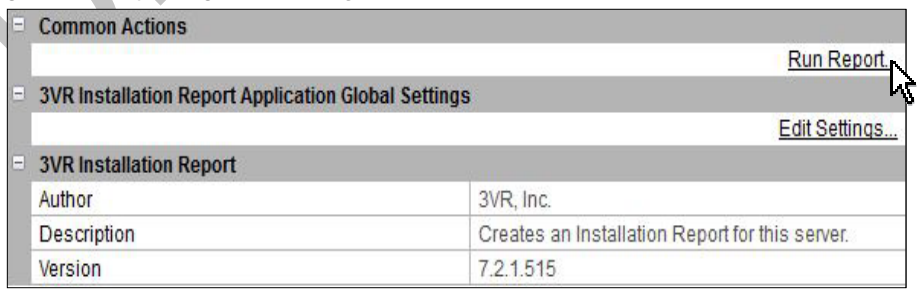
Note

The 3VR Installation Report plug-in is installed by default on all VisionPoint™ VMS systems. If it has been removed, contact 3VR Technical Support to request the report plug-in file, and install it on the VMS server by performing the steps in "Install Plug-ins" on page 76 .

Use the 3VR Installation Report plug-in to generate a report displaying the system information and settings, as well as details about the installation site. You can save this report to disk or email it directly from System Manager (if you configured email for the 3VR server).

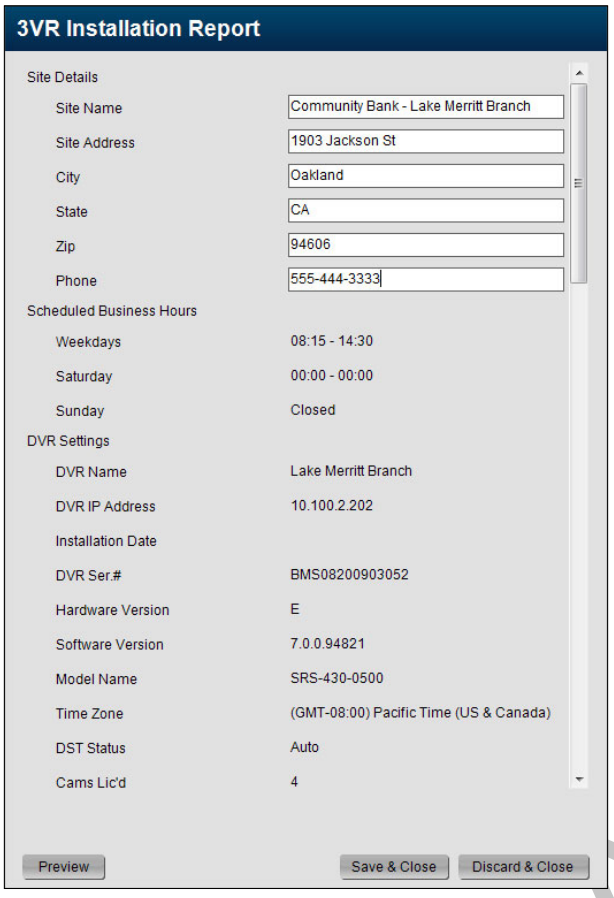
In addition, you can use this plug-in to search for 3VR servers on an Enterprise Server (see "Searching for VMS Servers on an Enterprise Server" on page 80 for information).

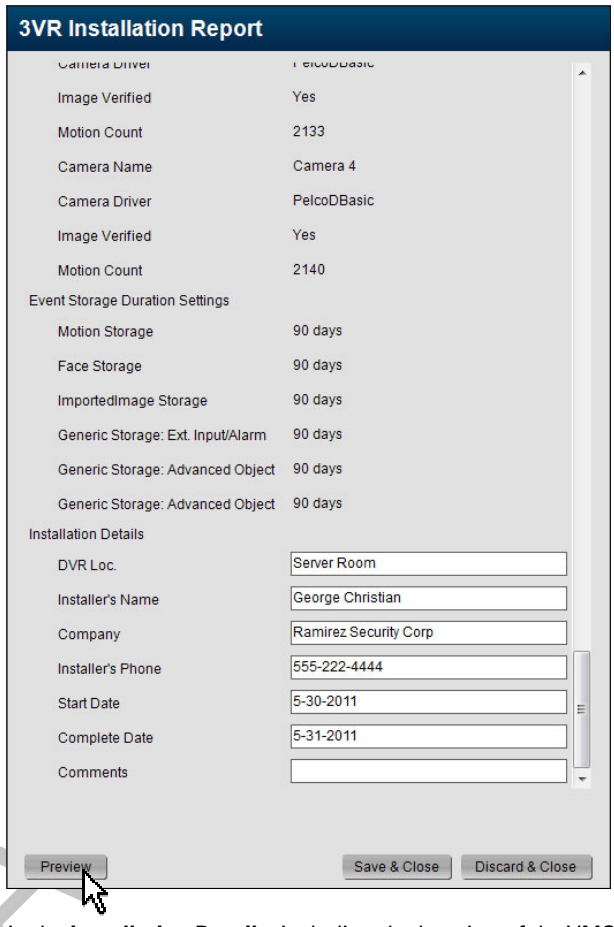
1. In the **Configure** panel of System Manager, click the plus sign next to **Plug-ins**.
2. Click **3VR Installation Report Application**.
3. Click Run Report.



DRAFT

4. Enter the name, address, and phone number of the installation location under **Site Details**.

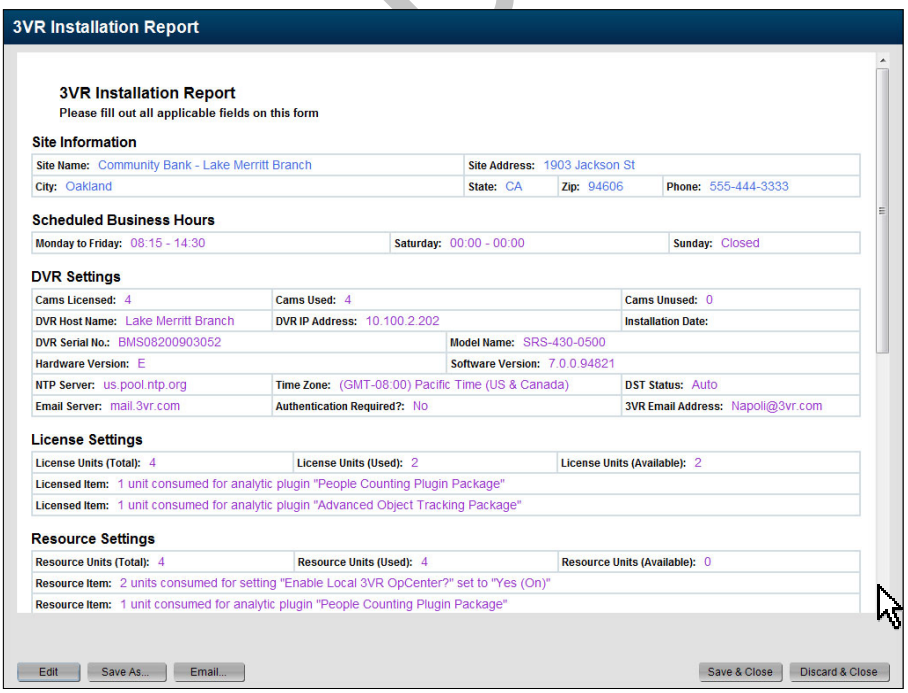




5. Scroll to the end of the **3VR Installation Report** dialog box. Fill in the **Installation Details**, including the location of the VMS server, the installation start and end dates, and your contact information.

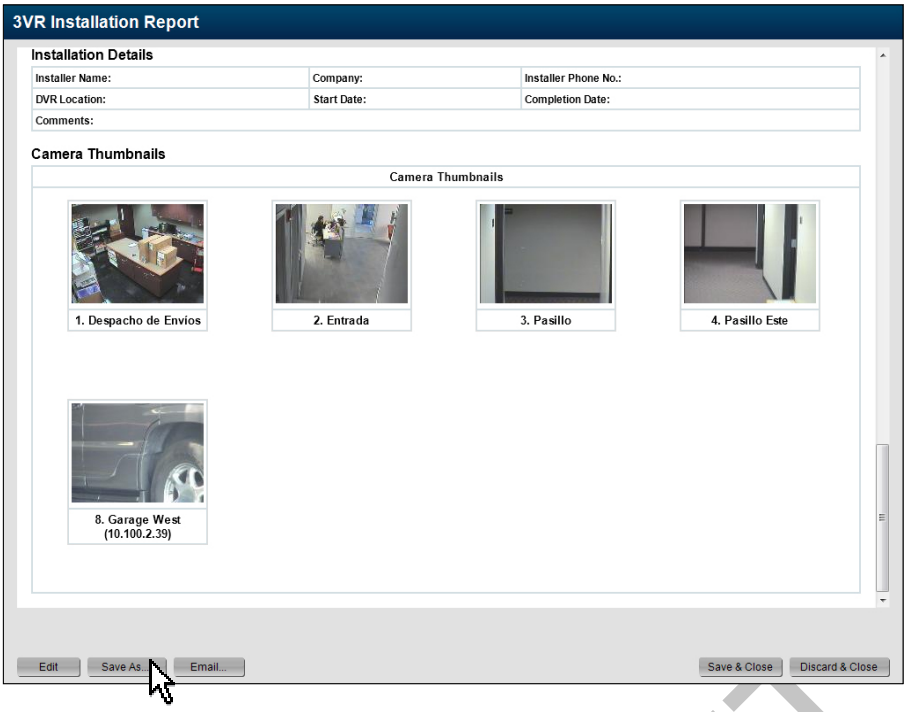
6. Click **Preview**.

7. Review the installation report preview for accuracy.

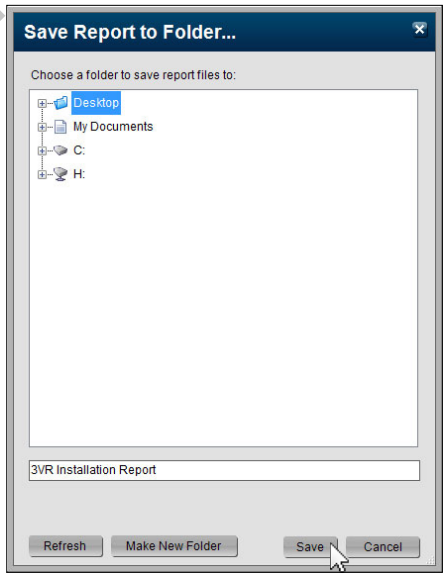


DRAFT

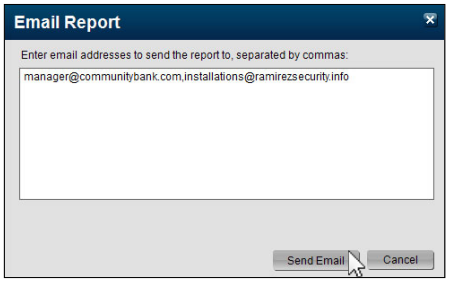
At the end of the report, thumbnails of all of the enabled cameras appear.



- To go back and make changes to the installation report form, click **Edit**.
- To save the preview on your computer as an HTML file, click **Save As** and navigate to the location where you wish to save the report.



- To email the report, click **Email**. Type the address of each report recipient, separated by commas, and then click **Send Email**.



Note
The VMS server must have mail server information configured in order to send email. See the section "Configure Outgoing Email Settings" on page 70 for details.

DRAFT

7.1 Searching for VMS Servers on an Enterprise Server

You can use the report plug-in to search for VMS servers installed on an Enterprise Server. You can search based on:

- Appliance name
- City, state, or zip code where the appliance is located:

To use the search feature, you must install one of these plug-ins:

- InstallationReport
- WellsFargoFaxbackReport
- TmobileInstallationReport

See "Install Plug-ins" on page 76 for instructions on installing plug-ins.

Setup Steps Before Conducting Searches

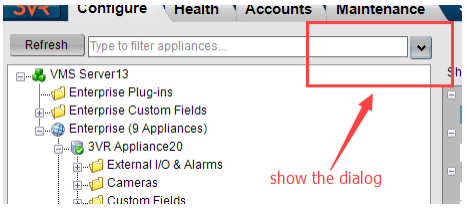
Before searching for VMS servers, you need to:

- Make sure you've installed the report plug-in on the VMS server.
- Added the VMS server to the enterprise (see "Step 4. Add System to Enterprise (Optional):" on page 41 for instructions).
- Entered city, state, and zip code information in the Site Details section of the installation or faxback report (see "Run the 3VR Installation Report" on page 77 for information).

Searching for a VMS Server

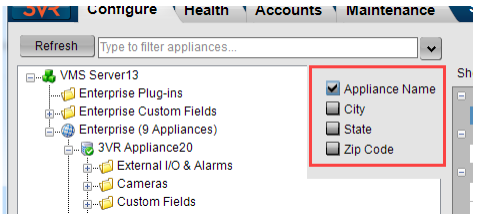
To search for VMS server, you select the desired information type (City, for example) and then enter the text to search on. The system performs "fuzzy" matching on the text you enter to detect matches based on text patterns.

1. Click the **Type to filter appliances** arrow button.



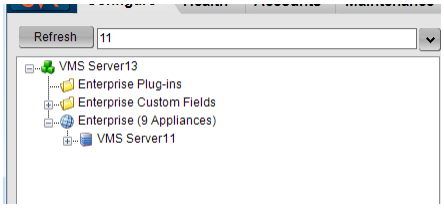
A set of check boxes appear. By default, the Appliance Name box is checked.

2. Select the information type you want to search on (for example, Appliance Name). Then, in the **Type to filter appliances** field, enter the specific information for the search. For example, if searching for a VMS server by name, enter all or part of the desired VMS server's name. The examples below show the information entered and the search results.

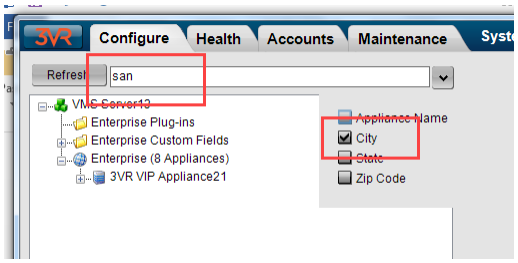


DRAFT

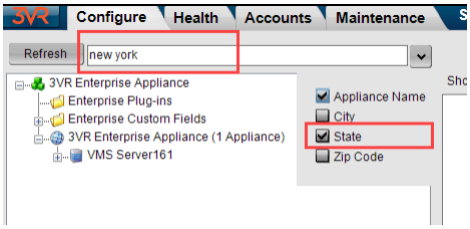
Search on Appliance Name



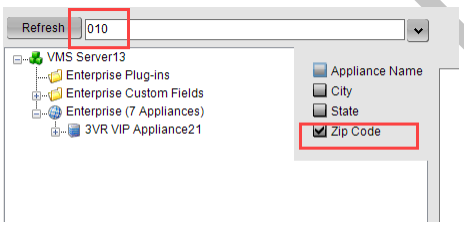
Search on City



Search on State



Search on Zip Code



DRAFT

Notes

The notes below describe some things to keep in mind regarding searches:

When you add a new VMS server to an Enterprise server, the related city, state and zip code are pushed to the enterprise immediately.

However, if you change the city, state or zip code for a VMS server by entering new information using the VMS server's report plug-in, it may take one day before this information is pushed to the Enterprise server. In other words, it may take a day after the change before you can locate the VMS server by conducting a search using System Manager on the Enterprise server side.

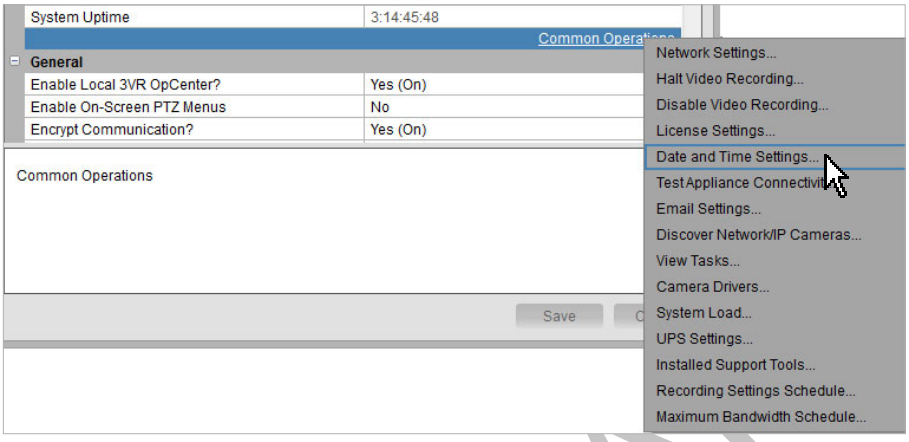
8. UPDATING DATE AND TIME SETTINGS

If using a 3VR appliance, you should perform initial configuration of the appliance's date and time settings with the Initial System Setup wizard (see "Run the 3VR Appliance Configuration Tool" on page 40). Thereafter, or if you are using third-party hardware, you can edit these settings in the **Configure** panel of System Manager.

8.1 Edit the Time Zone

1. In the **Configure** panel of System Manager, click the appliance name in the left-hand panel to view the system settings.

2. Under the **Appliance** category heading, click Common Operations, and then click **Date and Time Settings**.



3. In the **Date and Time Settings** dialog box, select the time zone where the unit is installed from the **System Time Zone** drop-down list.

4. Click **Save** to save your changes.

5. Click **OK** in the **Confirm Changes** dialog box.

DRAFT

8.2 Edit the NTP Server

1. Perform the steps in "Edit the Time Zone" on page 82 to open the **Date and Time Settings** dialog box.

2. Click **Automatically set time from a remote server**.

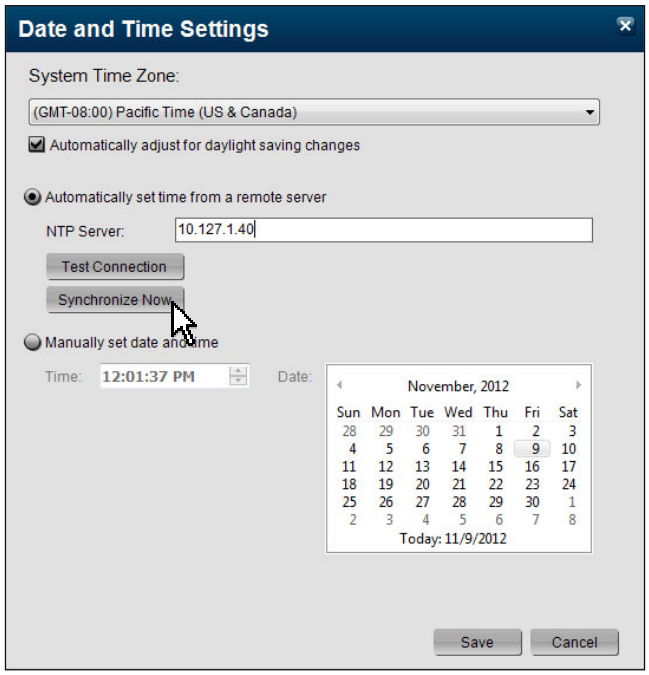
3. Type the address of the NTP server in the **NTP Server** field.

4. If desired, you may test the connection to the NTP server by clicking the **Test Connection** button. A message will appear indicating whether the test was successful.

5. Syncing to the NTP server occurs automatically on a periodic basis, but you may synchronize the time immediately by clicking **Synchronize Now**.

6. Click **Save**.

7. Click **OK** in the **Confirm Changes** dialog box.



8.3 Edit the System Date and Time

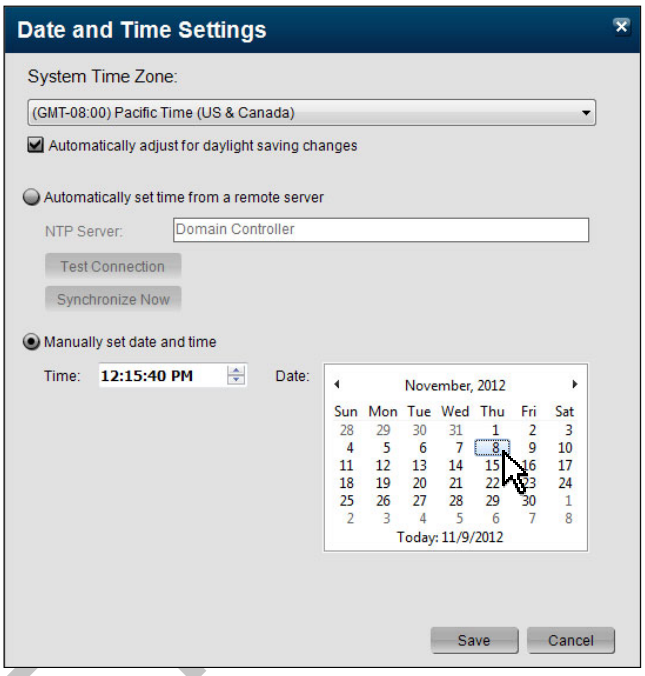
1. Perform the steps in “Edit the Time Zone” on page 82 to open the **Date and Time Settings** dialog box.

2. Click **Manually set date and time**.

3. Set the current date and time.

4. Click **Save**.

5. Click **OK** in the **Confirm Changes** dialog box.



9. NEXT STEPS

If you are installing a3VR appliance or a VMS server on third-party hardware, proceed to the chapter on general camera configuration. To add users on a stand-along VMS server, see the chapter on Enterprise servers.

If you are installing a VMS Enterprise server, proceed to the chapter on Enterprise servers. After you add VMS servers and users, proceed to the chapter on general camera configuration.

DRAFT

DRAFT

CHAPTER 4

Enterprise Servers, Regions, and User Accounts

1. MANAGING VMS SERVERS ON AN ENTERPRISE 87
   - 1.1 Adding a VMS Server 87
   - 1.2 Renaming a VMS Server 88
   - 1.3 Changing the Network Settings of a VMS Server Already on the Enterprise 88
   - 1.4 Removing a VMS Server from the Enterprise 91
2. MANAGING REGIONS ON AN ENTERPRISE 92
   - 2.1 Adding a Region 92
   - 2.2 Renaming a Region 92
   - 2.3 Removing a Region 93
   - 2.4 Moving a VMS Server to a Different Region 93
   - 2.5 Removing a VMS Server from a Region 94
3. WORKING WITH USER ACCOUNTS 95
   - 3.1 Creating a New User Account 95
   - 3.2 Editing a User Account 96
   - 3.3 Disabling a User Account with Password Expiration 96
   - 3.4 Re-Enabling a Disabled User Account 97
   - 3.5 Resetting a User's Password 97
   - 3.6 Deleting an Account 98
4. USER ROLES 98
   - 4.1 User Role Basics 98
   - 4.2 Viewing User Role Details 98
   - 4.3 Assigning Roles to User Accounts 99
   - 4.4 About the Default User Roles 99
   - 4.5 Creating Custom User Roles 101
   - 4.6 Sample Custom User Roles 102
5. ACCOUNT SECURITY 104
   - 5.1 User Password Constraints 104
   - 5.2 Unlocking a Suspended User Account 106
6. ACCOUNT ADMINISTRATION 106
   - 6.1 Exporting the User List 106
   - 6.2 Viewing Connected Users 107
   - 6.3 Auditing User Accounts (Fall Release-2015 (8.1.x and above) only) 108
7. ENTERPRISE USER MANAGEMENT 109
   - 7.1 Syncing Users with the Enterprise 109
   - 7.2 Synchronizing with LDAP Servers 110

DRAFT

DRAFT

1. MANAGING VMS SERVERS ON AN ENTERPRISE

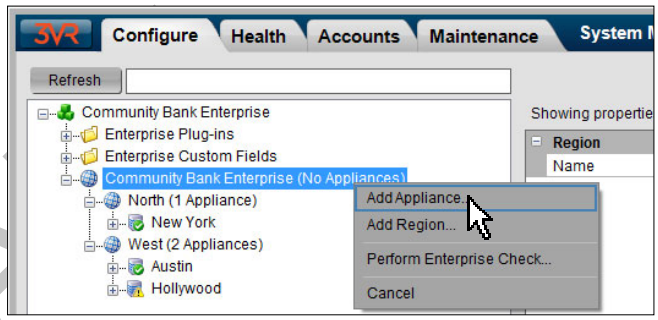
This section describes how to add, remove, and otherwise manage VMS servers on an Enterprise.

1.1 Adding a VMS Server

Important Notes

1) Prior to adding a new VMS server to an Enterprise, you should first log in to the VMS server directly to configure the system name, date, time, and network settings. See the on basic System Manager configuration for instruction on logging into a 3VR appliance or into a VMS server.
2) Any user accounts that have been created on the VMS server that do not exist on the Enterprise will be lost when the VMS server joins the Enterprise.
3) If you are adding a VMS server to an Enterprise as a replacement for another unit, you must force remove the original VMS server from the Enterprise before re-adding a new VMS server with the same IP address (see section 1.4 for removal instructions).
4) Cases are managed on the Enterprise server. Consequently, any cases created on the VMS server in OpCenter are transferred when the system joins the Enterprise.

Use the following steps to add a VMS server to an Enterprise:



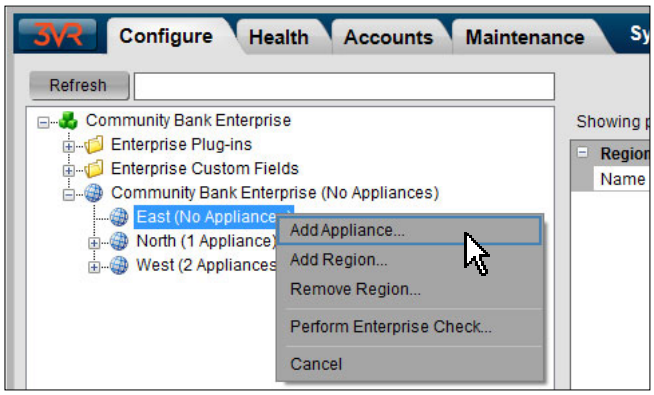
1. In the System Manager **Configure** panel:

   - To add the VMS server to the Enterprise without placing it in a region, right-click the Enterprise name and click **Add Appliance**.

   - To add the VMS server to a region or sub-region of the Enterprise, right-click the region and select **Add Appliance**. See "Managing Regions on an Enterprise" on page 92 for information on regions.

Note

You can repeat this step to add the same VMS server to more than one region.



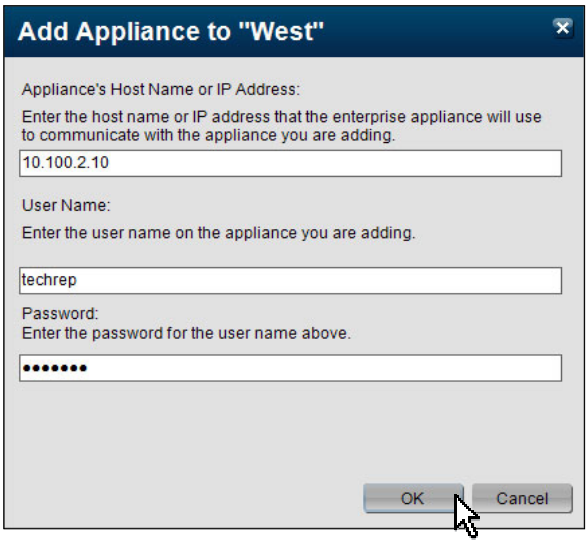
2. In the **Add Appliance** window, enter the IP address or host name of the VMS server.

3. If you are logged in with integrator permissions, the **User Name** and **Password** fields are pre-filled. Otherwise, enter your user name and password.

> **Important Note**
> The user name and password you use to add a VMS server to the Enterprise must exist on the VMS server.

4. Click **OK**.

   The newly added VMS server appears below the Enterprise name or the region name.



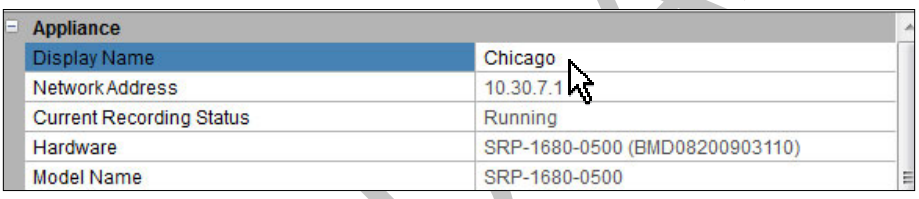
1.2 Renaming a VMS Server

To change the name of a VMS server after it has been added to the Enterprise:

1. Launch System Manager.

1. In the **Configure** panel, click the name currently assigned to the VMS server in the left-hand panel to view the system settings.

2. Click the **Display Name** box and edit the name.



3. Press the Enter key, and then click **Save** to save the new name.

1.3 Changing the Network Settings of a VMS Server Already on the Enterprise

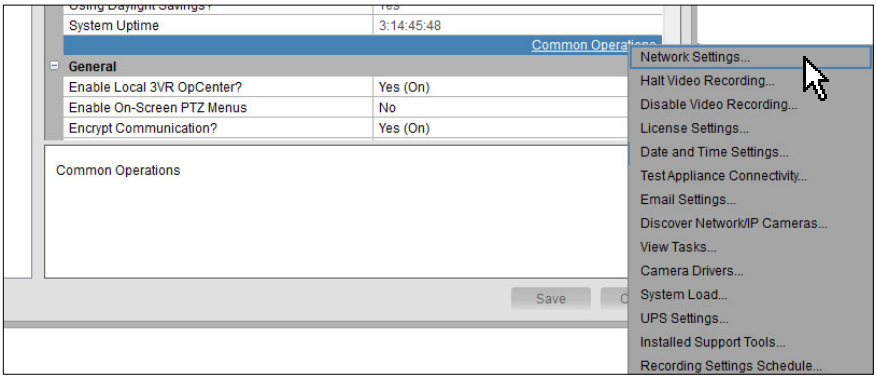
The Enterprise server uses the IP address to identify and communicate with a member VMS server. If a VMS server's assigned IP address changes, the Enterprise must be updated to reflect its new location on the network.

To change the IP address used to communicate with a VMS server on the Enterprise:

1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

DRAFT

2. Under the **Appliance** category heading, click Common Operations and then click **Network Settings**.



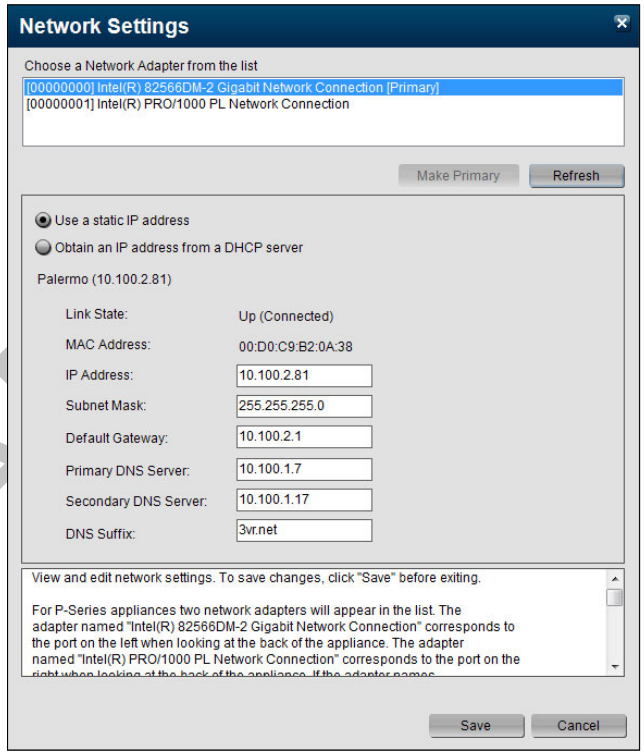
To assign a new static IP address to the VMS server:

3. Select the **primary** network adapter.

4. Click **Use a static IP address** and fill in the required information below.

5. Click **Save**.

6. Click **Change Network Settings** to confirm. System Manager closes.

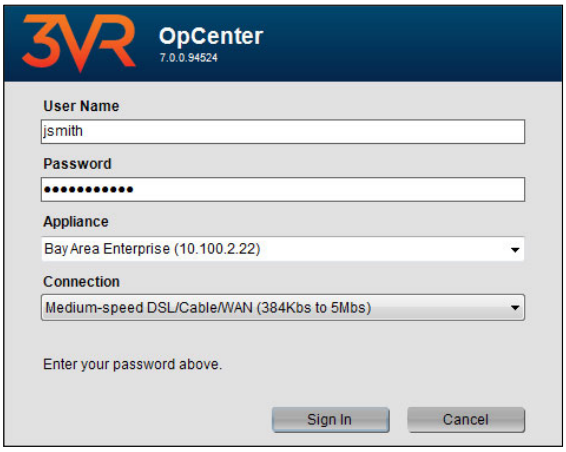


7. To verify connectivity, launch OpCenter.

8. At the sign in screen, type your 3VR user name and password.

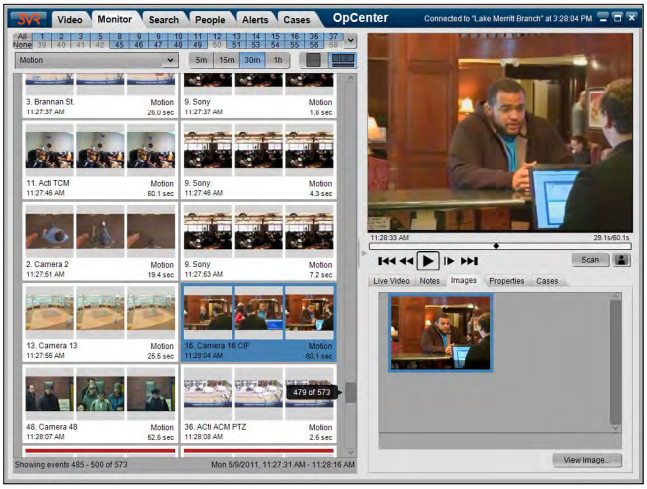
9. Type the new IP address of the VMS server in the **Appliance** box of the OpCenter sign in window.

10. Click **Sign in**.



DRAFT

11. Verify that you can connect to the VMS server and video playback and streaming look normal.

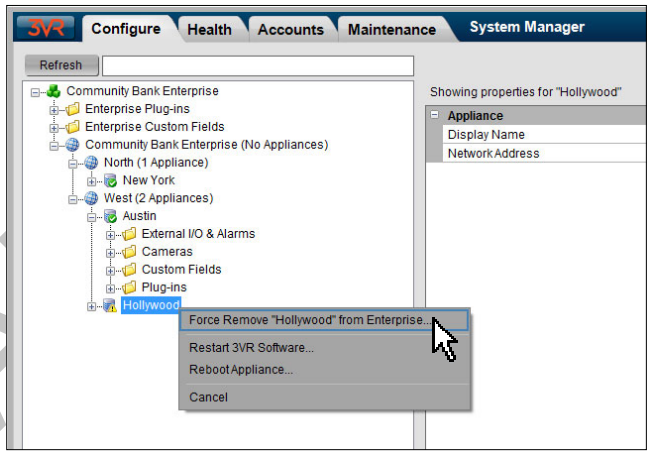


12. Launch System Manager and sign in to the Enterprise.

13. In the **Configure** panel, click the plus sign next to the Enterprise name to display all of the Enterprise's regions and VMS servers.

14. Right-click the VMS server's old IP address and select **Force Remove "[VMS Server Name]" from Enterprise**.

15. In the **Confirm Removal** window, click **Remove** to confirm.



16. Re-add the VMS server to the Enterprise with the new IP address following the instructions in the section "Adding a VMS Server" on page 87.

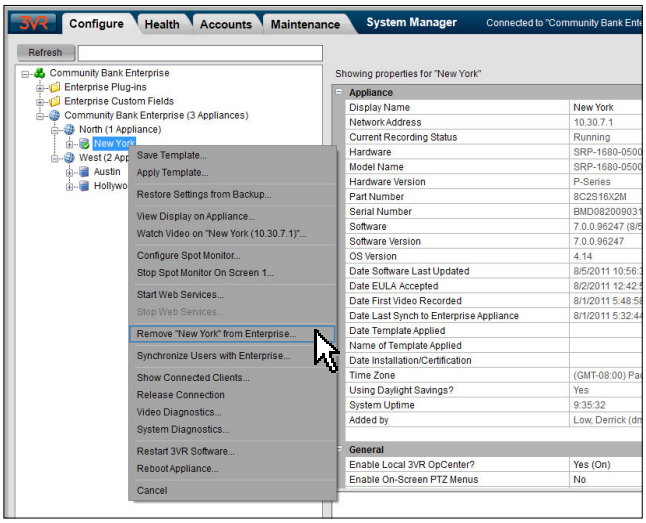
DRA

1.4 Removing a VMS Server from the Enterprise

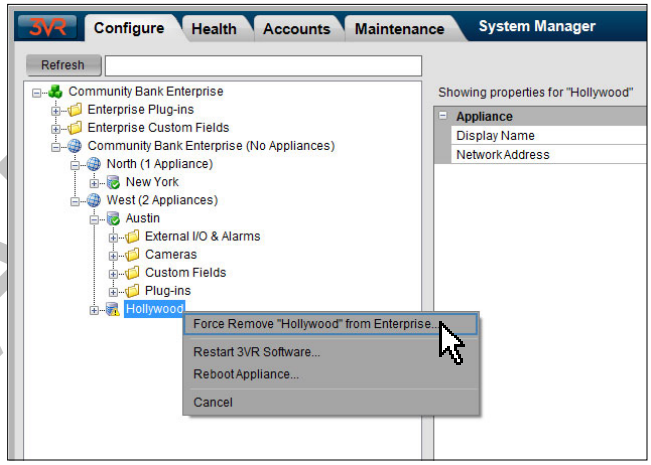
To remove a VMS server from an Enterprise server:

1. In the **Configure** panel, remove the VMS server from the Enterprise in one of two ways:

   - If the VMS server is online and accessible, right-click the VMS server and select **Remove "[VMS Server Name]" from Enterprise**.



   - If the VMS server is offline or otherwise inaccessible, right-click the VMS server's name and select **Force Remove "[VMS Server Name]" from Enterprise**.



2. In the **Confirm Removal** dialog box, click **Remove** to remove the VMS server.

DRA

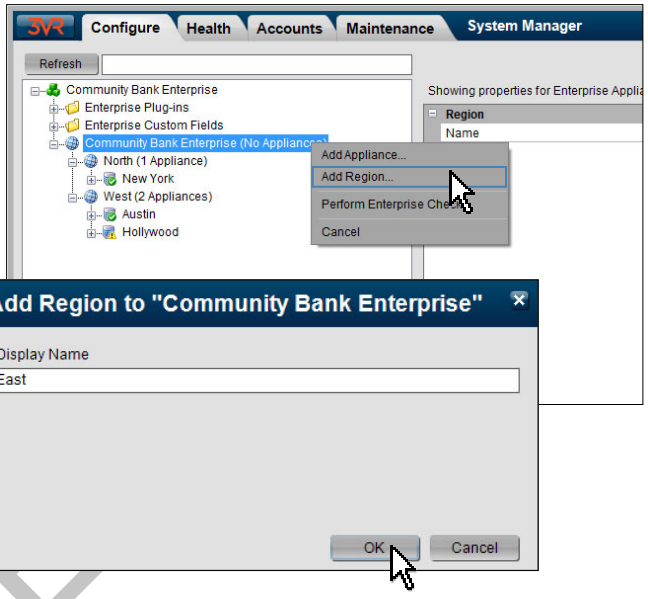
2. MANAGING REGIONS ON AN ENTERPRISE

To manage groups of VMS servers, you can create regions and sub-regions on the Enterprise server.

2.1 Adding a Region

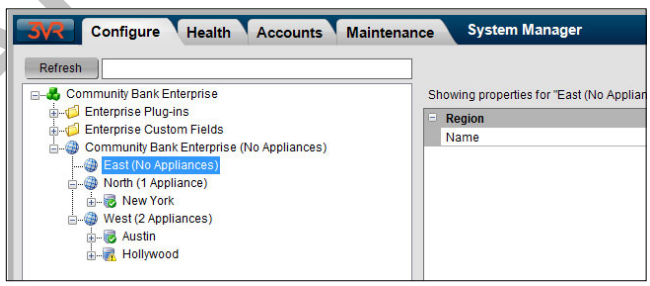
To add a region to an Enterprise server:

1. In the **Configure** panel of System Manager, right-click the Enterprise region and select **Add Region**.



2. Type a **Display Name** for the new region.
3. Click **OK**.

The new region appears below the Enterprise server name in the **Configure** panel.

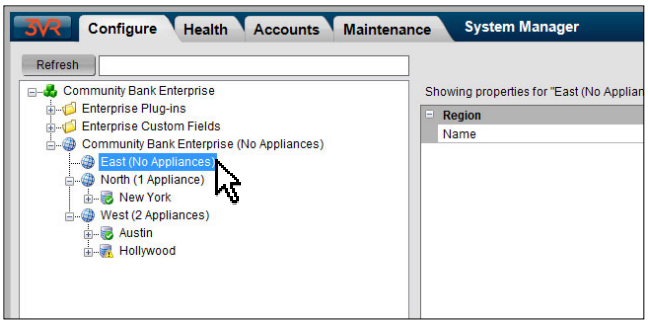


> **More**
> Create sub-regions by right-clicking on a region and repeating the steps above.

DRAFT

2.2 Renaming a Region

Perform the following steps to rename a region on an Enterprise server:



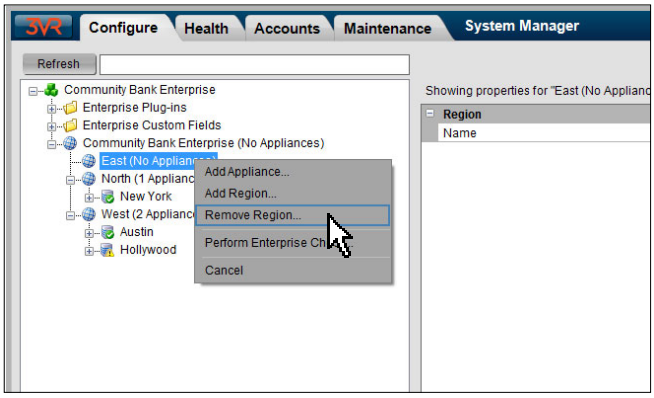
1. In the **Configure** panel, click the plus sign next to the Enterprise server name to display all of the Enterprise's regions and VMS servers.
2. Click the name currently assigned to the region.
3. Click in the box to the right of the **Name** field and edit the text.

4. Click **Save**.

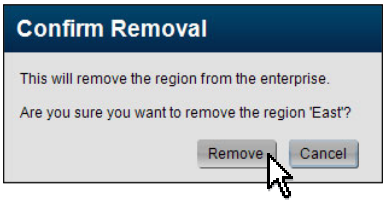
2.3 Removing a Region

1. In the **Configure** panel, click the plus sign next to the Enterprise server name to display all of the Enterprise's regions and VMS servers.

2. Right-click the name of the region you wish to delete and select **Remove Region**.



3. Click **Remove** to confirm the region should be removed from the Enterprise.



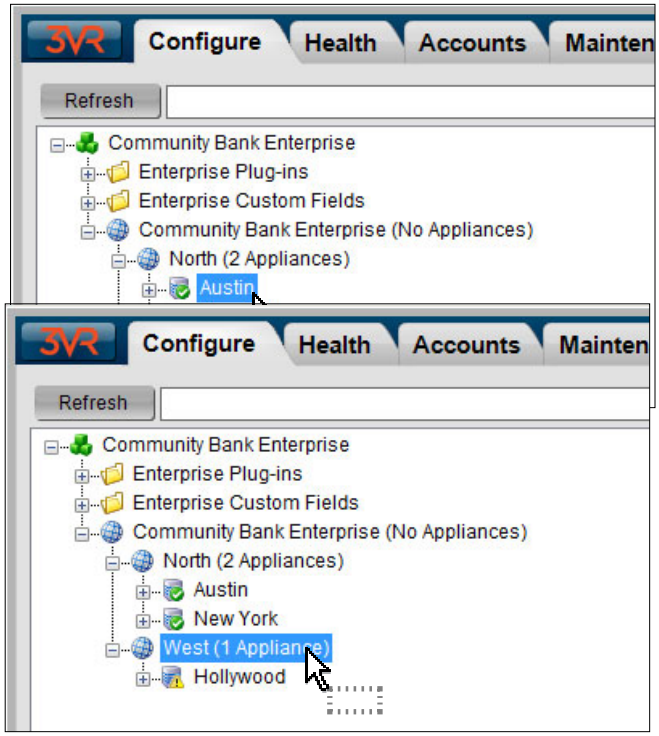
Note
Regions can only be deleted if they are empty. The **Remove Region** option will be grayed out until all of the region's VMS servers have been moved to other regions or removed from the Enterprise.

DRAFT

2.4 Moving a VMS Server to a Different Region

To move a VMS server from one region to another:

1. Click to select the VMS server name.

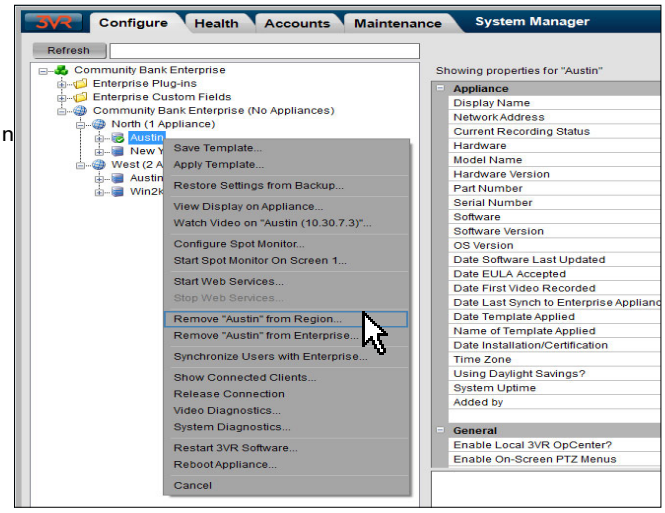


2. Hold down the left mouse button and move the mouse to the destination region. When the mouse is positioned correctly over a region name, a small gray box appears next to the cursor.

3. Release the mouse button.

2.5 Removing a VMS Server from a Region

If a VMS server has been added to multiple regions on a 3VR Enterprise server, you can remove the VMS server from one region without removing it from the entire Enterprise server:



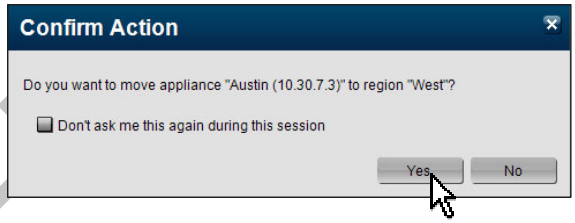
1. In the **Configure** panel, expand a region by clicking the plus sign beside the region name.

2. Right-click the VMS server you wish to remove and select **Remove "[VMS Server Name]" from Region**.

   The VMS server is removed from the region but is still accessible through any other regions to which it has been added.

3. Click **Yes** to confirm that you wish to move the VMS server.

   The **Configure** panel updates with the VMS server in its new location.



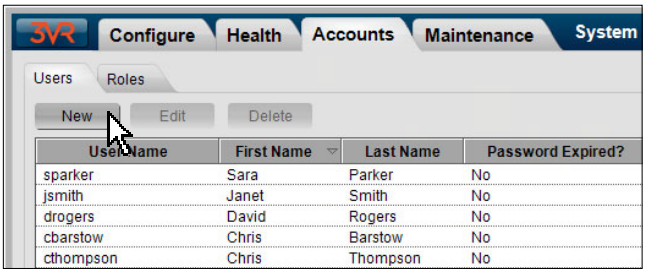
DRAFT

3. WORKING WITH USER ACCOUNTS

Note
For 3VR customers with a VisionPoint™ Enterprise server, you must perform all user management tasks from Enterprise System Manager.

3.1 Creating a New User Account

Perform the following steps to create a new user account:



4. In System Manager, click **Accounts** to go to the **Accounts** panel.
5. Click **New**.

In the **Edit User** dialog box, fill out the account details:

6. Type the **First Name** and **Last Name** of the new user.
7. Create a unique **User Name** for the account.
8. Type a password for the account in the **Password** and **Retype Password** fields.

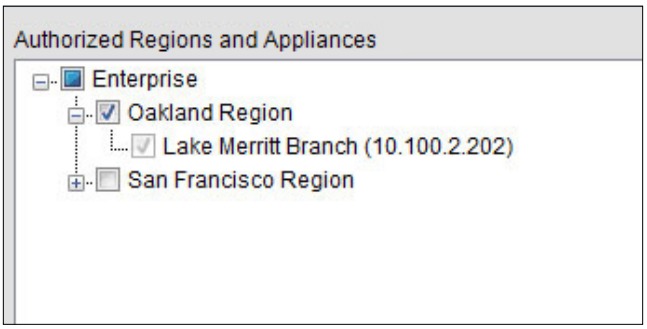
Details
Passwords must contain at least 5 characters, however, your organization may have enacted stricter rules governing the length and format of passwords. See section 5.1 for more information.

9. Select role for the user from the **Role** drop-down menu.

Reference
See section 4 for more information on assigning user roles.

10. If the user should automatically be signed out of the 3VR system after a period of inactivity, select the time period from the **Auto Sign Out** drop-down menu.
11. If this account is a temporary account, check the box next to **Expire password at a given date and time** and select the date and time you wish the user account to be disabled.

Reference
See section 3.3 for more information on disabling user accounts with password expiration.



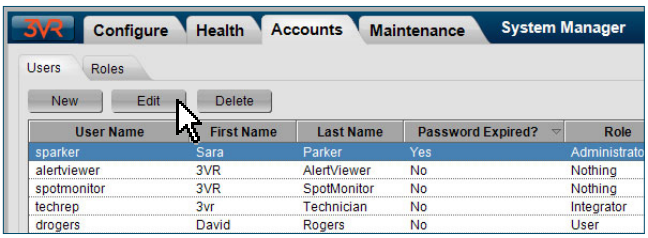
12. If you are creating the user account on an Enterprise server, select which VMS servers or regions the user is able to access in the **Authorized Regions and Appliances** panel:
    - Check the box next to the Enterprise to give the user access to every VMS server on the Enterprise.
    - Check the box next to a region to allow the user to connect to all VMS servers within the region (as well as any VMS servers added to the region in the future).
    - Check and uncheck individual VMS servers to grant or restrict access to only those VMS servers.
13. Click **Save** to create the new user account.

DRAFT

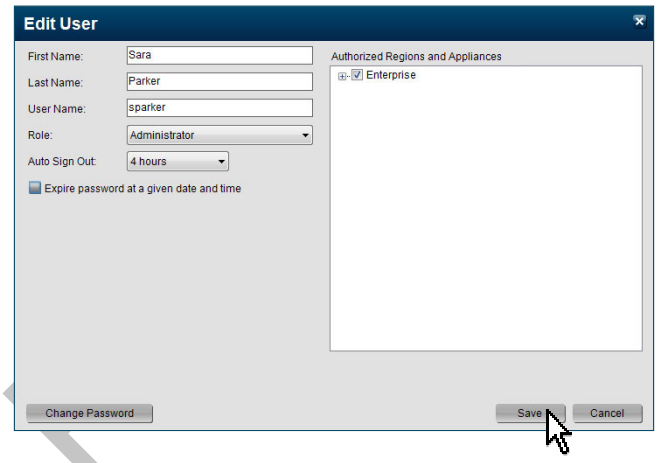
3.2 Editing a User Account

Perform the following steps to modify the details of an existing user account:

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Select the user account to edit from the list.
3. Click **Edit**.



4. In the **Edit User** dialog box, edit the user details as desired.
5. Click **Save**.

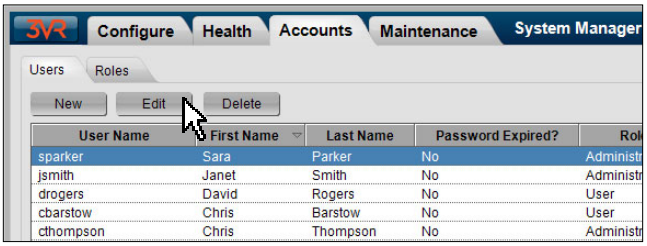


> **Important**
> Do not change the role assigned to your own user account. Also, make sure that the user list has at least one account with integrator access.

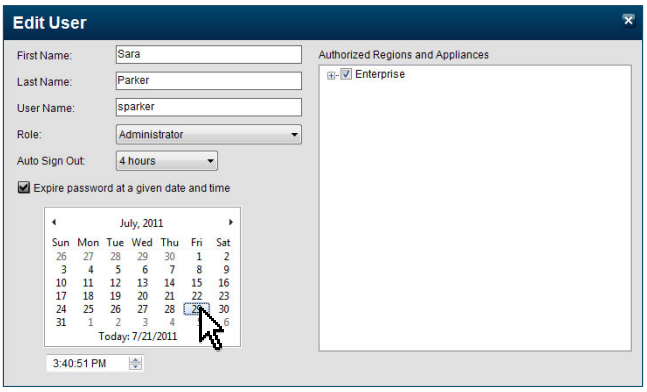
3.3 Disabling a User Account with Password Expiration

Password expiration allows you to automatically disable a user account after a period of time. The user account is retained on the system so you can reactivate it at a later date. To enable password expiration:

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Select the user account to disable from the list.
3. Click **Edit**.



4. In the **Edit User** dialog box, check the box next to **Expire password at a given date and time**.
5. Select the date and time on which you want to deactivate the user account. To immediately disable the account, select a date in the past.
6. Click **Save**.

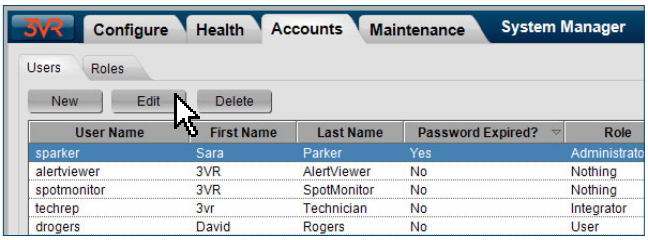


DRAFT

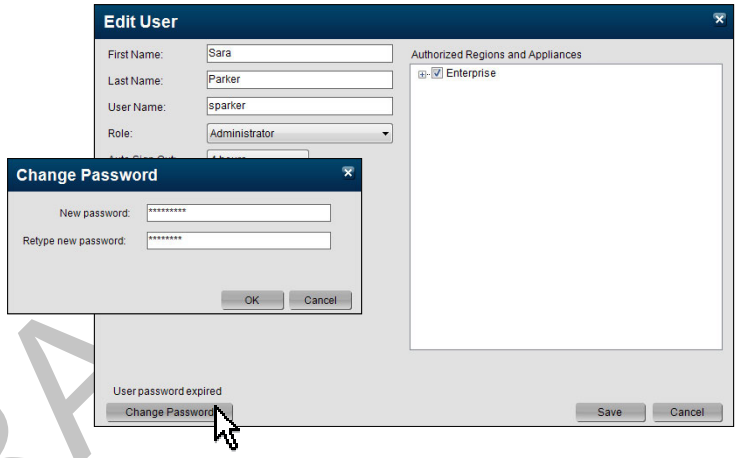
3.4 Re-Enabling a Disabled User Account

Perform the following steps to re-enable a user account that you disabled with password expiration:

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Select the expired user account from the list.
3. Click **Edit**.



4. To reactive the user account:
   - To reactivate the account without an expiration date, deselect **Expire password at a given date and time**.
   - To temporarily reactivate the account, select a new date in the future for the password to expire.
5. To reset the password of the account:
   a. Click **Change Password**.
   b. Enter the new password twice, and then click **OK**.

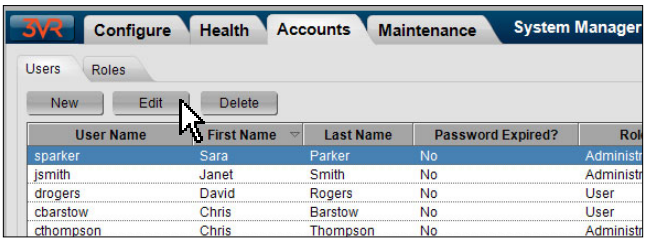


6. Click **Save** to enable the account.

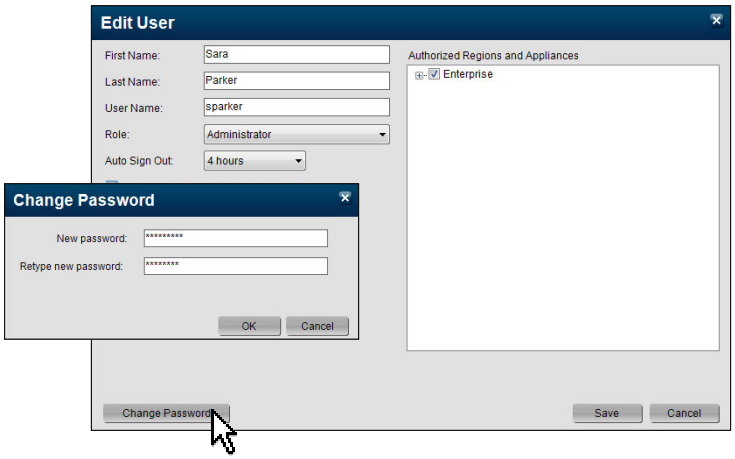
3.5 Resetting a User's Password

Perform the following steps to change the password of a user account:

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Select the account to reset from the list.
3. Click **Edit**.



4. Click **Change Password**.
5. Type the new password twice
6. Click **OK**.
7. Click **Save** to save changes and return to the **Accounts** panel.

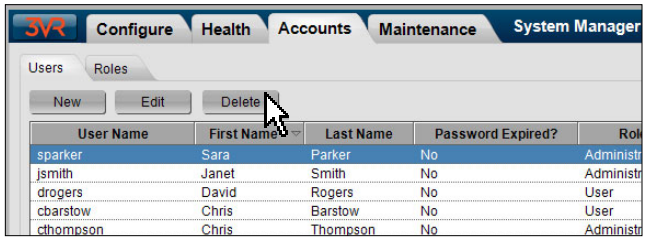


DRA

3.6 Deleting an Account

> **Warning**
> Deleting a user account is permanent and cannot be undone. For accounts that you may need later, disable them instead — see section 3.3 for more information.

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Select the user account to delete from the list.
3. Click **Delete**.
4. In the **Confirm** dialog box, click **Delete** to permanently delete the user account.



4. USER ROLES

Each user account on a VisionPoint™ VMS server must be assigned a user role. You should assign accounts a role that encompasses the highest level of access required for the user's day-to-day interaction with the system, without granting unnecessary permissions that may result in system configuration errors or accidental data loss.

4.1 User Role Basics

There are three default user roles. They are listed below in ascending order by degree of access to the system:

- **User**
- **Administrator**
- **Integrator**

If your organization needs a more granular system of user roles, a user with administrator or integrator permissions can define custom user roles in 3VR System Manager. Custom user roles allow you to create a new role and pick and choose which features you want to grant to users with that role.

The three default roles, as well as any custom user roles that you created, populate in the **Roles** drop-down menu of the **Edit User** dialog box.

DRAFT

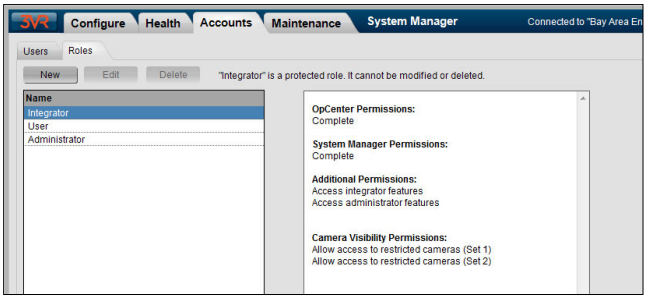
4.2 Viewing User Role Details

Accounts assigned a role with administrator or integrator permissions can view detailed information about all user roles with permissions equal to or less than their own from the **Accounts** panel.

To view the details of an existing role:

1. Click the **Roles** sub-tab.
2. Select a role from the list.

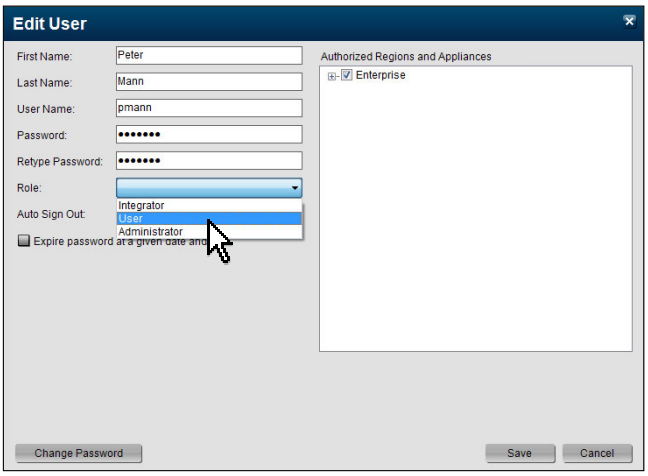
   The set of permissions that comprise the role are displayed in the right-hand panel.



4.3 Assigning Roles to User Accounts

Follow the steps below to change the role assigned to a new or existing user account:

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Click the user account you wish to modify, and then click the **Edit** button (or click the **New** button to create a new user).
3. Click the drop-down arrow next to **Role** and select one of the available **Roles**.
4. Fill out the remaining user details.
5. Click **Save**.



4.4 About the Default User Roles

This section describes the user roles that are included with the 3VR VisionPoint software.

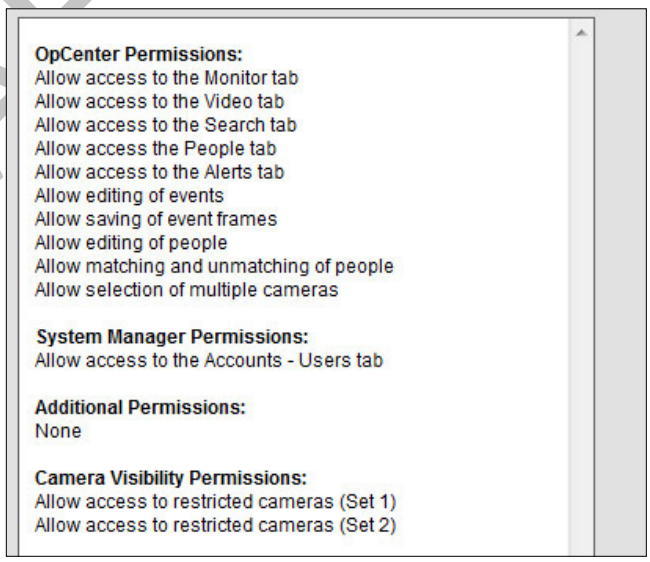
The "User" Role

Accounts assigned the default "user" role are allowed access to 3VR OpCenter only.

Within OpCenter, users can access all panels except the **Cases** panel.

Users can view and edit events and people, but can only view alerts and alert actions. They cannot create alerts or export video from the system.

The image on the right shows all of the permissions granted to the user role.



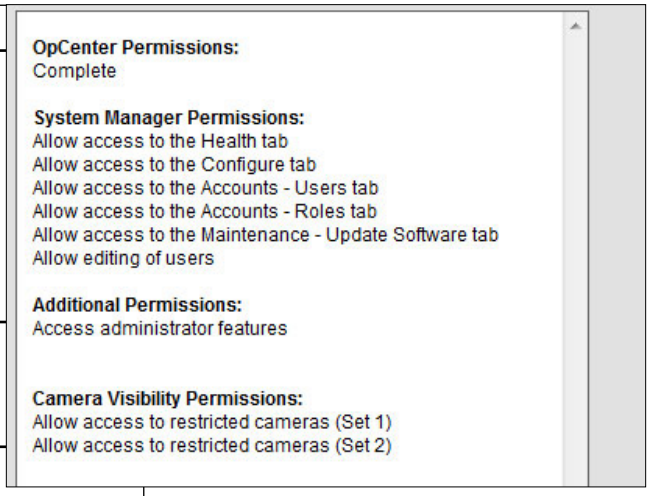
DRAFT

The “Administrator” Role

Administrators have full access to 3VR OpCenter. This includes the ability to export video, create alerts, and manage cases.

In 3VR System Manager, users with the administrator role are able to perform the following tasks:

Administrator Features	
General	Set system date and time Edit email settings Restart server/software View system storage projections Add/update license keys View current system status Edit UPS settings Set maximum bandwidth Set up recording schedules
Cameras	Change camera names Enable/disable cameras Edit video quality settings Enable continuous recording
Analytics	Configure face finding Configure motion and motion direction analysis
Accounts	Create/edit accounts with user and administrator permissions Create user roles
Maintenance	View/edit health alerts and copy system logs
Enterprise	Add/remove/move regions and VMS servers



The default user account for the administrator role is **admin**.

Reference

See the document *Configuring Covert Cameras* for more information about restricted camera sets 1 and 2.

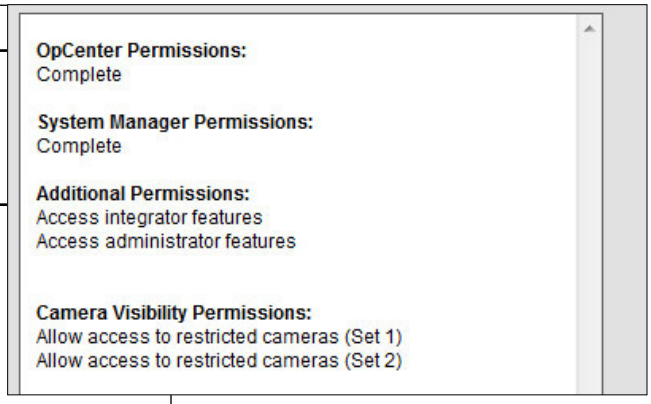
DRAFT

The “Integrator” Role

The integrator role incorporates all of the permissions of the user and administrator roles, as well the functions performed during initial system configuration and other settings that are modified only in specific use cases.

Integrators can perform the following tasks, in addition to the Administrator Features outlined in the previous section:

Integrator Features	
General	Configure network settings Set install/certification date Enable local OpCenter Configure storage settings View earliest content value
Cameras	Add/remove cameras Edit camera type Copy camera settings Restore camera to default Edit analog video input ID Edit camera visibility Edit advanced IP camera settings Set analog video detection precision
External I/O	Install and configure alarms and other digital I/O devices
Plug-ins	Install and configure plug-ins
Analytics	Configure advanced motion settings Configure advanced face settings
Accounts	Create/edit users with user, administrator, and integrator access Configure users with restricted camera visibility
Maintenance	Enable/disable health alerts Set alert thresholds Edit the known host setting
Enterprise	Edit database backup settings Set client application update URL



The default user account for the Integrator role is **techrep**.

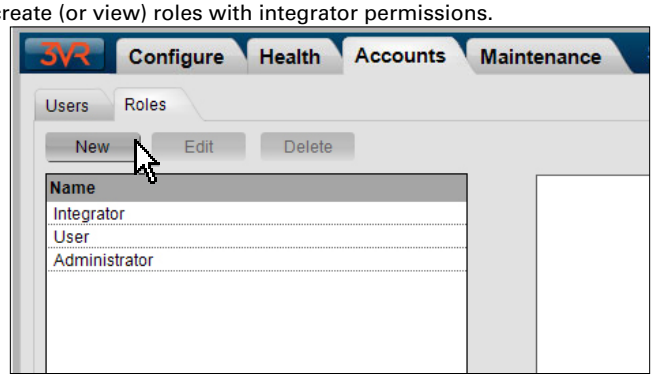
DRAFT

4.5 Creating Custom User Roles

Custom user roles allow you to pick and choose which features of your system a user can access. Both administrators and integrators can create custom user roles, but administrators cannot create (or view) roles with integrator permissions.

To create a custom user role:

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Click the **Roles** tab.
3. Click **New** to create a new role.



4. Enter a descriptive **Name** for the new role.

   This name appears in the **Roles** drop-down menu in the **Edit User** dialog box.

5. In the **Permissions** panel, define the features of OpCenter and System Manager you want to include in the user role:

   - To give the role access to all features in OpCenter or System Manager, check the boxes beside

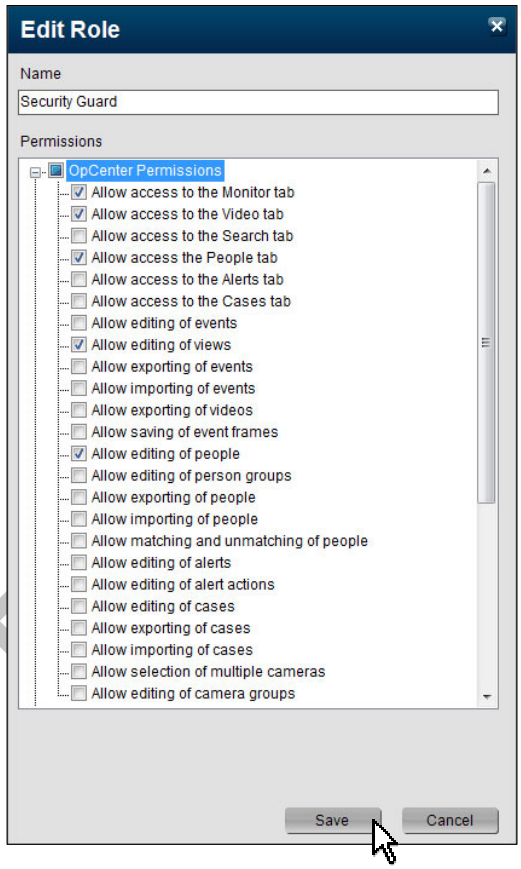
     3VR OpCenter Permissions or
     3VR System Manager Permissions

   - To limit access to specific functions within OpCenter or System Manager, check the box beside each function you wish to include in the role. For example, to create a user role with access to streaming video only, check the box next to **Allow access to the Video Tab**.

   - To grant administrative permissions, under Additional Permissions, check **Access Administrator Features**.

   Note
   See section 4.4 for the comprehensive list of Administrator features.

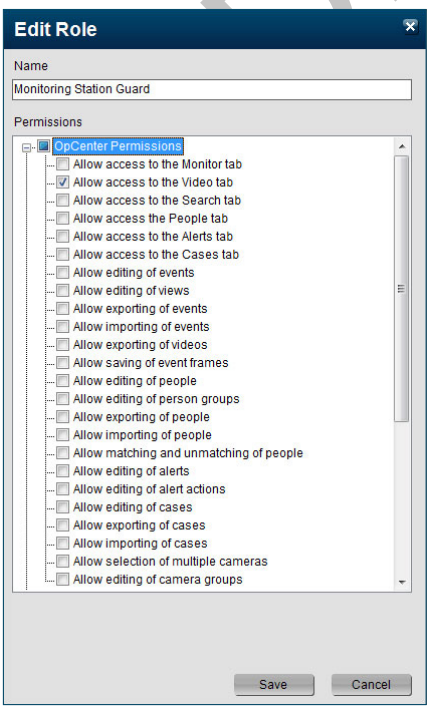
6. Click **Save** to create the role.



4.6 Sample Custom User Roles

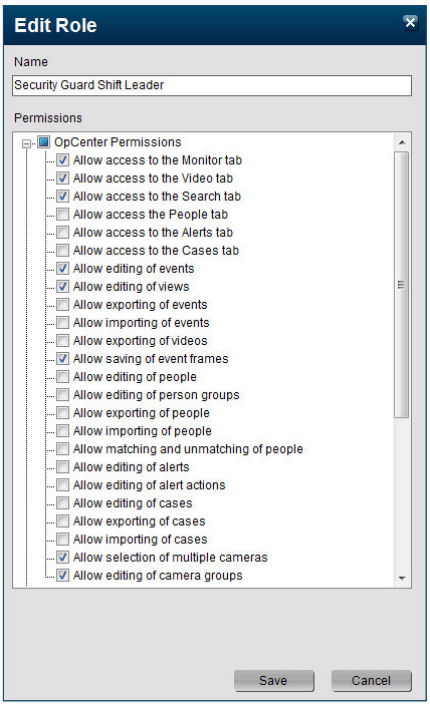
Monitoring Station Guard

Users with this role have access to live video feeds, but are not able to search for stored video or view events.



Security Guard Shift Leader

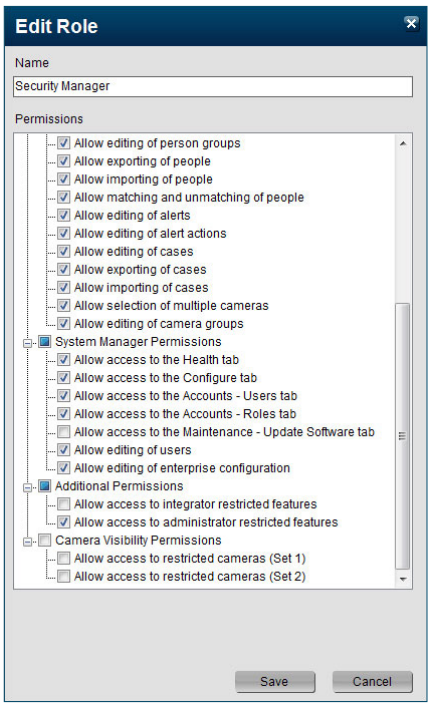
Users with this role are able to watch live and stored video, and view events (including face and transaction events).



DRAFT

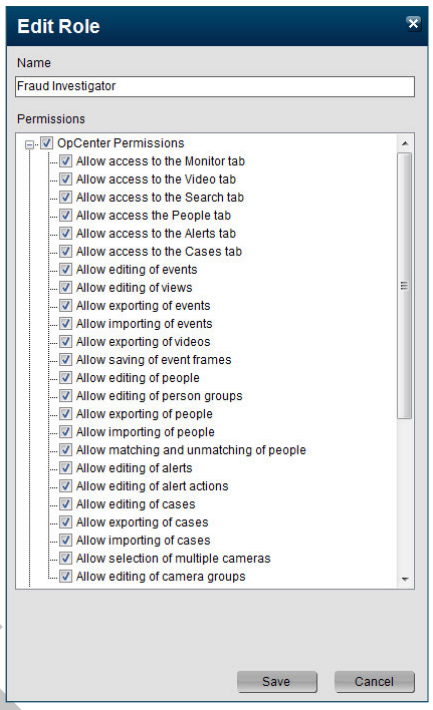
Security Manager

The manager role has full access to 3VR OpCenter. This includes advanced features, such as creating cases and setting up alerts and alert actions. In addition, the manager should have partial access to 3VR System Manager to perform administrative functions, like creating new users and checking system health alerts.



Fraud Investigator

A fraud investigator needs full access to 3VR OpCenter, including live and stored video, and the ability to create cases to manage ongoing investigations.



DRAFT

5. ACCOUNT SECURITY

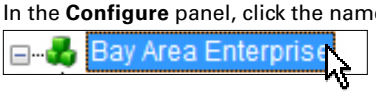
The section describes the rules relating to passwords and how to unlock a suspended user account.

5.1 User Password Constraints

By default, VisionPoint™ VMS places few restrictions on user behavior regarding passwords — users are not required to change their passwords, and any character combination is permissible as long as the password is a minimum of 5 characters. However, 3VR administrators may enforce stricter requirements on passwords by modifying the settings under the **Password Constraints** header in the **Configure** panel of System Manager.

Perform the following steps to enable password constraints on a VMS server or Enterprise server:

1. In the **Configure** panel, click the name of the VMS server or Enterprise server in the left-hand panel to view the system settings.

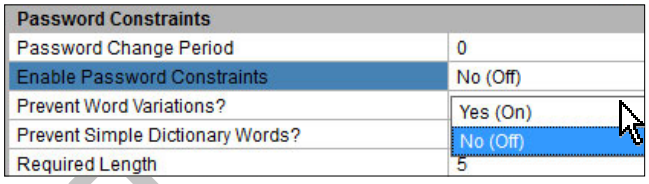


2. On the right side of System Manager, scroll down to the **Password Constraints** settings category.

3. Click the drop-down arrow next to **Enable Password Constraints** and select **Yes (On)**.

4. Click **Save**.

5. When **Enable Password Constraints** is set to **Yes (On)**, the following settings take effect to control the format of passwords:



DRAFT

Password Constraints	
Password Change Period	0
Enable Password Constraints	**Yes (On)**
Prevent Word Variations?	No (Off)
Prevent Simple Dictionary Words?	No (Off)
Required Length	5
Require Lower Case Characters?	No (Off)
Require Numeric Characters?	No (Off)
Require Non-Alphanumeric Characters?	No (Off)
Require Upper Case Characters?	No (Off)
Maximum Signin Failures	20
Maximum Inactive Days	365
Maximum Stored Old Passwords	0

Required Length

Default: **5 characters**
Range: **5-30 characters**

Require passwords to contain a minimum number of characters.

Require Lower Case Characters

Default: **No (Off)**

Require passwords to contain lowercase characters (a-z).

Require Upper Case Characters

Default: **No (Off)**

Require passwords to contain uppercase characters (A-Z).

Require Numeric Characters

Default: **No (Off)**

Require passwords to contain numbers (0-9).

Require Non-Alphanumeric Characters

Default: **No (Off)**

Require passwords to contain non-alphanumeric characters (#%*&@^ , etc.).

Prevent Simple Dictionary Words

Default: **No (Off)**

Reject passwords if found in a dictionary of common words (potato, hat, etc.)

Prevent Word Variations

Default: **No (Off)**

Reject passwords if the password is found in a dictionary of common words with only slight modification (p0tato, hat1, etc.)

The remaining **Password Constraints** settings restrict user behavior with respect to password changes.

Maximum Sign-in Failures

Default: **20 attempts**
Range: **3-20 attempts**

After this number of failed sign-in attempts, the user will be blocked from the system and their administrator will need to unlock the account.

Password Change Period

Default: **0**
Range: **0-1825 days**

The number of days a user may keep the same password, after which he/she is prompted to create a new password. Leaving this value at 0 (the default) disables this setting.

Maximum Inactive Days

Default: **365**
Range: **30-365 days**

If a user does not sign in to the system for this number of days, he/she will be prompted to create a new password at next login.

Maximum Stored Old Passwords

Default: **0**
Range: **0-9 passwords**

The number of previous passwords stored in memory. If password constraints are enabled and this value is not 0, a new password will only be accepted if it is different from this number of previous passwords.

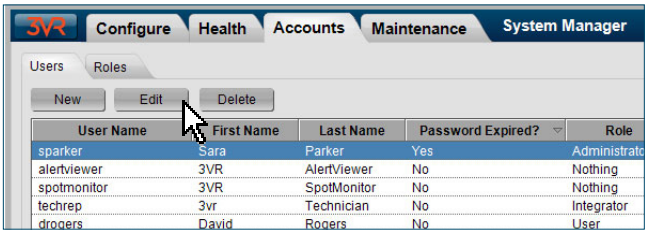
DRAFT

Locked Accounts
See section 3.4 for information on unlocking a user account that has been locked after too many failed sign-in attempts.

5.2 Unlocking a Suspended User Account

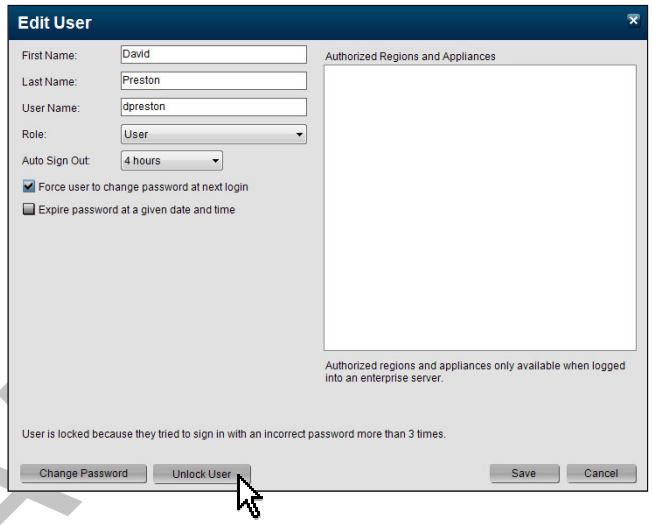
If **Enable Password Constraints** is set to **Yes (On)**, users who enter incorrect login credentials beyond the number of times specified in the **Maximum Sign-in Failures** setting will be locked out of the system until an administrator resets the account by performing the following steps:

1. In System Manager, click **Accounts** to go to the **Accounts** panel.
2. Select the suspended user account from the list.
3. Click **Edit**.



4. In the **Edit User** dialog box, click **Unlock User**.
5. If the user entered incorrect information because he or she has forgotten the password, reset it using the steps in section 3.4 of this chapter.

   Otherwise, check the box next to **Force user to change password at next login** so the user can reset his/her own password.



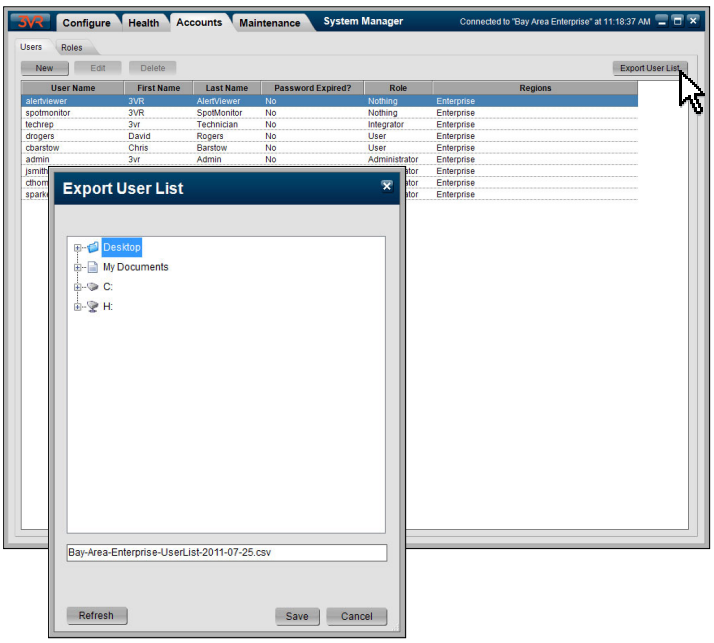
6. ACCOUNT ADMINISTRATION

This section describes how to perform common account administration tasks, including exporting user lists, viewing connected users, and auditing user accounts.

6.1 Exporting the User List

Perform the following steps to export the list of user accounts to a CSV (comma separated values) file:

1. In System Manager, go to the **Accounts** panel.
2. Click **Export User List**.
3. In the **Export User List** dialog box, navigate to the folder on your computer or an external drive where you wish to save the user list.
4. Click **Save**.



DRAFT

5. When the export is finished, click **OK** to return to the **Accounts** panel. You can open the exported CSV file in a spreadsheet application, such as Microsoft® Excel®.

Bay-Area-Enterprise-UserList-2011-08-26.csv

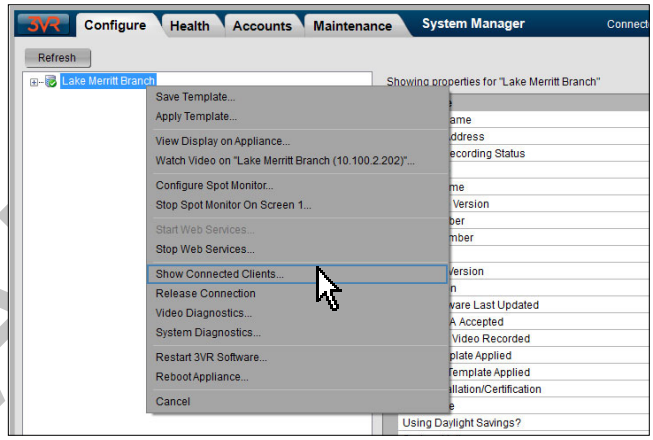
	A	B	C	D	E	F	G
1	User list generated by user '3vr Technician' on 8/26/2011 5:18:09 PM from Bay Area Enterprise (10.100.2.22)						
2	User Name	First Name	Last Name	Password Expired?	Role	Region	
3	techrep	3vr	Technician	No	Integrator	Enterprise	
4	drogers	David	Rogers	No	User	Enterprise	
5	cbarstow	Chris	Barstow	No	User	Enterprise	
6	admin	3vr	Admin	No	Administrator	Enterprise	
7	jsmith	Janet	Smith	No	Administrator	Enterprise	
8	cthompson	Chris	Thompson	No	Administrator	Enterprise	
9	sparker	Sara	Parker	No	Administrator	Enterprise	
10							

6.2 Viewing Connected Users

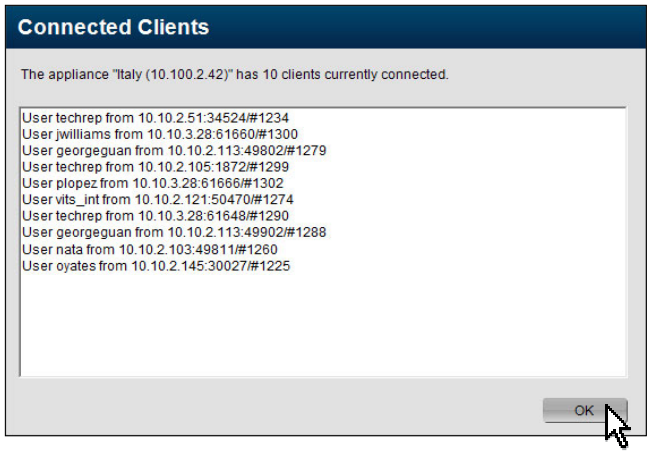
Perform the following steps to check which user accounts are currently logged in to VisionPoint™ VMS.

1. In System Manager, go to the **Configure** panel.

2. Right-click the VMS server display name and select **Show Connected Clients**. The **Connected Clients** dialog box display a list of the user names and IP addresses currently connected to the system.



3. When you finish reviewing the connected clients, click **OK** to return to the **Configure** panel.



DRAFT

6.3 Auditing User Accounts (Fall Release-2015 (8.1.x and above) only)

You can generate a report on the actions performed by users on a specified VMS server. User Audit provides audit information about users that access the system and the actions performed by the users, including the clients the users connected from.

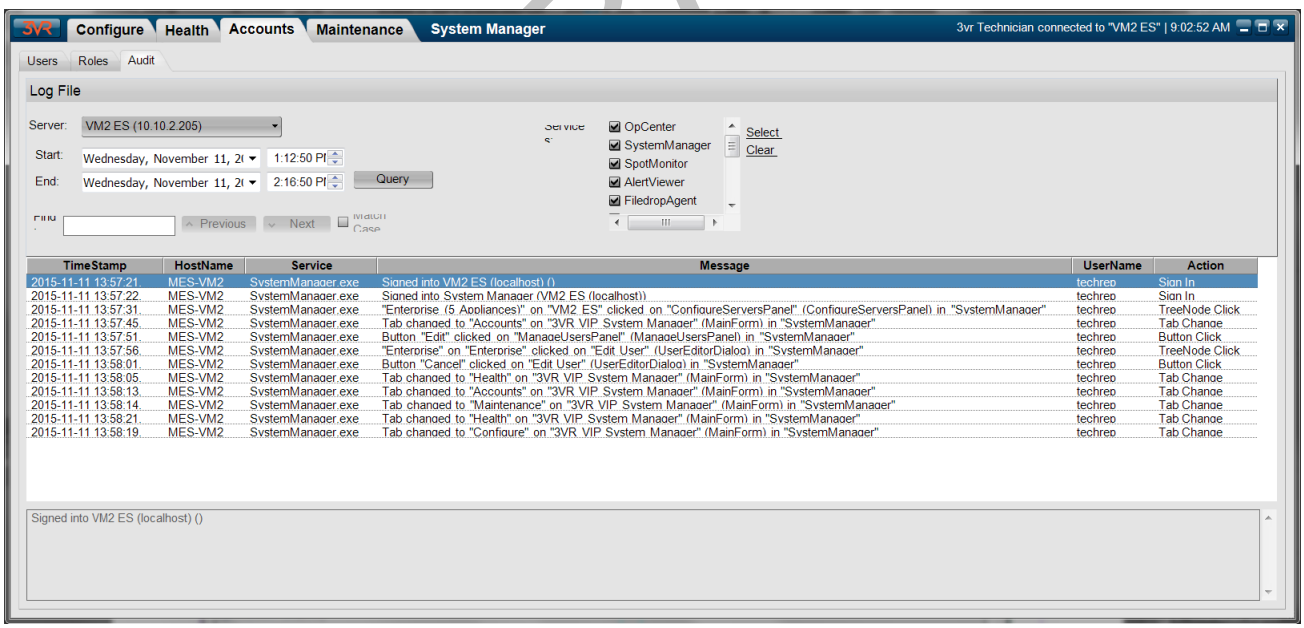
The information displayed includes:

- Username of the user who performed the actions.
- The actions the user performed, for example, signed in, clicked button, and so on. A message describing the action also appears, for example, “Signed into System Manager (VMS Server name, IP_Address)” where: VMS Server name is the name of the VMS server and IP_Address is the VMS server’s IP address. “localhost” shows that the user directly logged into the VMS server.
- The dates and times the actions occurred.
- The hostname of the machine used to log into the VMS server.
- The VMS server service involved, for example, SystemManager.exe.

If the appliance is connected to the enterprise, the **Audit** tab displays only when you log in to the enterprise; it will not display if you log in to the appliance directly. On a standalone appliance (that is not part of an enterprise), the **Audit** tab displays on the appliance side.

1. Click the **Accounts** tab and then click the **Audit** tab. The Audit pane appears.
2. Select the desired VMS server from the **Server** drop-down menu.
3. Select the desired start and end date/times using the **Start** and **End** controls. This selects the period of time for which you want to receive information.
4. Click the **Query** button. System Manager displays status messages about the process of downloading and parsing the system logs.

System Manager displays the audit information of the specified VMS server during the specified time range.



DRAFT

Filtering Services

When you initiate an audit, all the 3VR VMS server services are retrieved and displayed. You can then filter out service information to focus on specific service actions.

- To clear information about all services, click **Clear**. Check the boxes besides the services of interest.
- To display information about all services, click **Select**.

Searching Through the Audit Information

You can search on text in the displayed audit information.

1. Enter the desired text in the **FIND** field. Optionally, check the **Match Case** box to match the case.
2. Click **Next** to find the next instance; click **Previous** to find the previous instance. System Manager highlights the line containing the matching text.

7. ENTERPRISE USER MANAGEMENT

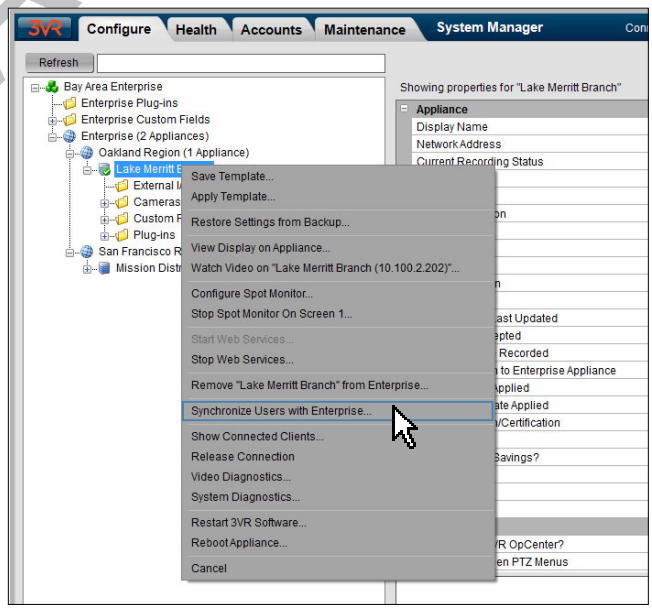
This section describes how to sync users with the Enterprise.

7.1 Syncing Users with the Enterprise

Whenever you add a new VisionPoint™ VMS server to the Enterprise, the user accounts on the unit automatically sync with the master list of users on the Enterprise. You may also manually sync the user accounts on a VMS server with the Enterprise at any time from the **Configure** panel of System Manager:

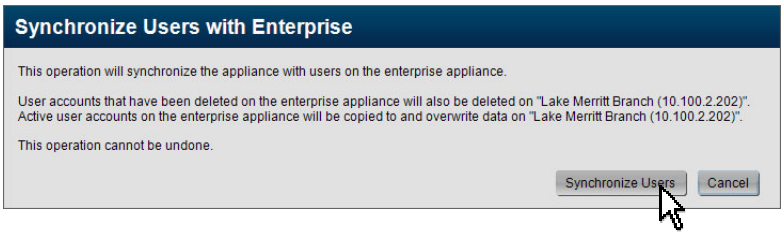
DRAFT

1. Right-click the name of the VMS server and select **Synchronize Users with Enterprise** from the menu.



2. In the dialog box that appears, click **Synchronize Users** to confirm.

   All user accounts on the system will be erased and replaced with the master user list on the Enterprise server.



7.2 Synchronizing with LDAP Servers

3VR Enterprise Server supports user synchronization with the following types of LDAP servers:

- Microsoft Active Directory (MSAD)
- Oracle Directory Server (ODSE)
- Lightweight Directory Access Protocol (LDAP)

By selecting your LDAP server type, configuring the correct settings, and synchronizing users, the VisionPoint software can transfer the accounts from your LDAP server to the 3VR system. This allows users to use their credentials from their Enterprise account to easily log into the 3VR system.

Note
Only users with Administrator or Integrator roles can configure LDAP. The 3VR system supports LDAP 2 and 3.

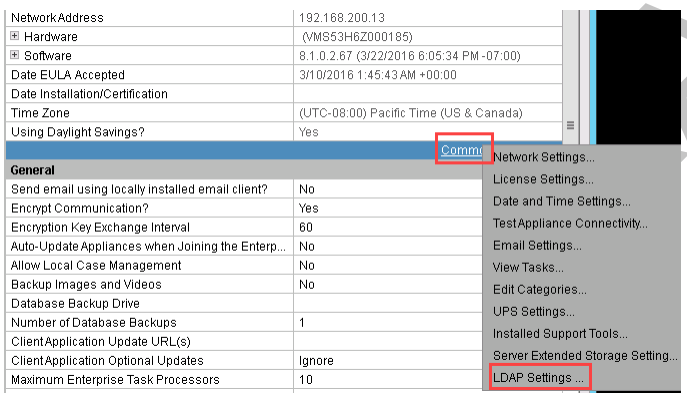
For additional information on LDAP configuration, you can refer to:

https://docs.oracle.com/cd/E17236_01/epm.1112/hss_admin/frameset.htm?ch03s05.html

Enabling LDAP

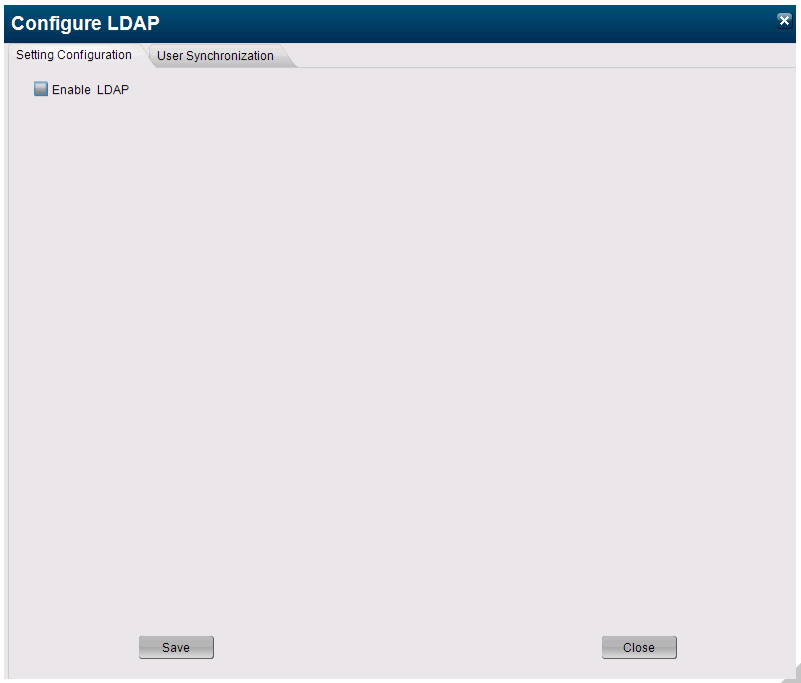
The first step with all types of LDAP servers is to enable LDAP.

1. From 3VR System Manager, log into the 3VR Enterprise Server.
2. In the Configure panel, click the 3VR Enterprise Server in the left-hand panel to view the system settings.
3. Under the Appliance category heading, click Common Operations, and then click **LDAP Settings**.



DRAFT

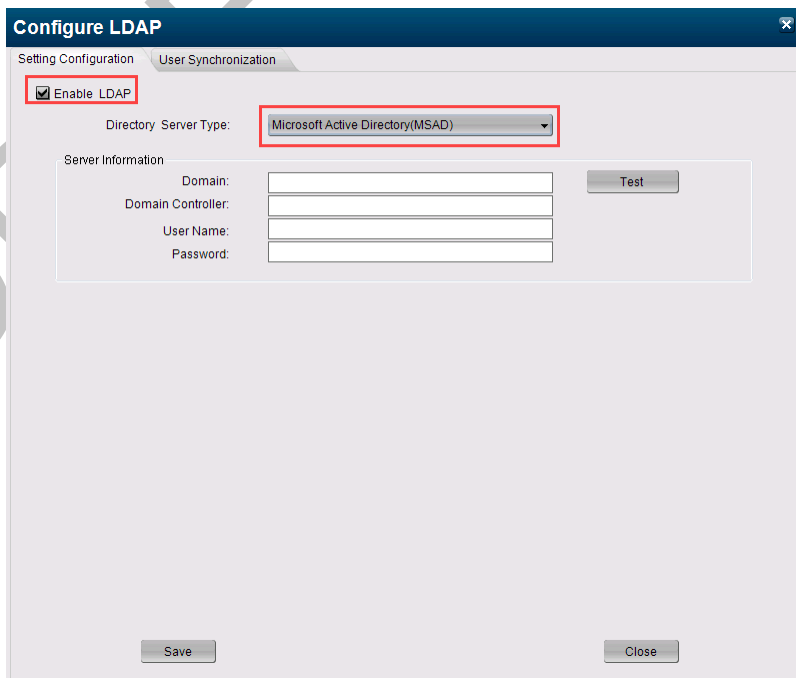
The Configure LDAP dialog box appears.



4. Check the Enable LDAP box. The following controls appear.

Configuring LDAP Server Settings

You need to select your Enterprise's LDAP server type and configure the settings that allow the 3VR system to synchronize with your LDAP server's user account information.



Configuring Microsoft Active Directory Settings

Perform the steps in this section if your Enterprise uses Microsoft Active Directory.

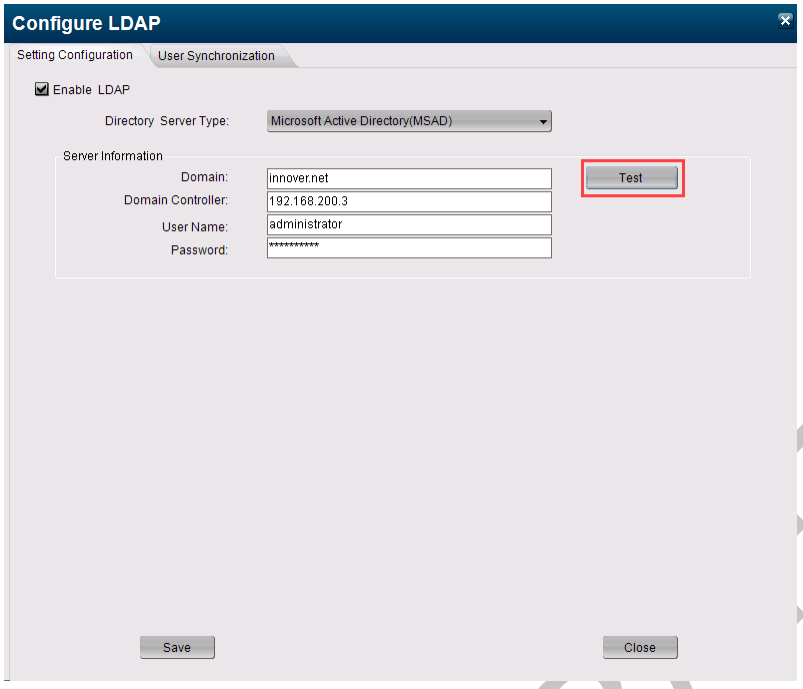
1. Select **Microsoft Active Directory (MSAD)** from the Directory Server Type drop-down menu. The controls for this directory server type appear.

2. Fill in the text boxes with the appropriate information for your MSAD server. If necessary, contact your system administrator for this info.

DRAFT

Setting	Description
Domain	Enter the domain name for your Enterprise.
Domain Controller	Enter the IP addresses of any domain controllers, separated by a comma.
User Name	Enter the valid user name of user who can connect to the LDAP server (this is typically a user with administrative privileges for the LDAP server).
Password	Enter the user's password.

See the screenshot below for an example.



3. When finished entering the info., click the **Test** button to test the connection to your LDAP server. The following messages appear to show the result of the test.

Message	Description
Successful	Shows the connection succeeded.
Server connection failed. Please check the domain controllers.	Shows the connection failed due to problems connecting to the domain controller. If this occurs, make sure you entered the correct info. for your LDAP server.
User name or password is wrong	Shows the connection failed due to the wrong credentials. If this occurs, make sure you entered the correct user credentials.
Password	Enter the user's password.

4. After successfully testing the connection, click **Save** to save the settings.

5. Proceed to "Synchronizing Users" on page 116 .

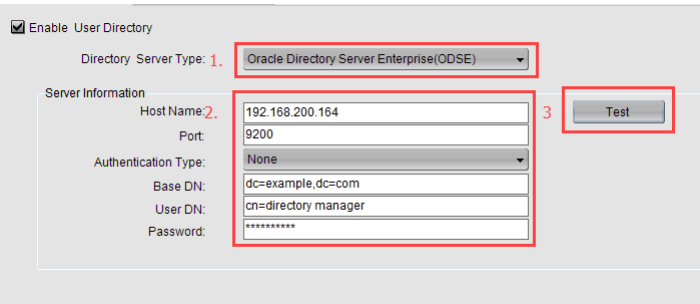
DRAFT

Configuring Oracle Directory Server Enterprise Settings

Perform the steps in this section if your Enterprise uses Oracle Directory Server Enterprise.

1. In the Configure User Directory dialog box, select the **Setting Configuration** tab, and then select **Oracle Directory Server Enterprise (ODSE)** from the Directory Server Type drop-down menu. The controls for this directory server type appear.

2. Use the drop-down menu and fill in the text boxes with the appropriate information for your LDAP server. See the screenshot above for an example. If necessary, contact your system administrator for this info.



Setting	Description
Host Name	Enter the IP address of your LDAP server.
Port	Enter the port on which LDAP is running.
Authentication Type	Select the authentication type used on the LDAP server from the drop-down menu. The options are: None and SSL. SSL enables secure communication with the LDAP server.
Base DN	Enter the distinguished name (DN) of the node where the search for users and groups should begin.
User DN	Enter the distinguished name of the user that Shared Services should use to bind with the LDAP server. This distinguished name must have read privileges within the Base DN common name of a user on the LDAP server.
Password	Enter the User DN password.

3. When finished entering the info., click the **Test** button to test the connection to your LDAP server. The following messages appear to show the result of the test.

Message	Description
Successful	Shows the connection succeeded.
Please check the ODSE configuration. Please check the domain controllers.	Shows the connection failed due to incorrect host name or port settings. If this occurs, make sure you entered the correct host name and port settings.
UserDN or password is wrong	Shows the connection failed due to the wrong credentials. If this occurs, make sure you entered the correct user credentials.
BaseDN is wrong	Shows the connection failed because the wrong BaseDN was entered. If this occurs, make sure you entered the correct BaseDN.

4. After successfully testing the connection, click **Save** to save the settings.

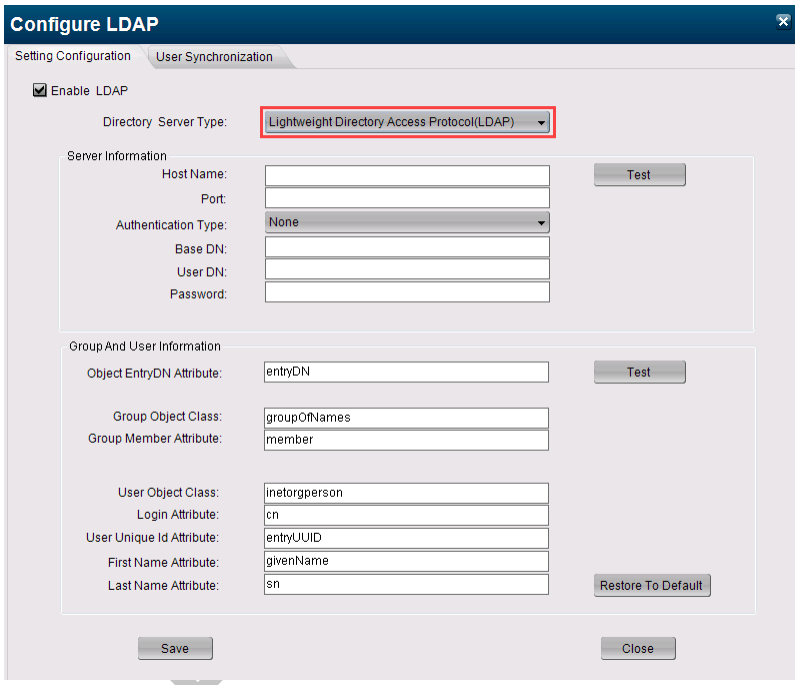
5. Proceed to "Synchronizing Users" on page 116 .

DRAFT

Configuring LDAP Settings

Perform the steps in this section if your Enterprise uses the Lightweight Directory Access Protocol.

1. In the Configure LDAP dialog box, select the Setting Configuration tab, and then select **Lightweight Directory Access Protocol (LDAP)** from the Directory Server Type drop-down menu. The controls for this server type appear.



2. Enter the correct Server Information settings for your network. See "Configuring Oracle Directory Server Enterprise Settings" on page 113 for information about these settings.

> **Note**
> The Group and User Information settings are provided as defaults that apply in several cases. However, you may need to modify them to match your LDAP configuration. If you change these settings and then decide you want to restore the default settings, click the **Restore to Default** button.

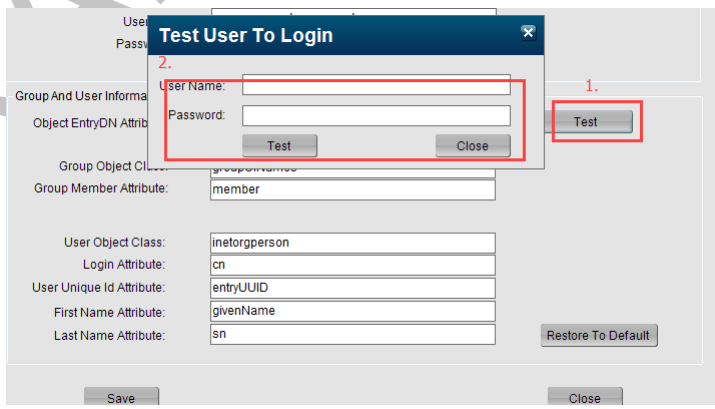
3. Fill in the text boxes with the appropriate information for your LDAP server. See the screenshot above for an example. If necessary, contact your system administrator for this info. The table below describes the parameters.

4. When finished entering the info., click the **Test** button to test the connection to your LDAP server. A dialog box appears.

5. Enter the user name and password for a valid user in the LDAP directory.

6. After successfully testing the connection, click **Save** to save the settings.

7. Proceed to the "Synchronizing Users" section.



DRAFT

Group and User Information Parameters [1]

Parameter Names	Description	Examples
ObjectEntryDN Attribute	The attribute that stores the EntryDN Attribute.	Distinguishedname(AD)/ entrydn(ODSE)/ others
Group Object Class	The object classes of the group. Using these object classes in the search filter, the 3VR system should find all groups associated with the user. If there is more than one value, join the values with a semicolon (;), for example, "groupclass1; groupclass2".	group(AD)/ groupOfUniqueNames(ODSE)/ groupOfNames/ others
Group Member Attribute	The attribute that stores the group member attribute.	member(AD)/ uniquemember(ODSE)/ others
User Object Class	Object classes of the user. Using these object classes in the search filter, the 3VR system can find all users who should be provisioned. If there is more than one value, join them with a semicolon (;), for example, "organizationalPerson; inetorgperson".	user(AD)/ inetorgperson(ODSE)/ others
Login Attribute	A unique attribute (can be a custom attribute) that stores the login name of the user.	sAMAccountName(AD)/ uid(ODSE)/ cn/ others
User Unique id Attribute	A read-only unique attribute (can be a custom attribute) of the user.	objectSid(AD)/ nsuniqueid(ODSE)/ entryUUID/ others
User First Name Attribute	The attribute that stores the user's first name.	givenName
User Last Name Attribute	The attribute that stores the user's last name.	sn

DRAFT

1 Note: In the examples in the table, (AD) denotes Active Directory examples; (ODSE) denotes ODSE examples; others denotes LDAP examples.

Synchronizing Users

After you configure the settings for your LDAP server, you need to sync users. When System Manager synchronizes with the LDAP server for the first time, the system automatically creates 3VR user accounts for each LDAP server user checked in the Select Users to Synchronize panel.

It is recommended to periodically manually or automatically sync changes to your LDAP directory. Changes include new employees added to the directory.

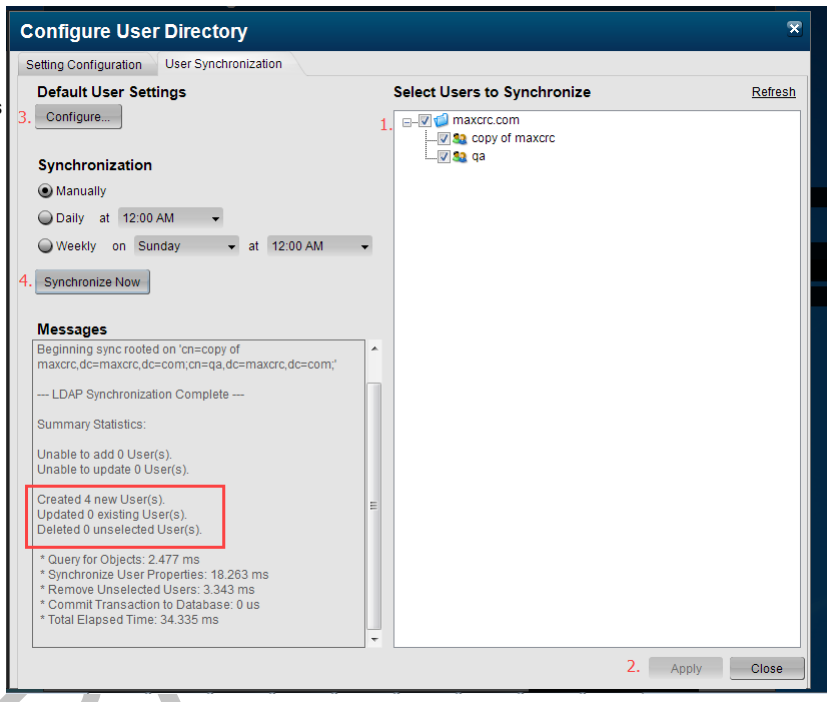
1. In the Configure User Directory dialog box, click the User Synchronization tab. The User Synchronization pane appears.

2. In the Select Users to Synchronize panel, specify the LDAP accounts you want to synchronize with the 3VR system. The top level represents your Enterprise domain. The entries below the domain represent security groups of users.

   - Check the box next to the domain name to create an account for every LDAP directory user.

   - Check the box next to a security group to create an account for every member of the group.

3. Click the **Apply** button.



4. Click the **Configure** button to configure the synchronized users. The Default User Settings dialog box appears. In this step, you specify the account settings to apply to each auto-generated account in the 3VR system.

5. Click the **Role** drop-down menu and select the role to assign to LDAP directory user accounts.

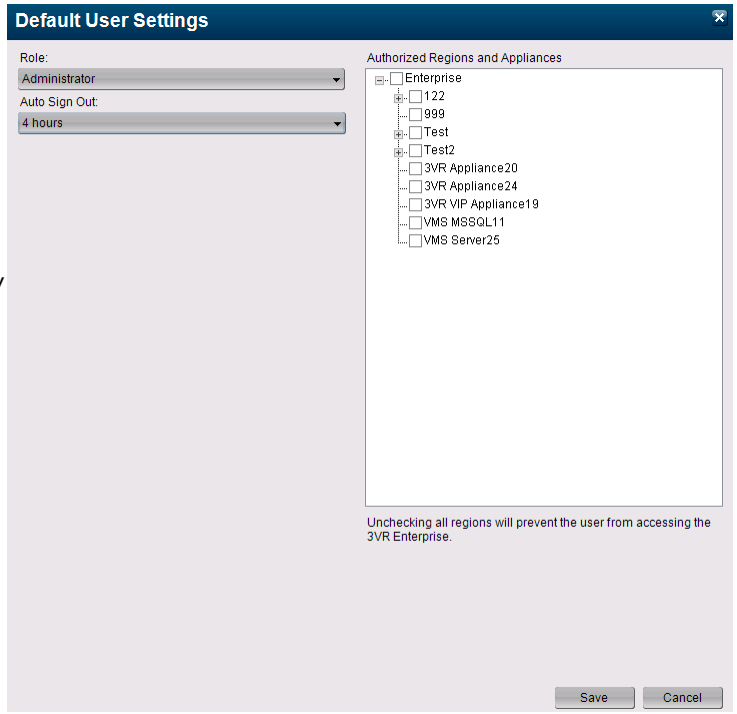
6. If you want to log out the LDAP directory user accounts from the system after a period of inactivity, select an auto sign out interval from the **Auto Sign Out** drop-down menu.

7. In the Authorized Regions and Appliances panel, select the VMS servers or regions you want the LDAP directory users to be able to access:

   - Check the box next to the Enterprise Appliance to grant access to every appliance on the Enterprise.

   - Check the box next to a region to allow users to connect to all appliances within the region.

   - Check and uncheck individual appliances to restrict access to only those appliances.

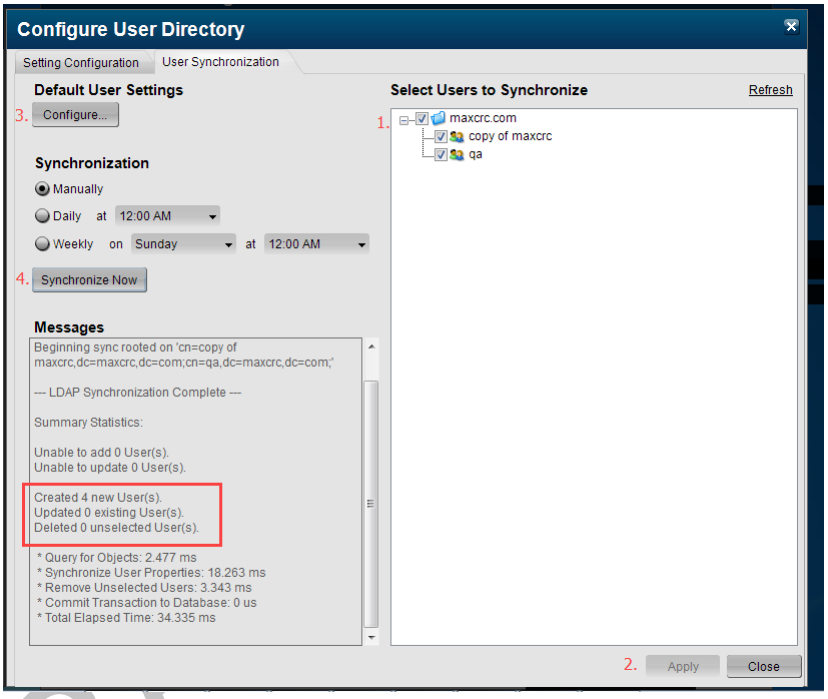


8. Select how you want to sync users.

   - Select the **Manually** button to sync just this one time.
   - To automatically sync users daily, select the **Daily** button and choose the desired time for the sync from the drop-down menu.
   - To automatically sync users weekly, select the **Weekly** button and choose the desired day of the week and time for the sync from the drop-down menus.

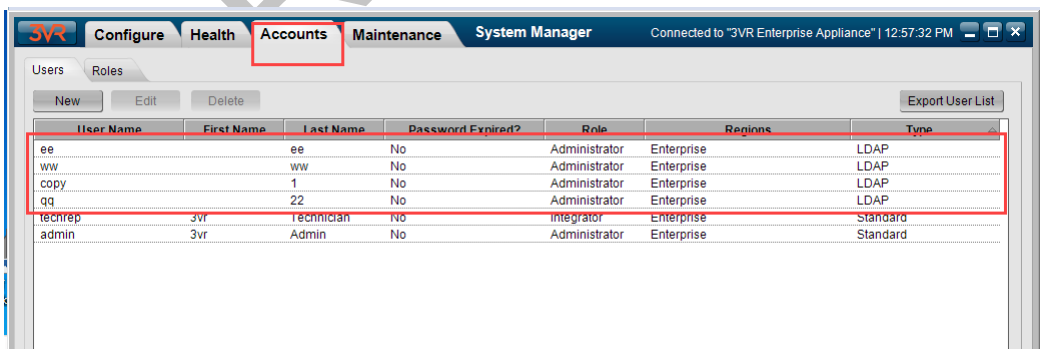
9. Click the **Synchronize Now** button. Messages about the sync appear.

10. Click **Close** when finished. You return to the Accounts pane.

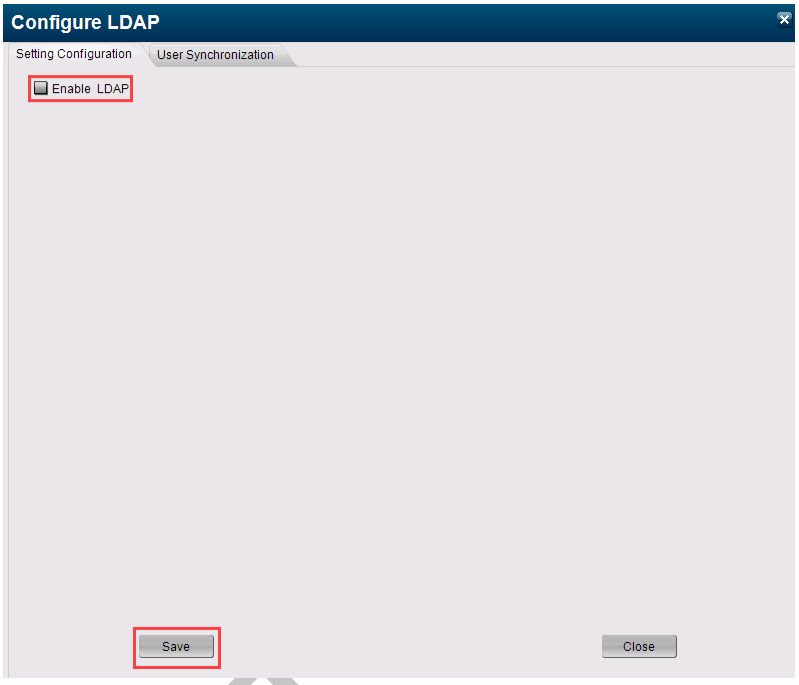


The users in the group(s) you selected are added to the Users list.

11. Verify that accounts were created for each selected LDAP directory user.



If you disable LDAP by clearing the Enable LDAP box, the LDAP users will be identified as “Standard” users in the Users list. You might want to do this if your LDAP server is down, but the users you’ve already synced need to log into the 3VR system. In this case, you need to reset the user password(s) in System Manager.



DRAFT

CHAPTER 5
General Camera Configuration

1. VIEWING CAMERAS IN SYSTEM MANAGER 121
   - 1.1 Watch Video on VMS Server 121
   - 1.2 Image Snapshot 121
2. BASIC CAMERA SETTINGS 122
   - 2.1 Viewing Camera Settings 122
   - 2.2 Camera Name 122
   - 2.3 Camera Type 123
   - 2.4 Camera Visibility 123
3. MOTION RECORDING SETTINGS 124
   - 3.1 Motion Sensitivity Settings 124
   - 3.2 Motion-Based vs. Continuous Recording 125
   - 3.3 Other Motion Settings 126
   - 3.4 Using Camera-Based Motion Detection (Fall Release-2015 (8.1.x and above) only) 127
4. FACE FINDING SETTINGS 133
   - 4.1 Enabling or Disabling Face Finding 133
   - 4.2 Measuring Eye Distance 133
   - 4.3 Configuring Face Exclusion Zones 134
5. EVENT VIDEO AND IMAGE SETTINGS 134
   - 5.1 Event Image Size 134
   - 5.2 Event Data Overlays 135
   - 5.3 Event Video and Image Buffering Settings 135
6. CAMERA DISPLAY SETTINGS 136
   - 6.1 Overlay Date and Time 136
   - 6.2 Mask Video in Region 137
   - 6.3 Enable Alarm for Video Loss 137
7. INTERACTING WITH CAMERAS 138
   - 7.1 Resetting a Camera to Default Settings 138
   - 7.2 Copying Camera Configuration 138
   - 7.3 Enabling or Disabling Cameras 139
   - 7.4 Adding a Camera 139
   - 7.5 Deleting a Camera 139

DRAFT

DRAFT

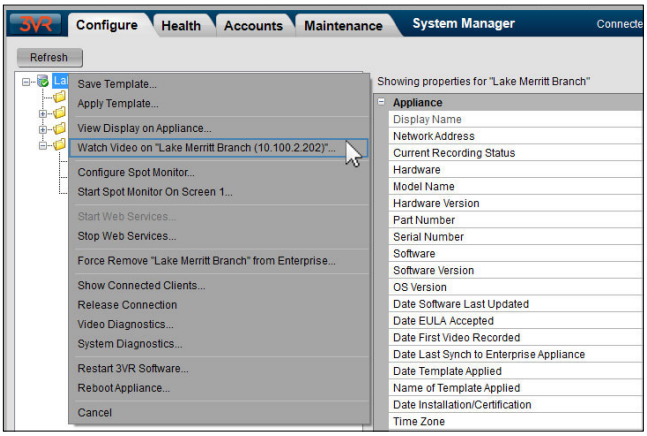
1. VIEWING CAMERAS IN SYSTEM MANAGER

You can use System Manager to view live video feeds from cameras.

1.1 Watch Video on VMS Server

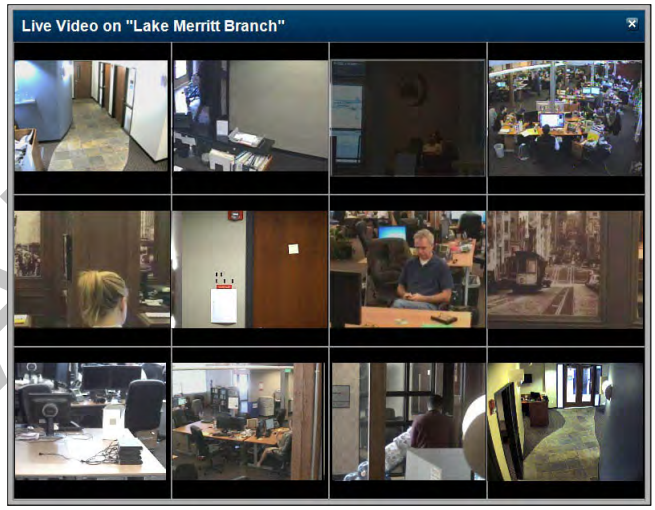
To view live video feeds from all enabled cameras in System Manager:

1. In the **Configure** panel, right-click the system display name and select **Watch Video on "[VMS Server Name]"**.



> **Note**
> [VMS Server Name] is a placeholder for the specified VMS server display name. See the chapter on basic System Manager configuration for information.

2. All of the enabled cameras automatically load when the live video window opens.



DRA

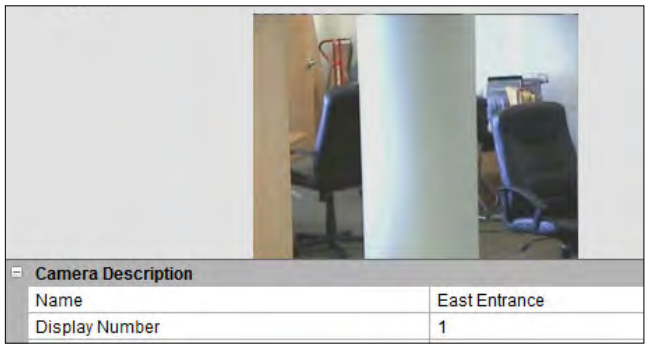
1.2 Image Snapshot

To quickly view a still frame from a single camera:

1. In the **Configure** panel, click the plus sign next to **Cameras** to display the list of all cameras on the system.
2. Select the camera of interest to view its settings.

3. On the right-hand side of System Manager, a thumbnail snapshot from the selected camera appears at the top of the camera settings.

   Click the snapshot to refresh the image.



2. BASIC CAMERA SETTINGS

You can define the name, type, and visibility for each camera.

2.1 Viewing Camera Settings

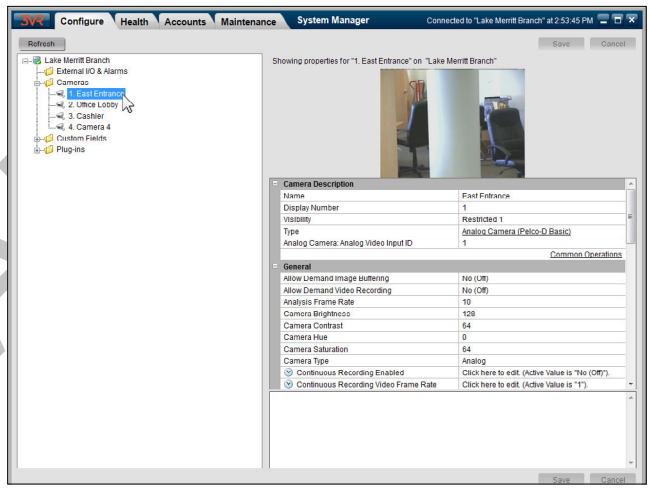
1. In the **Configure** panel of System Manager, click the plus sign (+) next to the VMS server name.

2. Click the plus sign next to **Cameras** to display the list of cameras on the server.

3. To view a camera's settings, click the camera name to highlight it.

   Information about the camera appears to the right, including a thumbnail image of the video feed.

   Use the scroll bar to scroll through the full list of camera settings.



DRA

2.2 Camera Name

Video in OpCenter is labeled with the camera name. By default, cameras are identified by the camera number (e.g., "Camera 1", "Camera 2", etc.). You should rename the cameras to something more descriptive of the camera view:

1. In the **Configure** panel of System Manager, click the plus sign (+) next to the VMS server name.

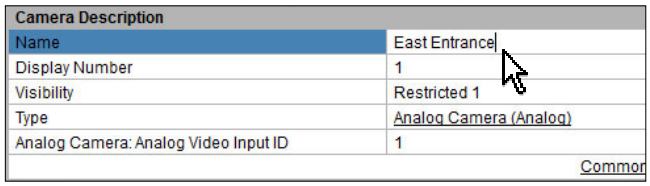
2. Click the plus sign next to **Cameras**.

3. Click to select the camera to be renamed. Information about the camera appears to the right.

4. Under **Camera Description**, locate the **Name** field.

   Edit the camera name according to your naming conventions.

5. Click the **Save** button.

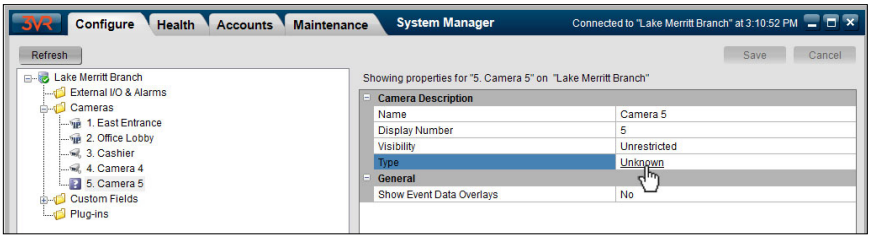


2.3 Camera Type

Though you should generally leave cameras set at their default camera type, there are a few situations when you need to modify the type. For example, if you purchase IP camera expansion for a hybrid 3VR appliance, you need to change the type of an existing camera from **Analog** to **Network Camera**. Perform the following steps to change the camera type of a camera:

1. In the **Configure** panel of System Manager, click the plus sign (+) next to the system name.
2. Click the plus sign next to **Cameras**.
3. Click a camera name to view its settings.

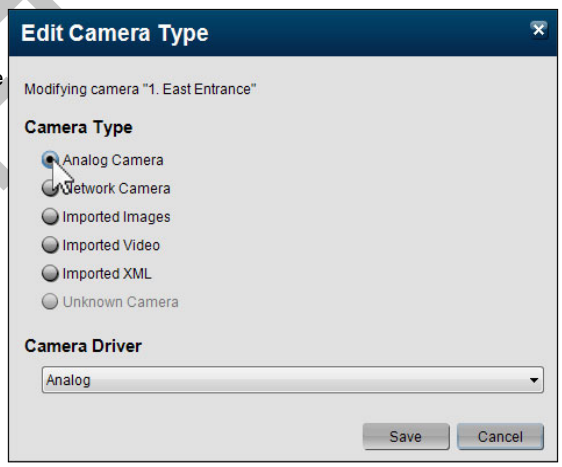
4. On the right-hand side of System Manager, click the link next to **Type** (the link text shows the current camera type, e.g. Analog, Network, or Unknown).



5. Select a different camera type.

   If necessary for the camera type, select a driver for the camera from the **Camera Driver** drop-down menu.

6. Click **Save** to save changes and return to the **Configure** panel.



> **Note**
> Network camera models that are not listed in the **Camera Driver** menu are not officially supported by 3VR.

The following camera types are available:

Analog Camera

See on analog camera configuration for more information about configuring analog cameras.

Network Camera

See the chapter on IP camera configuration for more information about configuring IP cameras.

Imported Images, Imported Video, Imported XML

See the *3VR VisionPoint™ VMS User Manual* for more information about imported content.

2.4 Camera Visibility

The **Camera Visibility** setting allows you to leave the camera as unrestricted or assign it to a restricted camera set. For more information about camera visibility, see the document *Configuring Covert Cameras* available on the 3VR Support Portal (http://partners.3VR.com) or the Installation and Resource DVD.

DRAFT

3. MOTION RECORDING SETTINGS

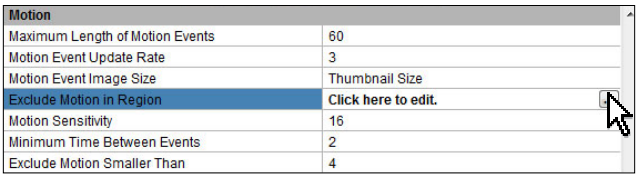
You can configure motion-sensitivity and other motion settings.

3.1 Motion Sensitivity Settings

Environmental factors in the camera's field of view, including background motion, reflections, or camera noise, may generate motion events when no meaningful motion has occurred. Use the following settings to fine-tune the motion-detection analytic:

Exclude Motion in Region

Default: **blank (no excluded regions)**



Motion	
Maximum Length of Motion Events	60
Motion Event Update Rate	3
Motion Event Image Size	Thumbnail Size
Exclude Motion in Region	**Click here to edit.**
Motion Sensitivity	16
Minimum Time Between Events	2
Exclude Motion Smaller Than	4

This setting allows you to exclude activity in specified regions of a camera view when determining whether a motion event has occurred. When you specify a region to exclude, motion detected entirely in that region will not generate a motion event.

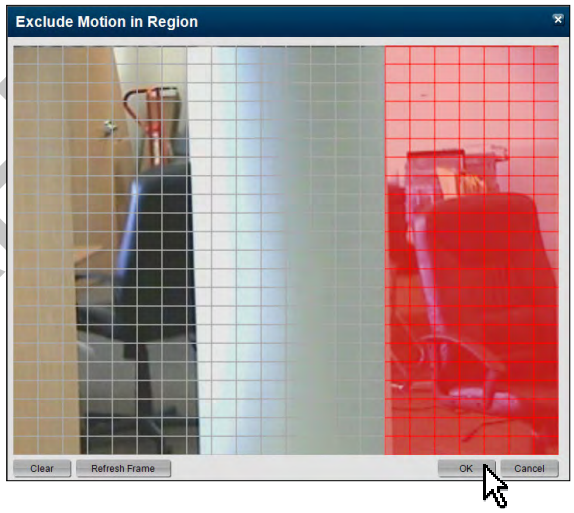
1. To display the camera view with a grid overlay, click the ellipsis (**...**) button beside **Exclude Motion in Region**.

2. Select the region you wish to exclude from motion analysis by clicking and dragging the mouse button. Release the button when the desired area is highlighted.

   - Repeat as necessary to block out multiple regions in the grid. These regions can be separate, contiguous, or overlapping.

   - Click **Clear** to remove all regions from the exclusion zone.

3. When you've selected the desired exclusion region blocks, click **OK** to save the selected regions as motion exclusion zones.



> **Important**
> When editing the **Exclude Motion in Region** setting, it is crucial to remember that the red zones represent the portion of the camera view to *exclude* from motion analysis. Activity in the camera field of view that falls entirely within a red zone will **not** generate motion events.

Exclude Motion Smaller Than

Default: **4**
Range: **2–100 grid blocks**

This setting controls the number of grid squares that must change from one video frame to the next before VisionPoint™ VMS determines a motion event has occurred.

- Set this value larger than 4 if small regions of the video image change enough between frames to generate non-meaningful motion events.

- Values smaller than 4 generally produce too many non-meaningful motion events, and should be set with caution.

- To view a grid overlay of the camera view for comparison, click the ellipsis (...) button beside the **Exclude Motion in Region** field.

Exclude Motion Shorter Than

Default: **1.5**
Range: **0.0–5.0 seconds**

This setting controls the minimum duration of continuous motion before VisionPoint™ VMS determines that a motion event has occurred.

- Set this value larger than 1.5 if brief motion in the camera generates too many non-meaningful motion events.
- Values smaller than 1.5 usually produce too many non-meaningful motion events, and should be set with caution.

Motion Sensitivity

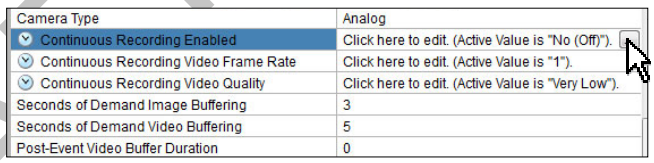
Default: **32**
Range: **0–255**

This setting represents the minimum average change in pixel values across two comparison regions required for motion to be detected.

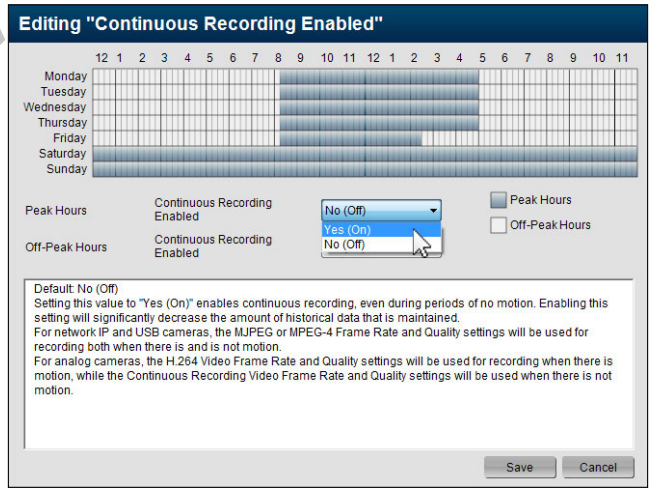
3.2 Motion-Based vs. Continuous Recording

By default, the 3VR system uses motion analysis to only record video when it detects motion in the camera's field of view. Motion-based recording uses significantly less storage space compared to recording continuously. However, you can enable continuous recording on a camera with the **Continuous Recording** setting.

1. Under the **General** settings category, click the ellipsis (...) button beside **Continuous Recording Enabled**.



2. Check the box next to **Peak Hours** or **Off-Peak Hours** and select **Yes**.
3. Click **Save**.



> **Note**
> For analog cameras only, you can apply different frame rate and video quality settings to event-driven and continuous recordings. See the chapter on analog camera configuration for more information.

DRAFT

3.3 Other Motion Settings

Pre-Event Video Buffer Duration

Default: **0.0**
Range: **0.0–10.0 seconds**

This setting regulates the length of video to buffer so that you can record video before video capture would otherwise be triggered by the start of a motion event.

Post-Event Video Buffer Duration

Default: **0.0**
Range: **0.0–10.0 seconds**

This setting regulates the length of video to record after the end of a motion event.

Minimum Time Between Events

Default: **2.0**
Range: **0.35–20.0 seconds**

This setting controls how long the system waits without detecting motion before closing an in-progress motion event.

- A lower value breaks motion events into separate, shorter events.
- A higher value delays breaking up motion events and combines consecutive events together to create longer motion events.

Maximum Length of Motion Events

Default: **60.0**
Range: **5.0–180.0 seconds**

This setting regulates the maximum length of a motion event.

Motion Event Update Rate

Default: **3**
Range: **1–60 seconds**

This setting defines the number of seconds between updates to the frames displayed on open motion event cards.

- If the number is too high, there will be fewer or no updates to the event card in the **Monitor** panel until the event closes.
- If the number is too low, VisionPoint™ VMS unnecessarily wastes resources by updating event cards that have had little or no change since the last update.

DRAFT

3.4 Using Camera-Based Motion Detection (Fall Release-2015 (8.1.x and above) only)

To minimize appliance system-resource usage, you can use the motion-detection functions on certain cameras. For all cameras, you need to disable the 3VR motion-detection feature using System Manager.

The cameras with motion detection that 3VR currently supports are:

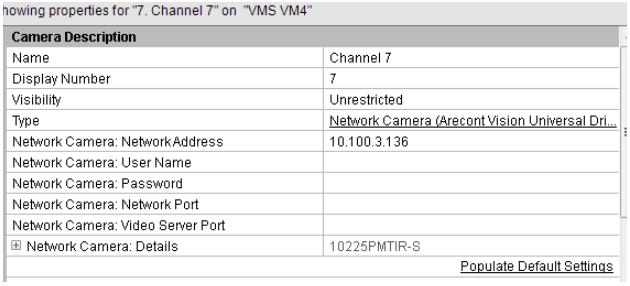
- Arecont Vision
- Axis Communications
- ONVIF[1]

For Arecont and Axis Communications cameras, use the Arecont Universal Driver and the Axis Communications Universal Driver.

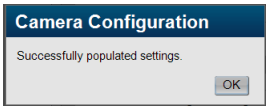
Arecont Camera Motion-Detection Configuration

Perform the steps below to configure motion-detection on Arecont network cameras.

1. Make sure you've set up and connected an Arecont network camera to a 3VR appliance.
2. Start up System Manager and log into the 3VR appliance that connects to the Arecont camera.
3. Click the **Configure** tab. The Configure options appear.
4. Add a new camera. See "7.4 Adding a Camera" on page 139 for information.
5. In the Camera Description section, click the **Unknown** link beside **Type**. The Edit Camera Type dialog box appears.
6. Select **Network Camera** as the Camera Type.
7. Choose **Arecont** from the **Camera Driver** drop-down list.
8. Choose **Arecont Vision Universal Driver** from the list. Click **Save**.
9. In the **Camera Description** section, enter the camera's IP address, and the username and password (if any) used to access the camera in the appropriate fields. Click **Save**.



10. Click the **Populate Default Settings** link. Click **Yes** in the confirmation dialog box. Click **Save**.



11. Right-click on the camera and choose **Enable "Camera #,"** where "#" is the number of the Arecont camera.
12. Scroll down to the **Motion** section, click in the field beside **Use 3VR Motion Detection**, and choose **No** to disable 3VR motion detection. Click **Save**. When you disable 3VR's motion detection, the camera's motion detection capability is automatically enabled.

After you enable camera motion detection, the following camera motion settings appear: Camera Motion Threshold, Camera Motion Zone Size, Camera Motion Detail, and Camera Motion Exclude Region.

The appliance pushes most changes you make to the **Motion** parameters to the camera. See the note below for exceptions.

1 3VR currently supports Axis, Sony, Samsung, Hikvision, and Canon cameras. More ONVIF cameras will be supported in the future.

Note
The system ignores changes made to the following parameters in System Manager:
Maximum Length of Motion Events and **Exclude Motion Shorter Than**.

DRAFT

See “Creating a Motion Exclusion Region” on page 131 for instructions on defining areas to exclude from motion detection. See the *VisionPoint VMS User Manual* for instructions on viewing and editing channels.

Motion	
Maximum Length of Motion Events	60
Motion Event Update Rate	3
Motion Event Image Size	Thumbnail Size
Minimum Time Between Events	2
Exclude Motion Smaller Than	4
Exclude Motion Shorter Than	1.5
Use 3VR Motion Presence Detection	**No**
Camera Motion Sensitivity	94
Camera Motion Threshold	3
Camera Motion Zone Size	4
Camera Motion Detail	2
Camera Motion Privacy Mask	Click here to edit.

Note

Due to variations between Arecont camera models, the **Camera Motion Sensitivity**, **Camera Motion Threshold**, **Camera Motion Zone Size**, and **Camera Motion Detail** settings might differ in System Manager and the camera.

Axis Communications Camera Motion-Detection Configuration

For Axis Communications cameras, the Axis video motion detection (VMD) application must be installed on the camera before using motion detection on the camera. 3VR currently supports VMD versions 3.0 and 2.0. Check the Axis Communications web site (http://www.axis.com/) for the VMD application that is compatible with your camera. You need to download the correct version of the VMD application from the Axis Communications website (search on “VMD” for information) before performing the steps below. Download the installer that requires an Internet connection. See the Axis Communications documentation for more information.

Perform the steps below to configure motion-detection on Axis Communications cameras.

1. Make sure you’ve set up and connected an Axis Communications network camera to a 3VR appliance.
2. Start up System Manager and log into the 3VR appliance that connects to the Axis camera.
3. Click the **Configure** tab. The Configure options appear.
4. Add a new camera. See “7.4 Adding a Camera” on page 139 for information.
5. In the **Camera Description** section, click the **Unknown** link beside **Type**. The Edit Camera Type dialog box appears.
6. Select **Network Camera** as the **Camera Type**.
7. Choose **Axis** from the **Camera Driver** drop-down list.
8. Choose **Axis Communications Universal Driver** from the list. Click **Save**.
9. In the **Camera Description** section, enter the camera’s IP address, and the username and password (if any) used to access the camera in the appropriate fields. Click **Save**.

Camera Description	
Name	Camera 6
Display Number	6
Visibility	Unrestricted
Type	Network Camera (Axis Communications Unive...
Network Camera: Network Address	10.10.2.14
Network Camera: User Name	root
Network Camera: Password	system
Network Camera: Network Port	
Network Camera: Video Server Port	
+ Network Camera: Details	AXIS P3215-V
	Populate Default Settings
	Common Operations

DRAFT

10. Click the **Populate Default Settings** link. Click **Yes** in the confirmation dialog box. Click **Save**.

11. Scroll down to the **Motion** section, click in the field beside **Use 3VR Motion Detection**, and choose **No** to disable 3VR motion detection. Click **Save**.

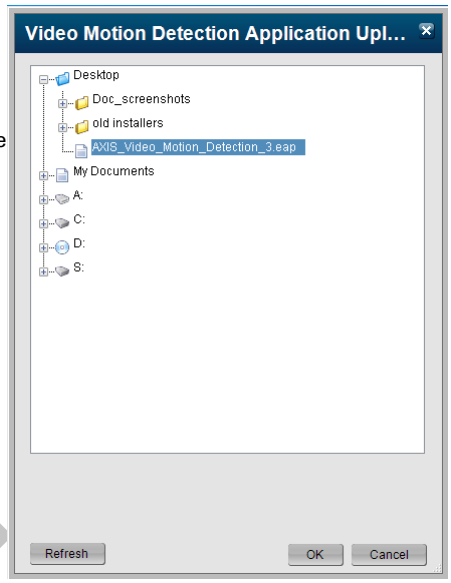
12. In the **Camera Description** section, click the **Common Operations** link and choose **Upload Motion Detection Application**. The Video Motion Detector Application Upload dialog box appears.

13. Navigate to the Axis Communications VMD installer file you previously downloaded and select it. Click **OK**. A status dialog box shows the upload in progress. When successfully completed, a dialog box appears.

14. Right-click on the camera in System Manager and choose **Enable "Camera #,"** where "#" is the number of the Axis camera.

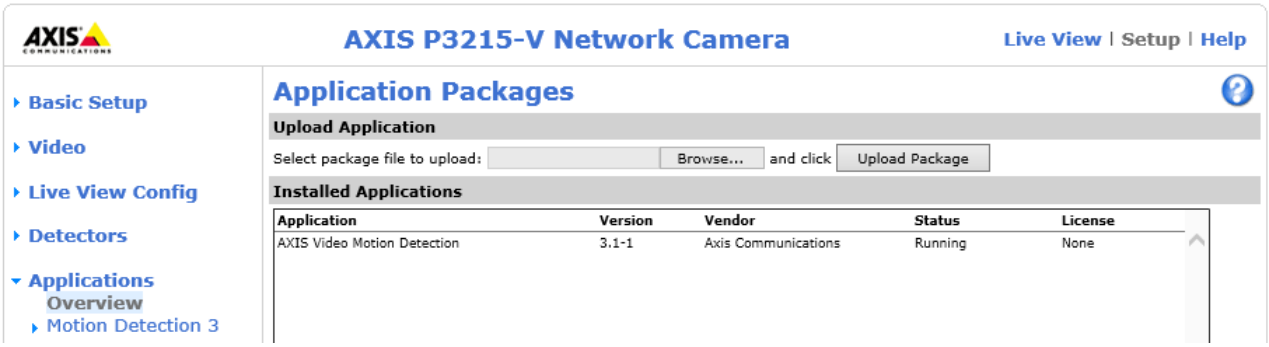
15. To verify configuration, open a web browser and enter the Axis camera's IP address in the address field. If prompted, enter the camera's username and password in the appropriate fields. Click **OK**. If properly configured, the Axis Network Camera window displays video from the camera.

16. Click the **Setup** link. The Basic Setup window appears.



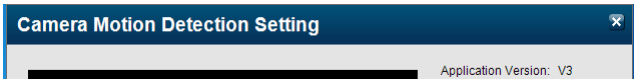
DRAFT

17. Click the **Applications** link. The Applications Packages window appears. Check that the Axis Communications VMD application version you installed is displayed and the status is **Running**. If the application is not running, select it in the list and click the **Start** button.



18. Another way to verify configuration is to go to System Manager, in the **Motion** section, click in the field beside **Camera Motion Detection Setting**, and then click the ellipsis (...) button. The Camera Motion Detection Setting dialog box appears.

19. Check that the Application Version number, for example, 3, matches the version of the Axis Communications VMD application you uploaded to the camera.



Note

In System Manager, the only settings in the **Motion** section that the system responds to are **Use 3VR Motion Detection** and **Camera Motion Detection Setting**. Refer to the Axis Communications documentation for information about configuring video settings.

See "Creating a Motion Exclusion Region" on page 131 for instructions on defining areas to exclude from motion detection. See the *VisionPoint VMS User Manual* for instructions on viewing and editing channels.

ONVIF Camera Motion-Detection Configuration

3VR supports motion detection from several camera vendors that support ONVIF drivers. Perform the steps below to configure motion-detection on supported cameras with ONVIF drivers.

1. Make sure you've set up and connected the ONVIF network camera to an appliance.
2. Start up System Manager and log into the 3VR appliance that connects to the ONVIF camera.
3. Click the **Configure** tab. The Configure options appear.
4. Select a camera.
5. In the **Camera Description** section, click the **Unknown** link beside **Type**. The Edit Camera Type dialog box appears.
6. Select **Network Camera** as the **Camera Type**.
7. Choose **Onvif** from the **Camera Driver** drop-down list. Click **Save**.
8. In the **Camera Description** section, enter the camera's IP address, and the username and password (if any) used to access the camera in the appropriate fields. Click **Save.**
9. Click the **Populate Default Settings** link. Click **Yes** in the confirmation dialog box. Click **Save**.
10. Right-click on the camera and choose **Enable "Camera #,"** where "#" is the number of the Axis camera.
11. Turn on motion detection on the camera. In most cases, to do this, open a web browser and enter the camera's IP address in the address field. If prompted, enter the camera's username and password in the appropriate fields. Click **OK**. Refer to the camera manufacturer's documentation for instructions on turning on motion detection.
12. In System Manager, click the **Configure** tab, select the camera, and scroll down to the **Motion** section. Click in the field beside **Use 3VR Motion Detection**, and choose **No** to disable 3VR motion detection. Click **Save**.

Camera Description	
Name	Camera 7
Display Number	7
Visibility	Unrestricted
Type	Network Camera (Onvif)
Network Camera: Network Address	10.30.4.44
Network Camera: User Name	admin
Network Camera: Password	Samsung!1
Network Camera: Network Port	
Network Camera: Video Server Port	
⊞ Network Camera: Details	Samsung Techwin - SNF-7010

Populate Default Settings

See the *VisionPoint VMS User Manual* for instructions on viewing and editing channels.

Note
Certain cameras, including cameras using the ONVIF driver, might stop sending motion events to the 3VR VMS server after several hours of continuous use. A possible workaround is to log into the camera directly and re-enable motion detection.

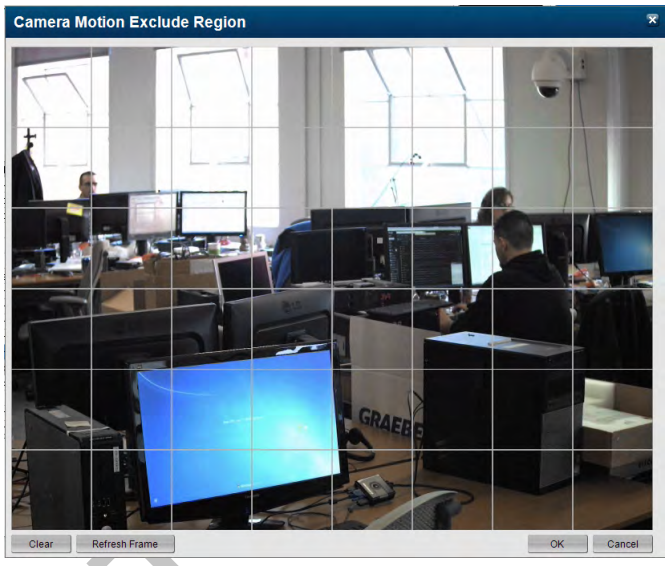
DRAFT

Creating a Motion Exclusion Region

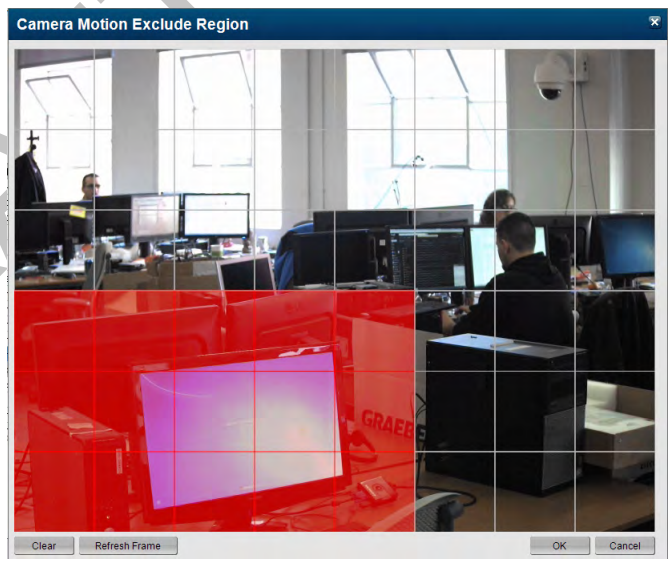
You can define an area you want to exclude from motion detection when using motion detection on certain brands of cameras.

Creating a Motion Exclusion Zone on Arecont Cameras

1. Select and enable the Arecont camera.
2. In the Motion section, click on **Click here to edit** in the **Camera Motion Exclude Region** row. Click on the ellipsis (...). The Camera Motion Exclude Region dialog box appears.



3. Place the pointer on the one of the regions in the image. To select the zone, press and hold left mouse button. The selected region is colored. To deselect the zone, press and hold right mouse button.
4. Optionally:
   - Click **Refresh Frame** to refresh the image.
   - Click **Clear** to clear the defined exclusion zone.
5. When finished defining the exclusion zone, click **OK**.
6. Click **Save** in the main System Manager window.

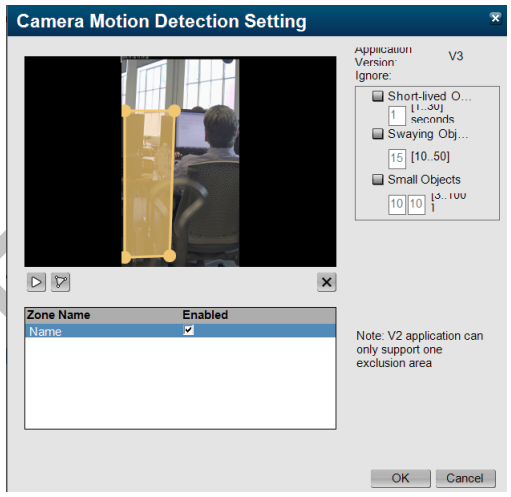


DRAFT

Creating a Motion Exclusion Zone on Axis Cameras

With Axis cameras, you click on the image to draw a mask to define the area you want to exclude from motion detection.

1. Select and enable the Axis camera.
2. In the Motion section, click on **Click here to edit** in the C**amera Motion Detection Setting** row. Click on the ellipsis (...). The Camera Motion Detection Setting dialog box appears.
3. Click the pause button to stop the video display.
4. Click the draw tool.
5. Position the pointer on the image where you want to start the mask. An endpoint appears at the tip of the pointer. Click the mouse button. The endpoint of the mask appears on the image.
6. Click on the image to define the other ends of the polygon for the mask. Click on the endpoint on the image to close and finish the mask.
7. Optionally, to assign a name to the mask, click under the Zone Name heading and enter a name.
8. Check the **Enabled** box to enable the mask.
9. Optionally, if using version 3 of the Axis motion detection application, you can create multiple exclusion zones, if desired. To do this, repeat steps 4 to 8.
10. When you are done editing the regions, click OK in the dialog box.
11. Click **Save** in the main System Manager window.



Important
Unless advised by 3VR, do not change other settings in the Camera Motion Detection Setting dialog box.

12. When finished, click **OK**.
13. Click **Save** in the main System Manager window.

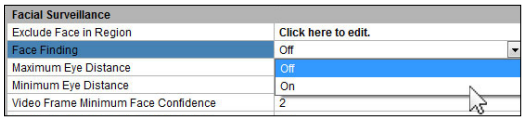
DRAFT

4. FACE FINDING SETTINGS

The settings displayed under the Face Finding heading affect how VisionPoint™ VMS detects and displays face events.

> **Important**
> The number of cameras that support face finding varies between 3VR appliance models, and may be affected by licensing and system-resource requirements. Check your model's data sheet or contact your 3VR sales representative for specific guidelines.

4.1 Enabling or Disabling Face Finding



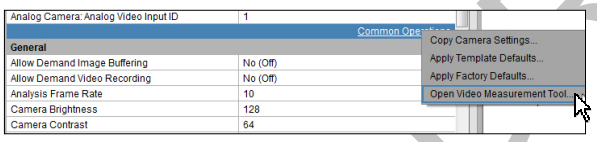
To enable facial surveillance with VisionPoint™ VMS:

1. Ensure the camera is properly aligned and focused in accordance with 3VR's guidelines for face recognition outlined in the "Image Guidelines for Facial Recognition" appendix.
2. Scroll through the camera settings until you see the **Facial Surveillance** settings category.
3. Click the **Face Finding** field.
4. Select **On**.
5. Click **Save** to save your changes.

4.2 Measuring Eye Distance

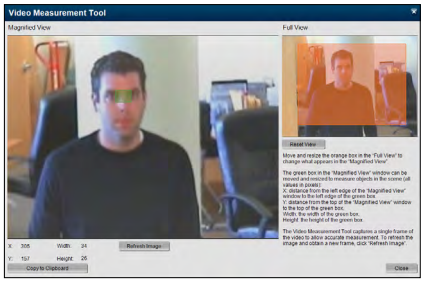
Cameras used for facial surveillance must record sufficient detail for the analytic to be able to identify faces. First, measure the video and verify that it is adequate for facial surveillance. If it is, adjust the Minimum Eye Distance and Maximum Eye Distance settings to encompass the range of possible values for the size of a face.

1. Click Common Operations, and then click **Open Video Measurement Tool**.



2. In the **Video Measurement Tool** window, click **Refresh Image** until the window returns a frame that contains a typical face.
3. Move and resize the green box until it covers the space between the eyes of the face.
4. The text in the bottom-left corner of the **Video Measurement Tool** window displays the measurements of the green box.

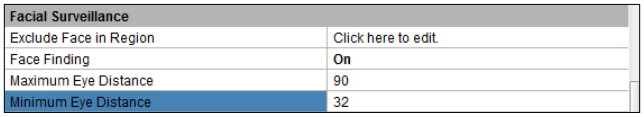
   Verify that the **Width** value is greater than 32 pixels.



   - If the **Width** value is less than 32 pixels, the camera is not providing enough detail for the facial surveillance analytic. Please adjust camera positioning according to "Image Guidelines for Facial Recognition" appendix.

5. Make a note of the **Width** value, and then click **Close** to return to the **Configure** panel.
6. Locate the **Minimum Eye Distance** setting.

   The formula for calculating **Minimum Eye Distance** (D_{min}) based on the **Width** (W) of an average face is as follows:

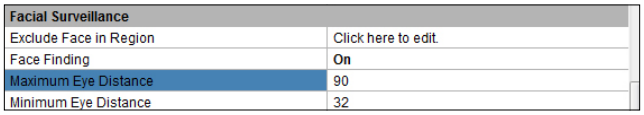


$$D_{min} = (W \times 2) / 3$$

   For example, if the face in the camera measures 60 pixels, set the **Minimum Eye Distance** to (60 x 2) / 3 = 40.

DRAFT

7. Locate the **Maximum Eye Distance** setting.



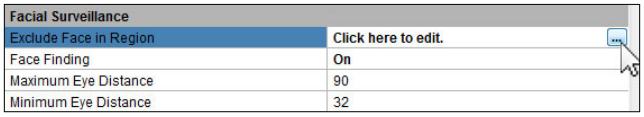
The formula for calculating **Maximum Eye Distance** (D_{max}) is as follows:

$$D_{max} = D_{min} \times 3$$

For example, given a **Minimum Eye Distance** of 40, the **Maximum Eye Distance** is equal to (40 x 3) = 120.

4.3 Configuring Face Exclusion Zones

By default, the facial surveillance analytic searches for faces on the full frame. The **Exclude Face in Region** setting allows you to exclude certain regions of the camera view from facial surveillance. When you specify an exclusion region, faces appearing entirely in the region do not generate a face event.



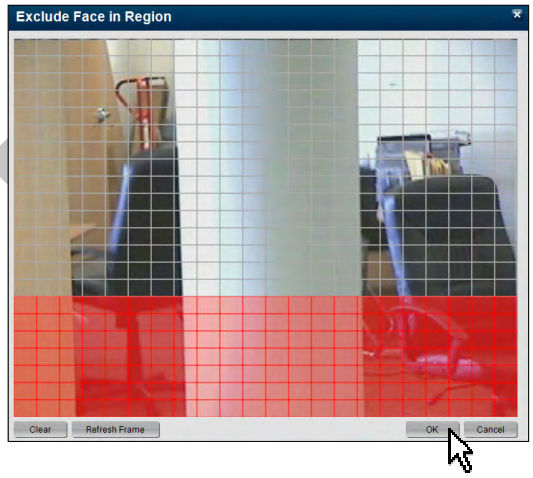
1. To display the camera view with a grid overlay, click the ellipsis (...) button beside the **Exclude Face in Region** field.

2. Select the region you wish to exclude by clicking and dragging the mouse button. Release the button when the area is highlighted in red.

   - Repeat as necessary to block out multiple regions in the grid. These regions can be separate, contiguous, or overlapping.

   - Click **Clear** to remove all regions from the exclusion zone.

3. When you've defined the desired exclusion regions, click **OK** to save.



Important
When editing the **Exclude Face in Region** setting, it is critical to remember that the red zones are *exclusion* zones. Faces appearing entirely in a red zone will not be analyzed.

DRAFT

5. EVENT VIDEO AND IMAGE SETTINGS

You can change the settings for event image size, image buffering, and demand video recording.

5.1 Event Image Size

VisionPoint™ VMS automatically saves three frames from each motion event video clip: an early frame, a middle frame, and a late frame. By default, the frames are saved as thumbnail images to preserve storage space. However, if larger images are desired, change the **Motion Event Image Size** setting to **Full Size**:

1. In the **Configure** panel of System Manager, click the plus sign next to the system name.

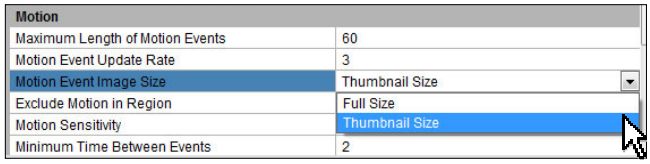
2. Click the plus sign next to **Cameras**.

3. Click a camera name to view its settings.

4. Scroll down to the **Motion** settings category.

5. Click the drop-down arrow next to the **Motion Event Image Size** setting and select **Full Size** from the drop-down menu.

6. Click **Save**.

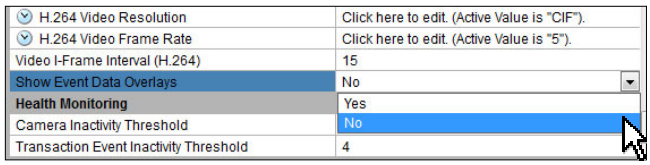


5.2 Event Data Overlays

Certain types of events have the ability to generate event data overlays: a stream of data placed on top of live or stored video. Perform the following steps to enable event data overlays on a per-camera basis:

1. In the **Configure** panel of System Manager, click the plus sign next to the system name.
2. Click the plus sign next to **Cameras**.
3. Click a camera name to view its settings.

4. Scroll down to the **General** settings category.
5. Click the drop-down arrow next to the **Show Event Data Overlays** setting and select **Yes** from the drop-down menu.
6. Click **Save**.



5.3 Event Video and Image Buffering Settings

You can use these settings when implementing data integration.

Enable Demand Image Buffering

Default: **No**

This setting enables and disables demand image buffering for a camera. When demand image buffering is enabled, images are available for a specified number of seconds.

Enable Demand Video Recording

Default: **No**

This setting enables and disables demand video recording for a camera. When demand recording is enabled, you can record video during circumstances when it normally would not be recorded.

DRAFT

6. CAMERA DISPLAY SETTINGS

You can overlay the date and time on video and configure a mask region for video.

6.1 Overlay Date and Time

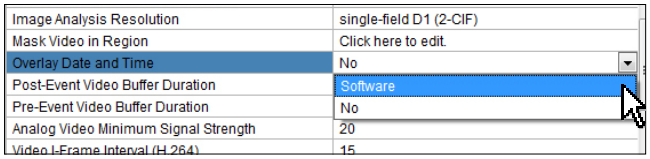
Use this setting to enable or disable date and time overlays for the camera. If date and time overlays are enabled, the current date and time is appended to each frame of live and stored video, and included on video exported from the camera.

Notes

1) Date and time overlays are not supported on MPEG4 cameras.
2) IP cameras may have a built-in date and time overlay feature; to conserve system resources, you should use the camera's built-in overlay feature, if available.

1. Click the camera you wish to edit to view its settings.

   Scroll down to the **General** settings category.



2. Click the drop-down arrow next to the **Overlay Date and Time** setting. Select one of the following options:

   - **Software**

     Adds an overlay of the date and time configured in System Manager. Available for all appliances and all camera types.

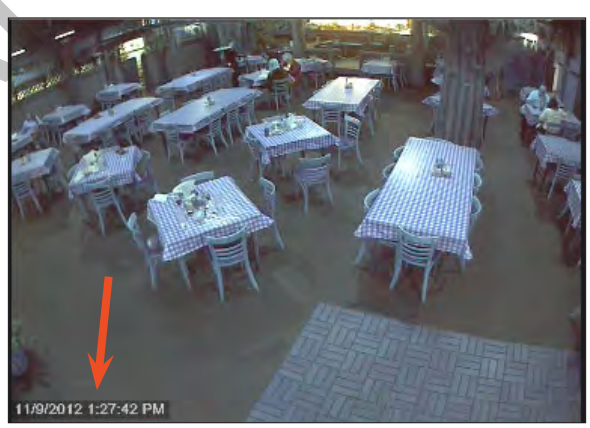
   - **Hardware**

     Adds an overlay of the date and time provided by the video encoder card. This option is only available for analog cameras on certain appliances, including the 5500-Series. If available, this is the preferred setting as it is less resource-intensive (see the "Warning" below for more information).

   - **No Overlay**

3. Click **Save**.

   A date and time overlay appears on video in OpCenter, as shown in the image to the right.



DRAFT

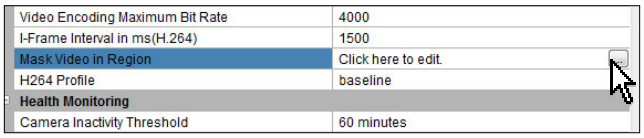
Warning

Appending date and time overlays using the **Software** option is a CPU-intensive process. 3VR recommends enabling overlays only on select cameras to conserve system resources. The number of overlay cameras supported depends on the model of appliance and the resolution and frame rate of the cameras, as well as whether any analytics are enabled.

6.2 Mask Video in Region

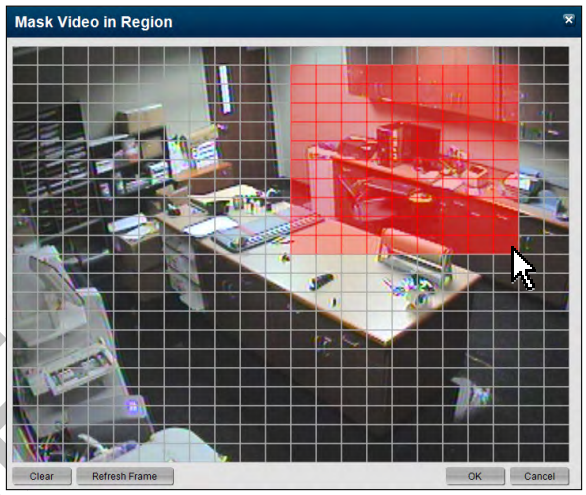
Use this setting to specify a masked region for the camera. When you mask a portion of the camera view, the masked area is replaced by a black box in both live and stored video. You can use this feature to block out part of the camera view that is not of interest or you don't want to record for security or privacy reasons.

> **Note**
> Video masking is not supported on MPEG4 cameras.
> You can create only one mask in the video window.



1. Click the camera you wish to edit to view its settings.
2. Scroll down to the **General** settings category.
3. To display the camera view with a grid overlay, click the ellipsis (...) button beside the **Mask Video in Region** field.
4. Select the region you wish to mask by clicking and dragging the mouse button.

   Release the button when the area is highlighted in red.
5. Click **OK**.

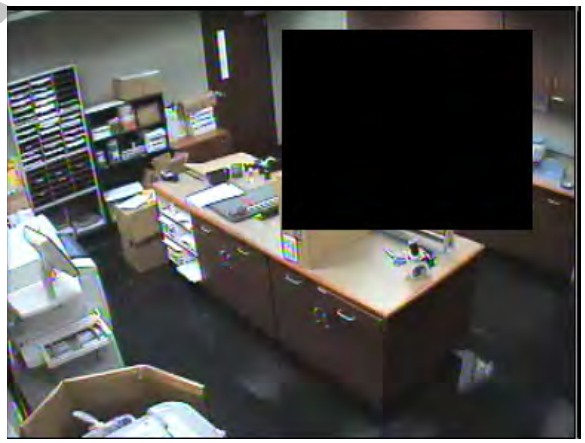


> **Warning**
> As with the **Overlay Date and Time** setting, masking video in a region uses more system resources than standard video recording and playback.

6. Click **Save** to save the masked region.

   Video for that camera replaces the selected region by a black box, as shown in the image to the right.

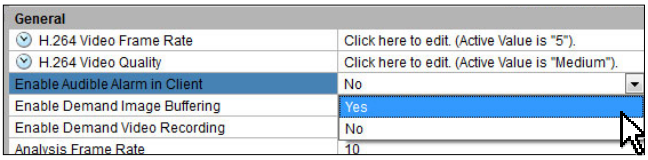
   The region is masked everywhere the camera appears: in OpCenter, System Manager, Spot Monitor, and in exported video.



> **Note**
> If you use a camera with a masked region for analytics, the masked portion of the video feed is excluded from analysis.

6.3 Enable Alarm for Video Loss

Use this setting to generate an audible alarm for video loss. The alarm will sound in 3VR OpCenter or Spot Monitor when a user is watching live video and the camera stops displaying video for any reason (whether it is malfunctioning, disabled, or offline).



1. Click the camera you wish to edit to view its settings.
2. Scroll down to the **General** settings category.
3. Click the drop-down arrow next to the **Enable Audible Alarm in Client** setting. Select **Yes** to enable the alarm.
4. Click **Save**.

DRAFT

7. INTERACTING WITH CAMERAS

You can add and delete, enable and disable cameras, and reset them to their factory default settings.

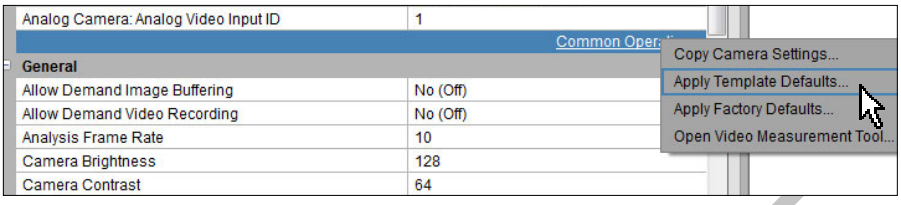
7.1 Resetting a Camera to Default Settings

Perform the following steps to reset a camera to the default camera settings:

1. Click the camera you wish to restore to view its settings.

2. Click Common Operations, and then click **Apply Factory Defaults** or **Apply Template Defaults** (only visible if you've created one or more templates):

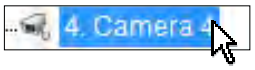
   - **Apply Factory Defaults** restores the camera settings to their default values.
   - **Apply Template Defaults** changes all of the camera settings to match the settings of the last template applied to the unit.



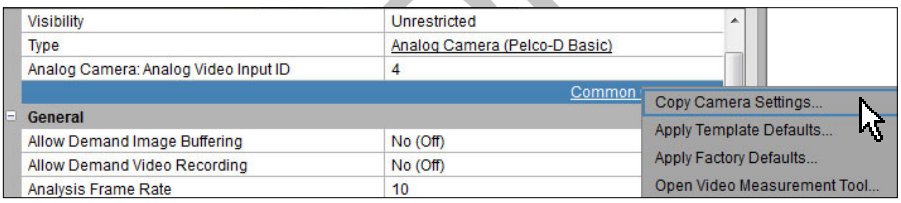
3. In the dialog box that appears, click **Yes** to confirm that you wish to discard the current settings and load the default factory or template settings for that camera type.

7.2 Copying Camera Configuration

If the same settings apply to multiple cameras, you only need to configure the settings on a single camera. You can then copy the settings from that camera to additional cameras with only a few mouse clicks:

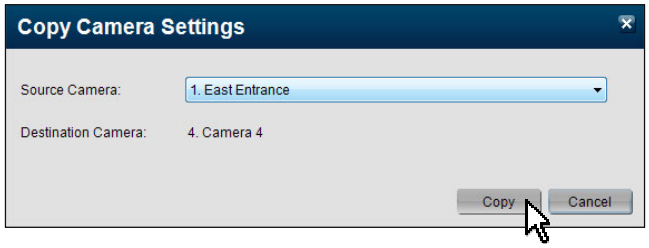
1. Click the destination camera (the camera to which you wish to apply the settings). 

2. Click Common Operations, and then click **Copy Camera Settings**.



3. In the **Copy Camera Settings** dialog box, open the **Source Camera** drop-down menu and select the camera from which you want to copy the settings.

   System Manager only displays cameras in the **Source Camera** drop-down list that are configured as the same camera type as the destination camera.

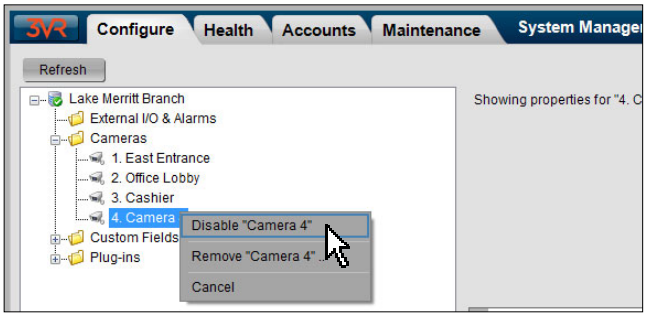


4. Click **Copy** to copy the settings from the source camera to the destination camera.

DRAFT

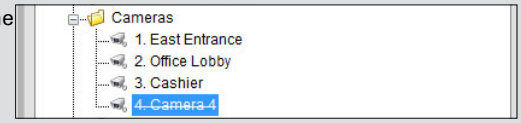
7.3 Enabling or Disabling Cameras

To preserve system resources, you should disable cameras that are not in use.



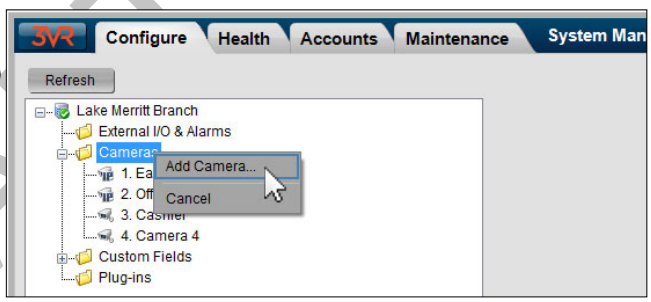
1. Right-click the name of the camera to be disabled or enabled.
2. Select **Disable "[Camera Name]"** (or **Enable "[Camera Name]"**).
3. In the dialog box that appears, click **Enable** or **Disable** to confirm the change.

> **Note**
> Cameras that are currently disabled appear with a strike through the camera name in the list of cameras:

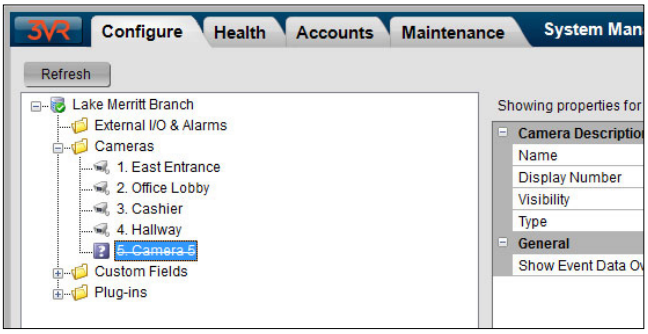


7.4 Adding a Camera

Perform the following steps to add a new camera to a VMS server:



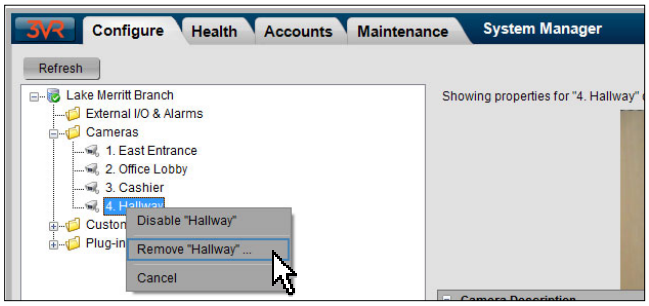
1. In the **Configure** panel of System Manager, click the plus sign (+) next to the system name.
2. Right-click **Cameras** and select **Add Camera** from the menu. A new, unconfigured camera appears at the bottom of the list of cameras.
3. Set the camera type of the new camera according to the instructions in section 2.3 of this chapter.



7.5 Deleting a Camera

Deleting cameras is not recommended. Instead, you should disable cameras that are not currently connected to a live video feed (see section 7.3 of this chapter).

> **Note**
> If using software versions earlier than version 7.3, if you delete a camera, all previously recorded video will be lost.



However, if you accidentally added a camera, you can delete it from System Manager by performing the following steps:

1. Right-click the camera name and select **Remove "[Camera Name]"**.
2. In the confirmation dialog box, click **Remove** to confirm the permanent camera deletion.

DRAFT

DRAFT

CHAPTER 6
Analog Camera Configuration

1. CONNECT ANALOG CAMERAS 143
   - 1.1 1000-Series 143
   - 1.2 3000-Series 143
   - 1.3 4000-Series 143
   - 1.4 5500-Series 144
2. VERIFY VIDEO QUALITY OF ANALOG CAMERAS 144
3. ANALOG CAMERA BASICS 145
   - 3.1 Camera Type 145
   - 3.2 Analog Video Input ID 145
   - 3.3 Supported Cameras 145
4. H.264 RECORDING SETTINGS 146
   - 4.1 H.264 Video Resolution 146
   - 4.2 H.264 Video Frame Rate 146
   - 4.3 H.264 Video Quality 147
5. CONTINUOUS RECORDING SETTINGS 147
   - 5.1 Continuous Recording Video Frame Rate 147
   - 5.2 Continuous Recording Video Quality 148
6. ANALOG CAMERA COLOR SETTINGS 148

DRAFT

DRAFT

1. CONNECT ANALOG CAMERAS

This section describes how to connect analog cameras to 3VR appliances.

Note
VisionPoint™ VMS does not currently support analog cameras for VMS servers running on third-party hardware. If you need to connect an analog camera to a VisionPoint™ system, you must use a 3VR appliance.

1.1 1000-Series

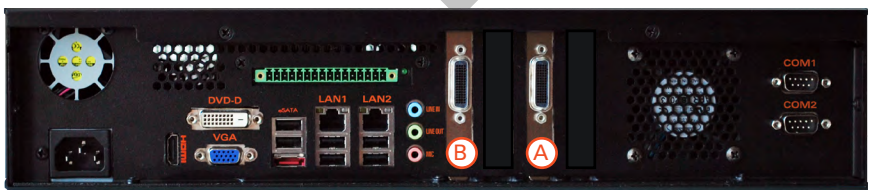
1. Connect the audio/video cable to port A (shown in the photo below). Connect cameras 1-16 to the BNC connectors.

1.2 3000-Series

1. Connect the audio/video cable to port A (shown in the photo below). Connect cameras 1-16 to the BNC connectors.

1.3 4000-Series

1. Connect the first audio/video cable to port A (shown in the photo below). Connect cameras 1-16 to the yellow BNC connectors. If using audio, connect audio inputs 1-16 to the red BNC connectors.
2. **32-camera units:** Connect the second audio/video cable to port B (shown in the photo below). Connect cameras 17-32 to the yellow BNC connectors. If using audio, connect audio inputs 17-32 to the red BNC connectors.



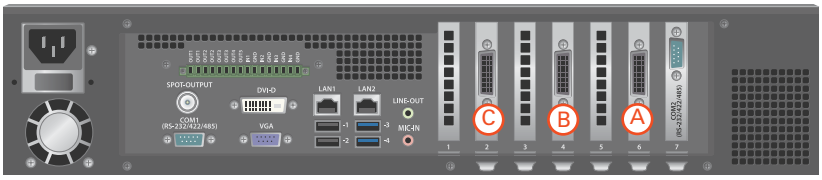
DRAFT

1.4 5500-Series

1. Connect the first audio/video cable to port A (shown in the photo below). Connect cameras 1-16 to the yellow BNC connectors. If using audio, connect audio inputs 1-16 to the red BNC connectors.

2. **32-camera units:** Connect the second audio/video cable to port B (shown in the photo below). Connect cameras 17-32 to the yellow BNC connectors. If using audio, connect audio inputs 17-32 to the red BNC connectors.

3. **48-camera units:** Connect the third audio/video cable to port C (shown in the photo below). Connect the remaining cameras to the yellow BNC connectors. If using audio, connect the remaining audio inputs to the red BNC connectors.



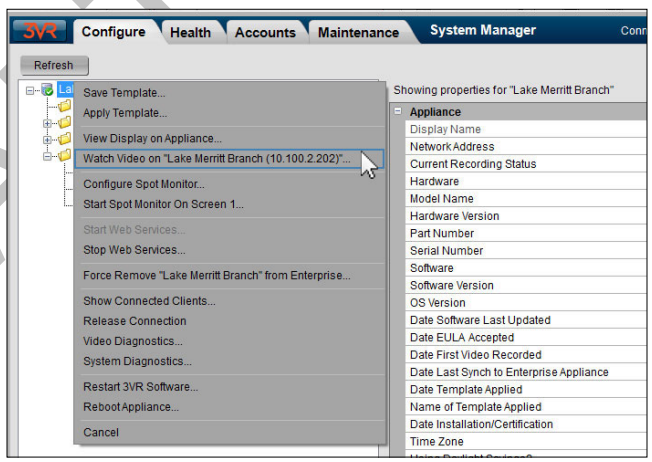
2. VERIFY VIDEO QUALITY OF ANALOG CAMERAS

After connecting cameras, verify that video is appearing on all cameras connected to a live video feed:

1. In the **Configure** panel of System Manager, right-click the appliance name.

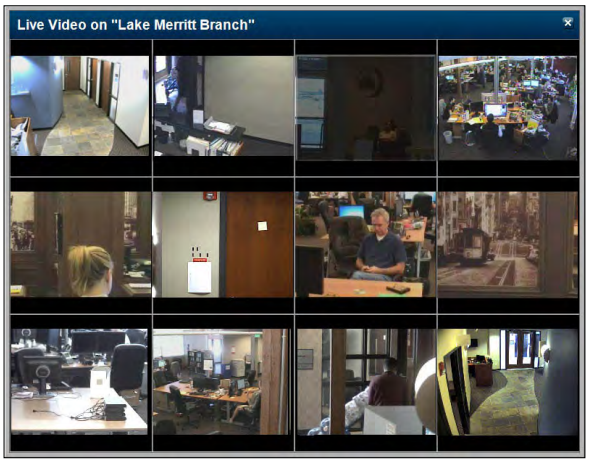
2. Select **Watch Video on "[VMS Appliance Name]"** from the menu.

> **Note**
> **[VMS Appliance Name]** is a placeholder for the display name that was configured in the section "Edit VMS Server Display Name" on page 66.



When the live video window loads, verify the video quality on all cameras. Close the live video window when finished viewing.

> **Note**
> For units with more than 32 cameras, you can view a maximum of 36 cameras at one time in multiplex mode.



DRAFT

3. ANALOG CAMERA BASICS

You configure analog camera settings in the **Configure** panel of System Manager.

To access the camera settings, click the plus sign beside the VMS server display name, and then click the plus sign beside **Cameras** to display the list of cameras on the system. Select the camera of interest to view its settings.

3.1 Camera Type

The **Type** for all analog cameras is **Analog**, and the **Camera Driver** must be set to "Analog" for all fixed analog cameras.

> **Reference**
> See the chapter on configuring PTZ cameras for information about analog PTZ cameras.

3.2 Analog Video Input ID

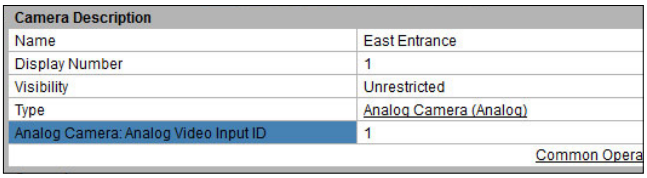
This setting refers to the physical position of the camera on the video input cable. By default, the **Analog Video Input ID** of an analog camera corresponds to the camera number. However, you may edit the input ID of a camera to associate a different physical input with the camera. You will also need to reset the **Analog Video Input ID** when changing a camera's type to analog from a different type.

To set the input ID of a camera:

1. Click the camera name to view its settings.

2. Locate the **Analog Camera: Analog Video Input ID** setting. Enter a new ID number in the text box.

3. Click **Save**.



Camera Description	
Name	East Entrance
Display Number	1
Visibility	Unrestricted
Type	Analog Camera (Analog)
Analog Camera: Analog Video Input ID	1
	Common Opera

3.3 Supported Cameras

3VR supports all fixed analog cameras. For the current list of supported analog PTZ cameras, see www.3VR.com.

> **Important**
> Analog cameras are only supported for VisionPoint™ VMS servers running on 3VR appliances. VMS servers running on third-party hardware must use network cameras. For more information on supported cameras for third-party hardware VMS servers, please refer to http://www.3vr.com/.

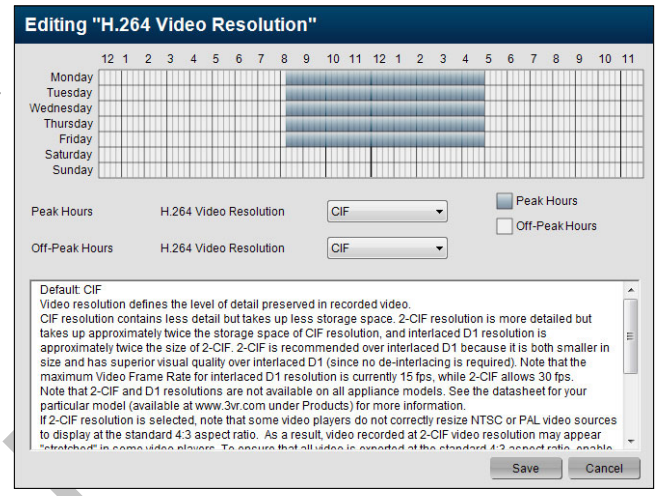
DRAFT

4. H.264 RECORDING SETTINGS

Note
You may independently configure select camera settings for Peak and Off-Peak hours. See the chapter on basic System Manager configuration for more information about configuring recording schedules.

4.1 H.264 Video Resolution

Default: **CIF**
Range: **CIF** (all models); **2-CIF, 4-CIF** (select models only)



This setting controls the resolution for recording video. When configuring the resolution of an analog camera, you should consider the trade-off between video quality and consumption of storage space:

- Video recorded at **CIF** resolution contains the least detail and takes up the least storage space.
- **2-CIF** resolution stores more detail but takes up approximately twice the storage space of CIF resolution.
- **4-CIF** resolution captures the most detail, but will consume storage space at the fastest rate.

To set the resolution of an analog camera:

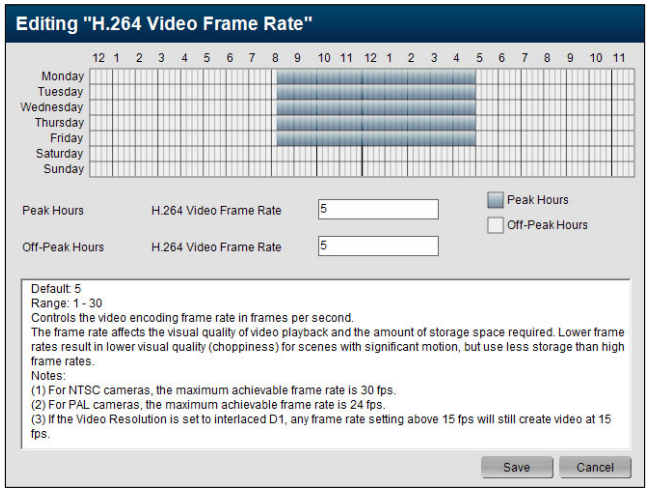
1. Click the ellipsis (**...**) button beside **H.264 Video Resolution**.
2. Select a new value from the **H.264 Video Resolution** drop-down menu for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.

DRAFT

4.2 H.264 Video Frame Rate

Default: **5**
Range: **1–30**

This setting controls the video encoding frame rate in frames per second. Frame rate affects fluid motion in the scene and the amount of storage space required. Lower frame rates result in lower visual quality (choppiness) for scenes with significant motion, but use less storage than high frame rates.



- For NTSC cameras, the maximum achievable frame rate is 30 fps.
- For PAL cameras, the maximum frame rate is 25 fps. If you select a higher frame rate (26-30 fps), video is still recorded at 25 fps.

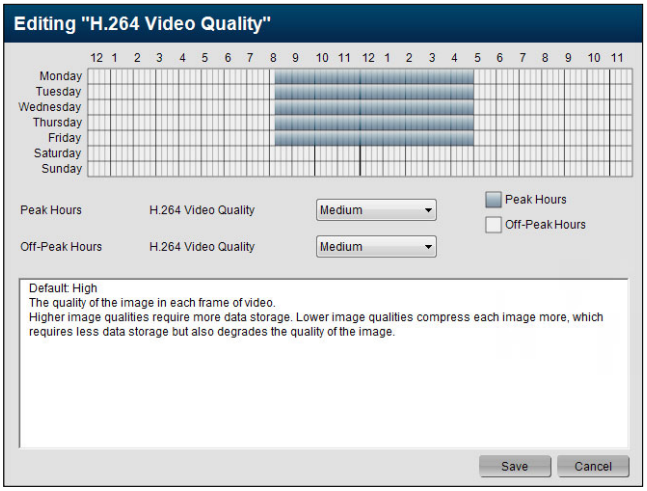
To set the frame rate of an analog camera:

1. Click the ellipsis (**...**) button beside **H.264 Video Frame Rate**.
2. Type a new value in the **H.264 Frame Rate** text box for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.

4.3 H.264 Video Quality

Default: **Medium**
Range: **Very Low–Very High**

This setting controls the quality of the image in each frame of video. A higher value results in higher image quality, but puts more load on the CPU. Also, each video clip takes up more storage space. Lower image quality compresses each image more, which results in smaller files but also degrades the quality of the image.



To set the video quality of an analog camera:

1. Click the ellipsis (**...**) button beside **H.264 Video Quality**.
2. Select a new value from the **H.264 Video Quality** drop-down menu for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.

5. CONTINUOUS RECORDING SETTINGS

For analog cameras, you can apply different frame rate and video quality settings to motion-based and continuous recording. (Different frame rates and video quality settings are not available when using IP cameras).

- When VisionPoint™ VMS does not detect any activity in the camera view, the frame rate and quality settings for **Continuous Recording** are applied.
- When motion is detected, the H.264 frame rate and quality settings (see previous section) are applied.

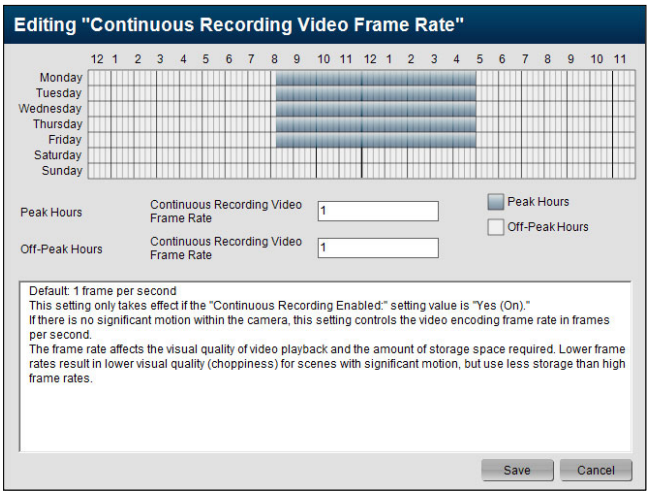
Note
Continuous recording is disabled by default for all camera types. See the chapter on general camera configuration for information on enabling continuous recording.

DRAFT

5.1 Continuous Recording Video Frame Rate

Default: **1**
Range: **1–30**

This setting controls the frame rate when **Continuous Recording** is enabled and there is no significant motion occurring in the camera field of view.



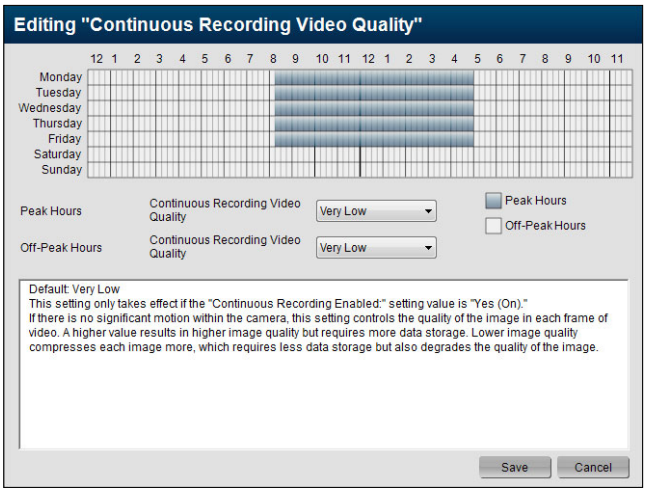
1. Click the ellipsis (**...**) button beside **Continuous Recording Video Frame Rate**.
2. Type a new value in the **Continuous Recording Video Frame Rate** text box for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.

5.2 Continuous Recording Video Quality

Default: **Very Low**
Range: **Very Low–Very High**

This setting controls the video quality when **Continuous Recording** is enabled and there is no significant motion detected in the camera field of view.

1. Click the ellipsis (**...**) button beside **Continuous Recording Video Quality**.
2. Select a new value from the **Continuous Recording Video Quality** drop-down menu for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.



6. ANALOG CAMERA COLOR SETTINGS

Important
Often the best way to improve the video feed is by adjusting the camera or its environment. You should only modify the settings in this section after exhausting other options.

DRAFT

Camera Brightness

Default: **128**
Range: **0–255**

If it is necessary to modify this setting, a range of 96 to 160 is usually sufficient.

Camera Contrast

Default: **64**
Range: **0–127**

If it is necessary to modify this setting, a range of 32 to 96 is usually sufficient.

Camera Hue

Default: **0**
Range: **0–255**

Changing this value usually lessens overall visual quality.

Camera Saturation

Default: **64**
Range: **0–127**

If it is necessary to modify this setting, a range of 32 to 96 is usually sufficient.

Camera Sharpness (5500-Series)

Default: **1**
Range: **1–15**

This setting controls how sharp or crisp an image appears. You should normally leave this setting should normally at the default value.

CHAPTER 7
Analog PTZ Camera Configuration

1. PTZ CAMERA BASICS 151
2. PTZ INTERFACES 151
   2.1 COM2 Serial Port 151
3. CONNECTING MULTIPLE PTZ CAMERAS 153
   3.1 Wire Splicing 153
   3.2 Daisy Chaining 153
   3.3 Coaxitron Translator 154
4. PTZ CAMERA CONFIGURATION 157
   4.1 Select the PTZ Camera Driver 157
   4.2 Configure PTZ Settings 157

DRAFT

DRAFT

1. PTZ CAMERA BASICS

This chapter explains how to connect one or more analog PTZ (pan, tilt, zoom) cameras to a 3VR appliance. 3VR appliances support both 2-wire and 4-wire PTZ configurations:

2-wire: Messages are sent unidirectionally from the 3VR appliance to the PTZ camera.
Supported protocols: Pelco-D, Panasonic, American Dynamics

4-wire: The PTZ camera both receives messages from the appliance and transmits signals back to the unit.
Supported protocols: Pelco-D, Panasonic, American Dynamics Speed Dome

Note
This chapter applies to analog PTZ cameras only. Refer to the chapter on IP camera configuration for configuration instructions for IP/network PTZ cameras.

2. PTZ INTERFACES

This section describes connections to 3VR appliances seral ports.

2.1 COM2 Serial Port

- 3000-Series and 5500-Series appliances each feature two RS-232/422/485 serial ports. COM1 on the 3000-Series is configurable through Bios to 422/485. The 1000-Series and 4000-Series each feature two RS-232 serial ports.

1000-Series

3000-Series

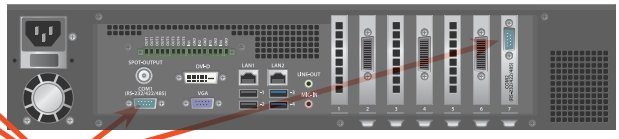
COM-1/2 Serial Ports

DRAFT

Required Materials

4000-Series

5500-Series

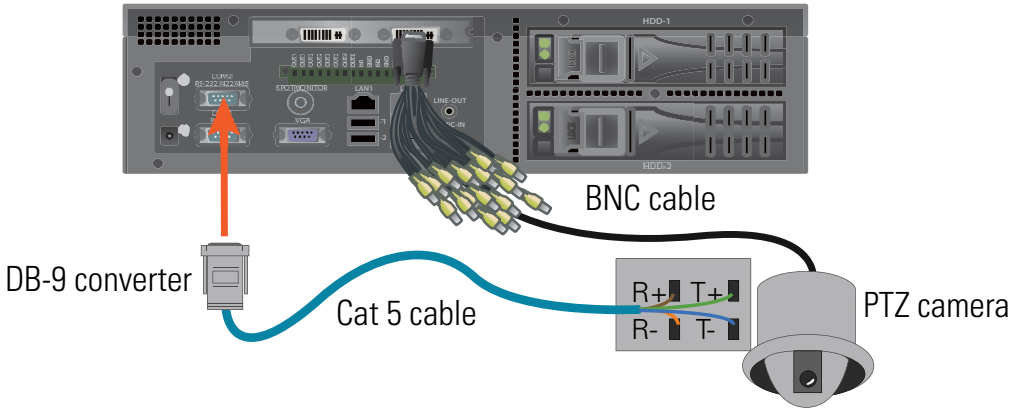


COM-2 Serial Ports

Note
The 1000-Series and 4000-Series only support RS-232. If you need an RS-422 or RS-485, you need to separately purchase an RS-232-to-RS-422/485 or USB-to-RS-422/485 converter from a different vendor.

- Cat 5 Ethernet cable (important: **DO NOT** use a crossover cable)
- DB-9 converter
- Wire cutters

Setup Diagram



Installation Steps

1. Cut off one end of the Cat 5 Ethernet cable to expose the wires.

2. Connect two wires from the exposed end to R+ and R- on the camera. Make note of the color of each wire for future reference:

R+	
R-	

Four wire installations only: Connect two additional wires from the exposed Cat 5 cable end to T+ and T- on the camera. Make note of the color of each wire for future reference:

T+	
T-	

3. Plug the other end of the Cat 5 cable into the DB-9 converter.

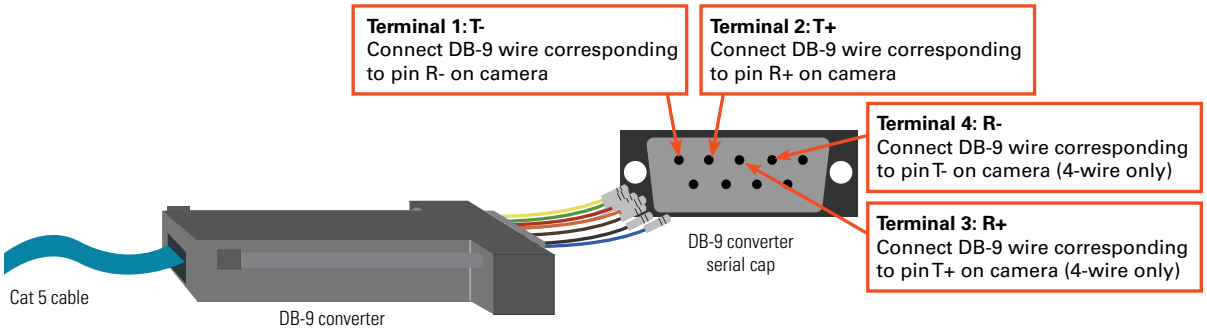
4. The Cat 5 cable wire colors recorded in step 2 correspond to the wire colors on the DB-9 serial end according to the following chart:

If you wired the _____ wire to the camera...	**...plug the _____ wire into the appropriate terminal on the DB-9 converter serial cap.**
brown	white
brown/white	brown
green	yellow
blue/white	green
blue	red
green/white	black
orange	orange
orange/white	blue

DRAFT

5. Arrange the wires corresponding to **R-** and **R+** on the DB-9 converter so that they match pins 1 and 2 (**T-** and **T+**) on the PTZ port.

   Four wire installations only: Arrange the wires corresponding to **T+** and **T-** on the DB-9 converter so that they match pins 3 and 4 (**R+** and **R-**) on the PTZ port.



6. Tuck the wires inside the DB-9 converter and push the serial cap into place.

7. Fasten the DB-9 converter to the COM2 serial port on the back of the 3VR appliance.

3. CONNECTING MULTIPLE PTZ CAMERAS

DRAFT

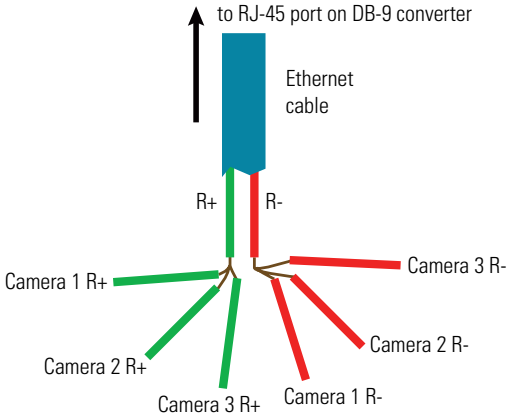
This section describes how to connect multiple PTZ cameras.

3.1 Wire Splicing

You can adapt any of the PTZ interfaces outlined in the previous section to support more than one camera using the wire splicing technique.

With wire splicing, you splice the wires connected to R+, R-, T+, and T- on each camera into a single wire that interfaces with the serial PTZ port on the appliance.

Splice the wires according to their polarity, as shown in the diagram to the right.



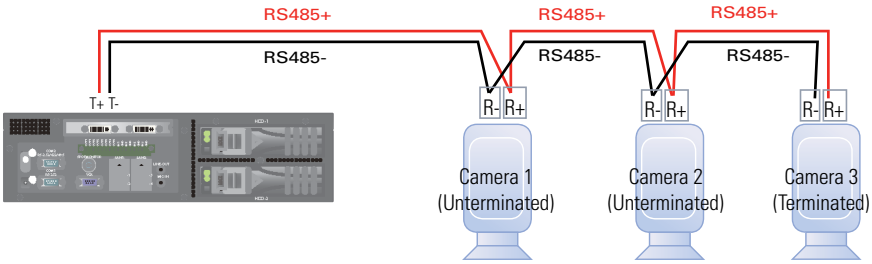
Wire splicing of three PTZ cameras (2-wire)

3.2 Daisy Chaining

"Daisy chaining" PTZ cameras refers to connecting multiple PTZ cameras to a DVR in a linked chain formation.

Connect the first camera to the 3VR appliance using the standard procedure (see "2. PTZ Interfaces" on page 151).

To add a second camera to the chain, run wires from R+ and R- on the second camera to R+ and R- on the first camera (use wire splicing to connect the wires). Repeat this process for any remaining cameras.



Daisy chaining of three PTZ cameras (2-wire)

Important Note

Cameras in the middle of the chain must have their termination set to **Off** (this state may be referred to as **Open**, **Unterminated, Middle, Infinite,** or ∞ depending on the camera model). You must set the final camera in the chain to **Terminated** (or **120 Ohm** or **End**). If termination is incorrect, you will not be able to move any of the cameras in the chain. Consult the camera documentation for help configuring termination.

3.3 Coaxitron Translator

- A coaxitron translator converts the RS-422/485 serial signal from the 3VR appliance to coax cable.

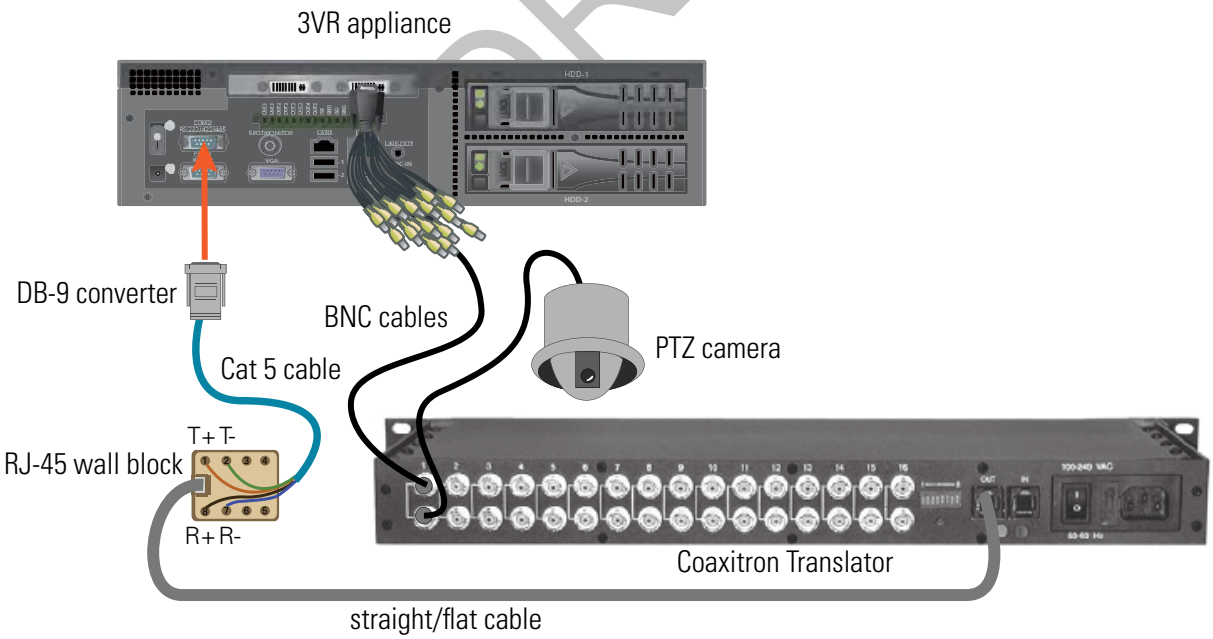
Source: Pelco

Required Materials

- RJ-45 wall box (included with the coaxitron translator)
- RJ-45 flat/straight cable (included with the coaxitron translator)
- Cat 5 Ethernet cable (important: **DO NOT** use a crossover cable)
- DB-9 converter
- Wire cutters
- Voltmeter

DRAFT

Setup Diagram

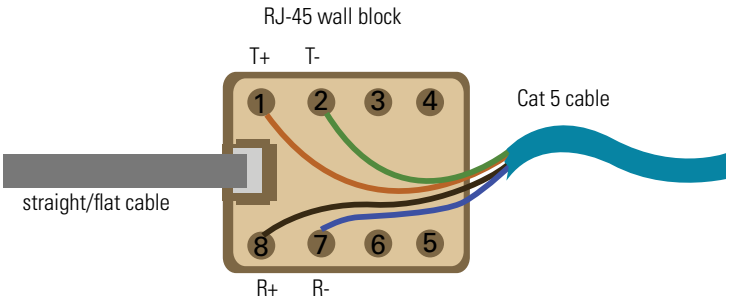


Installation Steps

1. Connect the straight/flat cable from the RJ-45 wall block to the **IN** port on the coaxitron translator.

2. Cut off one end of the Cat 5 cable to expose the wires.

3. Connect two wires from the exposed end of the Cat 5 cable to R+ (pin 8) and R- (pin 7) on the RJ-45 wall box. Make note of the color of each wire.



R+ (pin 8)	
R- (pin 7)	

Four wire installations only: Connect two additional wires from the exposed Cat 5 cable to the T+ (pin 1) and T- (pin 2) on the wall box. Make note of the color of each wire.

T+ (pin 1)	
T- (pin 2)	

4. Plug the other end of the Cat 5 cable into the DB-9 converter.

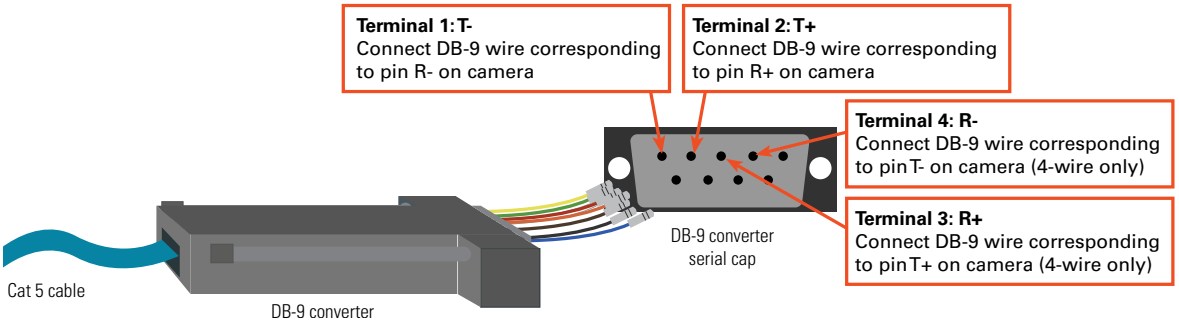
5. The wire colors recorded in Step 2 correspond to the wire colors on the DB-9 serial end according to the chart below:

If you wired the _____ wire to the wall box...	**...plug the _____ wire into the appropriate terminal on the DB-9 converter serial cap.**
brown	white
brown/white	brown
green	yellow
blue/white	green
blue	red
green/white	black
orange	orange
orange/white	blue

DRAFT

6. Arrange the wires corresponding to R- and R+ on the wall box so that they match pins 1 and 2 on the appliance's port.

Four wire installations only: Arrange the wires corresponding to **T-** and **T+** on the wall box so that they match pins 3 and 4 on the appliance's PTZ port.



7. Tuck the wires inside the DB-9 converter and push the serial cap into place.

8. Fasten the DB-9 converter to the COM2 serial port on the back of the 3VR appliance.

9. When all wiring is complete, test the connection from the 3VR appliance to the coaxitron translator:

   - Set the voltmeter to DC and put the leads on the R+/R- pins of the wall box. If you are getting 5/-5 volts, the 3VR appliance is sending a strong enough signal to the coaxitron translator.

10. The bottom row of BNC jacks on the coaxitron translator are receivers for your cameras. Connect a BNC cable from each of the PTZ cameras sequentially into the jacks.

11. The top row of BNC jacks on the coaxitron translator feed into the 3VR appliance. Connect these to the corresponding cameras using a 3VR video cable.

Configuring Dipswitches

On the camera

- Set the hardware ID to 1 on all cameras.
- Set the baud rate to 2400 to start, you can change this later, if necessary.
- Set everything else to off.

On the coaxitron translator

- DIP switches 1 and 2 correspond to 15-BIT or 32-BIT protocol "flavors." DIP 1 corresponds to BNC 1-8 and DIP 2 corresponds to BNC 9-16.

  15-BIT = Standard coaxitron / 32-BIT = Extended coaxitron

1	2	BNC 1-8	BNC 9-16
ON	OFF	15-BIT	32-BIT
OFF	ON	32-BIT	15-BIT
ON	ON	15-BIT	15-BIT
OFF	OFF	32-BIT	32-BIT

  Set DIP switches 1 and 2 to OFF (32-BIT/32-BIT).

- DIP 3 corresponds to the protocol type.

  1. ON – protocol D

  2. OFF – protocol P

  Set DIP 3 to ON for Pelco-D protocol.

- DIP 4 is reserved for future use. **Set DIP 4 to OFF**.

- DIP switches 5 and 6 correspond to the BAUD rate.

5	6	BAUD Rate
OFF	OFF	19200
OFF	ON	4800
ON	OFF	9600
ON	ON	2400

  You should use 2400 BAUD. **Set DIP switches 5 and 6 to ON.**

DRAFT

- DIP 7 is for cascaded configurations. If DIP 7 is set to OFF, the translator responds to addresses 1-16. If the switch is set to ON, the translator responds to addresses 17-32. In a cascaded configuration, set DIP 7 to OFF on the first translator and set DIP 7 to ON for the second translator.
- DIP 8 corresponds to the equipment type. Setting switch 8 to ON corresponds to Spectra receivers, setting it to OFF corresponds to Intercept receivers. 3VR does not support Intercept receivers, set **DIP 8 to ON**.

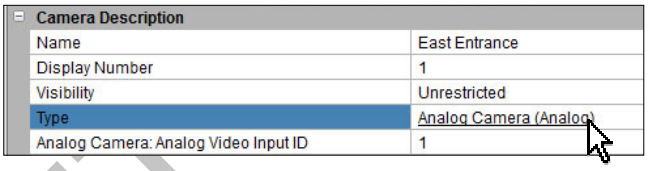
4. PTZ CAMERA CONFIGURATION

This section describes how to select the PTZ camera driver and configure PTZ settings.

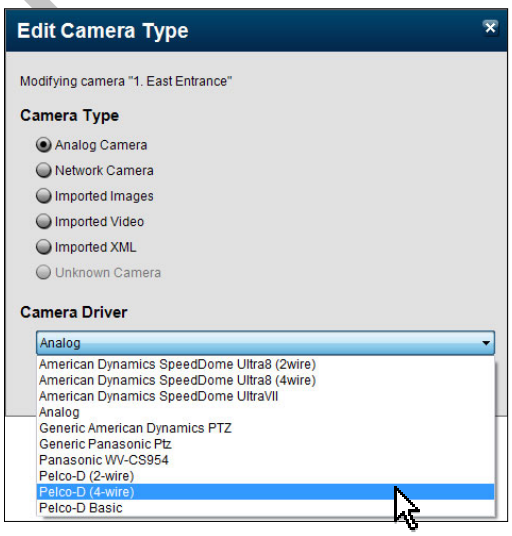
4.1 Select the PTZ Camera Driver

1. Log in to 3VR System Manager.
2. In the **Configure** panel, click the plus sign next to the system display name, and then click the plus sign next to **Cameras**.
3. Select the PTZ camera to view its settings.

4. On the right side of the System Manager screen, click the link next to the camera **Type** (e.g. Analog Camera).



5. In the **Edit Camera Type** dialog box, open the **Camera Driver** drop-down menu. Select the correct driver for the PTZ camera from the list.
6. Click **Save**.



DRAFT

4.2 Configure PTZ Settings

With the PTZ camera still selected, locate the **PTZ Cameras** settings category on the right side of the System Manager screen.

1. Edit the **Serial Port COM Port** setting as follows:
   - 5500-Series: COM 2

PTZ Cameras	
Camera Hardware Address	1
Serial Port Baud Rate	9600 bps
Serial Port COM Port	COM2
Full Frame Motion Threshold	50
Return to Home preset after this many seconds of...	30

2. Set the **Serial Port Baud Rate**.

PTZ Cameras	
Camera Hardware Address	1
Serial Port Baud Rate	9600 bps
Serial Port COM Port	COM2
Full Frame Motion Threshold	50
Return to Home preset after this many seconds of...	30

3. Set the **Camera Hardware Address**.

   This is the hardware address set by the DIP switch on the PTZ camera.

   For cameras arranged with wire splicing or daisy chaining, the **Camera Hardware Address** is used to control cameras independently.

PTZ Cameras	
Camera Hardware Address	2
Serial Port Baud Rate	9600 bps
Serial Port COM Port	COM2
Full Frame Motion Threshold	50
Return to Home preset after this many seconds of...	30

Important

The **Serial Port Baud Rate** and **Camera Hardware Address** are camera-specific and must be set correctly for the 3VR appliance to be able to control the camera. Consult the camera's documentation for help determining the baud rate and hardware address. If you are uncertain what these values should be, reboot the camera while watching the video feed. Most models of PTZ camera output their settings on restart.

4. If desired, modify the remaining PTZ settings:

Full-Frame Motion Threshold

Default: **50 percent**
Range: **0–100 percent**

PTZ camera motion can generate spurious motion events. If events appear on the PTZ camera when no genuine motion has occurred, increase this value.

Return to Home preset...

Default: **300 seconds**
Range: **0–9999 seconds**

If you defined a home preset for this camera in OpCenter, the camera view returns to the home view after being idle for the specified number of seconds.

Tilt Speed Profile (Pelco-D Basic Driver Only)

Default: **Linear**

Sets the speed profile to use for tilt movements.

Pan Speed Profile (Pelco-D Basic Driver Only)

Default: **Linear**

Sets the speed profile to use for pan movements.

Reference

See chapter 2 of the *VISIONPOINT™ VMS USER MANUAL* for more information on PTZ tours and presets.

DRAFT

CHAPTER 8
IP Camera Configuration

1. OVERVIEW 161
   1.1 Supported Cameras 161
   1.2 IP Camera Connection Methods 161
2. CONFIGURE CAMERA NETWORK SETTINGS 161
3. CONNECT CAMERA(S) 162
4. CONFIGURE SECONDARY NIC (CLOSED NETWORK SETUP ONLY) 163
5. ENTER SYSTEM LICENSE KEY (HYBRID APPLIANCES ONLY) 163
6. CONFIGURE IP CAMERAS 164
   6.1 Manual Camera Configuration 164
   6.2 Discover Network/IP Cameras 165
   6.3 Export Settings to CSV 167
   6.4 Universal Drivers 167
7. IP CAMERA SETTINGS 169
   7.1 Select Video Mode 170
   7.2 Configure Video Recording Settings for MJPEG Video 171
   7.3 Configure Video Recording Settings for MPEG-4 Video 172
   7.4 Configure Video Recording Settings for H.264 Video 174
   7.5 Configure 360-Degree Panomorph Camera Settings (Fall Release-2015 (8.1.x and above) only) 175
   7.6 Smart Streaming 178
   7.7 Camera-Specific Settings When Smart Streaming is set to YES 179
   7.8 Hardware Rendering 179
8. USING THE GENERIC IP CAMERA DRIVER 180
   8.1 Identifying the URL Path 180
   8.2 Configuring a Generic IP Camera 180
9. IP CAMERA TROUBLESHOOTING 181
   9.1 IP Camera Fails To Load 181
   9.2 Generic IP Camera Driver Troubleshooting 183
10. CONFIGURING IP CAMERA VIRTUAL REGIONS 183
   10.1 About Virtual Regions 183
   10.2 Configuring Virtual Regions 183
11. CONFIGURING MULTIPLE PIPELINE MANAGER 186

DRAFT

DRAFT

1. OVERVIEW

This chapter explains how to install and configure IP cameras on a 3VR appliance.

1.1 Supported Cameras

Prior to beginning an IP camera installation, please verify that the camera you intend to install is supported by 3VR. You can cross-reference the camera model name with the current list of supported cameras posted on the FAQ section of www.3VR.com (click **Support** > **FAQ**). 3VR partners may also visit the Support Portal (partners.3VR.com) for detailed camera and driver support information. Please contact 3VR Technical Support with any questions regarding supported cameras or drivers.

Even if the camera is not explicitly supported, it may still be possible for the 3VR appliance to connect to it using the generic IP camera driver. See section 8 of this chapter for details.

1.2 IP Camera Connection Methods

There are two ways to connect one or more IP cameras to a 3VR system. Before beginning, review the two connection methods and decide which is the most appropriate for the installation:

A. LAN Setup

With this method, you connect cameras to a switch, and enter the camera's IP address in System Manager. There is no physical connection between the camera and the 3VR appliance, and the camera is still accessible on the LAN (for example, a user could view the camera by entering the camera's IP address in a web browser).

This setup is supported on all 3VR appliance models, provided that the unit is licensed for IP cameras (NVR systems and hybrid systems with IP camera expansion*).

B. Closed Network Setup

With this method, you physically connected cameras to the 3VR appliance's secondary network port using an Ethernet cable and a PoE injector or switch. In this configuration, the camera is not accessible on the LAN, and consequently you can only view video through 3VR applications. Only 3VR appliances (listed below) with two network adapters support the closed network setup:

- 1000, 3000, 4000, 5500-Series Hybrid* and NVR

***Note**
Customers with hybrid (both analog and IP) systems must purchase IP camera expansion licenses for each IP camera they wish to connect to the system. Contact 3VR Orders (orders@3VR.com) to purchase IP cameras and obtain a system license key. See section 5 of this chapter for more information.

DRAFT

2. CONFIGURE CAMERA NETWORK SETTINGS

IP Camera Discovery Tool
You can configure all of the camera's settings in System Manager using the IP Camera Discovery Tool. See section 6.2 for information about the IP Camera Discovery Tool.

A. LAN Setup

1. Connect your laptop to the IP camera using an Ethernet cable.
2. Launch the IP camera configuration utility (usually included on a disc in the box with the camera).
3. Configure the camera's network settings to the values assigned to the camera by the organization's IT department.

B. Closed Network Setup

1. Connect your laptop to the IP camera using an Ethernet cable.
2. Launch the IP camera configuration utility (usually included on a disc in the box with the camera).
3. Set the static IP address of the first camera to a valid IP address for your network and any remaining cameras to valid IP addresses in the final octet. For example, if you set the IP address for the first camera to **192.168.1.6**, set the IP address for the second camera to **192.168.1.7** and the third camera to **192.168.1.8**.

3. CONNECT CAMERA(S)

This section describes how to connect a network camera on a LAN and directly to a 3VR appliance.

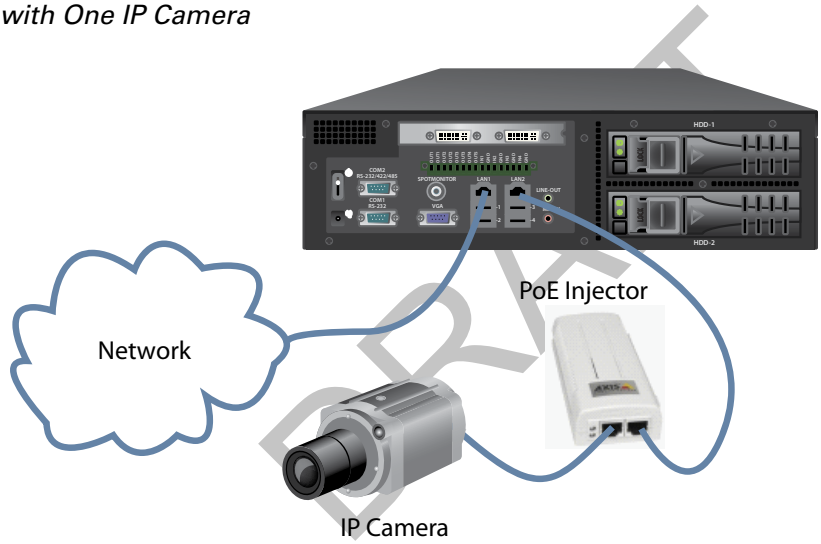
A. LAN Setup

Connect the camera(s) to a switch.

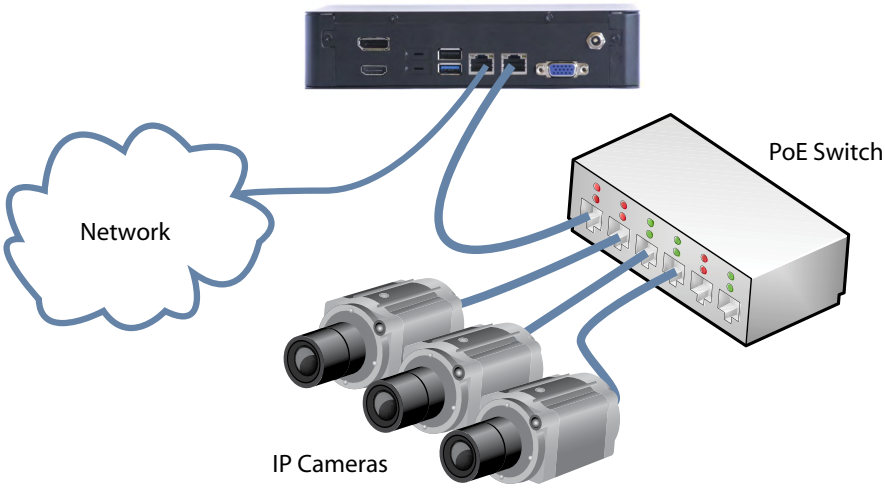
B. Closed Network Setup

Use the following sample installation diagrams to assist with the physical setup of the 3VR appliance and camera(s). Please note that on appliances with two network adapters, the secondary network adapter is the right-hand port.

Installation with One IP Camera



Installation with Multiple IP Cameras

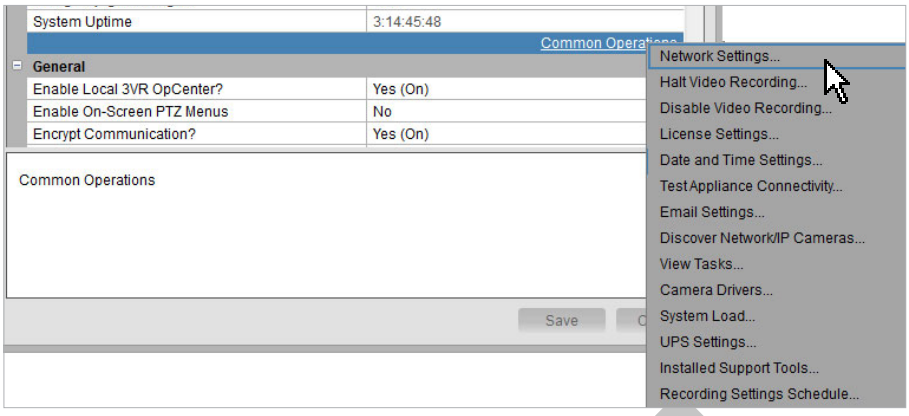


4. CONFIGURE SECONDARY NIC (CLOSED NETWORK SETUP ONLY)

For cameras physically connected to an appliance, in order for the appliance to connect to the cameras you must edit the network settings of the appliance's secondary network adapter as follows:

1. In the **Configure** panel of System Manager, click the appliance name in the left-hand panel to view the system settings.

2. Under the **Appliance** category heading, click Common Operations, and then click **Network Settings**.



3. In the **Network Settings** dialog box, select the secondary network adapter from the list. This is the adapter that is not labeled **[Primary]**.

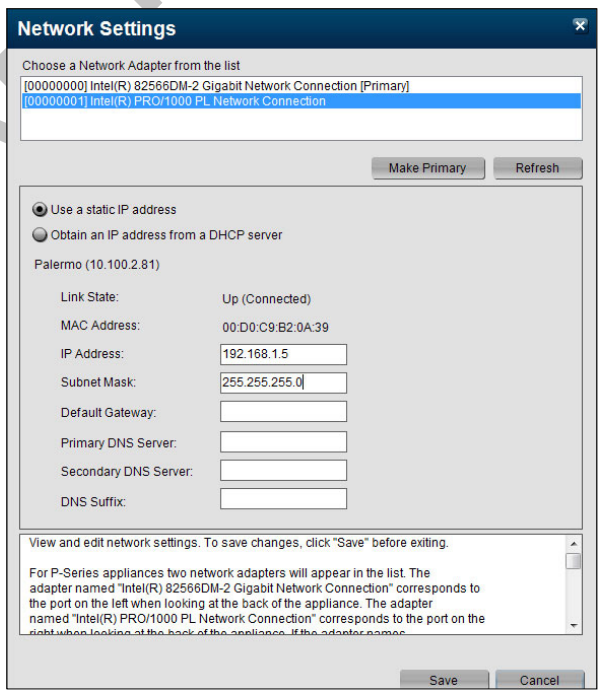
4. Edit the network settings of the secondary adapter as follows:

   - IP Address: **192.168.1.5**
   - Subnet Mask: **255.255.255.0**

   Leave the remaining fields blank.

5. Click **Save**. A confirmation dialog appears.

6. Click **Change Network Settings** to continue.



DRAFT

5. ENTER SYSTEM LICENSE KEY (HYBRID APPLIANCES ONLY)

If you are configuring a hybrid appliance (i.e., the appliance has analog camera inputs), you may need to license the appliance for IP camera expansion prior to configuring IP cameras.

Contact 3VR Orders (orders@3VR.com) to purchase an IP camera expansion license. The relevant SKUs are listed in the 3VR Commercial SKU Guide, available on the Support Portal (partners.3VR.com). Upon receipt of a P.O., 3VR Orders will provide you with a system license key, which you apply to the unit using the instructions in chapters on installing appliances and VMS software .

6. CONFIGURE IP CAMERAS

This section describes how to manually add and automatically discover IP cameras.

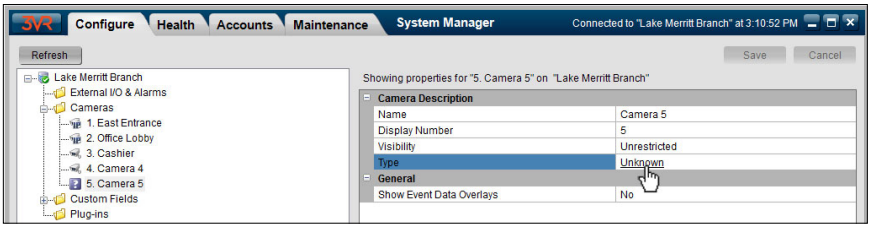
6.1 Manual Camera Configuration

1. In the **Configure** panel, click the plus sign next to the system display name.

2. Click the plus sign next to **Cameras** to display the list of cameras on the unit.

3. Select the camera designated for the first IP camera.

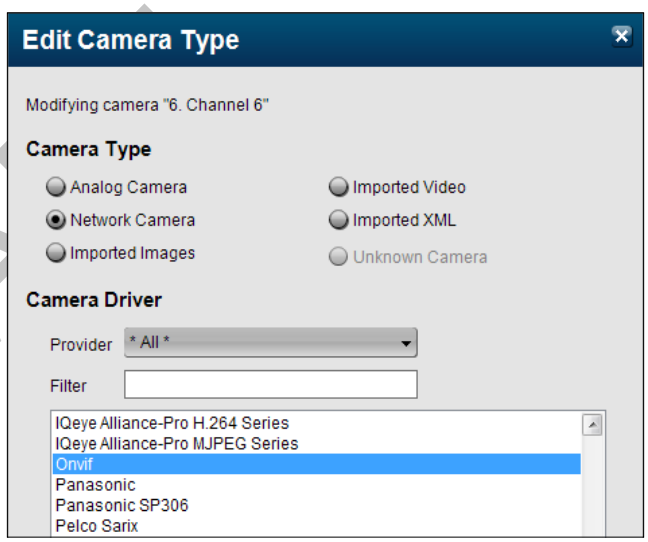
4. On the right-hand side of System Manager, click the link next to **Type** (the link text will be the current camera type, e.g. Analog, Network, or Unknown).



5. In the **Edit Camera Type** dialog box, click **Network Camera** if it is not already selected.

6. Choose the appropriate driver for the IP camera from the **Camera Driver** drop-down menu.

7. Click **Save** to save changes and return to the **Configure** panel.



> **Camera Driver Not Listed?**
> If the camera you are configuring is not listed in the **Camera Driver** drop-down menu, it is not officially supported by 3VR. However, it may be possible to connect to the camera using the generic IP camera driver. See section 8 of this chapter for details.

8. The camera settings will update to only display the settings appropriate for the selected driver.

   Click the field to the right of **Network Camera: Network Address** and enter the camera's IP address.

   - For cameras on a LAN, this is the IP address that was assigned to the camera by the customer's IT department.
   - For cameras physically connected to the appliance, this is the address in the format **192.168.1.x** that you set on the camera using the manufacturer's utility.

9. Type the user name and password used to connect to the camera in the **Network Camera: User Name** and **Network Camera: Password** boxes.

Camera Description	
Name	Office Lobby
Display Number	2
Visibility	Unrestricted
Type	Network Camera (Axis Q1755)
Network Camera: Network Address	192.168.1.6
Network Camera: User Name	
Network Camera: Password	
Network Camera: Network Port	
Network Camera: Video Server Port	

> **Note**
> Many IP camera models ship from the factory with authentication enabled. For password-protected cameras, you must enter the correct user name and password in System Manager in order for the 3VR appliance to connect. Consult the camera's documentation to obtain the default user name and password information for your camera model.

10. Click **Save**.

11. Repeat steps 3-10 to configure any additional IP cameras.

6.2 Discover Network/IP Cameras

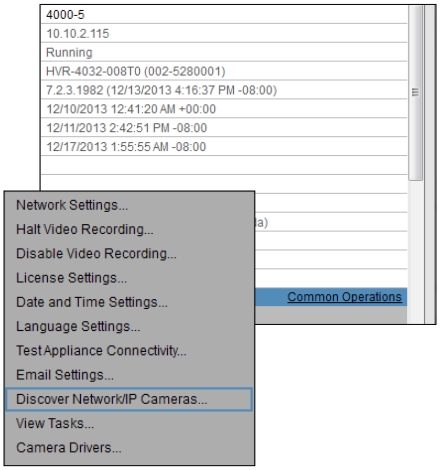
You can use the Discover Network/IP Cameras tool to assist with finding IP cameras that are available for use by the 3VR appliance. These cameras can either be part of the open network or a closed POE network.

Finding Available IP Cameras

To discover and add cameras to a 3VR appliance using this method, perform the following steps:

12. Open System Manager, and choose the Configure tab.

13. Select your 3VR appliance

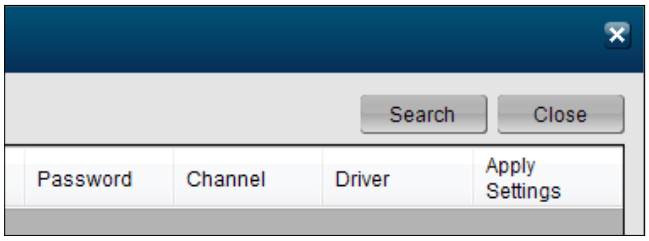


14. Select the Common Operations hyperlink on the right-hand side of the screen under the Appliance settings.

15. Choose **Discover Network/IP Cameras**. The Discover Network/IP Cameras window opens.

16. Use this window to perform a search for existing IP cameras. (This window also displays the available Resource and License Units currently available on the system.)

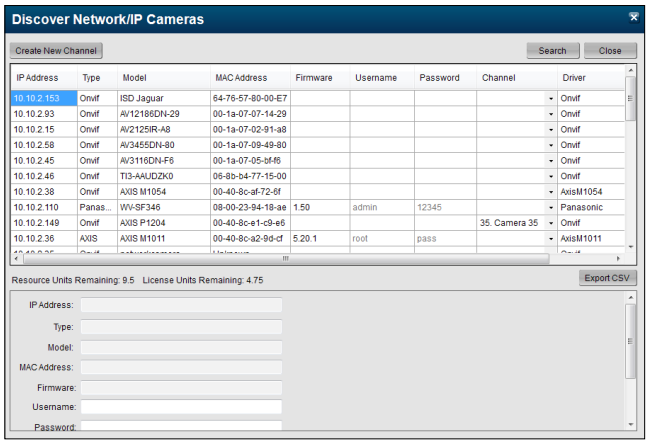
- To perform a search, select the **Search** button in the top right of the Discover Network/IP Cameras window. The search processes for 60 seconds. During this time, the window populates with information for all available IP cameras.



DRAFT

Settings displayed are as follows:

- IP Address
- Camera Type
- Camera Model
- MAC Address
- Camera Firmware
- Camera Username
- Camera Password
- Assigned Channel
- Camera Driver

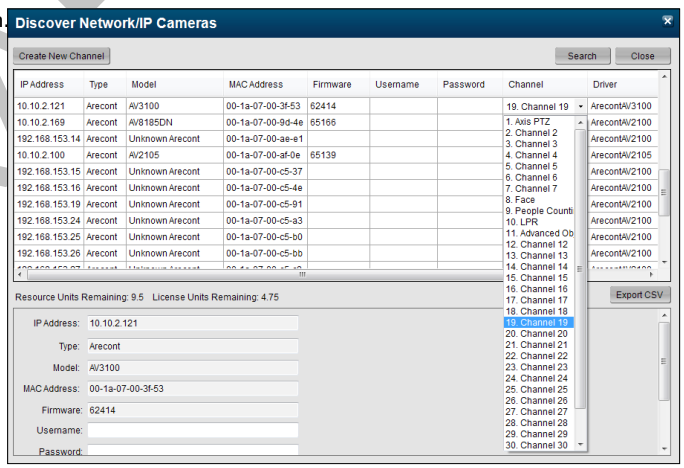


Adding IP Cameras Using Discover Network/IP Cameras Tool

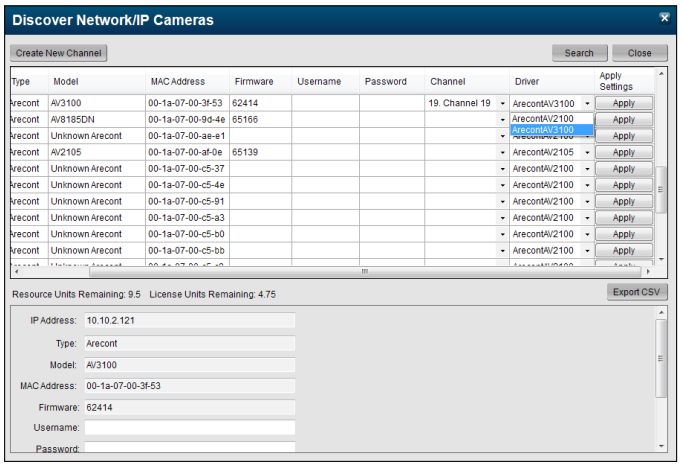
Note
Some ONVIF cameras might not be compatible with the 3VR system. For information, go to: http://www.3vr.com/resources/supportedcameras and search for your camera..

You can assign cameras found during the search to a channel using the following process:

1. Identify the camera that needs to be added to the 3VR system.
2. Using the Channel drop-down menu, select the channel to assign to the camera. If there are no free channels, you can create a new channel by selecting the **Create New Channel** button in the top-left corner of the window.



3. Using the **Driver** drop-down menu, select the correct driver for the camera being added.
4. If the camera requires a username and password, enter the correct username and password.
5. You can enter the username, password, channel, and driver using the table at the top of the window or by selecting the camera and using the form at the bottom of the window.
6. When the correct information is completely entered, select **Apply** to commit these settings to the camera.
7. Repeat this process until you've added all needed IP cameras.



DRAFT

6.3 Export Settings to CSV

You can generate a spreadsheet containing the settings described above for all added IP cameras by selecting the **Export CSV** button. When you select this button, a window opens. Use this window to specify the destination and name for the .csv file.

When completed, select **Close** to close the window and return to System Manager.

6.4 Universal Drivers

Usernames and Passwords with ONVIF

The Auto Discovery Tool always shows the default usernames and passwords that are set up by the camera manufacturer. These are shown in a gray caption. User-defined usernames and passwords for cameras appear in a black caption. The Auto Discovery Tool does not record username and passwords that are set through it. The tool always reverts to showing the default username and password for the camera once the Auto Discovery Tool window is closed and reopened.

To allow for a wider range of cameras for use with the 3VR appliance, 3VR has added several universal drivers. These drivers allow for easier integration with IP cameras.

The following universal drivers are now supported for use with 3VR appliances:

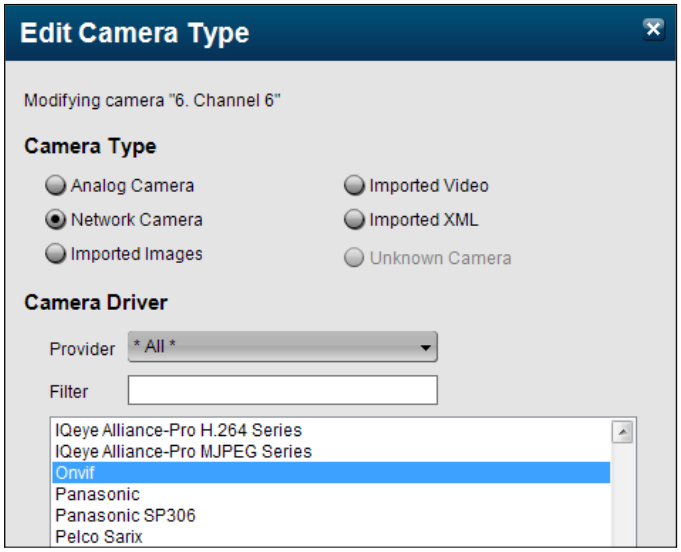
- ONVIF Driver
- Axis Communications Universal Camera Driver (aka Axis VAPIX)
- Arecont Vision Universal Driver (aka Generic Arecont)
- Vivotek Universal Driver
- Hikvision Universal Driver
- Panasonic Universal Camera Driver
- Samsung Universal Camera Driver

DRAFT

Using the Universal Camera Drivers

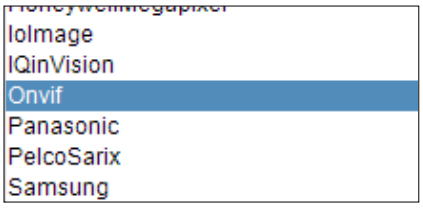
The process for using the universal camera drivers is as follows:

1. In System Manager, under the Configure tab, select or add the camera you want to use for one of the above drivers. See the General Camera Configuration chapter for instructions on how to add cameras.
2. Select the link in the field beside **Type**. (For a new camera, the link is Unknown.) The Edit Camera Type dialog box opens.
3. Choose **Network Camera** from the list of Camera Types.



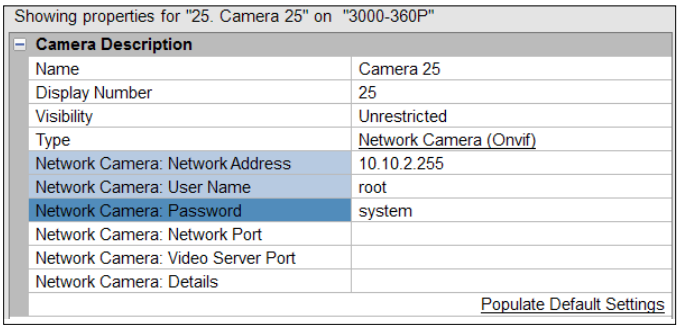
4. Choose the camera manufacturer from the **Provider** drop-down menu. For an ONVIF camera, choose **Onvif**.

5. Choose one of the universal camera drivers from the drivers list. The ONVIF driver may be populated by default.

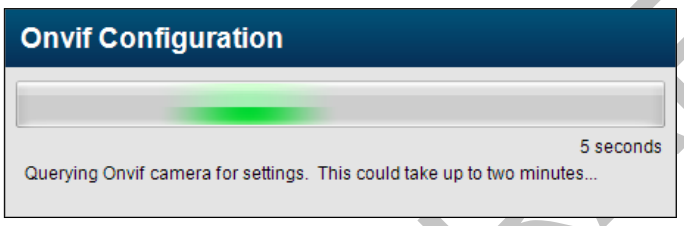


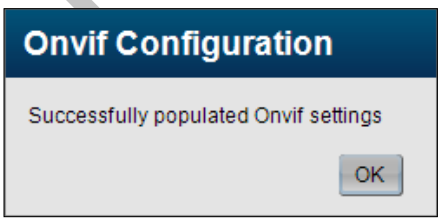
6. Click **Save**.

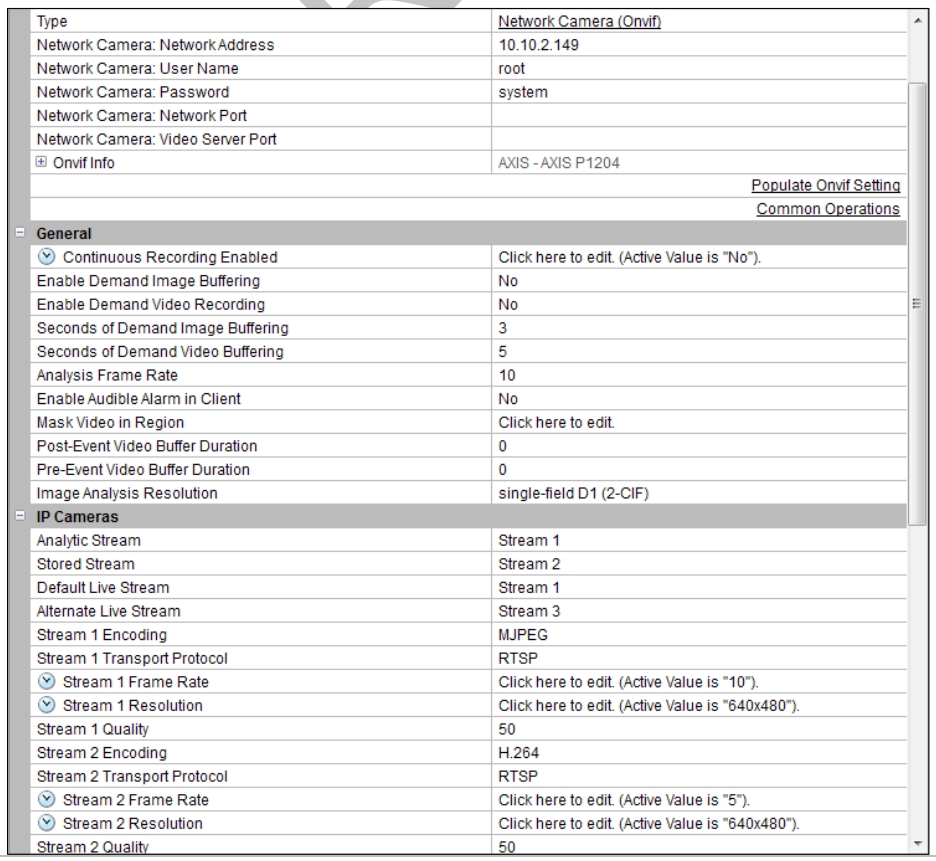
7. Enter the network address for the camera in the **Network Camera: Network Address** field. If applicable, enter the user name and password required to access the camera in the **Network Address: User Name** and **Network Camera: Password** fields, respectively.



8. Choose **Populate Default Settings**. Click **Yes** to proceed. System Manager queries the camera for settings (this might take a few moments). If successful, the camera settings window is populated with the relevant settings downloaded from the network camera.







Repopulating Universal Driver Settings

You must click **Populate Default Settings** every time you change a network-related setting on the camera to ensure that the camera works properly with the 3VR system.

Default Settings

Populating camera settings on a specific channel overwrites all camera settings on that channel, returning them to the camera default.

The populated universal camera driver settings differ between camera manufacturers.

The most common causes of the 3VR system failing to populate universal camera driver settings are as follows:

- The camera is not supported.
- The system timed out while contacting the camera.
- The credentials for logging into the camera are incorrect.
- There is a networking issue preventing successful completion.

You can find all the Universal Camera Driver settings under the IP Camera Settings section. These drivers have multiple camera streams. Once you configure these streams, you can assign them to the following:

- Analytic Stream
- Stored Stream
- Default Live Stream
- Alternate Live Stream

ONVIF with Axis Cameras

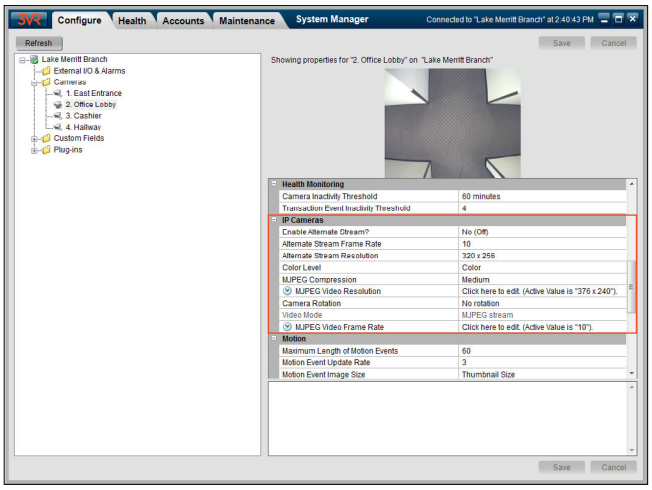
In order for Axis cameras to successfully use the ONVIF settings on the camera user interface, you must first manually add user credentials to the ONVIF account list within the camera user interface. Once you do this, ONVIF settings should populate to the camera correctly.

DRAFT

7. IP CAMERA SETTINGS

For each IP camera that you configured in section 6, you can adjust the way the video is recorded and displayed by modifying the camera-specific settings. To access these settings:

1. Select the camera name in the navigation panel. Scroll down through the camera settings until you locate the **IP Cameras** category. The options displayed here will vary depending on the **Camera Driver** that you selected when configuring the camera.

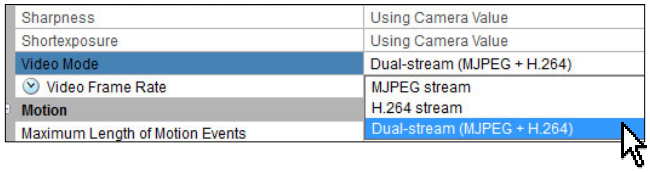


The remainder of this section provides an overview of some of the most common IP camera settings.

If the setting you would like to modify is not listed in this document, please refer to the help text displayed in the lower panel of System Manager for more information about the setting.

7.1 Select Video Mode

The first step in configuring the settings of an IP camera is to select the **Video Mode**. This setting specifies the video compression standard and streaming mode for the camera.



Depending on the model of camera, one or more of the following options will appear in the **Video Mode** drop-down menu. Select the mode that is most appropriate for the customer's network, storage, and video quality needs:

- **MJPEG stream**
  When recording in MJPEG mode, each video frame is captured as an individual JPEG compressed image. MJPEG mode creates high-quality individual video frames, but requires significant network bandwidth and storage space.

  Set the **Video Mode** for cameras used for video analytics to **MJPEG stream** if there is sufficient network bandwidth, and the camera does not support **Dual-stream** mode.

- **MPEG-4 stream**
  MPEG-4 consumes bandwidth and storage space more efficiently than MJPEG because the camera transmits only the changes to each successive video frame, rather than the entire image. This makes MPEG-4 ideal for installations with strict limitations on network bandwidth or storage space. However, recording MPEG-4 video is more CPU intensive than MJPEG.

- **H.264 stream**
  The benefits and drawbacks of H.264 are comparable to MPEG-4.

- **Dual-stream (MJPEG + MPEG-4** or **MJPEG + H.264)**
  In dual-stream mode, the 3VR appliance receives one of each type of stream from the camera. Dual-stream mode achieves both the quality image of MJPEG mode and the reduced storage consumption of MPEG-4 or H.264. Dual-stream mode requires more bandwidth than MPEG-4 or H.264 alone, though it uses roughly the same bandwidth as MJPEG mode.

  Dual-stream mode is recommended if the network has sufficient bandwidth and the camera supports dual-stream mode.

DRAFT

7.2 Configure Video Recording Settings for MJPEG Video

The settings in this section apply to MJPEG video. They take effect when the **Video Mode** is set to **MJPEG Stream, Dual-stream (MJPEG + MPEG-4)**, or **Dual-stream (MJPEG + H.264)**.

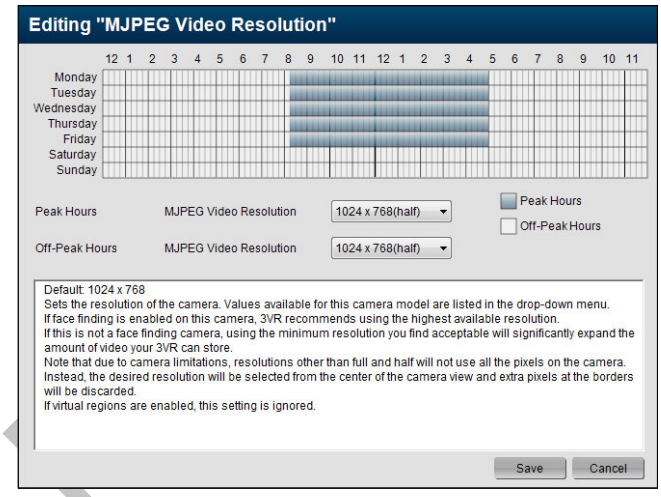
MJPEG Video Resolution

Default: Camera-specific
Range: Camera-specific

This setting controls the resolution of MJPEG video. If you plan to enable video analytics on this camera, 3VR recommends using 2-CIF resolution. Otherwise, you should set the resolution to the minimum value that provides acceptable video quality.

To set the MJPEG resolution of an IP camera:

1. Click the ellipsis (**...**) button beside **MJPEG Video Resolution**.
2. Select a new value from the **MJPEG Video Resolution** drop-down menu for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.



Video Frame Rate

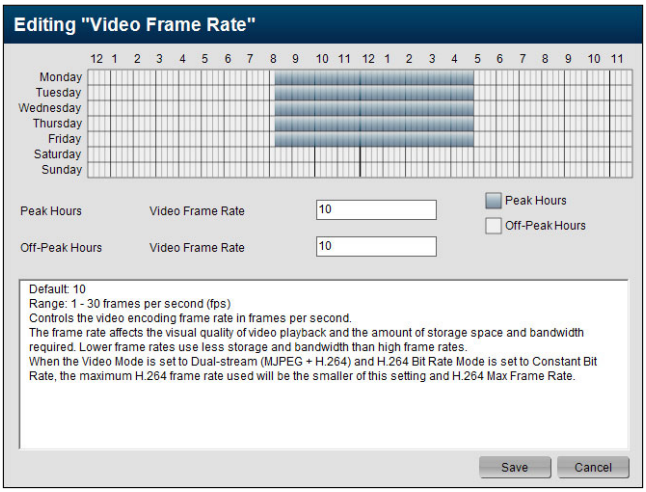
Default: **10**
Range: **1–60 fps**

This setting controls the video encoding frame rate in frames per second (fps).

The frame rate affects the visual quality of video playback and the amount of bandwidth and storage space required. Higher values result in smoother video playback and more successful application of video analytics, but higher frame rates also consume more bandwidth and storage space. Lower frame rates use less bandwidth and storage space. 3VR recommends a frame rate between 5 and 10 frames per second.

To set the frame rate of an IP camera:

1. Click the ellipsis (**...**) button beside **Video Frame Rate**.
2. Type a new value in the **Video Frame Rate** text box for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.

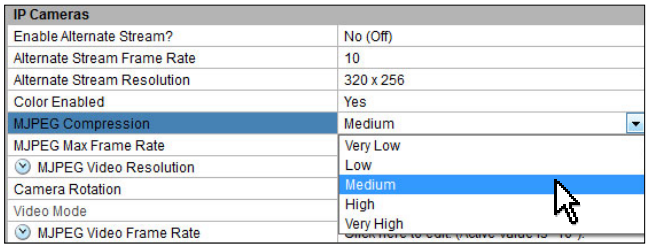


DRAFT

Compression

Default: **Low**
Range: **Very Low - Very High**

When selecting a compression value, there is a trade-off between image size and quality. Setting the compression value to **Very Low** results in high-quality video, but the image files are also at their largest size. Conversely, using **Very High** compression results in low-quality video with a smaller file size. Also, higher compression values require more CPU processing.



If you plan to enable video analytics on this camera, 3VR recommends using the lowest compression value available. Otherwise, you should set the compression to the highest value that provides acceptable video quality.

7.3 Configure Video Recording Settings for MPEG-4 Video

The settings in this section apply to MPEG-4 video. They take effect when the **Video Mode** setting is set to **MPEG-4 stream** or **Dual-stream (MJPEG + MPEG-4)**.

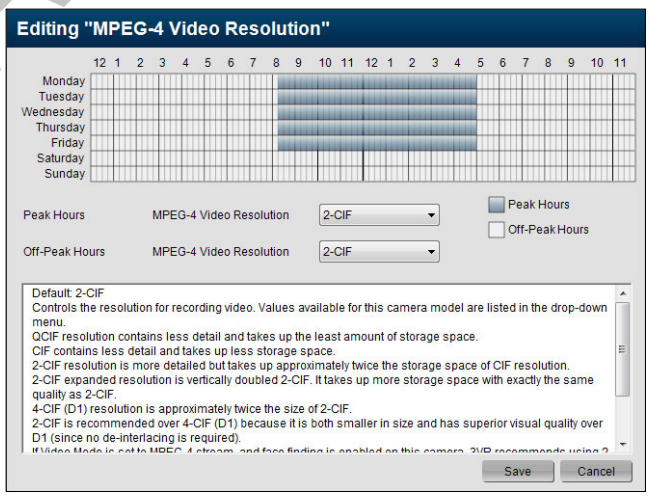
MPEG-4 Video Resolution

Default: Camera-specific
Range: Camera-specific

This setting controls the resolution of MPEG-4 video. If you plan to enable video analytics on this camera, 3VR recommends using the highest available resolution. Otherwise, you should set the resolution to the minimum value that provides acceptable video quality.

To set the MPEG-4 resolution of an IP camera:

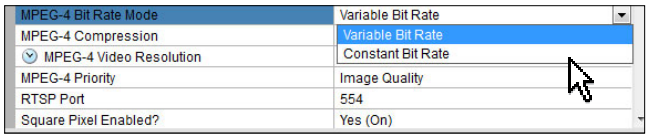
1. Click the ellipsis (**...**) button beside **MPEG-4 Video Resolution**.
2. Select a new value from the **MPEG-4 Video Resolution** drop-down menu for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.



MPEG-4 Bit Rate Mode

Default: **Variable Bit Rate**

The **MPEG-4 Bit Rate Mode** setting controls how the camera selects frame rate and compression values for MPEG-4 video.



- **Variable Bit Rate**: When using variable bit rate, the camera keeps the quality of the video stream (compression and frame rate) constant while allowing bit rate to fluctuate, up to a maximum bandwidth threshold. If there is no need for the camera's bandwidth consumption to be a constant value, 3VR recommends leaving this setting at **Variable Bit Rate** for maximum control over compression and frame rate.

DRAFT

- **Constant Bit Rate**: This mode allows you to specify a target bit rate for the camera. The camera then automatically adjusts its compression and frame rate settings to maintain a constant bit rate. If the camera should always consume the same amount of bandwidth, select **Constant Bit Rate** as the **MPEG-4 Bit Rate Mode**.

MPEG-4 Variable Bit Rate Settings

When **Variable Bit Rate** is selected as the bit rate mode for a camera recording MPEG-4, the following settings take effect:

MPEG-4 Max Bit Rate

MPEG-4 Max Bit Rate	2000
MPEG-4 Max Compression	Low
MPEG-4 Max Frame Rate	10

Default: **2000**
Range: **0–1000000 bps**

This setting represents the maximum bandwidth the camera can use, defined as the maximum allowable bit rate for the stream.

The bit rate affects how much bandwidth and storage will be used by video from this camera. Higher values result in higher video quality and frame rate, but require a greater amount of bandwidth and storage space.

3VR recommends setting the maximum bit rate equal to 90 percent of the total network bandwidth available for video streaming divided by the number of cameras. For example, if you have a 100 Mbps dedicated network with 90 cameras, set this value to 1000000 (1 Mbps).

MPEG-4 Compression

See section 7.2 for more information on setting the compression.

Video Frame Rate

See section 7.2 for more information on setting the frame rate.

DRAFT

MPEG-4 Constant Bit Rate Settings

When **Constant Bit Rate** is selected as the bit rate mode for a camera, the following settings take effect:

MPEG-4 Priority

MPEG-4 Priority	Image Quality
RTSP Port	Frame Rate
Square Pixel Enabled?	Image Quality

Default: **Image Quality**

This setting determines whether the camera bit rate controller should prioritize **Image Quality** or **Frame Rate**.

- Select **Image Quality** to prioritize the image quality of the recorded image over the frame rate of the video. When **Image Quality** is selected, individual images are more detailed, but the video stream may be choppy during scenes with significant motion.
- Select **Frame Rate** to prioritize video stream smoothness over the quality of the captured image. When **Frame Rate** is selected, the video stream is smoother during scenes with significant motion, while the images may be of lower quality to compensate.

MPEG-4 CBR Target Bit Rate

Video Mode	MJPEG stream
MPEG-4 CBR Target Bit Rate	1000
Video Frame Rate	Click here to edit. (Active Value i

Default: **1000**
Range: **0–1000000 bps**

This setting represents the maximum allowed bit rate for the stream.

The bit rate affects how much bandwidth and storage are used by video from this camera. Setting a higher bit rate requires a greater amount of bandwidth and storage space, but results in higher video quality and/or frame rate.

3VR recommends setting the target bit rate equal to the total network bandwidth available for video streaming divided by the number of cameras. For example, if you have a 100 Mbps dedicated network with 100 cameras, set this value to 1000000 (1 Mbps).

MPEG-4 Min Frame Rate

Default: **5**
Range: **1–30 fps**

MPEG-4 Max Frame Rate

Default: **10**
Range: **1–30 fps**

These settings represent the lower and upper limits on the frame rate.

MPEG-4 Max Frame Rate	10
MPEG-4 Min Compression	Very Low
MPEG-4 Min Frame Rate	5
MJPEG Video Resolution	Click here to edit. (Active Value is "2-(

MPEG-4 Max Compression	Low
MPEG-4 Max Frame Rate	10
MPEG-4 Min Compression	Very Low
MPEG-4 Min Frame Rate	5

Note
The 3VR appliance uses the smallest of either the **MPEG-4 Max Frame Rate** or **Video Frame Rate** settings as the maximum frame rate for MPEG-4 video.

7.4 Configure Video Recording Settings for H.264 Video

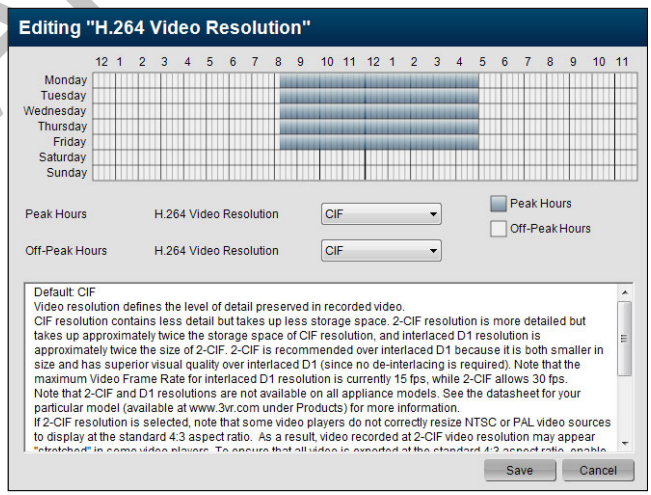
H.264 Video Resolution

Default: Camera-specific
Range: Camera-specific

If you plan to enable video analytics on the camera you are configuring, 3VR recommends using the highest available resolution. Otherwise, you should set the resolution to the minimum value that provides acceptable video quality.

To set the H.264 resolution of an IP camera:

1. Click the ellipsis (**...**) button beside **H.264 Video Resolution**.
2. Select a new value from the **H.264 Video Resolution** drop-down menu for peak hours or off-peak hours.
3. Click **Save** to save changes and return to the **Configure** panel.



H.264 Compression

See section 7.2 for more information on setting the compression.

Video Frame Rate

See section 7.2 for more information on setting the frame rate.

DRAFT

7.5 Configure 360-Degree Panomorph Camera Settings (Fall Release-2015 (8.1.x and above) only)

Note
Make sure you use the latest System Manager version to use this feature.

360-degree cameras cover a 360-degree view area. You can pinpoint the view you want to concentrate on without impacting the entire view. This provides functionality similar to PTZ cameras, without the lag due to PTZ operation. You can record the entire area and, using OpCenter, focus on a particular region of interest.

Select the Camera's Universal Driver and Populate Camera Settings

For all the supported cameras, you can use either the camera's universal driver or the ONVIF driver. The table below shows the universal drivers to use for the currently supported 360-degree panomorph cameras.

Camera	Universal Driver to Use
Arrecont	Arecont Vision Universal Driver
Sony	Sony Universal Driver
Vivotek	Vivotek Universal Driver
Axis	Axis Communications Universal Driver
OnCam	OnCam Universal Driver
ONVIF	Onvif

1. Select the correct universal driver for your camera. Refer to the section, "Universal Drivers" on page 167, for details.
2. After you select the driver, make sure you select **Populate Default Settings**.

Camera-Specific Settings

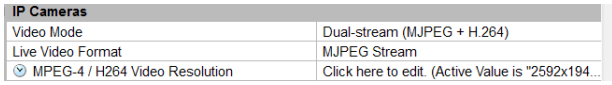
Refer to the appropriate section below for information about the settings specific to your camera. In general, if you have a camera other then the ones documented below, you can use the steps in the section, "ONVIF Cameras" on page 177. Just make sure you select the **Panorama Dewarp Type** for your camera.

To change a setting, click in the field to the right of the desired parameter, for example, **Live Video Format**. Click the down arrow and select the desired setting from the pop-up menu. The selected setting appears in the field to the right of the parameter.

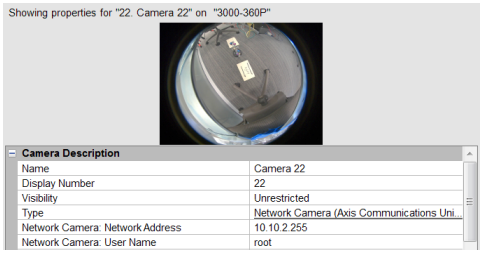
Axis Cameras

If using an Axis camera, perform the steps below to complete camera configuration.

1. Select the channel connected to the Axis camera from the channel tree on the left. The camera settings appear on the right.
2. Scroll down the to **IP Cameras** section.
3. Make sure that for the **Live Video Format** is set to **MJPEG Stream.**



4. Select **Axis** as the **Panorama Dewarp Type**.
5. Select the **Panorama Mount Type** that matches your camera installation. For a camera mounted on the ceiling, select **Ceiling**; for a camera mounted on a wall, select **Wall**; for a camera mounted on the floor, select **Floor**.
6. Click **Save**.
7. Right-click on the camera you are configuring in the camera tree and select **Enable Camera**. Click **Yes** to confirm. In a short while, the unmodified camera image appears in the viewer on the right.



DRAFT

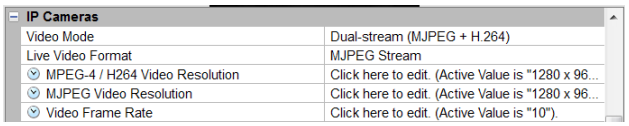
Arecont/Sony Cameras

If using an Arecont or Sony camera, perform the steps below to complete camera configuration.

1. Select the channel connected to the Arecont Vision or Sony camera from the channel tree on the left. The camera settings appear on the right.

2. Scroll down the to **IP Cameras** section.

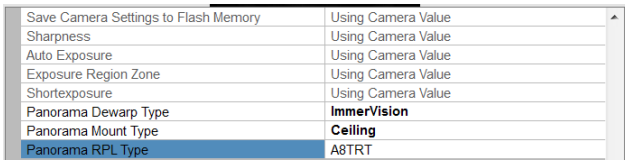
3. Make sure **MJPEG Stream** is set for the **Live Video Format.**



IP Cameras	
Video Mode	Dual-stream (MJPEG + H.264)
Live Video Format	MJPEG Stream
MPEG-4 / H264 Video Resolution	Click here to edit. (Active Value is "1280 x 96...
MJPEG Video Resolution	Click here to edit. (Active Value is "1280 x 96...
Video Frame Rate	Click here to edit. (Active Value is "10").

4. Select **ImmerVision** as the **Panorama Dewarp Type**.

5. Select the **Panorama Mount Type** that matches your camera installation. For a camera mounted on the ceiling, select **Ceiling**; for a camera mounted on a wall, select **Wall**; for a camera mounted on the floor, select **Floor**.

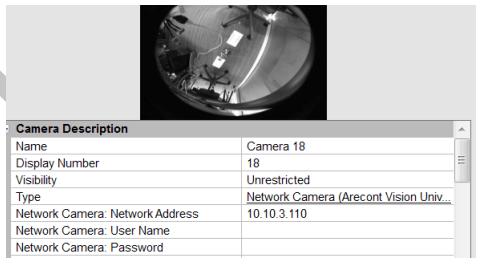


Save Camera Settings to Flash Memory	Using Camera Value
Sharpness	Using Camera Value
Auto Exposure	Using Camera Value
Exposure Region Zone	Using Camera Value
Shortexposure	Using Camera Value
Panorama Dewarp Type	**ImmerVision**
Panorama Mount Type	**Ceiling**
Panorama RPL Type	A8TRT

6. For ImmerVision lenses, you need to specify the lens type, which is provided by the lens manufacturer. Select the correct lens type next to **Panorama RPL (Registerd Panomorph Lens) Type**.

7. Click **Save**.

8. Right-click on the camera you are configuring in the camera tree and select **Enable Camera**. Click **Yes** to confirm. In a short while, the unmodified camera image appears in the viewer on the right.



Camera Description	
Name	Camera 18
Display Number	18
Visibility	Unrestricted
Type	Network Camera (Arecont Vision Univ...
Network Camera: Network Address	10.10.3.110
Network Camera: User Name	
Network Camera: Password	

DRAFT

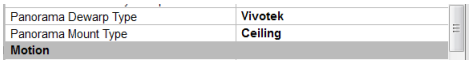
Vivotek Cameras

If using a Vivotek camera, perform the steps below to complete camera configuration.

1. Select the channel connected to the Vivotek camera from the channel tree on the left. The camera settings appear on the right.

2. Scroll down the to **IP Cameras** section.

3. Select **Vivotek** as the **Panorama Dewarp Type**.

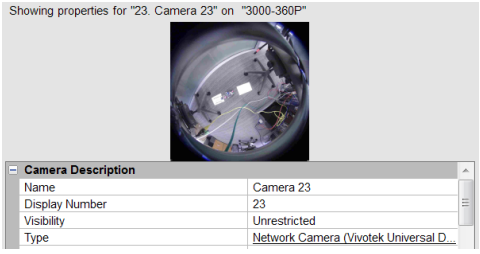


Panorama Dewarp Type	**Vivotek**
Panorama Mount Type	**Ceiling**
Motion	

4. Select the **Panorama Mount Type** that matches your camera installation. For a camera mounted on the ceiling, select **Ceiling**; for a camera mounted on a wall, select **Wall**; for a camera mounted on the floor, select **Floor**.

5. Click **Save**.

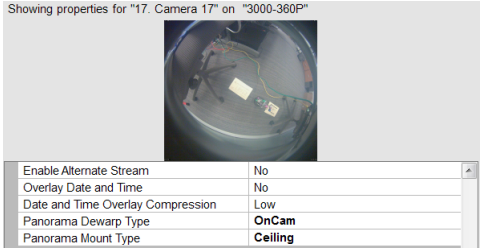
6. Right-click on the camera you are configuring in the camera tree and select **Enable Camera**. Click **Yes** to confirm. In a short while, the unmodified camera image appears in the viewer on the right.



OnCam Cameras

If using an OnCam camera, perform the steps below to complete camera configuration.

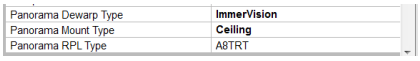
1. Select the channel connected to the OnCam camera from the channel tree on the left. The camera settings appear on the right.
2. Scroll down the to **IP Cameras** section.
3. Select **OnCam** as the **Panorama Dewarp Type**.
4. Select the **Panorama Mount Type** that matches your camera installation. For a camera mounted on the ceiling, select **Ceiling**; for a camera mounted on a wall, select **Wall**; for a camera mounted on the floor, select **Floor**.
5. Click **Save**.
6. Right-click on the camera you are configuring in the camera tree and select **Enable Camera**. Click **Yes** to confirm. In a short while, the unmodified camera image appears in the viewer on the right.



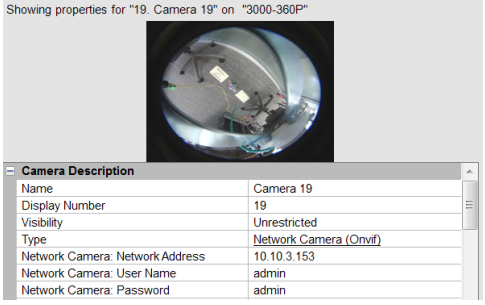
ONVIF Cameras

If using the ONVIF driver with your camera, perform the steps below to complete camera configuration.

1. Select the channel connected to the camera configured with the ONVIF driver from the channel tree on the left. The camera settings appear on the right.
2. Scroll down the to **IP Cameras** section.
3. Select the correct camera type for the **Panorama Dewarp Type**. For Arecont and Sony cameras, select **ImmerVision**.



   - For ImmerVision lenses, you need to specify the lens type, which is provided by the lens manufacturer. Select the correct lens type next to **Panorama RPL (Registerd Panomorph Lens) Type**.
4. Select the **Panorama Mount Type** that matches your camera installation. For a camera mounted on the ceiling, select **Ceiling**; for a camera mounted on a wall, select **Wall**; for a camera mounted on the floor, select **Floor**.
5. Click **Save**.
6. Right-click on the camera you are configuring in the camera tree and select **Enable Camera**. Click **Yes** to confirm. In a short while, the unmodified camera image appears in the viewer on the right.



DRAFT

7.6 Smart Streaming

To improve the 3VR application performance, 3VR has implemented the Smart Streaming feature.

- Smart Streaming is available for IP camera channels.
- Smart Streaming settings are on a per channel basis.
- Smart Streaming works with both live video and recorded video playback.
- Smart Streaming is disabled by default.

> Default: No
> Setting this value to "Yes" uses second stream in multi channel layout for viewing live video and stored video in 3VR client applications.
> When this setting is enabled, second stream will be recorded along with regular stream and the second stream resolution is determined by the resolution for smart streaming setting. When this setting is disabled, the live video stream uses the settings of the storage stream.
> Note: Setting the value to "Yes" increases the storage space requirement.

When the **Smart Streaming** setting is set to **No**:

- The live video stream uses the settings defined in the **Live Video Format**.

When the **Smart Streaming** .setting is set to **Yes**:

- It uses a second stream in multi-channel layout for viewing live video and stored video in 3VR client applications.
- A second stream is recorded along with the regular stream; the second stream resolution is determined by the **Resolution for Smart Streaming** setting.
- By default , the **Resolution for Smart Streaming** is auto-populated using the Camera manufacturer's setting. The user can change this.
- **Smart Streaming** and **Alternate Stream** settings are mutually exclusive.

Note
Setting the **Smart Streaming** value to **Yes** increases the storage space requirement.

Once the channel is configured for Smart Streaming, the feature will automatically take effect without further user interaction.

To enable Smart Streaming, open System Manager.

1. Select the name of the appliance and navigate to the Cameras folder.
2. Select the IP camera that will be using Resolution for Smart Streaming and scroll down to the IP Cameras section of the camera settings.

DRAFT

7.7 Camera-Specific Settings When Smart Streaming is set to YES

For Axis, Arecont, and Panasonic camera drivers:

IP Cameras	
Video Mode	Dual-stream (MJPEG + H.264)
Live Video Format	**H.264 Stream**
MPEG-4 / H264 Video Resolution	**Click here to edit. (Active Value is "640x480").**
MJPEG Video Resolution	**Click here to edit. (Active Value is "800x450").**
Video Frame Rate	**Click here to edit. (Active Value is "30").**
Smart Streaming	**Yes**
Resolution for Smart Streaming	640 x 360 (16:9)
Enable Alternate Stream	No
Alternate Stream Frame Rate	10
Alternate Stream Resolution	160 x 90 (16:9)
RTP Protocol	TCP

For Vivotek, Hikvision, and ONVIF camera drivers:

IP Cameras	
Analytic Stream	Stream 1
Stored Stream	Stream 2
Default Live Stream	Stream 1
Alternate Live Stream	Stream 3
Stream 1 Encoding	MJPEG
Stream 1 Transport Protocol	RTSP
Stream 1 Frame Rate	Click here to edit. (Active Value is "10").
Stream 1 Resolution	Click here to edit. (Active Value is "640x360").
Stream 1 Quality	4
Stream 2 Encoding	H.264
Stream 2 Transport Protocol	RTSP
Stream 2 Frame Rate	Click here to edit. (Active Value is "5").
Stream 2 Resolution	Click here to edit. (Active Value is "640x360").
Stream 2 Quality	4
Stream 3 Encoding	MJPEG
Stream 3 Transport Protocol	RTSP
Stream 3 Frame Rate	Click here to edit. (Active Value is "5").
Stream 3 Resolution	Click here to edit. (Active Value is "640x360").
Stream 3 Quality	4
Smart Streaming	No
Enable Alternate Stream	No
Overlay Date and Time	No
Date and Time Overlay Compression	Low
Brightness	64
Contrast	128

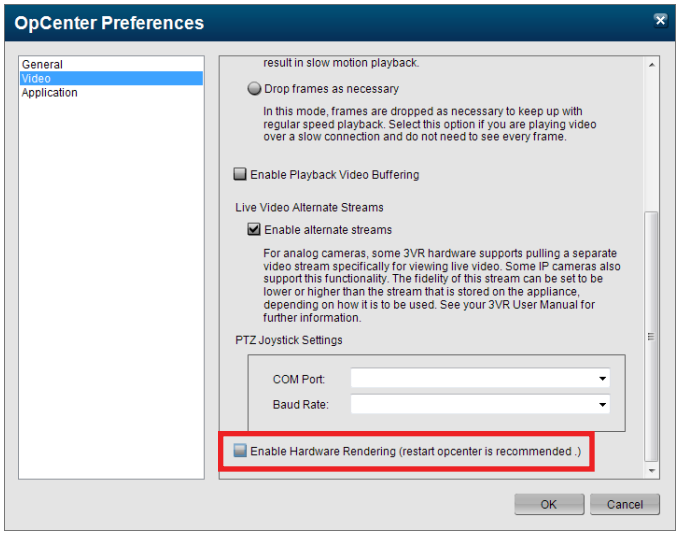
DRA

7.8 Hardware Rendering

To take advantage of the modern graphics video cards, OpCenter implemented hardware decoding. This feature is enabled by default.

To disable hardware rendering, perform the following steps:

1. Open OpCenter.
2. Select **Options.** The OpCenter Preferences window opens.
3. Choose the **Video** option on the left-hand side of the window. The **Hardware Rendering** setting appears at the bottom of the Video section.
4. **Uncheck this option to disable** hardware rendering and click **OK** to save.



8. USING THE GENERIC IP CAMERA DRIVER

You might be able to access IP camera models that do not have a camera-specific driver available in System Manager using the generic IP camera driver.

In addition, switching to the generic driver may also be a useful step for troubleshooting a camera that fails to load with a model-specific driver.

8.1 Identifying the URL Path

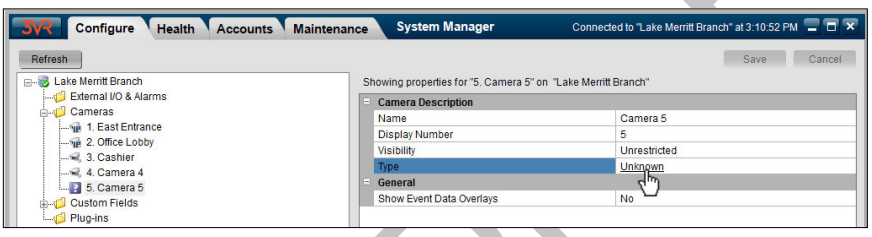
In order to connect to an IP camera using the generic driver, you need to know the protocol (HTTP or RTSP) and the video mode (MJPEG, MPEG-4, or H.264) of the URL used to access the camera's video stream over the network. This information is usually found in the camera's documentation. To see the URL paths for some common IP camera manufacturers, go to: http://www.3vr.com/resources/supportedcameras

8.2 Configuring a Generic IP Camera

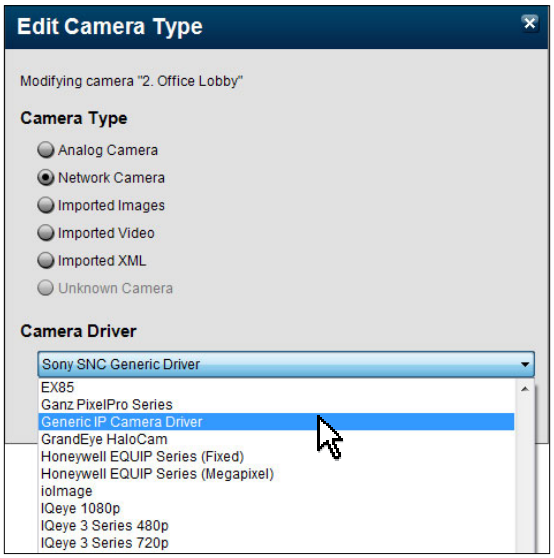
Perform the following steps to configure a camera to use the generic IP camera driver:

1. In the **Configure** panel, click the plus sign (+) next to the system display name.
2. Click the plus sign next to **Cameras** to display the list of cameras on the unit.
3. Select the camera designated for the generic IP camera.

4. On the right-hand side of System Manager, click the link next to **Type** (the link text will be the current camera type, e.g. Analog, Network, or Unknown).



5. In the **Edit Camera Type** dialog box, click **Network Camera**.
6. Choose **Generic IP Camera Driver** from the **Camera Driver** drop-down menu.
7. Click **Save** to save changes and return to the **Configure** panel.



DRAFT

8. Click the field to the right of **Network Camera: Network Address** and type the camera's IP address.

9. Type the camera's user name and password, if applicable.

10. Click **Save**.

11. Scroll down through the camera settings to the **IP Cameras** category.

Camera Description	
Name	Office Lobby
Display Number	2
Visibility	Unrestricted
Type	Network Camera (Generic IP Camera Driver)
Network Camera: Network Address	10.100.3.75
Network Camera: User Name	
Network Camera: Password	

12. Type the URL path for the camera stream in the appropriate box for the type and video mode of the stream:

    - **HTTP URL Path (MJPEG)**
    - **HTTP URL Path (MPEG-4 or H.264)**
    - **RTSP URL Path (MJPEG)**
    - **RTSP URL Path (MPEG-4 or H.264)**

HTTP URL Path (MJPEG)	/axis-media/media.amp?videocodec=mjpeg
RTSP URL Path (MPEG-4 or H.264)	
RTSP URL Path (MJPEG)	
Video Frame Rate	Click here to edit. (Active Value is "10").
HTTP URL Path (MPEG-4 or H.264)	

    You should only enter the portion of the URL that comes after the IP address. For example, if the URL for the HTTP MJPEG stream is **http://10.93.42.3/video.mjpg**, you should enter **/video.mjpg** as the URL path.

13. Click **Save**.

9. IP CAMERA TROUBLESHOOTING

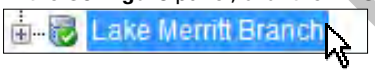
This section describes how to troubleshoot IP camera issues.

9.1 IP Camera Fails To Load

If one or more IP cameras fails to load properly, perform the following steps to troubleshoot the connection.

- Verify that the user name and password you entered for the camera is correct.
- Verify that the IP address entered for the **Network Camera: Network Address** setting in System Manager matches the IP address of the camera. Make sure you can access the camera with that IP address in a web browser.
- If the camera's network information is correct, make sure the 3VR appliance can ping the camera. To test this:

  1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

  2. Click Common Operations, and then click **Test Appliance Connectivity**.
  3. Click the **From Appliance** tab.
  4. Type the IP address of the camera in the **To** box.

DRAFT

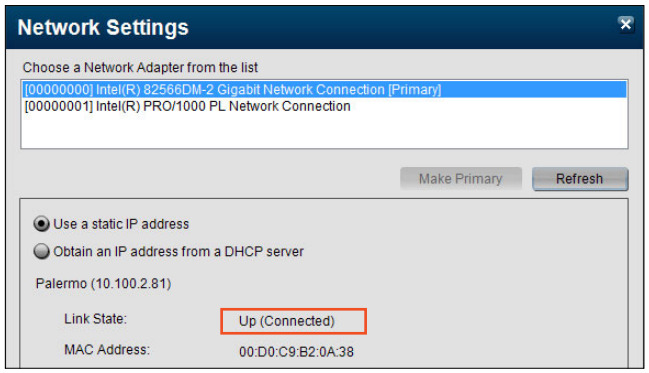
5. Click **Ping to Address**. A message appears indicating whether the ping was successful.

If the ping fails:

Ping failed. Check network address.

Close the **Test Appliance Connectivity** dialog box and check the 3VR appliance's network settings (click Common Operations, and then click **Network Settings**):

- If the IP cameras are on the LAN, verify that the link state of the **primary** network card is **Up (Connected)** and the network settings are correct.
- If the IP cameras are physically connected to the appliance, verify that the link state of the **secondary** network card is **Up (Connected)** and the IP address of the card and the camera(s) are on the same subnet.



If the ping succeeds:

Ping Succeeded:

- Make sure that the **Network Camera: Port** information is correct. If left blank, the port defaults to port 80. If an incorrect value is entered, the 3VR appliance will be able to ping the camera but not access its video feed.

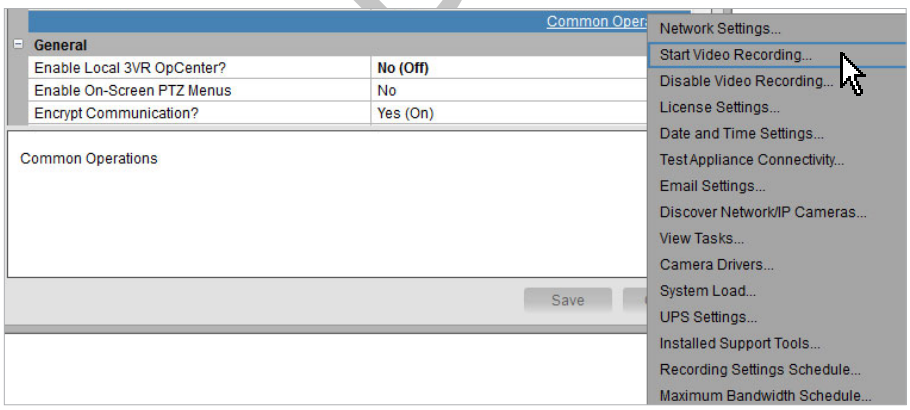
Network Camera: Network Address	10.100.3.40
Network Camera: User Name	
Network Camera: Password	
Network Camera: Network Port	
Network Camera: Video Server Port	

If the camera connection test succeeds, but there is still no video

- Verify that video recording has not been stopped or disabled. To check this, click the name of the 3VR appliance to display its settings. On the right-hand side of System Manager, under the **Appliance** heading, make sure that the **Current Recording Status** field shows **Running**.

Appliance	
Display Name	Lake Merritt Branch
Network Address	10.100.2.202
Current Recording Status	Running
Hardware	SRS-430-0500 (BMS08200903052)

If it show **Disabled** or **Halted**, click Common Operations, and then click **Enable Video Recording** or **Start Video Recording**.

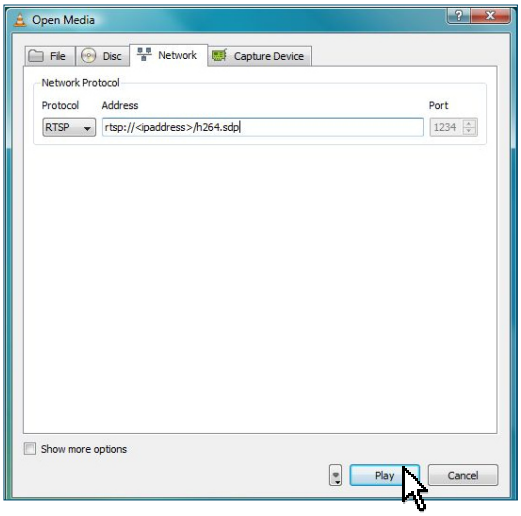


- If the IP camera is a video recorder, make sure that the **Network Camera: Video Server Port** value is entered. A video distributor accepts multiple video inputs (analog or IP), and then outputs that to a single network card.
- Clear the **Network Camera: Network Port** setting. In most cases, the **Network Camera: Network Port** setting should be left blank. An incorrect value entered here will prevent the appliance from connecting to the camera.

DRAFT

9.2 Generic IP Camera Driver Troubleshooting

If a camera configured with the generic IP camera driver produces no output, verify that this camera supports the generic driver by accessing its feed in VLC, a free media player.



1. Download VLC from www.videolan.org and install the application.
2. Launch VLC and select **Open Network Stream**. Select the **Protocol** (RSTP or HTTP) and enter the **Address** of the IP camera's network stream (this information should be listed in the camera documentation).
3. Click **Play**.
   - If video appears, the camera is compatible with the generic driver.
   - If video does not appear, the camera network stream URL is wrong or the camera does not support network streaming.

10. CONFIGURING IP CAMERA VIRTUAL REGIONS

Licensed Feature
Creating virtual regions on a hybrid 3VR appliance requires the purchase of an IP camera expansion pack to license each enabled IP camera. Contact your 3VR Sales representative for more information. This restriction does not apply to NVRs.

10.1 About Virtual Regions

"Virtual regions" are cropped sections of the field of view of an IP camera. Once defined on a camera, each virtual region appears and acts as if it were a separate camera.

Currently, you can configure virtual regions on Arecont, IQeye, Axis, and Vivotek cameras only, but support may be added for other cameras in the future. Check the Supported Cameras FAQ on www.3VR.com for an up-to-date list.

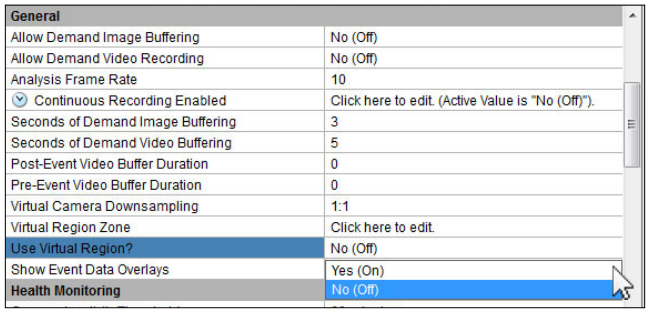
DRAFT

10.2 Configuring Virtual Regions

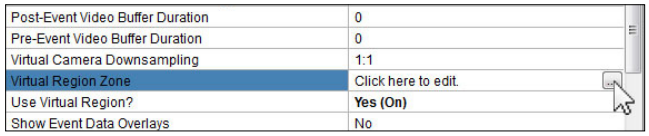
Perform the following steps to configure an IP camera using virtual regions:

1. Click the plus sign (+) next to name of the VMS server to expand the list of configuration options.
2. Click the plus sign next to **Cameras** to display all cameras on the system.
3. Select the camera to be configured with the first IP camera virtual region.

4. On the right side of System Manager, scroll down through the camera settings. Change the **User Virtual Region** setting to **Yes (On)**.
5. Click **Save**.
6. Click the ellipsis (...) button next to **Virtual Region Zone**.



General	
Allow Demand Image Buffering	No (Off)
Allow Demand Video Recording	No (Off)
Analysis Frame Rate	10
Continuous Recording Enabled	Click here to edit. (Active Value is "No (Off)").
Seconds of Demand Image Buffering	3
Seconds of Demand Video Buffering	5
Post-Event Video Buffer Duration	0
Pre-Event Video Buffer Duration	0
Virtual Camera Downsampling	1:1
Virtual Region Zone	Click here to edit.
Use Virtual Region?	No (Off)
Show Event Data Overlays	Yes (On)
Health Monitoring	No (Off)

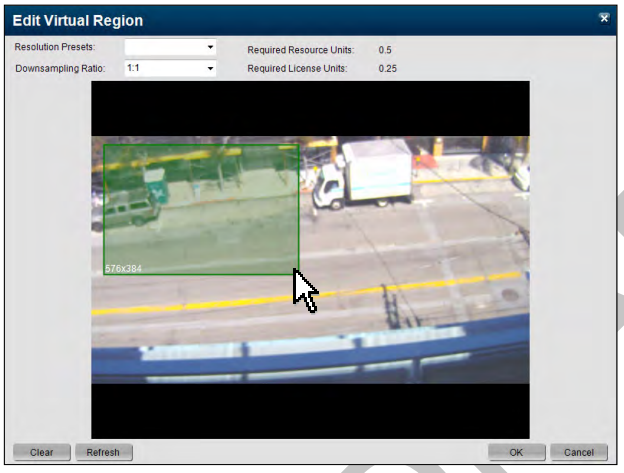


Post-Event Video Buffer Duration	0
Pre-Event Video Buffer Duration	0
Virtual Camera Downsampling	1:1
Virtual Region Zone	Click here to edit.
Use Virtual Region?	**Yes (On)**
Show Event Data Overlays	No

7. In the **Edit Virtual Region** dialog box, define the size and shape of the virtual region in one of the following ways:

- Select a preset resolution from the **Resolution** Presets menu.

- Click and drag the mouse to draw a custom region. When you are finished defining the region, click **OK**.

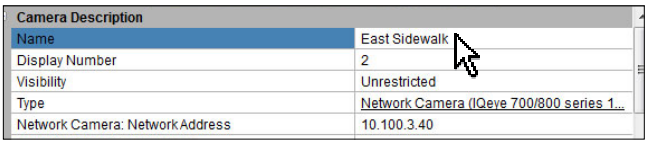


A dialog box appears warning you that creating a virtual region will affect any motion or face exclusion zones that have been configured.

8. Click **Yes** to proceed.

9. With the camera still selected, click the **Name** setting.

10. Edit the camera name to reflect the virtual region (for example, in the image to the right, we renamed the camera "East Sidewalk").



11. Click **Save** to store the new name.

12. To configure a second virtual region using the same camera, select another camera in the **Cameras** list.

DRAFT

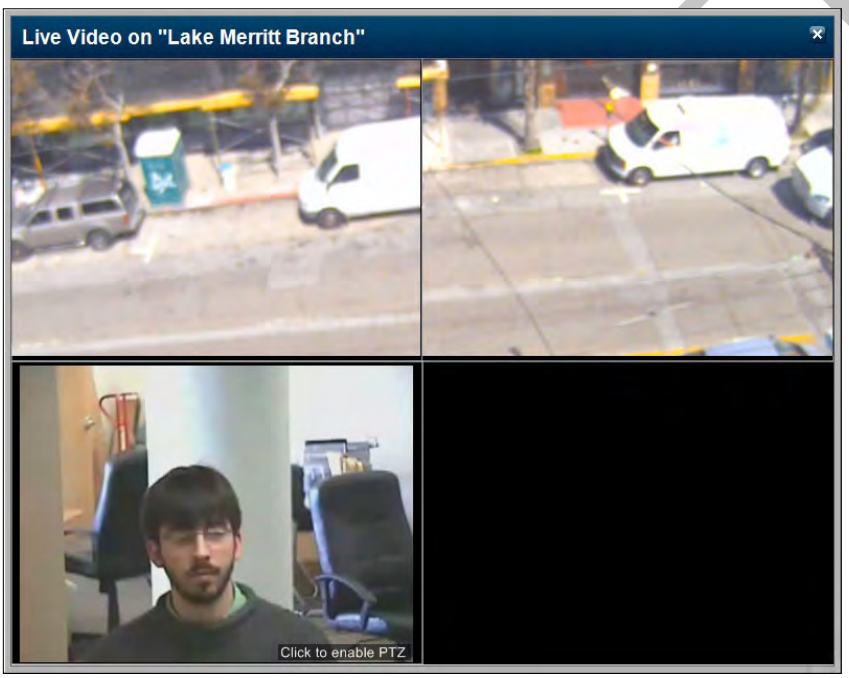
13. Configure the camera driver, IP address, and other settings to match the settings of the first camera.

14. Repeat steps 8-11 for the second camera.

    Note that any existing virtual regions will be shown in yellow and labeled with the camera name in the **Edit Virtual Region** window.

15. To view video on all cameras, including those that have a virtual region configured, right-click the name of the VMS server and select **Watch Video on "[VMS Server Name]"**.

16. When the live video panel loads, verify that the virtual regions appear as expected.



If one of the regions needs adjustment, return to the **Edit Virtual Region** window and click the **Clear** button to delete the region, and then re-draw it by clicking and dragging the mouse.

11. CONFIGURING MULTIPLE PIPELINE MANAGER

This section describes how to use the multiple pipeline manager, which you can use to help balance the load of multiple Network/IP Cameras on a 3VR appliance

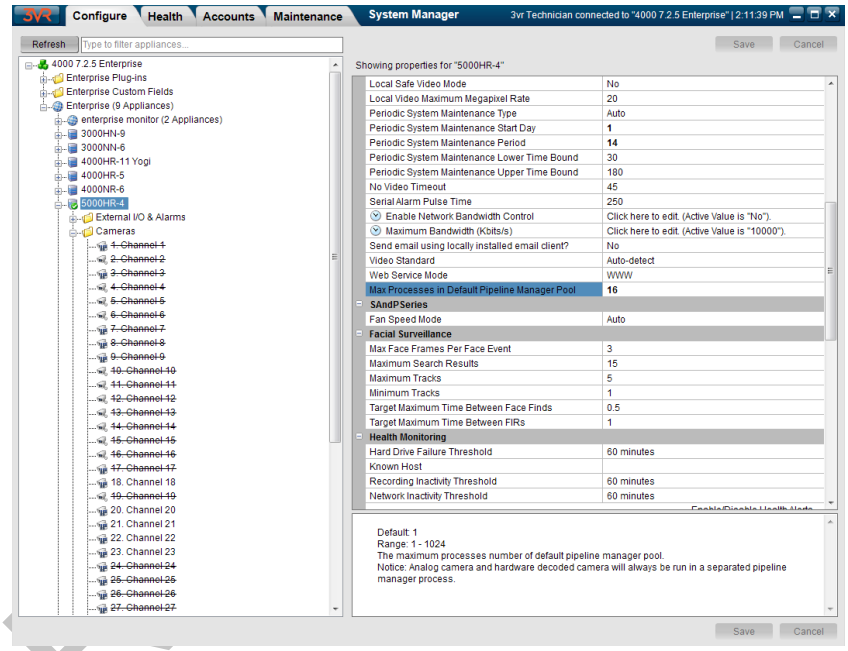
Configuring Multiple Pipeline Manager

Multiple Pipeline Manager allows video distribution across multiple processes within the VMS software. If you specify a value greater than one, OpCenter distributes the channels in a round-robin manner across the processes. You should configure Multiple-Pipeline Manager based on the CPU capacity and memory available on the VMS appliance.

Max Processes in Default Pipeline Manager Pool

This setting controls how many different Pipeline Manager Processes are being used to handle the video from network/IP cameras. The default setting is 1; the allowed values are 1-64.

To find this setting in System Manager, select the name of the 3VR appliance. It is the last setting in the **General** section.

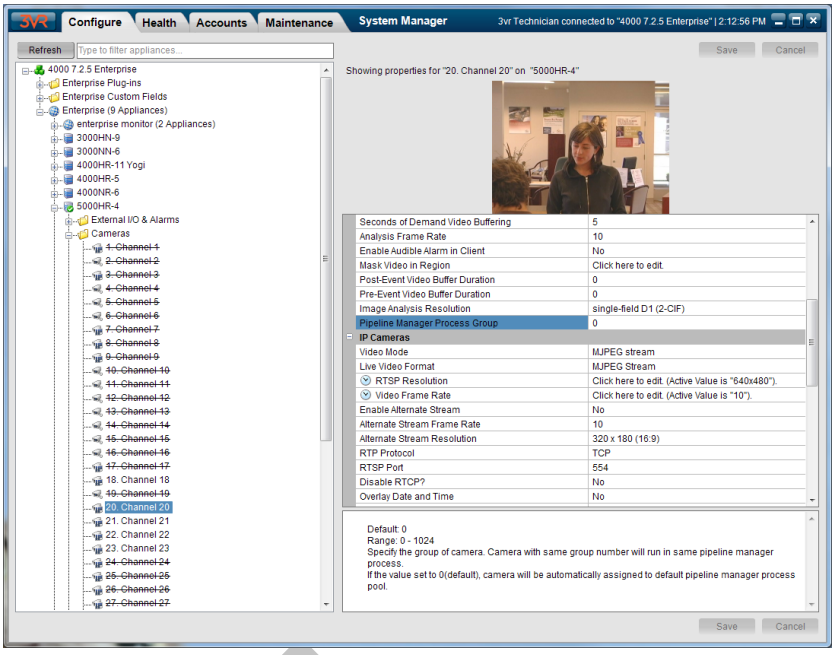


DRAFT

Pipeline Manager Process Group

You can use this setting to place any number of cameras into a group. All cameras within the group will be handled by the same Pipeline Manager Process. This feature lets you assign a specific process to a channel to ensure that the channel is able to use the process memory needed for smooth display. This allows for further control of network/IP cameras in order to balance the processing load. The default settings is 0.

This is the last setting in the **General** section. Select the channel/camera you wish to associate with a group.



DRAFT

DRAFT

CHAPTER 9
Configuration With Templates

1. TEMPLATES OVERVIEW 191
   - 1.1 About Templates 191
   - 1.2 Templatable System Settings 191
   - 1.3 Templatable Camera Settings 192
2. CREATING TEMPLATES 195
   - 2.1 Defining a New Template 195
3. APPLYING A TEMPLATE TO A VMS SERVER 197
   - 3.1 Applying a Template from a File 197
   - 3.2 Applying a Template Saved on the Enterprise 199
   - 3.3 Renaming a Template 202
4. MANAGING TEMPLATES ON THE ENTERPRISE 203
   - 4.1 Deleting a Template 203
   - 4.2 Exporting a Template 204
   - 4.3 Importing a Template 205

DRAFT

DRAFT

1. TEMPLATES OVERVIEW

You can store a VMS server's system and camera configuration as a template and then apply the template to other VMS servers, significantly reducing on-site programming time and risk of error.

1.1 About Templates

When you apply a template to a VMS server, all fields listed below are overwritten with the value stored in the template. If the setting is not customized in the template, the default values listed below are applied.

1.2 Templatable System Settings

This describes the system settings you can save in a template.

General Settings

	Setting	Default Value
General	Enable Local 3VR OpCenter?	Yes (On)
	Enable On-Screen PTZ Menus	No
	Encrypt Communication?	Yes (On)
	Encryption Key Exchange Interval	60
	Local Video Maximum Pixel Rate	0
	No Video Time-out	45
	Serial Alarm Pulse Time	250
	Enable Network Bandwidth Control	No
	Maximum Bandwidth (Kbits/s)	10240
	Send email using locally installed email client?	No
	Video Standard	Auto-detect
	Web Service Mode	WWW
Email Settings	3VR Appliance Email Address	<blank>
	Email Server Network Address	mail.yourcompany.com
	Email Server Requires Authorization	No
	Email User Name	<blank>
	Email Password	<blank>
Health Monitoring	Hard Drive Failure Threshold	60 min.
	Known Host	<blank>
	Network Inactivity Threshold	60 min.
	Recording Inactivity Threshold	30 min.
Facial Surveillance	Maximum Face Frames per Face Event	3
	Maximum Search Results	15
	Maximum Tracks	5
	Minimum Tracks	1
	Target Maximum Time Between Face Finds	.5
	Target Maximum Time Between FIRs	1

DRAFT

Smart Storage	Default Storage Time for Custom Event Types	90
	Default Video Export Extension	.mp4
	Minimum Days Of Video	7
	Normalize Sample Aspect Ratio for Exported Video	No (Off)
	Special Reduced Storage Cameras	<blank>
	Special Reduced Storage Duration	3

Event Trimming Schedule

	Motion Event Storage	90
	Face Event Storage	90
	Imported Image Event Storage	90

External I/O & Alarms

	Active?	No
	Name	Connection/Alarm Input #
	Camera	None
	Normally Open?	No

Peak/Off-Peak Hours

	Recording Settings Schedule	All hours peak
	Maximum Bandwidth Schedule	All hours peak

Time (NTP) Settings

	NTP Server Address	<blank>

Plug-in Settings

Settings vary depending on the installed plug-ins.

DRAFT

1.3 Templatable Camera Settings

Below are the camera settings you can save in a template.

Settings for All Camera Types

Motion	Maximum Length of Motion Events	60.0
	Motion Event Update Rate	3
	Motion Event Image Size	Thumbnail Size
	Motion Sensitivity	16
	Minimum Time Between Events	2
	Exclude Motion Smaller Than	4
	Exclude Motion Shorter Than	0.5

Health Monitoring	Camera Inactivity Threshold	60 minutes
	Transaction Event Inactivity Threshold	4

Facial Surveillance	Face Event Closure Time-out	6.0
	Maximum Eye Distance	90
	Minimum Eye Distance	32
	Video Frame Minimum Face Confidence	2
	Video Frame Maximum Eye Confidence	1.1
	Video Frame Minimum Eye Confidence	.6
	Minimum Subgroup Similarity	.71
	Minimum Time Between Face Finds When Not Tracking	.5

Analog Camera Settings

	Setting	Default Value
General	Channel Name*	Channel [Number]
	Visibility	Unrestricted
	Type	Based on source camera
	Allow Demand Image Buffering	No
	Allow Demand Video Recording	No
	Analysis Frame Rate	10
	Camera Brightness	128
	Camera Contrast	64
	Camera Hue	0
	Camera Saturation	64
	Camera Type	Analog
	Continuous Recording Enabled	No (Off)
	Continuous Recording Video Frame Rate	1
	Continuous Recording Video Quality	Very Low
	Seconds of Demand Image Buffering	3
	Seconds of Demand Video Buffering	5
	Post-Event Video Buffer Duration	0
	Pre-Event Video Buffer Duration	0
	H.264 Video Frame Rate	5
	H.264 Video Quality	Medium
	H.264 Video Resolution	CIF
PTZ Cameras	Camera Hardware Address	1
	Pan Speed Profile	Linear
	Serial Port Baud Rate	9600
	Serial Port COM Port	COM2
	Full Frame Motion Threshold	50
	Return to home preset after this many seconds	30

DRAFT

*Channel names are only templatable when applying a template to all cameras on a VMS server, not single cameras. See section 2.1 for more information about applying templates.

IP Camera Settings

IP camera settings vary depending on the model selected as the template camera. Listed below are some common IP camera settings and their default values.

	Setting	Default Value
General	Channel Name*	Channel [Number]
	Visibility	Unrestricted
	Type	Based on source camera
	Allow Demand Image Buffering	No
	Allow Demand Video Recording	No
	Analysis Frame Rate	10
	Continuous Recording Enabled	No (Off)
	Seconds of Demand Image Buffering	3
	Seconds of Demand Video Buffering	5
	Post-Event Video Buffer Duration	0
	Pre-Event Video Buffer Duration	0
IP Cameras	Enable Alternate Stream?	No (Off)
	Alternate Stream Frame Rate	10
	Alternate Stream Resolution	320 x 240
	MJPEG Compression	Low
	MJPEG Video Resolution	640 x 480
	Camera Rotation	No rotation
	RTSP Port	554
	Video Mode	MJPEG
	MJPEG Video Frame Rate	10

*Channel names are only templatable when applying a template to all cameras on a VMS server, not single cameras. See section 3 for more information about applying templates.

DRAFT

2. CREATING TEMPLATES

This section describes how to select the settings you want and save them in a template.

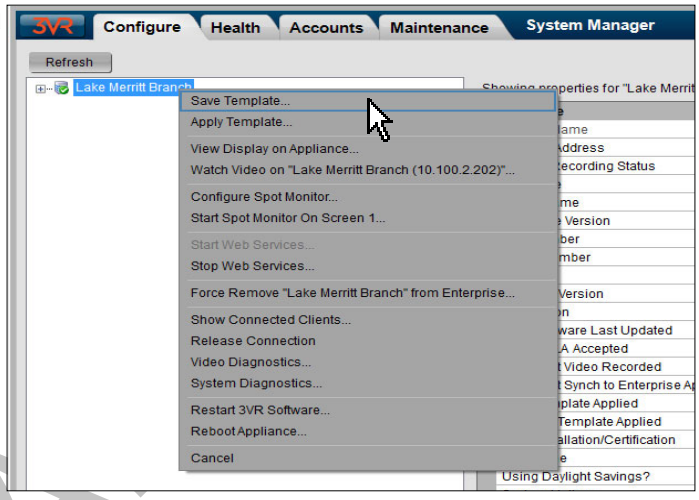
2.1 Defining a New Template

Perform the following steps to create a new template:

1. Modify the settings on a VMS server to the settings you'd like to save in a template and then apply to other VMS servers.

> **Reference**
> See chapters 1-8 for information on configuring the system and camera settings of a 3VR VMS server.

2. Right-click the VMS server name in the **Configure** panel and select **Save Template**.

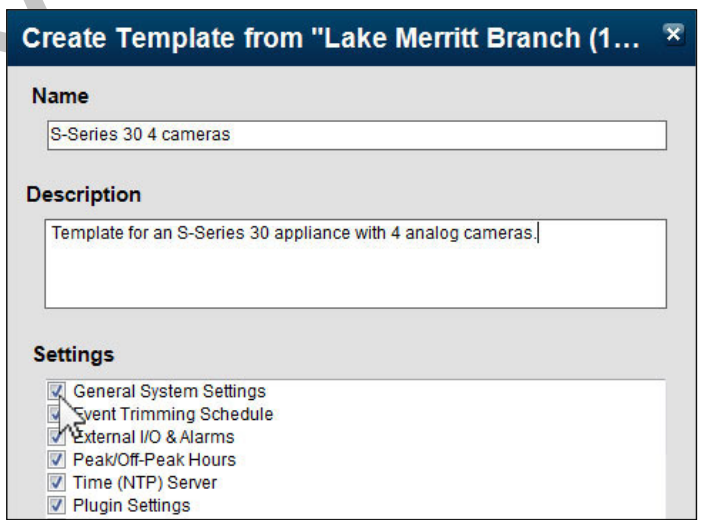


3. In the **Create Template** dialog box, type a name for the template in the **Name** box.

4. In the **Description** box, type a description that clearly communicates what the template is to be used for.

5. In the **Settings** panel, check the boxes next to the settings categories to include in the template (refer to section 1 of this chapter for a list of templatable settings arranged by category).

   - ☐ **General System Settings**
   - ☐ **Event Trimming Schedule**
   - ☐ **External I/O & Alarms**
   - ☐ **Peak/Off-Peak Hours**
   - ☐ **Time (NTP) Server**
   - ☐ **Plug-in Settings**

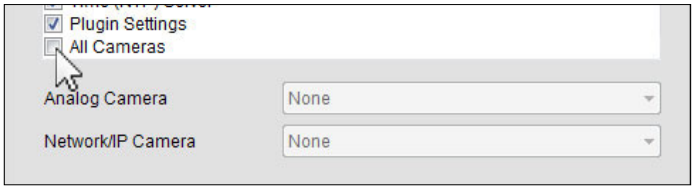


DRAFT

6. If you want the template to also configure camera settings, select one of the following options for camera configuration:

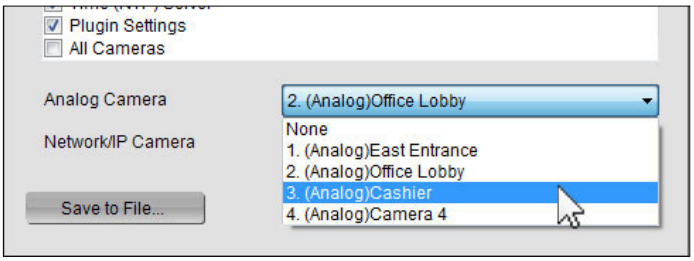
   - To configure **all** cameras on the destination VMS server to match **all** cameras on the source server:

     Check the box next to **All Cameras**.



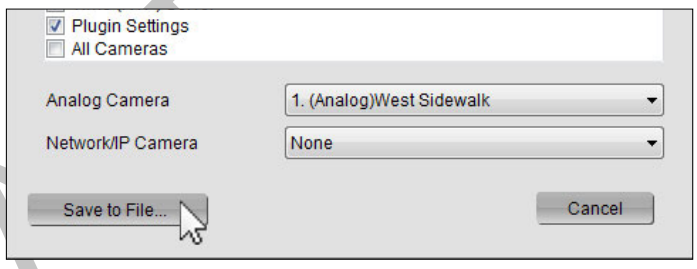
   - To configure **all** cameras on the destination server to match a **single camera** of that type on the source server:

     Select the camera to use as the model for all analog cameras and/or all network cameras from the **Analog Camera** and **Network/IP Camera** drop-down menus.



When you are finished selecting options for the template, save the template to a directory or drive:

7. Click **Save to File**.

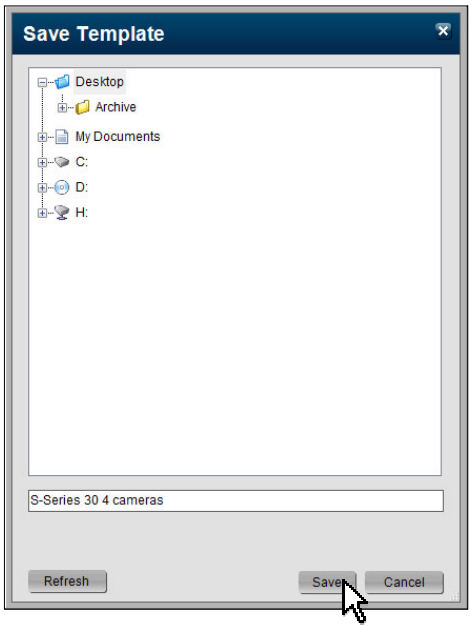


8. In the **Save Template** dialog box, select the location on your computer or an external drive where you wish to save the template file.

9. Edit the file name if desired.

10. Click **Save** to save the template file.

    The file is saved in the designated location with a .3cf extension (3VR Configuration File).

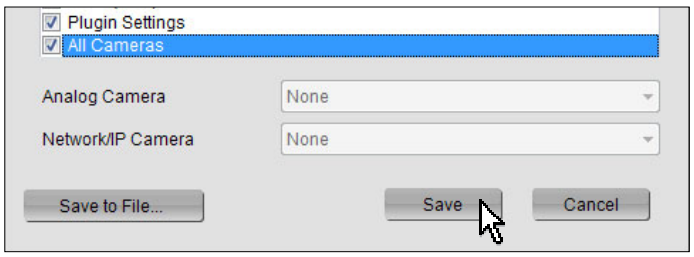


DRAFT

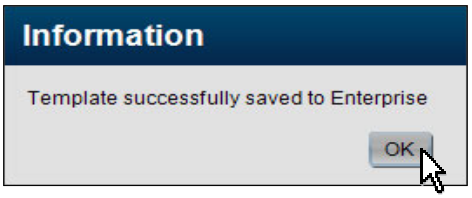
Saving to the Enterprise

To save the template file to the Enterprise Template Manager:

1. Click **Save**.



2. A pop-up dialog will appear to notify you that the template was saved successfully. Click **OK** to continue.



3. APPLYING A TEMPLATE TO A VMS SERVER

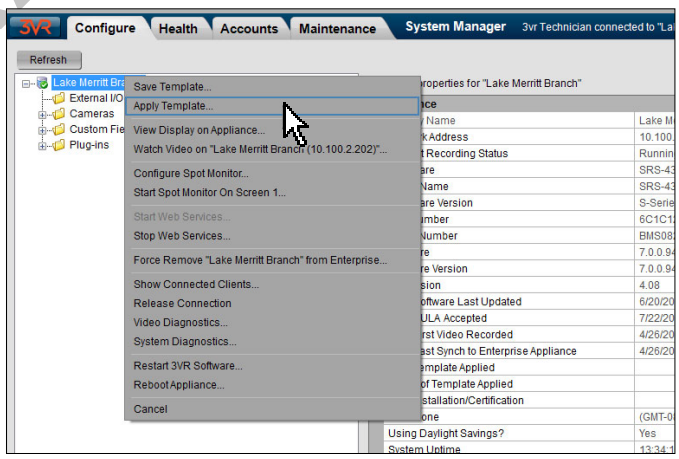
You can apply a template from a template file or a file saved on the Enterprise.

Warning
You should apply templates prior to adjusting system or camera settings. Any settings included in the template that have been previously configured will be overwritten. Applying a template cannot be undone.

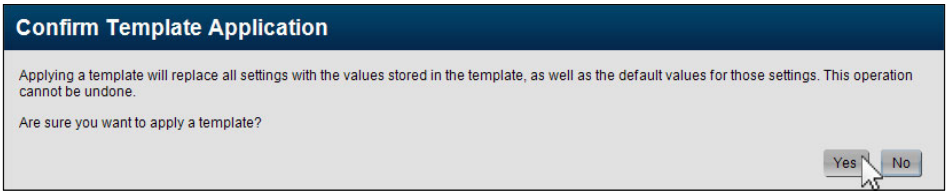
3.1 Applying a Template from a File

To configure a VMS server using a template file:

1. Launch System Manager.
2. In the **Configure** panel, right-click the VMS server name and select **Apply Template**.

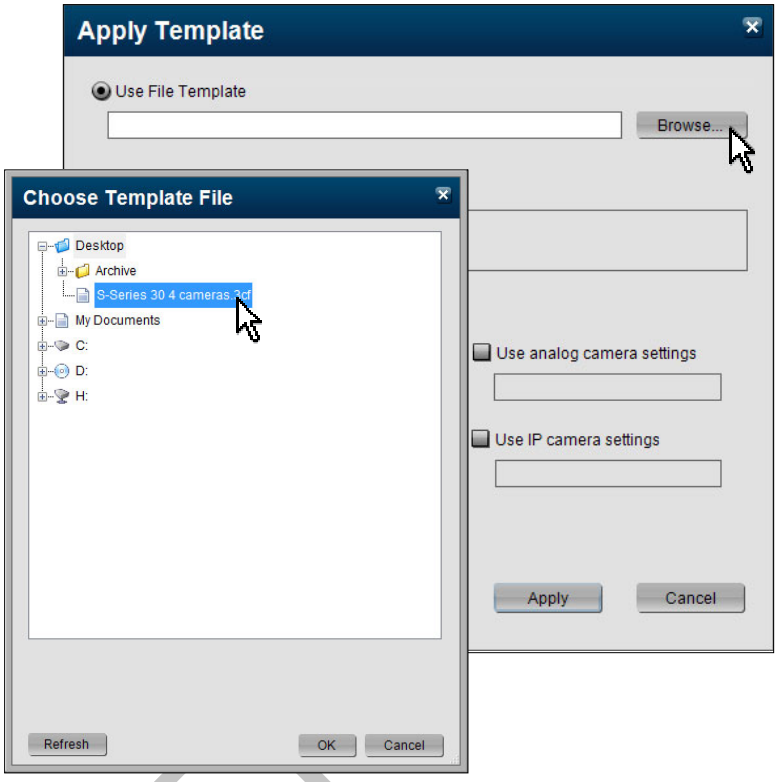


3. A pop-up dialog box appears, warning you that applying a template will replace all of the templatable settings on the system with the settings included in the template. Click **Yes** to proceed.



DRAFT

4. In the **Apply Template** dialog box, click **Browse**.



5. In the **Choose Template File** dialog box, browse to the location on your computer or an external drive where you saved the template file.

6. Select the file name, and then click **OK**.

7. The **Apply Template** dialog box updates based on the selected template file:

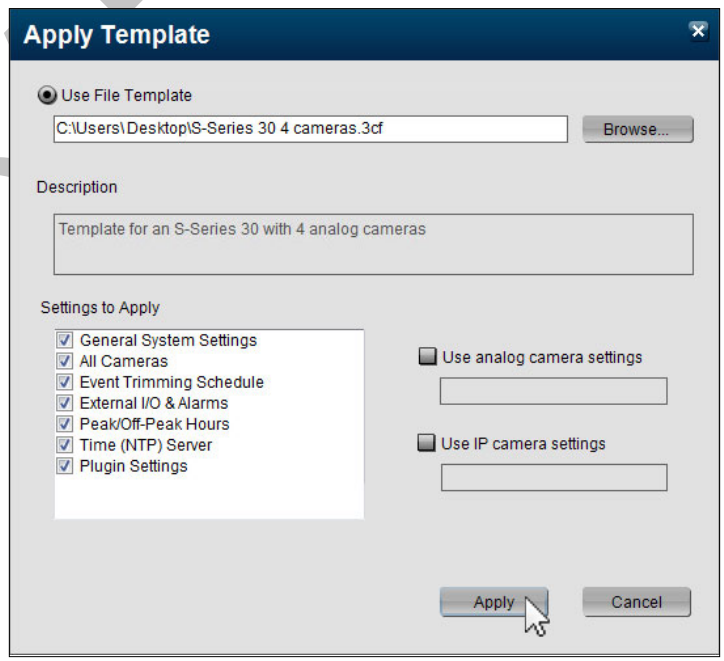
   - The **Description** box shows a description of the template (if you saved a description with the template definition).

   - The options under **Settings to Apply** update to show only settings categories that are included in the template.

8. By default, System Manager applies all of the settings included in the template to the VMS server.

   If you wish to apply only a subset of the settings, de-select the check boxes next to the settings categories that you don't want to apply.

9. Click **Apply** to apply the template.

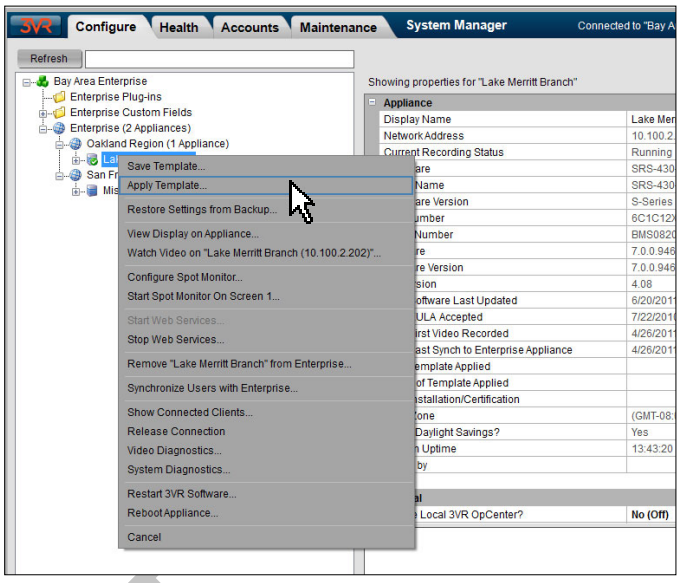


DRAFT

3.2 Applying a Template Saved on the Enterprise

To apply a template that has been saved on the Enterprise to a VMS server:

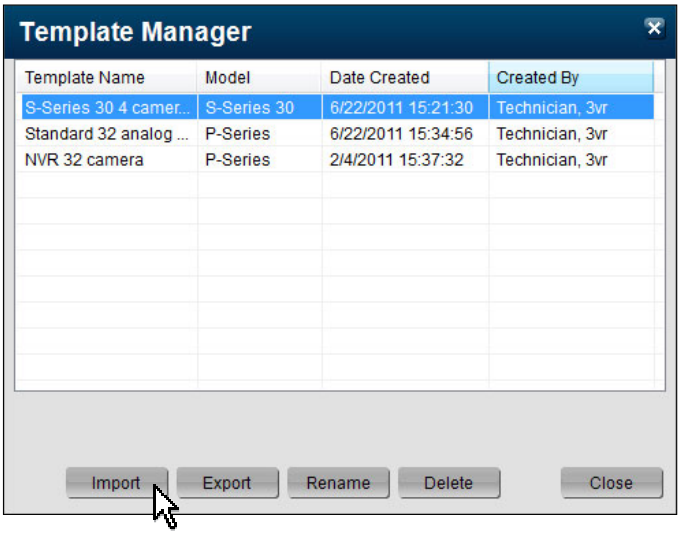
1. Right-click the VMS server name and select **Apply Template**.



2. A pop-up dialog appears and warns you that applying a template will replace all of the templatable settings on the system with the settings included in the template. Click **Yes** to proceed.

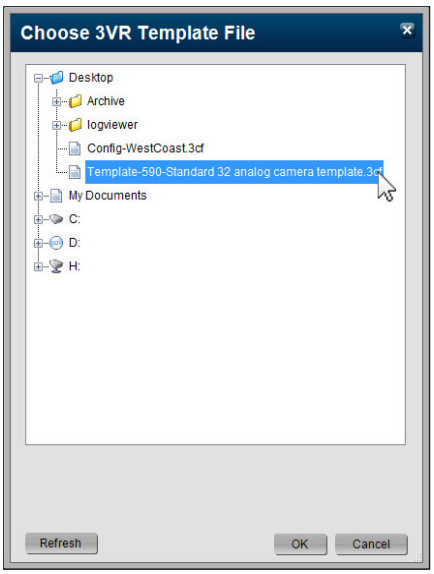
DRAFT

3. Click **Import**.



4. In the **Choose 3VR Template File** dialog box, navigate to the location on your computer or an external drive where you have saved the template file (file extension **.3cf**).

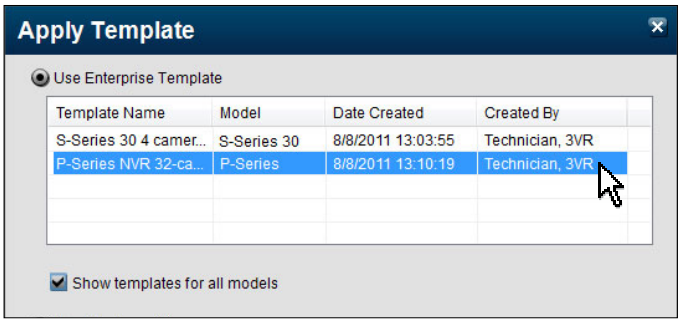
5. Select the file name, then click **OK**.



DRAFT

6. In the **Apply Template** dialog box, click **Use Enterprise Template**.

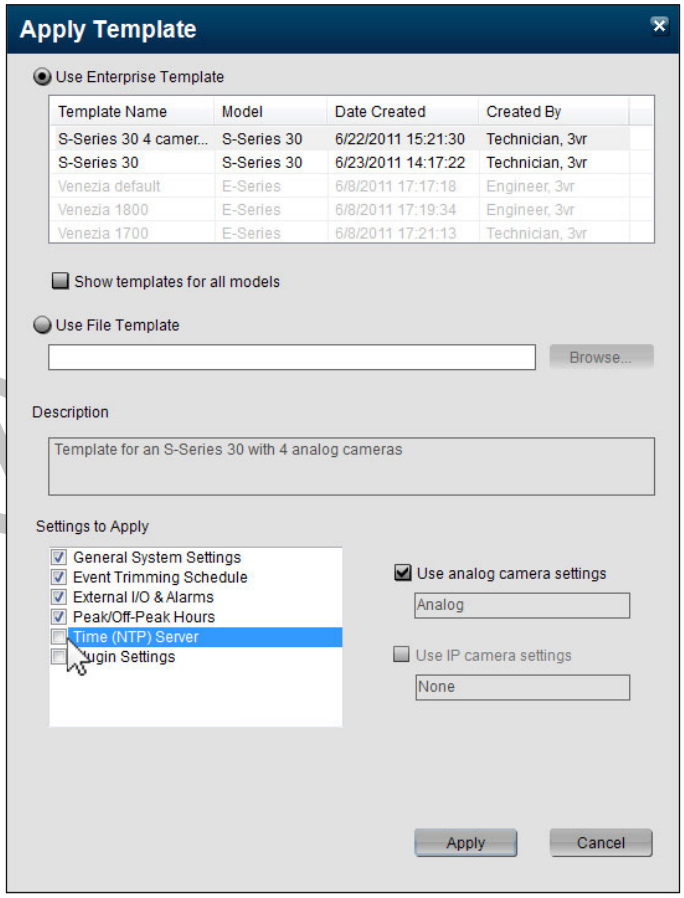
7. Select the template to apply from the list of templates.



> **Note**
> By default, the **Apply Template** dialog will only show templates matching the model of appliance. To see all templates that have been saved on the Enterprise, select **Show templates for all models**.

8. The **Apply Template** dialog box updates based on the selected template:

   - The **Description** box will show a description of the template (if one was saved with the template definition).
   - The options under **Settings to Apply** will update to only show settings categories that are included in the template.



9. By default, System Manager will apply all of the settings included in the template to the VMS server.

   If you wish to apply only a portion of the settings, deselect the check boxes next to the settings categories that should not be included.

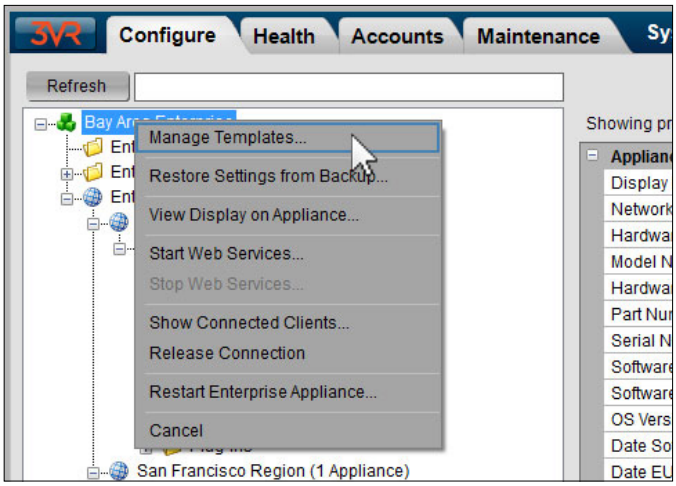
10. Click **Apply** to apply the template.

DRA

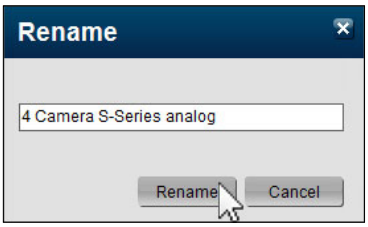
3.3 Renaming a Template

To rename an existing template:

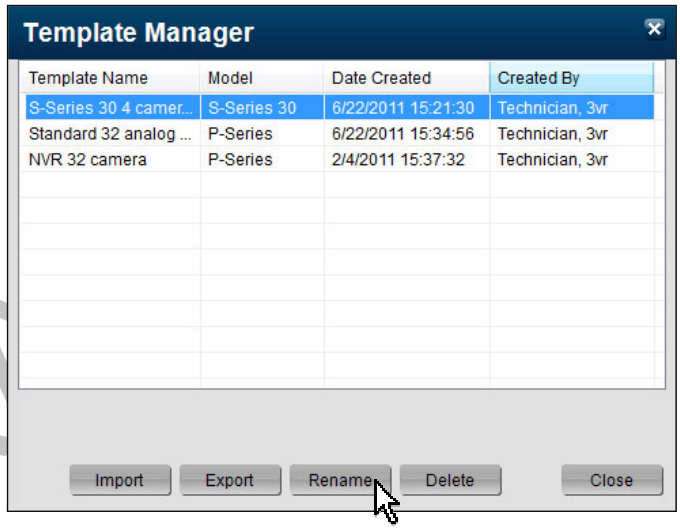
1. Right-click the Enterprise server name and select **Manage Templates**.



2. Select the name of the template to be renamed.
3. Click **Rename**.
4. Enter a new name for the template.



5. Click the **Rename** button to save the new name.



DRA

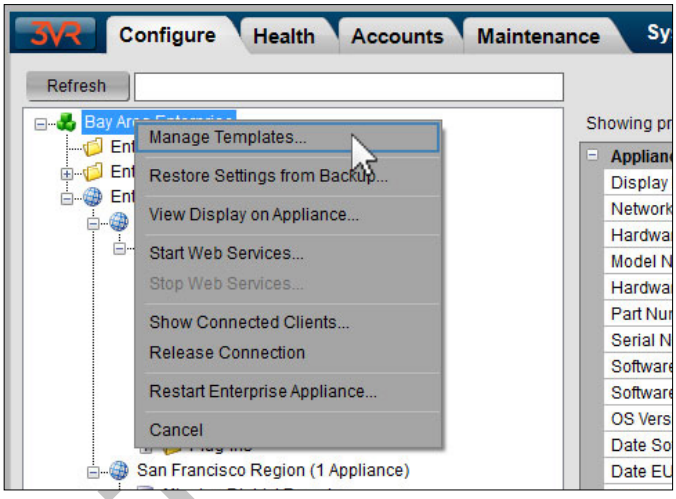
4. MANAGING TEMPLATES ON THE ENTERPRISE

This section describes how to manage templates on an Enterprise server.

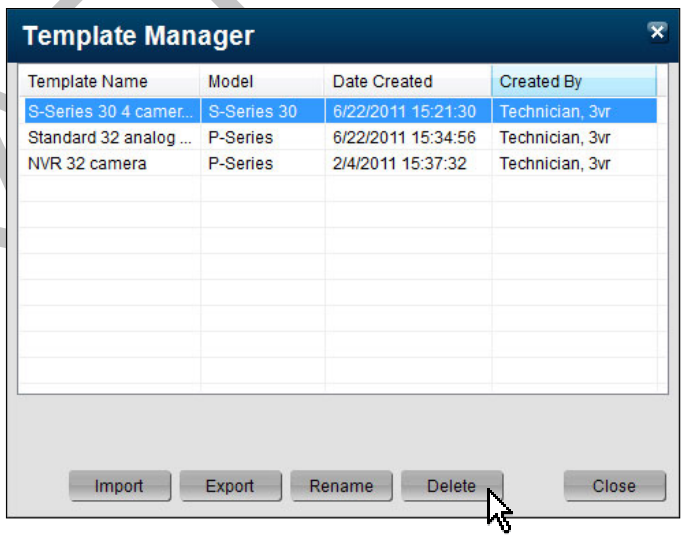
4.1 Deleting a Template

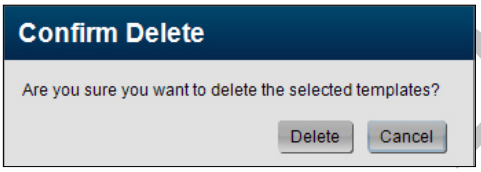
To delete a template that is no longer needed:

1. Right-click the Enterprise server name and select **Manage Templates**.



2. Select the name of the template to be removed.
3. Click **Delete**.
4. In the pop-up dialog that appears, click **Delete** to confirm that the template should be permanently deleted from the Enterprise.

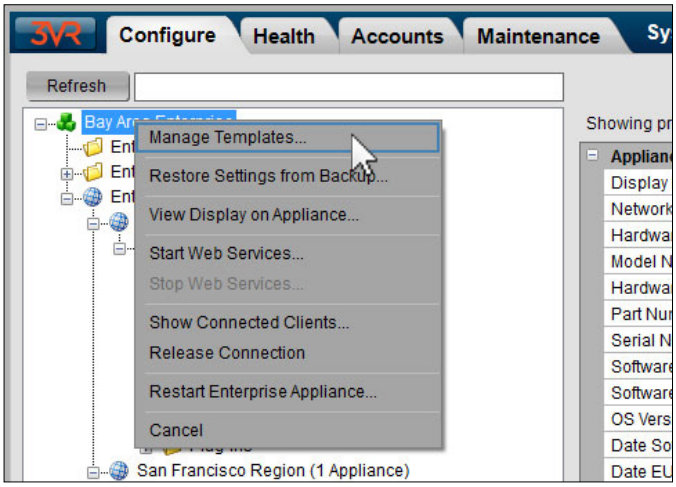




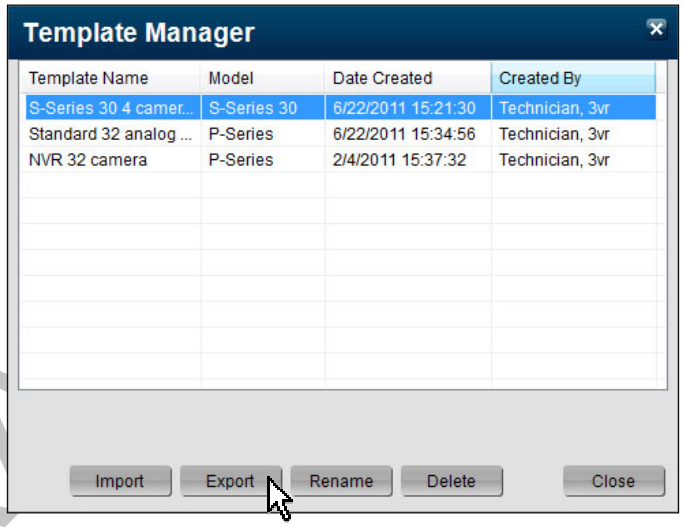
4.2 Exporting a Template

To export a template as a backup or to use on a different Enterprise server:

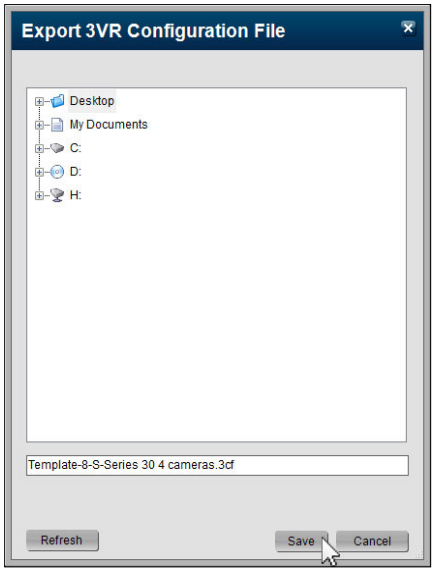
1. Right-click the Enterprise server name and select **Manage Templates**.



2. Select the name of the template to export.
3. Click **Export**.



4. In the **Export 3VR Configuration File** dialog, select the location on your computer or an external drive where you wish to save the template file.
5. If desired, edit the file name of the template.
6. Click **Save** to save the template.

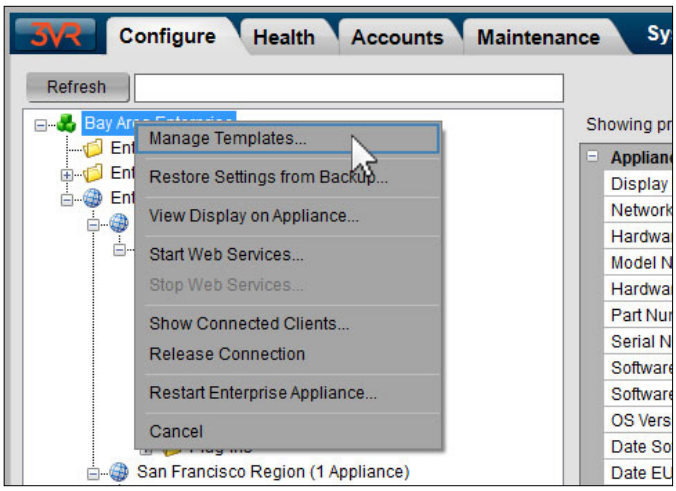


DRA

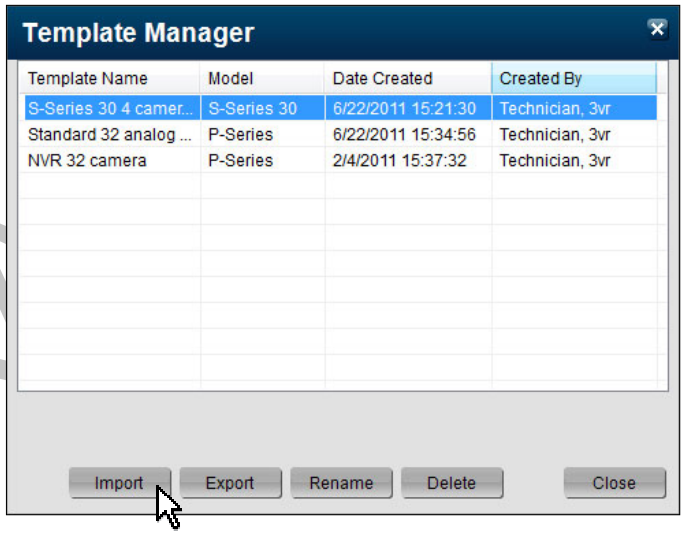
4.3 Importing a Template

Use the following steps to import a 3VR configuration file onto the Enterprise:

1. Right-click the Enterprise server name and select **Manage Templates**.

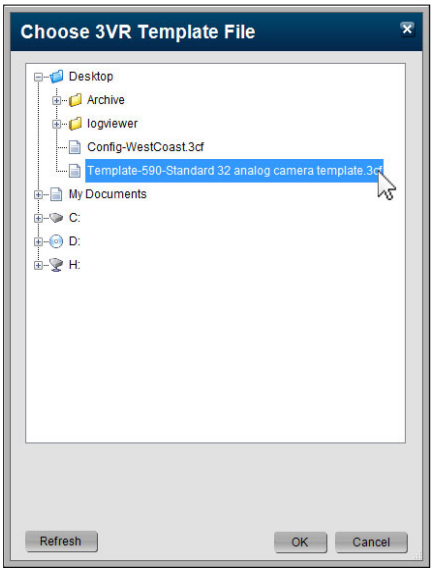


2. Click **Import**.



3. In the **Choose 3VR Template File** dialog, navigate to the location on your computer or an external drive where you have saved the template file (file extension **.3cf**).

4. Select the file name, then click **OK**.



DRAFT

CHAPTER 10
Audio Configuration

1. AUDIO OVERVIEW 209
2. CONNECT ANALOG AUDIO CABLES (IF APPLICABLE) 209
   - 2.1 1000-Series 209
   - 2.2 3000-Series 209
   - 2.3 4000-Series 210
   - 2.4 5500-Series 210
3. ENABLE AUDIO RECORDING (IF APPLICABLE) 210
4. CONFIGURE AUDIO CAMERAS 211
5. AUDIO SETTINGS REFERENCE 212

DRAFT

DRAFT

1. AUDIO OVERVIEW

3VR added support for audio in the 7.1 software release; 3VR supports both analog and IP audio sources. Please refer to the following chart for detailed information about audio support for your model of 3VR appliance:

Model	Analog Audio Input	IP Audio Input
1000-Series Hybrid	YES	YES*
1000-Series NVR	NO	YES*
2000-Series NVR	NO	YES*
3000-Series Hybrid	YES	YES*
3000-Series NVR	NO	YES*
4000-Series Hybrid	YES	YES*
4000-Series NVR	NO	YES*
5500-Series Hybrid	YES	YES*
5500-Series NVR	NO	YES*
5500-Series Hybrid	YES	YES*
5500-Series NVR	NO	YES*

**Refer to www.3VR.com for a complete list of IP cameras supported by 3VR.*

2. CONNECT ANALOG AUDIO CABLES (IF APPLICABLE)

This section describes how to connect audio cables to 3VR appliances.

2.1 1000-Series

1000-Series appliances use combined audio/video dongles with both yellow video connectors and red audio connectors on the same dongle. To connect analog audio sources to a 1000-Series appliance, connect the audio inputs to the red BNC connectors on the audio/video connectors already installed on the appliance.

1. Connect audio inputs 1-16 to the red BNC connectors on the audio/video dongle connected to port A.

2.2 3000-Series

3000-Series appliances use combined audio/video dongles with both yellow video connectors and red audio connectors on the same dongle. To connect analog audio sources to a 3000-Series appliance, connect the audio inputs to the red BNC connectors on the audio/video connectors already installed on the appliance.

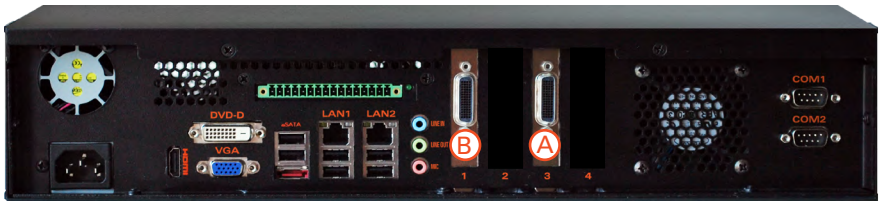
1. Connect audio inputs 1-16 to the red BNC connectors on the audio/video dongle connected to port A.

DRAFT

2.3 4000-Series

4000-Series appliances use combined audio/video dongles with both yellow video connectors and red audio connectors on the same dongle. To connect analog audio sources to a 4000-Series appliance, connect the audio inputs to the red BNC connectors on the audio/video connectors already installed on the appliance.

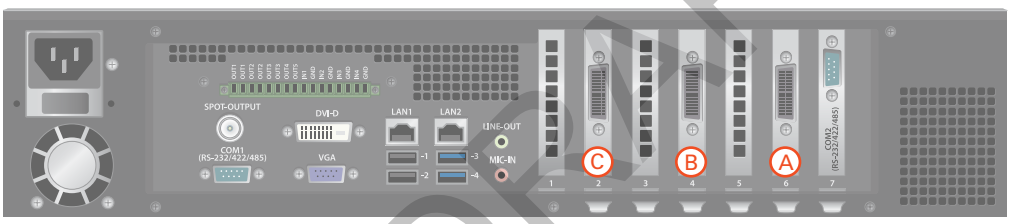
1. Connect audio inputs 1-16 to the red BNC connectors on the audio/video dongle connected to port A.
2. **32-camera units**: Connect audio inputs 17-32 to the red BNC connectors on the audio/video dongle connected to port B.



2.4 5500-Series

5500-Series appliances use combined audio/video dongles with both yellow video connectors and red audio connectors on the same dongle. To connect analog audio sources to a 5500-Series appliance, connect the audio inputs to the red BNC connectors on the audio/video connectors already installed on the appliance.

1. Connect audio inputs 1-16 to the red BNC connectors on the audio/video dongle connected to port A.
2. **32-camera units**: Connect audio inputs 17-32 to the red BNC connectors on the audio/video dongle connected to port B.
3. **48-camera units**: Connect audio inputs 33-48 to the red BNC connectors on the audio/video dongle connected to port C.



DRAFT

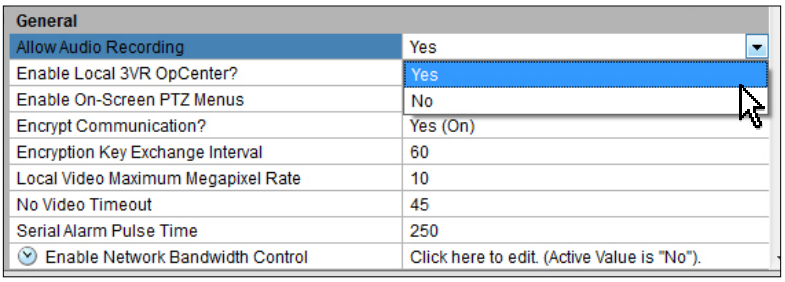
3. ENABLE AUDIO RECORDING (IF APPLICABLE)

In many locales it is prohibited by law to record audio without the consent of all recorded parties. Therefore, audio recording is disabled by default and cameras configured with audio will be set up for live streaming only.

If you wish to configure a channel to record audio, you must first change the **Allow Audio Recording** system setting to "Yes" to expressly enable audio recording.

1. In the **Configure** panel of System Manager, click the appliance name in the left-hand panel to view the system settings.

2. Under the **General** category heading, click **Allow Audio Recording** and select **Yes** from the drop-down menu.



3. Click **Save**.

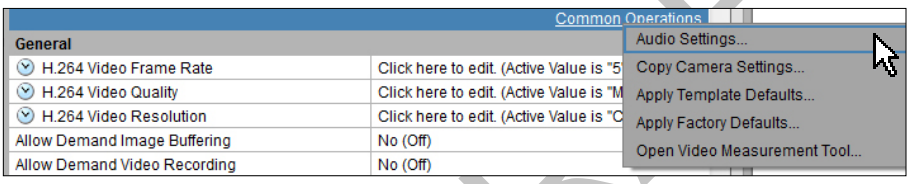
4. CONFIGURE AUDIO CAMERAS

When configuring audio, each audio source (microphone or line in) connected to the appliance must be linked to a video source (camera), so that VisionPoint™ VMS will know which audio source to stream when the user selects a camera in OpCenter.

Use the following steps to enable and configure audio on a camera:

1. In the **Configure** panel of System Manager, click the plus sign (+) next to the appliance name.
2. Click the plus sign next to **Cameras** to display the list of cameras on the appliance.
3. To view a camera's settings, click the camera name to highlight it.

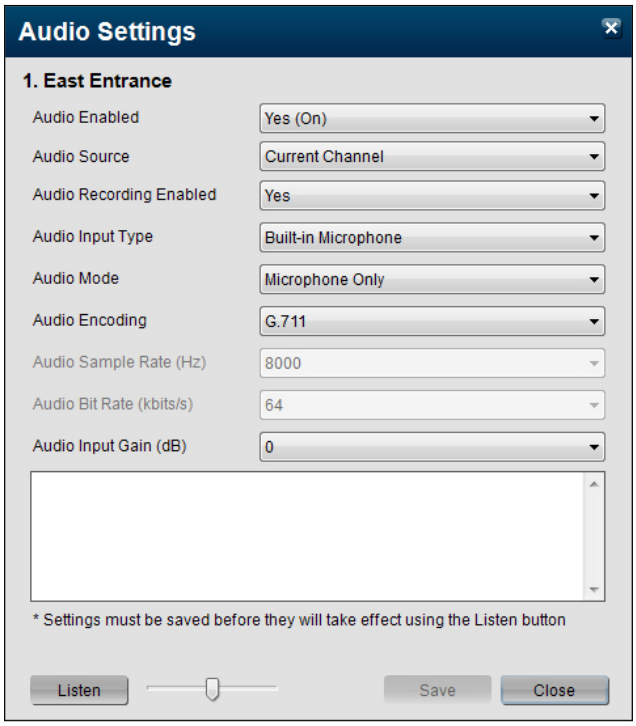
4. Click Common Operations, and then click **Audio Settings**.



5. In the **Audio Settings** dialog box, change the **Audio Enabled** setting to **Yes (On)**.
6. Specify the **Audio Source** for the camera:
   - If the selected camera has an audio source (e.g., the camera is an IP camera with audio or there is an analog audio input connected at this position), select **Current Channel**.
   - If the selected camera has audio, but you wish to link another audio source with this camera, select one of the other audio-enabled cameras from the **Audio Source** drop-down menu. The remaining settings will be grayed out and you may skip ahead to step 10.
   - If the selected camera does not support audio, choose one of the other audio-enabled cameras from the **Audio Source** drop-down menu. Skip ahead to step 10.
7. If you would like to record audio on this camera, change the **Audio Recording Enabled** setting to **Yes**.

> **Important**
> This setting may be overridden by the system-wide **Allow Audio Recording** setting (refer to section 3 of this chapter for details).

8. Select the audio input type (not all options will be available for all audio sources):



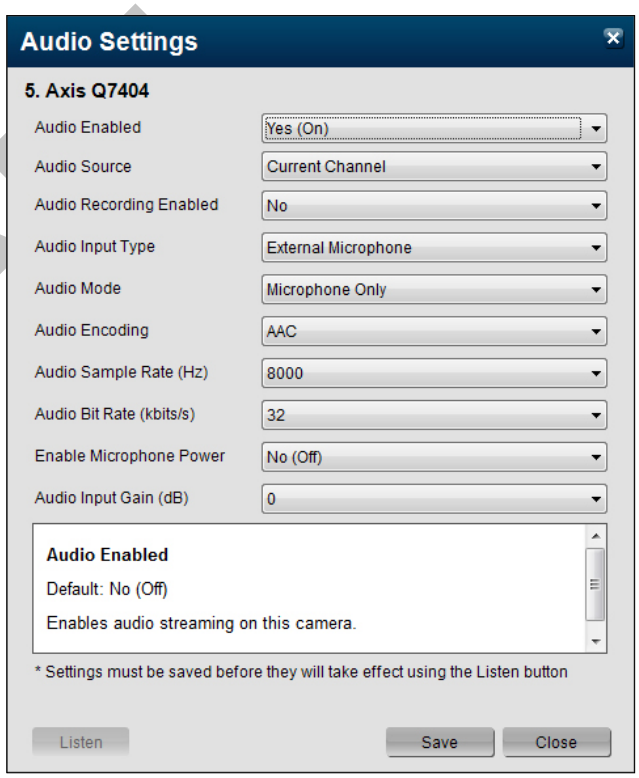
DRAFT

- **External Microphone** – an external microphone connected to the camera.
- **Internal Microphone** – a microphone built into the camera.
- **Line** – another external audio source.

9. If you set the **Audio Source** to **Current Channel** in step 6, configure the audio settings for the input as desired. Refer to the following section for information about the most common audio settings.
10. Click **Save** to save your changes.
11. Click **Listen** to listen to the audio stream and verify that audio quality is sufficient.
12. Click **Close** to close the dialog.
13. Repeat steps 3-11 for any remaining audio cameras.

5. AUDIO SETTINGS REFERENCE

The settings that appear in the **Audio Settings** dialog box vary depending on the driver of the selected camera. If the setting you would like to modify is not listed in this document, please refer to the help text displayed in the lower panel of the **Audio Settings** dialog box for more information about the setting.



Audio Mode

Leave this setting as **Microphone Only** for live streaming and recording.

Audio Encoding

Specify which audio encoding type to use (some audio sources will have only one option):

- **G.711** – Encoding scheme optimized for speech. Select this option if the audio source is placed in an area with little non-speech background noise.
- **AAC** – General purpose encoding scheme that supports a wide range of sampling and bit rates. Select this option if the audio source is recording in an area with background noise, such as music.

Audio Sample Rate (Hz) - AAC Only

Select the audio sample rate.

Audio Bit Rate (kbits/s) - AAC Only

Specify the audio bit rate. In general, larger values correspond to an increase in quality, but also increased bandwidth consumption and file size.

Enable Microphone Power

Specify whether or not microphone power is on. If your microphone is dynamic or battery powered, you should set this to off.

Audio Input Gain (dB)

Gain (in dB) for sound sent from the audio source.

DRAFT

CHAPTER 11
Spot Monitor

1. PHYSICAL SETUP 215
   - 1.1 1000-Series 215
   - 1.2 2000-Series 215
   - 1.3 2100-Series 215
   - 1.4 3000-Series 215
   - 1.5 4000-Series 216
   - 1.6 5500-Series 216
2. CONFIGURING SPOT MONITOR 216
   - 2.1 Configuring Spot Monitor from the Local Console 216
   - 2.2 Configuring Spot Monitor from System Manager 217
   - 2.3 Spot Monitor Display Settings 217
   - 2.4 Starting Spot Monitor 220
   - 2.5 Stopping Spot Monitor 221
3. DUAL SPOT MONITORS 222
   - 3.1 About Dual Spot Monitors 222
   - 3.2 Physical Setup 222
   - 3.3 Enabling Dual Spot Monitors 223
   - 3.4 Configuring Dual Spot Monitors from the Local Console 224
   - 3.5 Configuring Dual Spot Monitors from System Manager 225

DRAFT

DRAFT

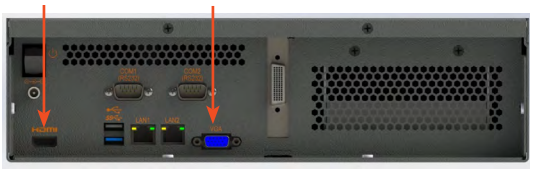
1. PHYSICAL SETUP

Important
3VR appliances require the BNC monitor used as a Spot Monitor to be terminated. If the monitor is not terminated, no output will appear on the Spot Monitor. If necessary, you can install a BNC T-connector with a 75 ohm BNC terminator on the open T-connection between the monitor and the 3VR appliance.

The procedure for setting up a Spot Monitor varies depending on the model of 3VR appliance and the type of Spot Monitor adapter you use for the installation. You may need an HDMI to CVBS Converter to extend video output to a monitor that uses BNC or RCA connectors. Please reference Appendix C for HDMI to CVBS for further information and installation instructions.

1.1 1000-Series

1. Connect the TV to the VGA or HDMI output port on the back of the appliance.



2. Reboot the appliance by pressing the power button on the front of the unit. Press the button once, do not press and hold. When the system has safely shut itself down, press the power button again.

1.2 2000-Series

1. Connect the TV to the HDMI output port on the back of the appliance.

2. Reboot the appliance by pressing the power button on the top of the unit. Press the button once, do not press and hold. When the system has safely shut itself down, press the power button again.

1.3 2100-Series

1. Connect the TV to the HDMI output port on the back of the appliance.
2. Reboot the appliance by pressing the power button on the front of the unit. Press the button once, do not press and hold. When the system has safely shut itself down, press the power button again.

1.4 3000-Series

1. Connect the TV to the VGA or HDMI output port on the back of the appliance.

2. Reboot the appliance by toggling the power switch on the back of the unit. When the system has safely shut itself down, toggle the power button again.

DRAFT

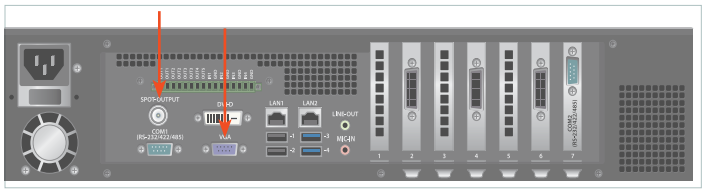
1.5 4000-Series

1. Connect the TV to the VGA, HDMI, or DVI-I output port on the back of the appliance.

2. Reboot the appliance by pressing the power button on the front of the unit. Press the button once, do not press and hold. When the system has safely shut itself down, press the power button again.

1.6 5500-Series

1. Connect the TV to the BNC or VGA output port on the back of the appliance.



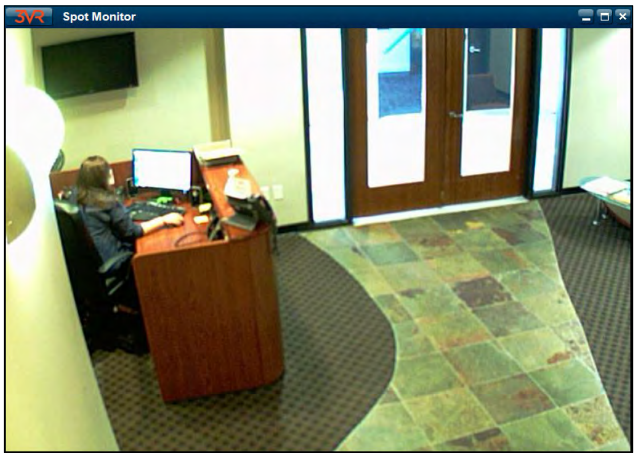
2. Reboot the appliance by pressing the power button on the front of the unit, behind the front cover. Press the button once, do not press and hold. When the system has safely shut itself down, press the power button again.

2. CONFIGURING SPOT MONITOR

This section describes how to configure Spot Monitor from a local console and from System Manager. It also describes how to configure Spot Monitor settings and turn Spot Monitor on and off.

2.1 Configuring Spot Monitor from the Local Console

Perform the following steps to configure Spot Monitor when connected to the appliance with a monitor, mouse, and keyboard:



1. At the sign-in screen, enter the user name **spotmonitor** and password **spotmonitor**.

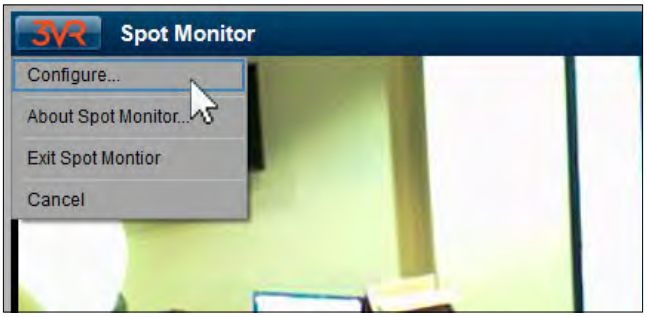
2. Click **Sign In**.

   The Spot Monitor application launches automatically. By default, Spot Monitor sequences through all enabled video cameras, displaying a new camera every five seconds.

DRAFT

3. To modify the cameras or sequence of the Spot Monitor display, move the mouse cursor to the top of the monitor. Click the **3VR** button in the top-left corner of Spot Monitor and select **Configure** from the menu.

4. Continue to section 2.3.



2.2 Configuring Spot Monitor from System Manager

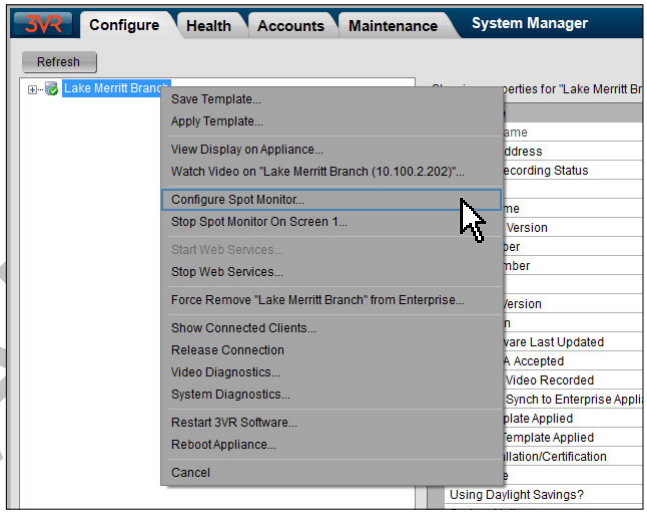
Perform the following steps to configure Spot Monitor from System Manager:

1. Launch 3VR System Manager.

2. At the sign-in screen, log in to the system with a user account with technician permissions (e.g. techrep or the customer-specific equivalent).

3. In the **Configure** panel of System Manager, right-click the appliance display name and select **Configure Spot Monitor**.

4. Continue to section 2.3.



DRA

2.3 Spot Monitor Display Settings

The settings in the **Spot Monitor Configuration** dialog box control the appearance and behavior of Spot Monitor. First, choose the view mode for Spot Monitor:

- To display live video from one camera at a time in a cycling display, select **Sequential View**.

- To display live video from multiple cameras at the same time, select **Multiplex View**.

Sequential View Settings

When Spot Monitor is configured with sequential view, cameras are displayed on the Spot Monitor one at a time, in ascending order by camera number, at full-screen resolution.

1. Click the camera number of each camera to include in the sequence.

2. Select the information that should be placed as an overlay on each camera:

> **Note**
> The maximum number of channels that you can view at one time in multiplex mode is 36. For systems with more than 36 channels of video, you can set up a second Spot Monitor using the remote application to allow users to view the remaining cameras

- **Display camera names**
- **Display date and time**

3. Use the slider bar under **Display interval for each camera (seconds)** to specify the number of seconds each camera should be shown on the screen.

4. To display alerts generated by VisionPoint™ VMS in Spot Monitor, check **Enable alert interrupts**.

   Enter the duration for alert interrupts into the **Alert interrupt duration** text box. When an alert is generated on the system, it will be displayed on the monitor in place of the live video feed for the specified length of time.

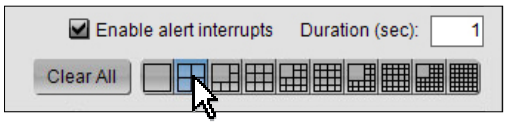
5. The Spot Monitor application restarts itself periodically to ensure the application continues to run smoothly for days and weeks at a time. By default, the restart occurs once every 24 hours, but you may set a different restart interval in the **Refresh Interval (hours)** box.

DRAFT

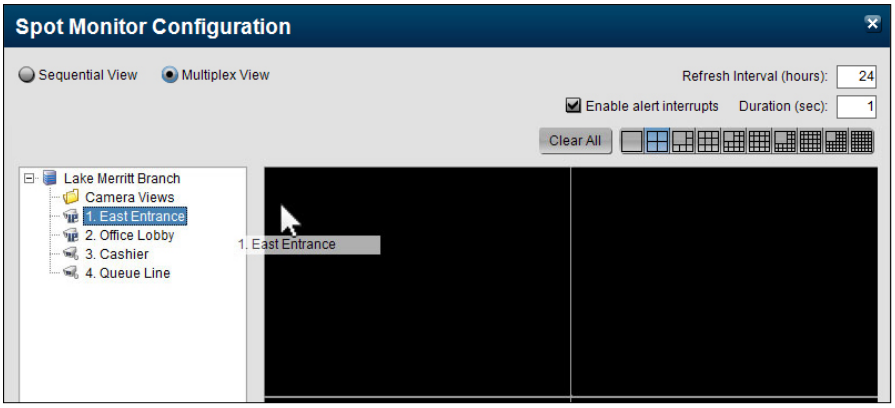
Multiplex View Settings

When you configure Spot Monitor with multiplex view, cameras are displayed on the Spot Monitor simultaneously in the number and arrangement of your choosing.

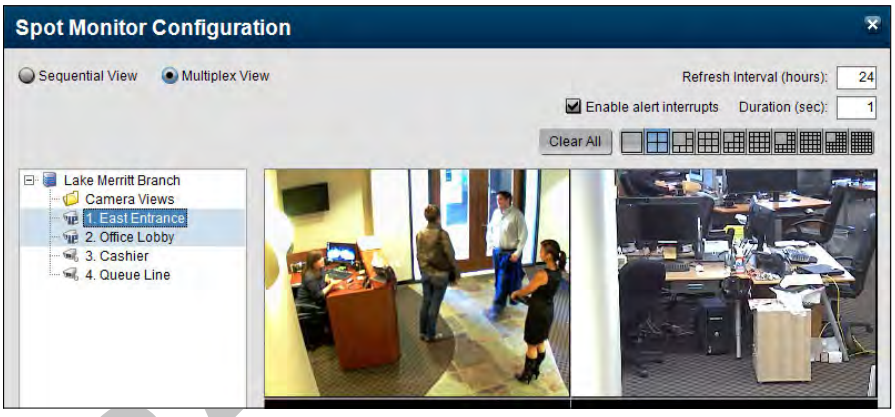
1. Select a layout for the Spot Monitor from the layout selector. Click a new layout button to increase or decrease the number and positioning of players as desired. You can display up to 36 cameras at once.



2. After you select a layout, click and drag a camera from the camera tree to each blank video player.



Live video from the selected cameras streams in each position in the video grid.



If you would like to display information about the camera on top of each video player, change the camera overlays by performing the following steps:

3. Right-click anywhere in the video grid.

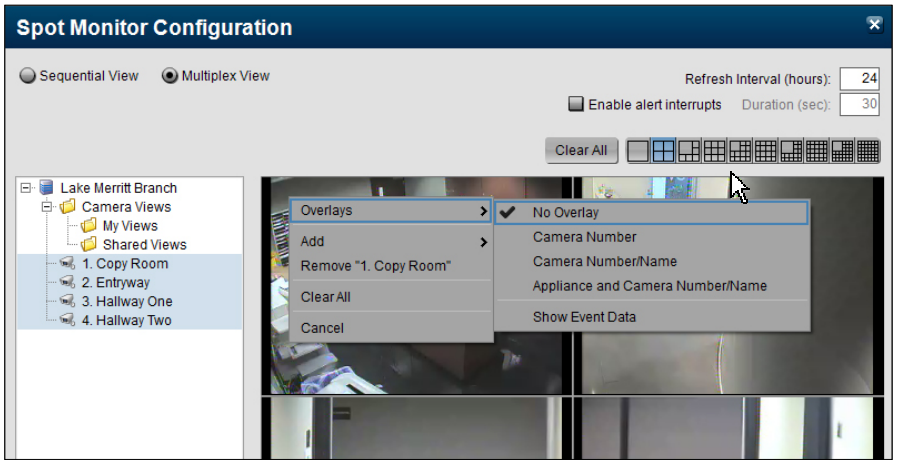
4. Select **Overlays >**, and then choose an overlay from the submenu. The current overlay options are:

- **No Overlay**
- **Camera Number**
- **Camera Number and Name**
- **Appliance and Camera Number/Name**
- **Show Event Data**

DRA

5. To display alerts generated by VisionPoint™ VMS in Spot Monitor, check **Enable alert interrupts**.

   Enter the duration for alert interrupts into the **Alert interrupt duration** text box. When an alert is generated on the system, it will be displayed on the monitor in place of the live video feed for the specified length of time.



6. The Spot Monitor application restarts itself periodically to ensure the application continues to run smoothly for days and weeks at a time. By default, the restart occurs once every 24 hours, but you may set a different restart interval in the **Refresh Interval (hours)** box.

DRAFT

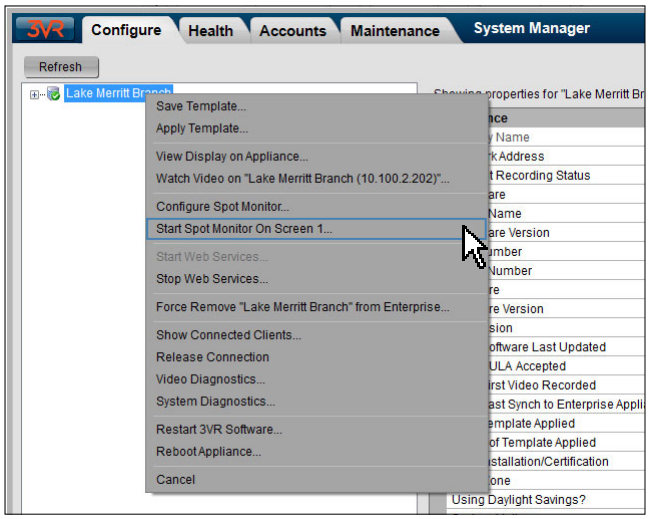
2.4 Starting Spot Monitor

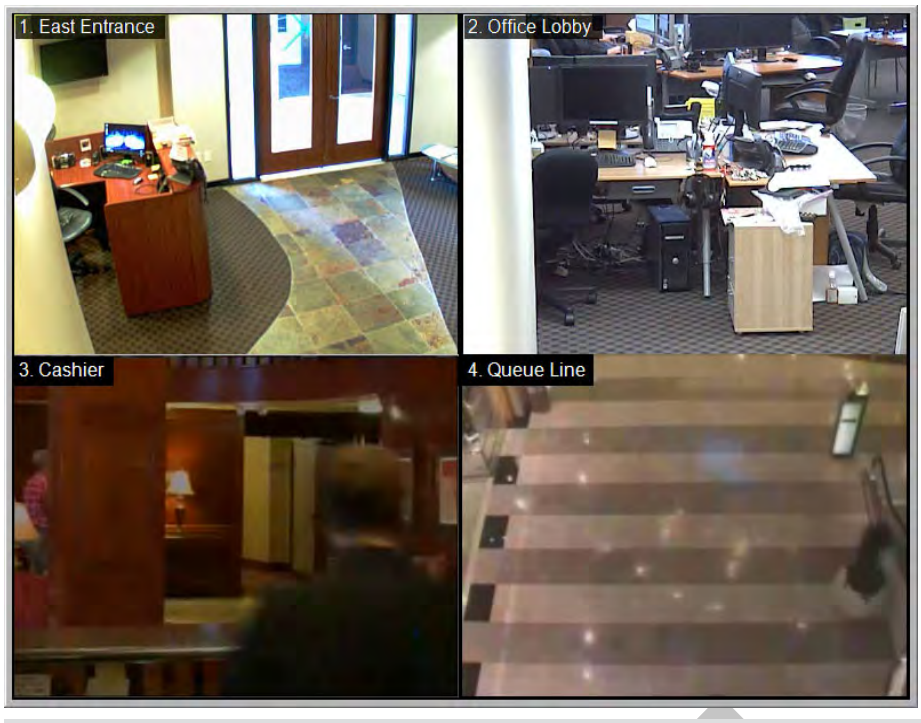
1. When you finish configuring the Spot Monitor display settings, click **OK** to save your changes and exit the **Spot Monitor Configuration** dialog box.

2. To start Spot Monitor:

   - **Connected to the appliance with a monitor, mouse, and keyboard:** After you click **OK**, Spot Monitor automatically loads with the specified configuration.

   - **From System Manager**: right-click the name of the VMS server and select **Start Spot Monitor**.





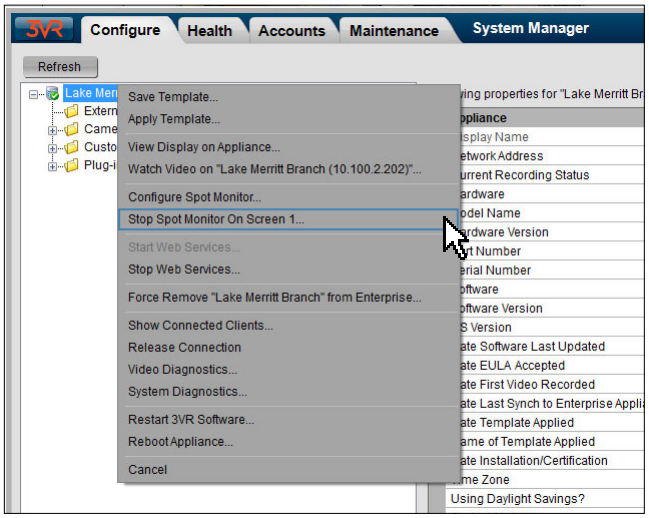
Note
If the 3VR appliance reboots while Spot Monitor is running, the system will restart Spot Monitor when it powers back up.

2.5 Stopping Spot Monitor

To stop Spot Monitor:

- **Connected to the appliance with a monitor, mouse, and keyboard:** move the mouse to display the application's title bar. Click the **X** in the top-right corner to close Spot Monitor and return to the sign-in screen.

- **From System Manager**: right-click the name of the 3VR appliance and select **Stop Spot Monitor**.



3. DUAL SPOT MONITORS

Dual Spot Monitors refers to configuring two instances of Spot Monitor on separate monitors (designated as the primary and secondary monitor).

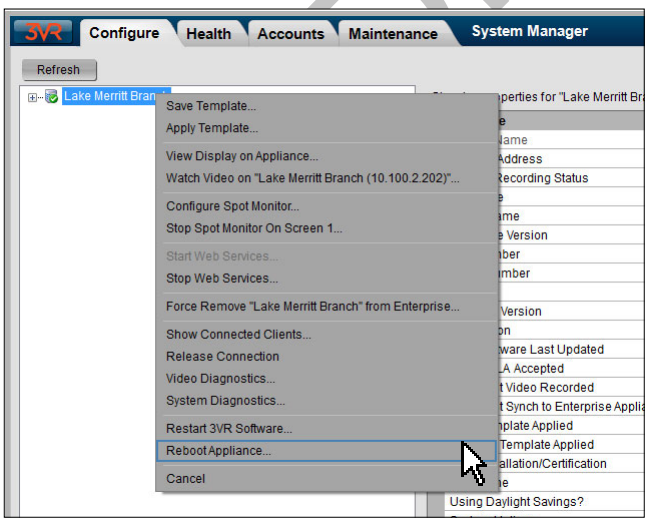
3.1 About Dual Spot Monitors

In order to configure Dual Spot Monitors, the model of 3VR appliance must support multiple displays. Refer to the following chart for specifics for each model:

Platform	VGA Out	BNC Out	DVI Out	HDMI Out	Dual Spot Monitor Support?
1000-Series	X			X	Yes
2000-Series				X	Yes
3000-Series	X			X	Yes
4000-Series	X		X	X	Yes
5500-Series	X	X	X		Yes
Server Class	X	X	X		Yes

3.2 Physical Setup

1. Connect the primary monitor to the VGA output port.
2. Connect the secondary monitor to the BNC or DVI output port. Position the second monitor to the right of the primary monitor.
3. Reboot the appliance:
   - **2000-Series, 4000-Series, and 5500-Series**: Press the power button **once**, do not press and hold. When the appliance safely shuts itself down, press the power button again.
   - **1000-Series and 3000-Series**: Toggle the power switch. When the appliance safely shuts itself down, toggle the power switch again.
   - **From System Manager**: In the **Configure** panel, right-click the name of the appliance and select **Reboot Appliance**.



DRAFT

Note
Refer to the product diagrams in “Physical Setup” on page 215 for assistance identifying the VGA, BNC, HDMI, and DVI ports on the 3VR appliance.

3.3 Enabling Dual Spot Monitors

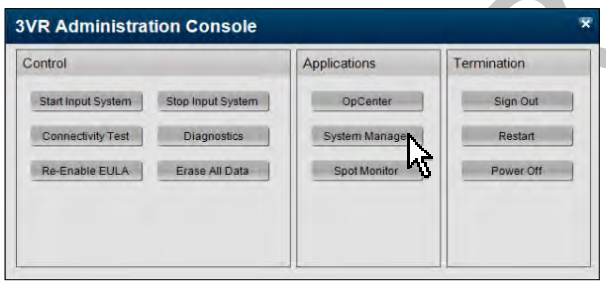
Important Notes

- **You must be connected to the appliance with a monitor, mouse, and keyboard in order to enable dual Spot Monitor.**
- If possible, 3VR recommends using remote Spot Monitor (an instance of the Spot Monitor program installed on a separate PC) rather than dual Spot Monitor to configure multiple Spot Monitors.

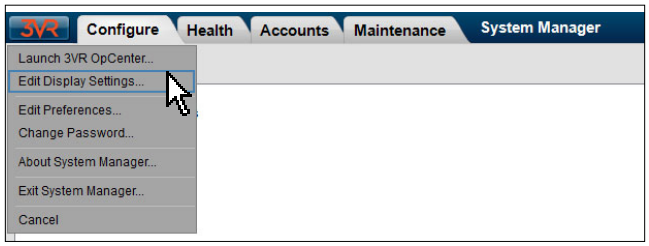
1. When the system powers up to the local sign-in screen, log in with a user account with technician permissions (e.g., techrep or the customer-specific equivalent).

Note
Refer to the product diagrams in “Physical Setup” on page 215 for assistance identifying the VGA, BNC, HDMI, and DVI ports on the 3VR appliance.

2. From the 3VR Administration Console, click the **System Manager** button to launch System Manager.



3. Click the **3VR** button in the top-left corner of System Manager and select **Edit Display Settings** from the options menu.



4. Edit the display settings as follows:

   Primary Monitor:

   - Connected to: **VGA-Out**
   - Shows on startup: **Spot Monitor**.

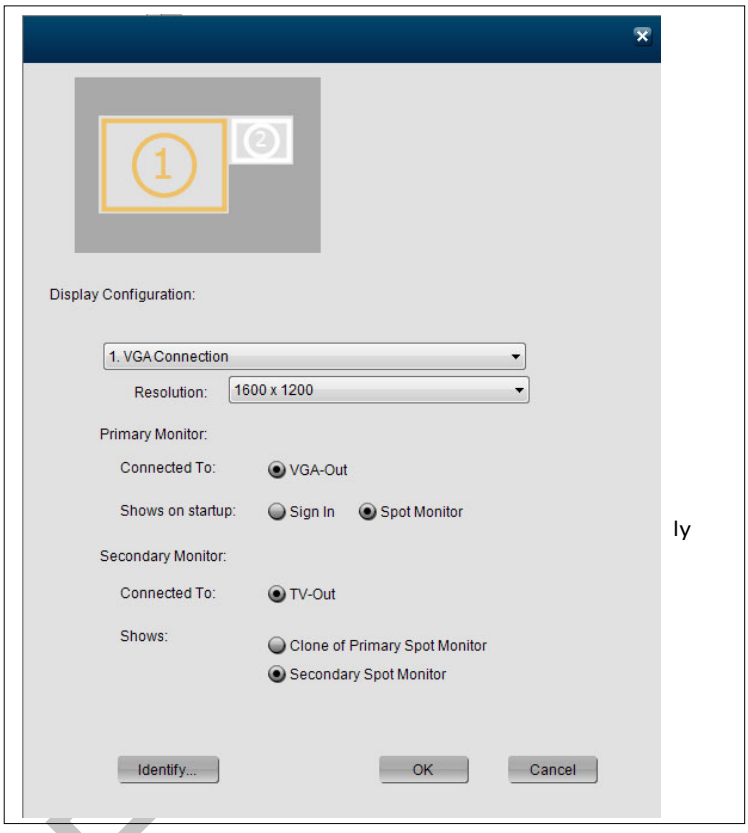
   Secondary Monitor:

   - Connected to: **TV-Out, HDMI-Out**, or **DVI-Out**.
   - Shows on startup: **Secondary Spot Monitor**.

5. Click **OK**.

6. Click **Yes** to confirm the settings change, and then click **Yes** again to save the new display configuration.

   5500-Series: Spot Monitor appears immediately on both monitors, there is no need to reboot.



Primary or Secondary?
If you need assistance determining which monitor is which, click **Identify**. The primary and secondary monitor will be labeled with 1 and 2, respectively.

DRAFT

3.4 Configuring Dual Spot Monitors from the Local Console

Perform the following steps to configure the display of Dual Spot Monitors when connected with a monitor, mouse, and keyboard:

1. Move the cursor to the top of the monitor. Click the 3VR button in the top-left corner of Spot Monitor and select **Configure** from the drop-down menu.

2. Configure the Spot Monitor display as desired according to the instructions in section 2.3.

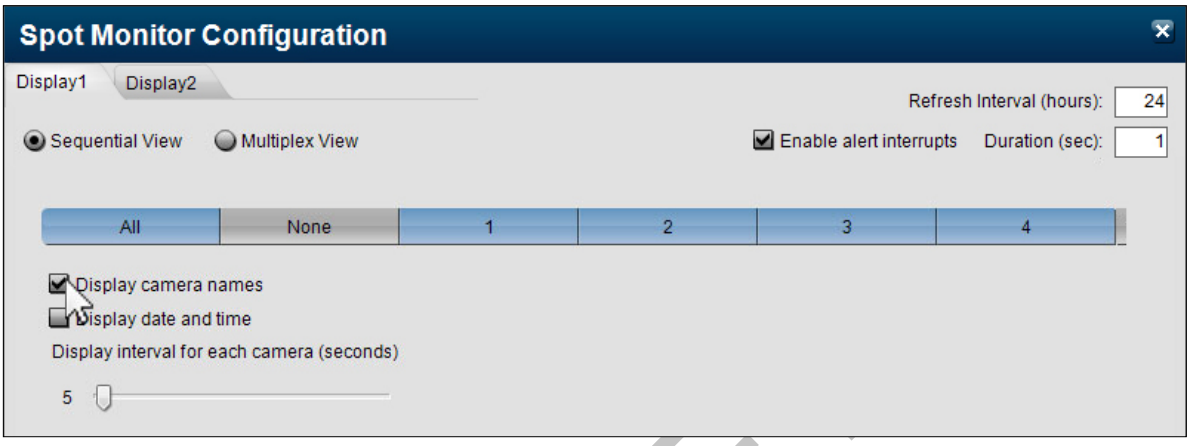
3. When you are finished, click **OK** to save the configuration.

4. Repeat steps 1-3 on the secondary monitor.

3.5 Configuring Dual Spot Monitors from System Manager

Perform the following steps to configure the display of dual Spot Monitors from System Manager:

1. Launch 3VR System Manager.
2. In the **Configure** panel of System Manager, right-click the system display name and select **Configure Spot Monitor**.
3. The **Spot Monitor Configuration** dialog box shows a tabbed interface with one tab for each monitor (**Display 1** and **Display 2**). Configure each Spot Monitor display as desired according to the instructions in section 2.3.
4. Click **OK** to save the configuration.



DRAFT

DRAFT

CHAPTER 12
Health Monitoring and Maintenance

1. HEALTH MONITORING 229
   - 1.1 Filtering Health Alerts 229
   - 1.2 Acknowledging Health Alerts 231
   - 1.3 Exporting Health Alerts 232
   - 1.4 Configuring Email Notification of Health Alerts 233
   - 1.5 Enabling or Disabling Health Alert Notifications 235
   - 1.6 Customizing Health Alert Thresholds 235
   - 1.7 Health Alerts Reference 237
2. DIAGNOSTIC AND SUPPORT TOOLS 240
   - 2.1 System Status Indicator (Not Applicable to All Models) 240
   - 2.2 RAID/Disk Settings (3VR Appliance Only) 240
   - 2.3 Test Appliance Connectivity 241
   - 2.4 Uninterruptible Power Supply Settings 242
   - 2.5 License Settings and Resource Units 244
3. SYSTEM STORAGE 245
   - 3.1 System Storage: Two Approaches 246
   - 3.2 Best Practices for Smart Storage Consumption 246
   - 3.3 Monitoring Storage Consumption 247
   - 3.4 Storage Upgrades 247
4. ENTERPRISE HEALTH CHECK 248
5. TROUBLESHOOTING 249
   - 5.1 Troubleshooting Resources 249
   - 5.2 Exporting Logs 249
   - 5.3 Exporting System Diagnostics 252
   - 5.4 System Information (Fall Release-2015 (version 8.1.x and above) only) 254

DRAFT

DRAFT

1. HEALTH MONITORING

The VMS server performs frequent self-monitoring checks for potential issues with its hardware, network connectivity, video recording status, and other concerns. When a problem is detected, VisionPoint™ VMS generates a health alert, which includes a description of the problem and the date and time the issue was first detected.

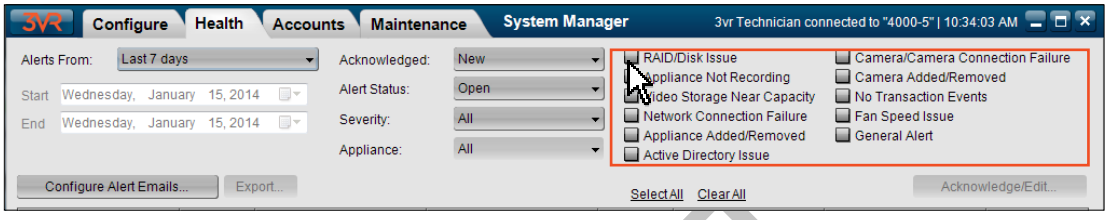
You can view and acknowledge health alerts from the **Health** panel of System Manager.

1.1 Filtering Health Alerts

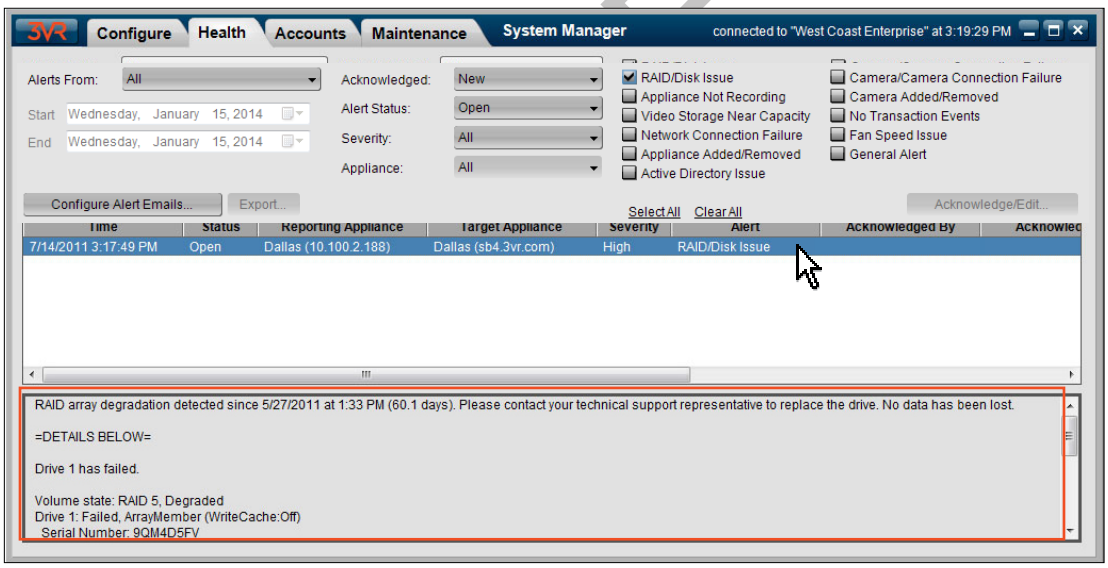
The controls at the top of the **Health** panel allow you to filter health alerts by their type, date/time, or alert status.

Filtering by Alert Type

At the top of the panel, the types of health alert are listed with check boxes:



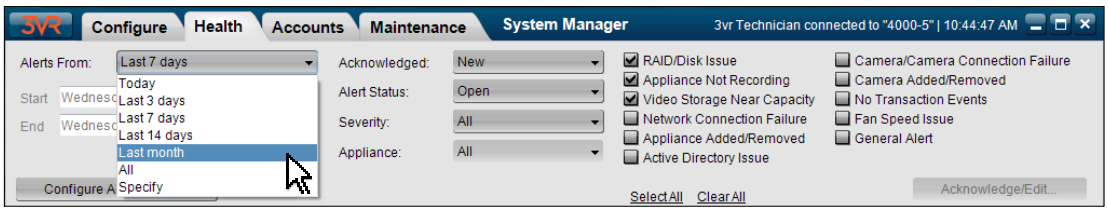
When you select more alert types, the **Health** panel populates with any health alerts that have been generated of that type. Click to select an alert. Details about the alert appear below.



Filtering by Time

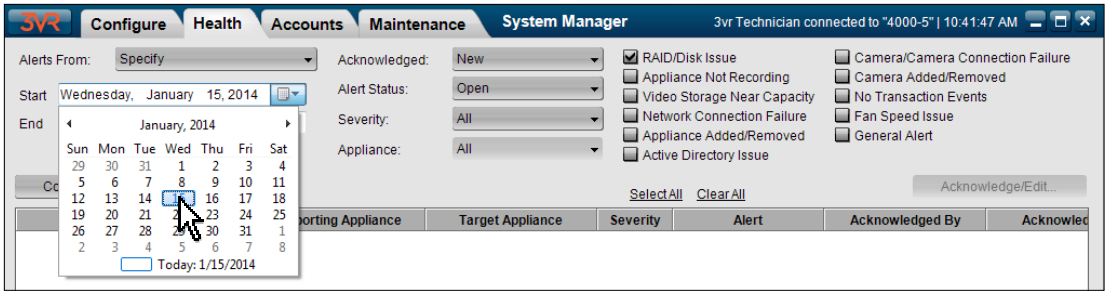
To filter health alerts by time, choose one of following options:

- Select one of the pre-defined time ranges from the **Alerts From** drop-down menu.



- If the time range you wish to filter by is not listed in the **Alerts From** menu, select **Specify**.

  Click to highlight the month, date, or year in the **Start** and **End** controls and press the arrow up or down keys to change the values. Or click the arrow button to display a drop-down calendar.

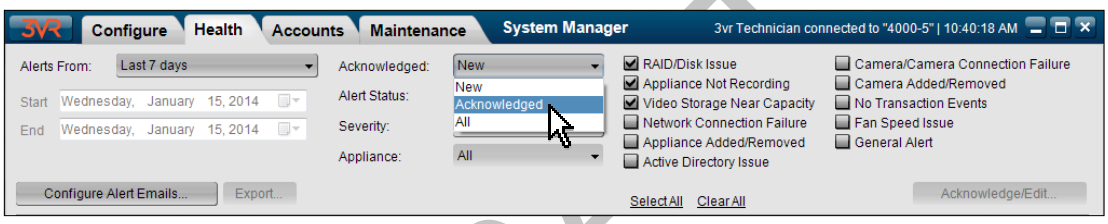


The **Health** panel automatically updates to only show health alerts that occurred within the selected time range.

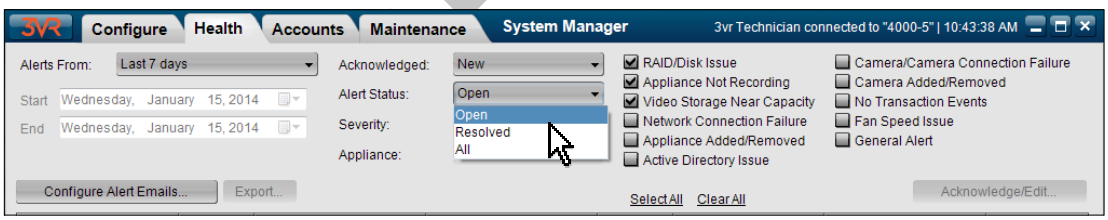
Filtering by Alert Status

To filter health alerts by the status of the alert, choose one of following options:

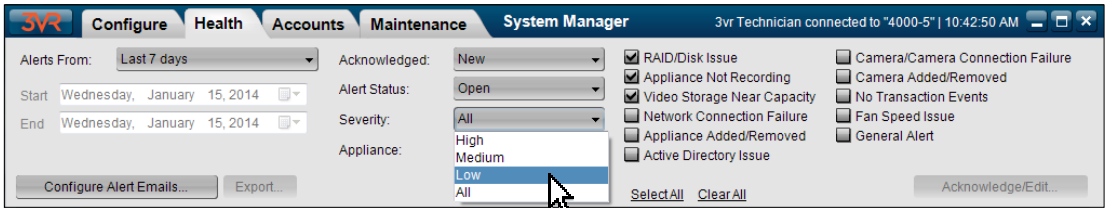
- To filter health alerts by whether or not they have been acknowledged, open the **Acknowledged** drop-down menu and select **New**, **Acknowledged**, or **All**.



- To filter alerts by whether or not they have been resolved, open the **Status** drop-down menu and select **Open**, **Resolved**, or **All**.



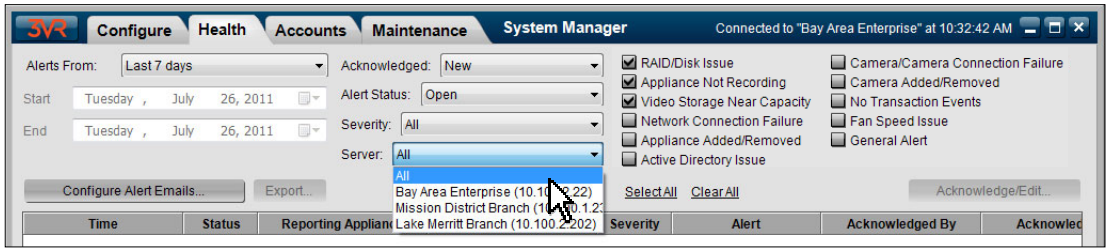
- To filter alerts by their severity, open the **Severity** drop-down menu and select a severity level.



The **Health** panel automatically updates to only show health alerts with the specified status.

Enterprise System Manager | Filtering by VMS Server

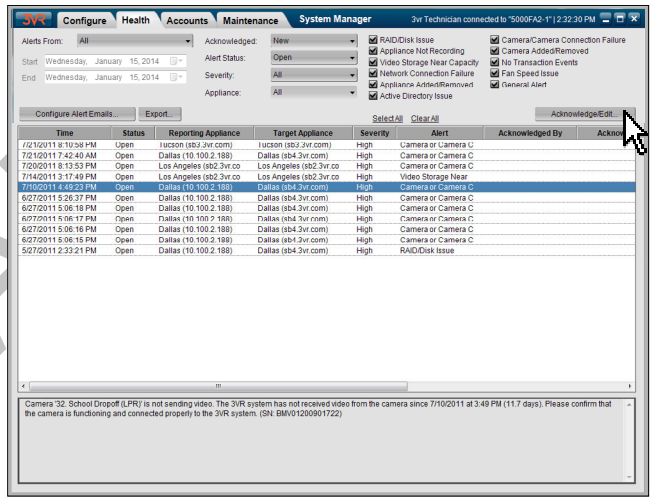
If you are connected to an Enterprise server, you may also filter the health alerts by VMS server. Open the **Server** drop-down menu and select the VMS server of interest to view health alerts from only that server.



The **Health** panel automatically updates to only show health alerts generated by the selected server.

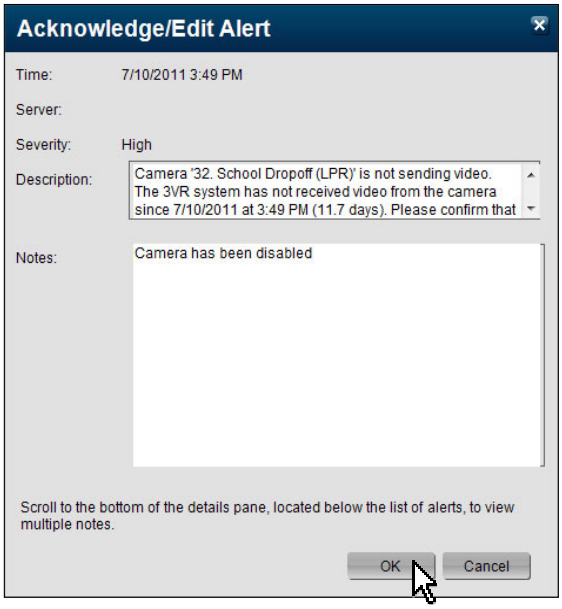
1.2 Acknowledging Health Alerts

Acknowledging health alerts allows you to indicate if an alert has been reviewed and to note whether any action has been taken to resolve the situation.



1. Click the **Health** tab to go to the **Health** panel.
2. Select a health alert from the list. Information about the alert appears at the bottom of the panel.
3. To acknowledge the selected alert, click **Acknowledge/Edit**.

DRA



4. The **Acknowledge/Edit Alert** window displays information about the health alert.

   Type in any notes you may have about the alert, such as steps taken to resolve the issue.

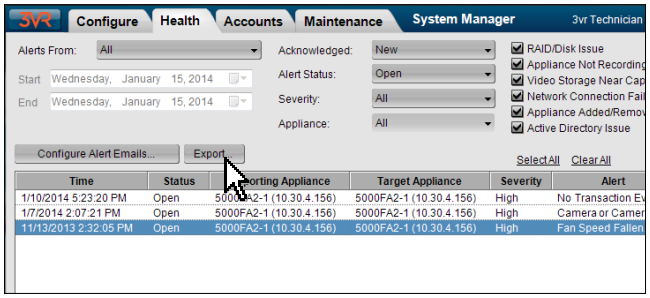
5. Click **OK** to acknowledge the alert.

> **More**
> To acknowledge multiple alerts at one time, hold down the CTRL key and click to select alerts, or click and drag over alerts to select them, and then click **Acknowledge/Edit**.

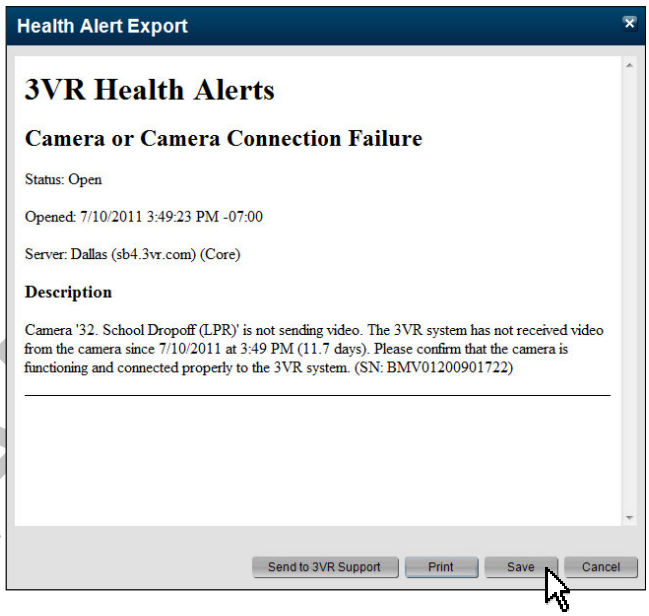
1.3 Exporting Health Alerts

With the **Export** function, you can easily print, save, or email health alerts from System Manager.

1. Click the **Health** tab to go to the **Health** panel.
2. Select a health alert from the list. Information about the alert appears at the bottom of the panel.
3. Click **Export**.



4. In the **Health Alert Export** window, a summary of the selected alert(s) appears under the heading **3VR Health Alerts**.



Send to 3VR Support

To email the alert summary to 3VR for troubleshooting, click **Send to 3VR Support**.

1. In the dialog box that appears, enter the **Customer Company Name**. The **Location or Appliance Name** field should be pre-filled with the name of the 3VR appliance and its IP address.

   a. Click **Send**.

Notes

1) Please contact 3VR Technical Support after clicking **Send** to obtain a support ticket for troubleshooting.
2) The VMS server must be configured to send email in order to email health alerts. See the chapter on basic System Manager configuration for details.

DRA

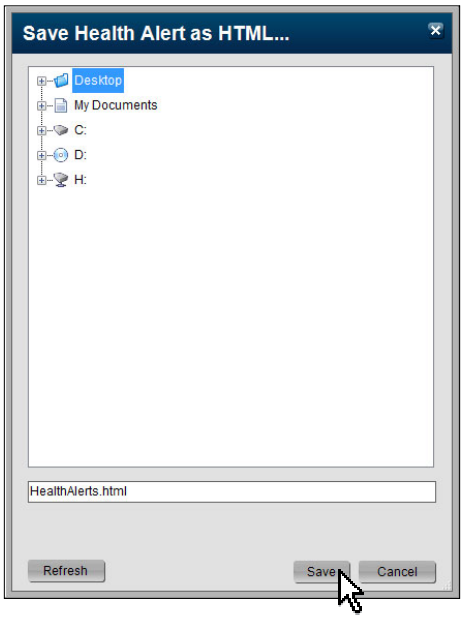
Print

Click **Print** if you would like to print the alert summary. This brings up the Windows Print dialog box on your PC.

Save

To save the summary to disk as an HTML file, click **Save**.

1. In the **Save Health Alert as HTML** dialog box, navigate to the folder where you wish to save the alert summary.
2. If desired, edit the file name of the exported HTML file. By default, the file will be named **HealthAlerts.html**.
3. Click **Save**.

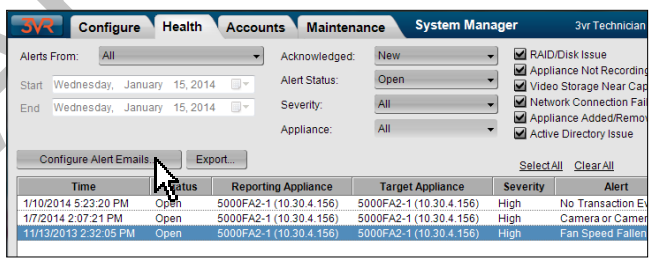


1.4 Configuring Email Notification of Health Alerts

You can configure System Manager to automatically forward incoming health alerts to one or more email addresses.

To configure health alert emails on the system:

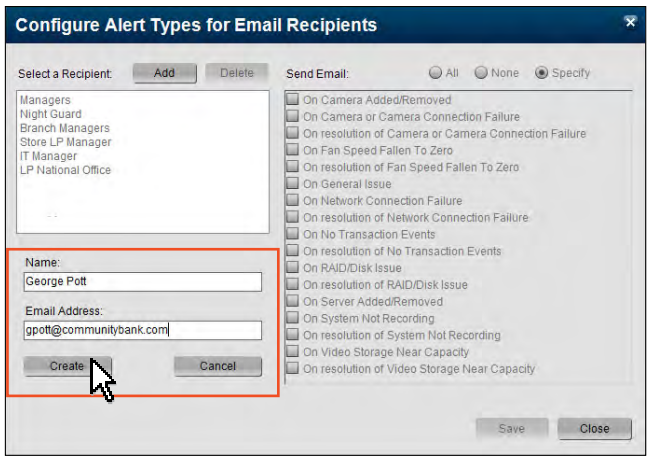
1. Click the **Health** tab to go to the **Health** panel.
2. Click **Configure Alert Emails**.



You can perform the following tasks from the **Configure Alert Types for Email Recipients** dialog box.

Create a New Recipient

1. Click **Add**.
2. Enter a name and email address and click **Create**.

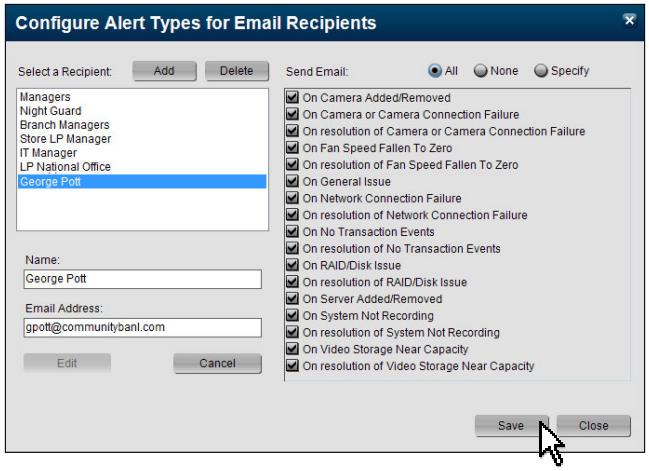


DRAFT

3. In the **Send Email** panel, specify which types of alerts you want to send to the recipient:

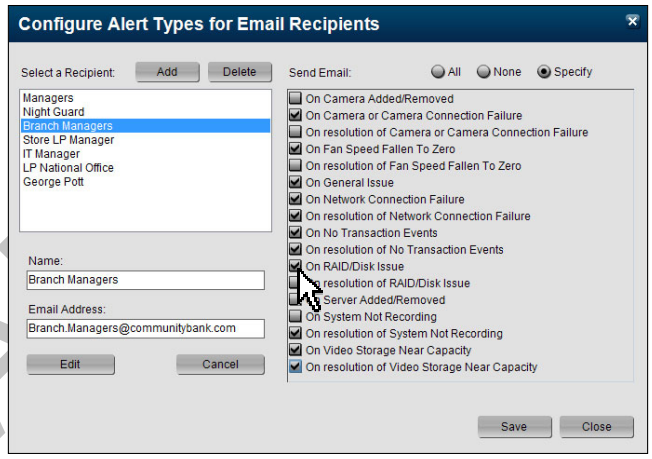
   - Select **All** to send the recipient all alert emails or **None** to disable the recipient.
   - To pick and choose which alerts to send to the recipient, click **Specify** and check or uncheck boxes next to alert types.

4. Click **Save** to save your changes.



Modify an Existing Recipient

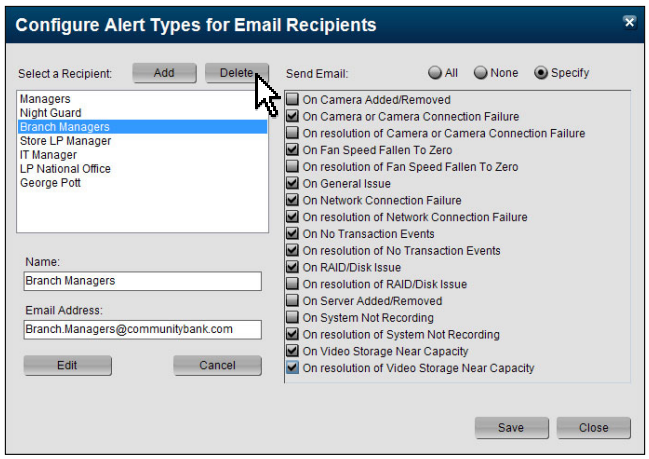
1. Select the recipient from the list.
2. Modify the name, email address, or subscriptions of the recipient as desired.
3. Click **Save** to save your changes.



Delete a Recipient

1. Select the recipient to delete.
2. Click **Delete**.

   The email recipient is deleted from the system.

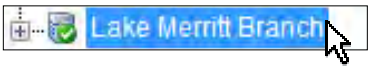


DRA

1.5 Enabling or Disabling Health Alert Notifications

Perform the following steps to disable health alert notifications for one or more alert types:

1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

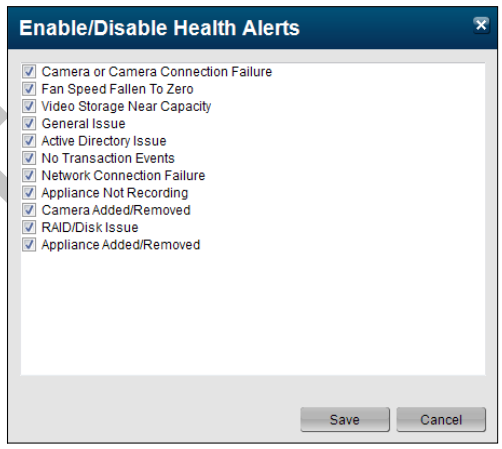


2. Scroll down to the **Health Monitoring** settings category.

3. Click Enable/Disable Health Alerts.

4. In the **Enable/Disable Health Alerts** dialog box, check or uncheck alert types to customize which alerts should be generated on the system.

5. Click **Save**.



DRAFT

1.6 Customizing Health Alert Thresholds

To avoid false alarms, VisionPoint™ VMS must detect a problem or status update for a minimum period of time before it generates the alert. By default, 60 minutes must pass between detection and alerting. If desired, you can reduce or lengthen this interval by modifying the health alert threshold settings.

VMS Server Health Alert Thresholds

To modify the health alert thresholds for video recording problems, drive failures, and other system-wide issues:

1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

2. On the right-hand side of System Manager, scroll down to the **Health Monitoring** settings category.

Recording Inactivity Threshold

Health Monitoring	
Hard Drive Failure Threshold	60 minutes
Known Host	www.google.com
Recording Inactivity Threshold	60 minutes
Network Inactivity Threshold	60 minutes

Default: **60 minutes**
Range: **10 minutes–4 hours**

The system generates a health alert after this length of time if no video is recorded on any of the cameras.

Hard Drive Failure Threshold

Default: **60 minutes**
Range: **10 minutes–4 hours**

If one of the hard drives in the system's RAID array fails, a health alert is generated after this length of time.

Network Inactivity Threshold

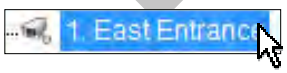
Default: **60 minutes**
Range: **10 minutes–4 hours**

If the IP address or host name entered in the **Known Host** setting does not respond to a ping for the specified length of time, a health alert is generated.

DRAFT

Camera Health Alert Thresholds

To modify the health alert thresholds for camera-specific issues:

1. In the **Configure** panel of System Manager, click the plus sign (+) next to name of the appliance.
2. Click the plus sign next to **Cameras** to display the list of all cameras on the system.
3. Select the camera of interest. 

4. On the right-hand side of System Manager, scroll down to the **Health Monitoring** settings category.

Transaction Event Inactivity Threshold

Health Monitoring	
Camera Inactivity Threshold	60 minutes
Transaction Event Inactivity Threshold	4

Default: **4 days**
Range: **1–10 days**

If no transaction events occur on a camera for the specified length of time, a health alert is generated.

This setting only takes effect after at least one transaction event has been generated on the camera.

This alert can be disabled on the camera by setting this field to **0**.

Camera Inactivity Threshold

Default: **60 minutes**
Range: **10 minutes–4 hours**

If the camera is down for a period of time longer than specified in the **Camera Inactivity Threshold**, a health alert is generated.

1.7 Health Alerts Reference

This section outlines the types of health alerts that may appear on your 3VR appliance, outlining the sample alert text for your reference and steps to take to resolve the issue.

Not using a 3VR appliance?
Some health alerts, including RAID/disk and fan speed issues, are hardware-specific and therefore are not currently supported for VMS servers running on third-party hardware.

System Not Recording

Sample alert text	*The 3VR system has not been recording since 2/24/2016 at 3:39 PM (1.4 days). Please restart the system or contact your technical support representative for assistance.*
What it means	No video has been recorded by the system since the specified time. This may be because video recording has been disabled, or there is another issue preventing video from being recorded.
Troubleshooting	Restart the 3VR appliance, and then check live and stored video in OpCenter. If video does not return after the reboot: • In the **Configure** panel, click to select the name of the appliance. On the right-hand side of System Manager, verify that the Current Recording Status field says "Running." If it says "Disabled" click Common Operations and then click **Enable Video Recording** to start video recording. • If these steps fail to resolve the issue, contact 3VR Technical Support.

Video Storage Near Capacity

Sample alert text	*Low disk space reported since 7/1/2015 at 3:38 PM.*
What it means	When the amount of free disk space on the appliance drops below a specified threshold, the normal behavior of the system is to begin trimming old event data to free up space. This alert indicates that the 3VR is trimming data, but not quickly enough.
Troubleshooting	Usually this alert occurs because the appliance is overloaded. Consider reducing the rate at which storage is consumed by lowering the resolution, frame rate, and quality of recorded video. If these adjustments do not resolve the alert in 24 hours, contact 3VR Technical Support.

Network Connection Failure

Sample alert text	*The network connection to the server Financial District Branch (10.100.2.115) from the enterprise server Community Bank Enterprise (10.100.2.161) has not been available since 2/26/2016 at 1:10 AM (3.6 days). Check network connectivity, DNS, and hostname information.* or *The known host '10.100.1.1' has not responded to network requests since 6/25/2015 at 1:26 AM (6.5 days). Check network connectivity, DNS, and hostname information. The known host is configured on the Configure panel.*

DRAFT

What it means	This alert occurs in two situations: • An Enterprise server loses network connectivity to one of its VMS servers. • A VMS server or Enterprise is unable to ping the IP address listed in the **Known Host** setting in System Manager.
Troubleshooting	1. Check the back of the 3VR appliance to make sure that there the link lights on the primary Ethernet port are lit, indicating the physical connection of the network cable is secure. 2. Reboot the 3VR appliance. 3. If the network connectivity alert was generated because it could not access a known host, verify that the known host is online by pinging it from another computer on the same network. 4. If none of these steps resolve the issue, contact 3VR Technical Support.

Server Added/Removed (Enterprise Only)

Sample alert text	*Removed appliance South City Branch (10.100.2.10). The 3VR enterprise now has 3 appliances. (SN: BMD01201004967)*
What it means	A VMS server was added to or removed from the Enterprise.

Active Directory Issue (Enterprise Only)

Sample alert text	*DNS Lookup: OK, Backup Server(s): OK, Authentication: Error, Root Browsing: Error (SN: 002-7990002)*
What it means	A credentials issue exists that is preventing the 3VR Enterprise from syncing with Active Directory.

Camera/Camera Connection Failure

Sample alert text	*Camera '14. East Sidewalk' is not sending video. The 3VR system has not received video from the camera since 2/5/2016 at 4:38 PM (11.7 days). Please confirm that the camera is functioning and connected properly to the 3VR system.*
What it means	A camera has been disconnected from the VMS server, or there is a problem with the camera or the input on the video cable.
Troubleshooting	• If you intentionally disconnected the camera from the system, make sure to disable the corresponding camera in System Manager to stop false alerts from being generated. • If the camera is still connected, first check that all cables are securely fastened. Next, swap the camera at that video input with a known good camera to rule out an issue with the camera itself. If neither of these steps resolves the problem (e.g., there is no video on the camera with either camera), contact 3VR Technical Support.

Camera Added/Removed

Sample alert text	*Added 1 cameras. The 3VR system now has 8 cameras.*
What it means	A camera was enabled or disabled on the VMS server.

No Transaction Events

Sample alert text	*There has been no transaction event activity on the 3VR system from Camera '1. Front Entrance' for at least 6 days. For further assistance please contact your technical support representative.*
What it means	This alert occurs when a camera that had previously been receiving transaction events does not receive any events for a specified time period.

DRAFT

Troubleshooting	If you made networking changes at the location, it is possible that the transaction server and the 3VR VMS server are no longer communicating. Do a test transaction and see if an event appears in OpCenter. If this health alert was generated because no transaction events occurred during the given time frame (false alarm), increase the **Transaction Event Inactivity Threshold** in the **Configure** panel of System Manager to prevent false alerts. See section 1.6 for information about this setting.

General Alert

What it means	Varies.
Troubleshooting	Contact 3VR Technical Support.

RAID/Disk Issue (3VR Appliance Only)

Sample alert text	*RAID array degradation detected since 7/8/2015 at 11:28 am (10 minutes). Please contact your technical support representative to replace the drive. No data has been lost.*
What it means	RAID (Redundant Array of Independent Disks) is a technology that protects against a hard drive failure by mirroring data on multiple disks. This health alert indicates that one of the drives in the 3VR appliance's RAID array failed and the system is operating with just the backup disk. Though no data has been lost and the 3VR appliance will continue to function normally, you should promptly replace the failed drive to restore the protections of RAID.
Troubleshooting	You need to obtain a new hard drive, replace the failed drive, and rebuild the RAID array in System Manager. See **http://www.3vr.com/services-support/faq/3vrhardware** for information on how to obtain and install a new drive.

Fan Speed Issue (3VR Appliance Only)

Sample alert text	*Fan 1's speed has fallen to 0 rpm.*
What it means	One of the fans on the system has stopped. Either there is something blocking the fan (for example, a loose wire) or the fan has failed.
Troubleshooting	Contact 3VR Technical Support. The support representative will assist you with opening up the 3VR appliance's chassis to check whether something is obstructing the fan or if the fan is not operating properly.

DRAFT

2. DIAGNOSTIC AND SUPPORT TOOLS

This section describes status indicators on certain appliances and diagnostic tools in System Manager.

2.1 System Status Indicator (Not Applicable to All Models)

The 3VR 5500-Series Appliance features a glowing 3VR logo on the front panel that indicates the system's status in a color-coded pattern. The indicator light changes color according to the following conditions:

White: Normal Operation

Flashing Blue: System is experiencing a RAID drive failure.

The number of flashes indicates which drive needs replacing.

Red: System is no longer recording video; troubleshooting is needed (not applicable to Enterprise appliances).

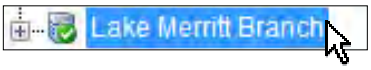
> **Note**
> In some cases, the white light indicating normal operation may be tinted very faintly pink, blue, or purple. This is a result of the placement of the LEDs and does not indicate a problem. The bright, colored indicator lights are strongly differentiated from this faint tint.

DRAFT

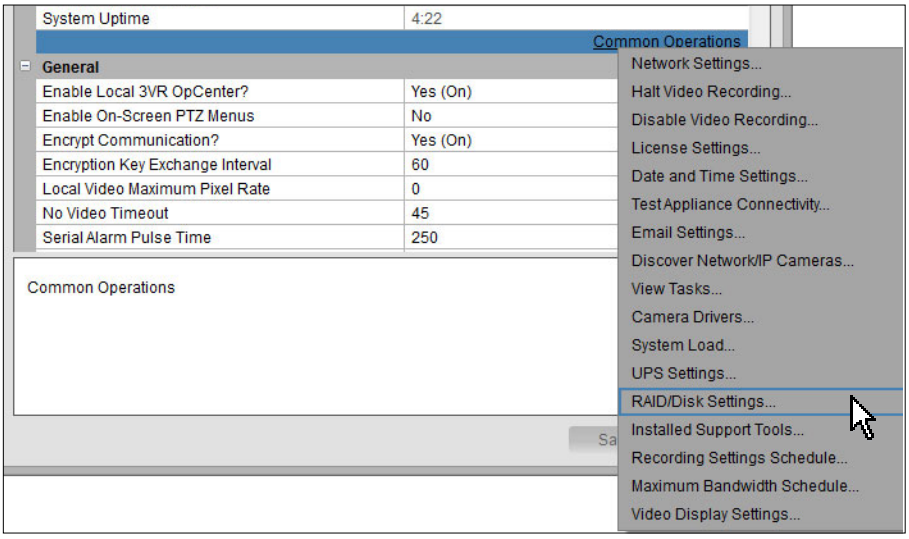
2.2 RAID/Disk Settings (3VR Appliance Only)

If the 3VR appliance has RAID (Redundant Array of Independent Disks), you may check the status of the RAID array in the **RAID/Disk Settings** dialog box:

1. In the **Configure** panel, click the appliance name in the left-hand panel to view the system settings.



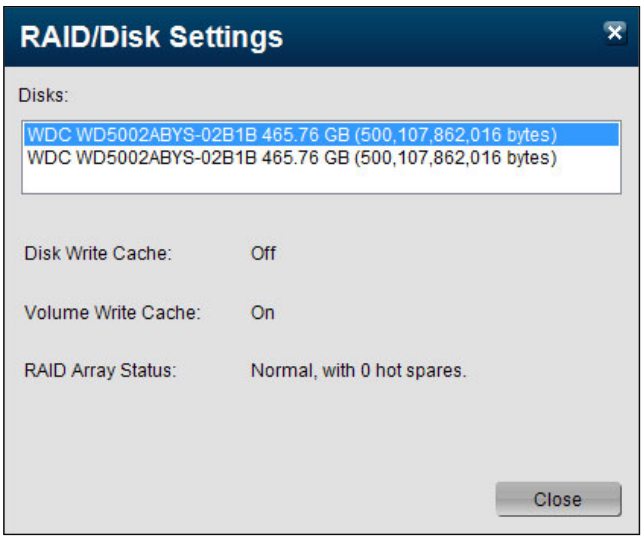
2. Click Common Operations, and then click **RAID/Disk Settings**.



3. During normal operation, the **RAID/Disk Settings** dialog box lists the part number and size of the hard drives on the system, and the **RAID Array Status** is "Normal".

   If there is a RAID drive failure, the failed drive does not appear the list of disks and the status of the RAID array changes to "Degraded."

4. When you finish reviewing the **RAID/Disk Settings**, click **Close**.

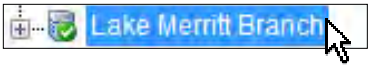


Reference
If one of the drives on the system fails, go to http://www.3vr.com/services-support/faq/3vrhardware for information on hard drive replacements.

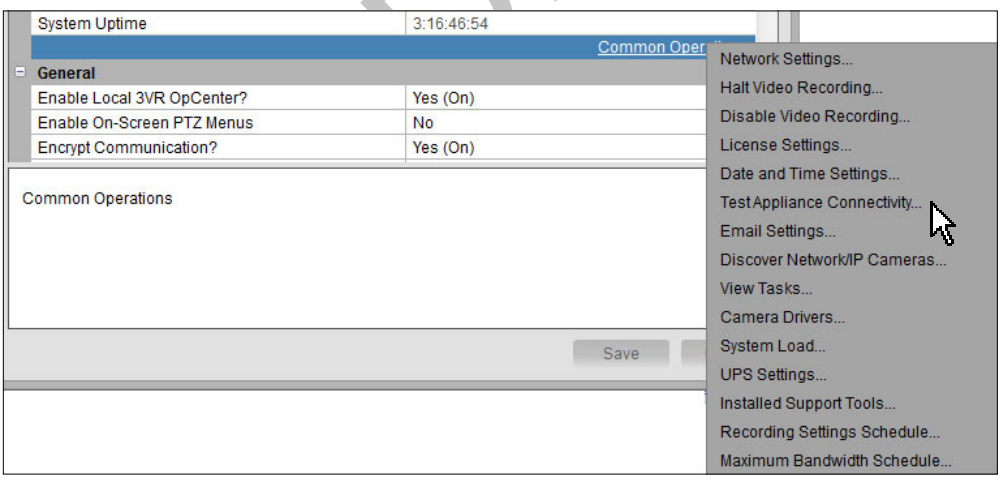
2.3 Test Appliance Connectivity

If a VMS server is not online or the network connection is intermittent, use the **Test Appliance Connectivity** feature to test the connection between the VMS server and other devices on the network:

1. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.



2. Click Common Operations, and then click **Test Appliance Connectivity**.



DRAFT

3. In the **Test Appliance Connectivity** dialog box, click the **From Appliance** tab.

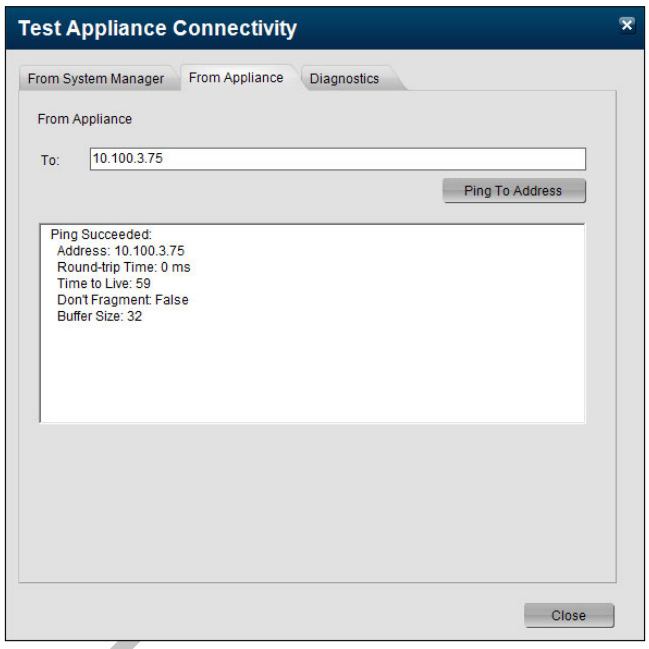
4. In the **To** text box, type the IP address of the appliance to ping.

5. Click **Ping to Address**.

   - If the connection is successful, the results box displays the message "Ping Succeeded" with the reply time.

   - If the connection is not successful, the results box displays "Ping Failed".

6. When you are finished testing the network connectivity, click **Close**.



2.4 Uninterruptible Power Supply Settings

You should always connect 3VR appliances to a UPS (Uninterruptible Power Supply) to protect the system against damage from power outages or surges. While you may use any model of UPS that meets the minimum power requirements* to fulfill this requirement, you can connect certain models of UPS to the system via USB and configure their settings in System Manager to safely shut down the system in the event of a power loss.

Note
Refer to "3VR System Environmental Conditions" on page 33 for the power requirements for 3VR appliances.

Supported UPS Models

You can use System Manager to configure all APC-brand UPS models that connect via USB and meet the minimum power requirements for the model of 3VR appliance.

Hardware Setup

1. If the appliance is currently running, shut down the system:

   - **5500-Series**: Press the power button **once**, do not press and hold.

2. Plug the 3VR appliance's power cable into an available socket on the UPS.

3. Connect the USB cable from the UPS to the 3VR appliance.

4. Plug the UPS into a power source.

5. Power on the UPS and the 3VR appliance.

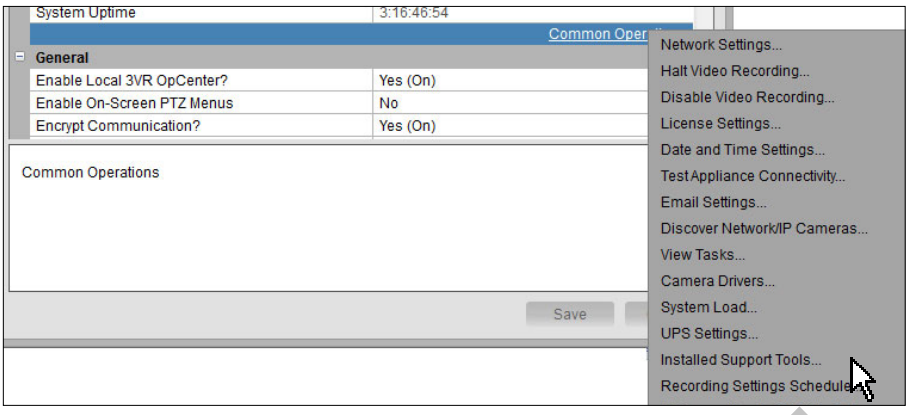
DRAFT

Software Configuration

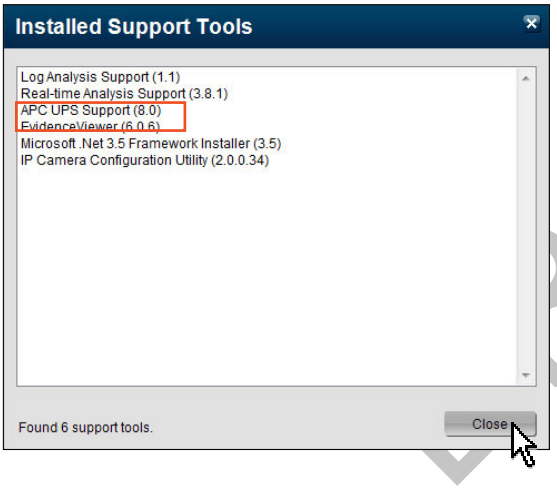
1. Launch 3VR System Manager.

2. In the **Configure** panel, click the VMS server name in the left-hand panel to view the system settings.

3. Click Common Operations, and then click **Installed Support Tools**.

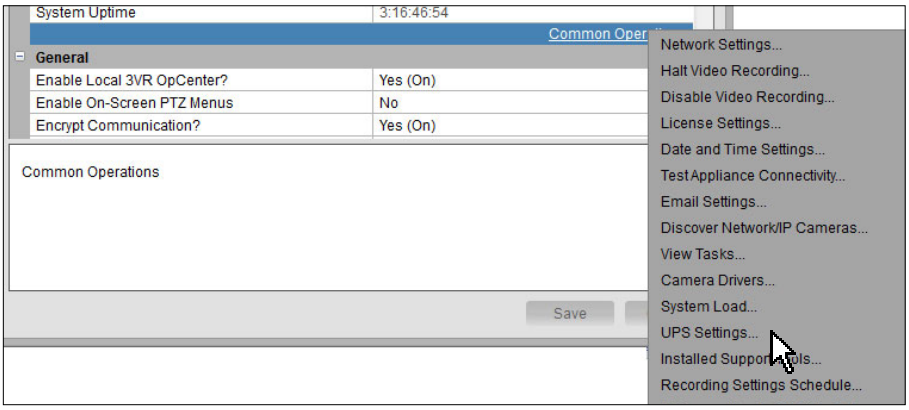


4. Ensure that **APC UPS Support** is listed in the resulting dialog box, and then click **Close** to return to the **Configure** panel.

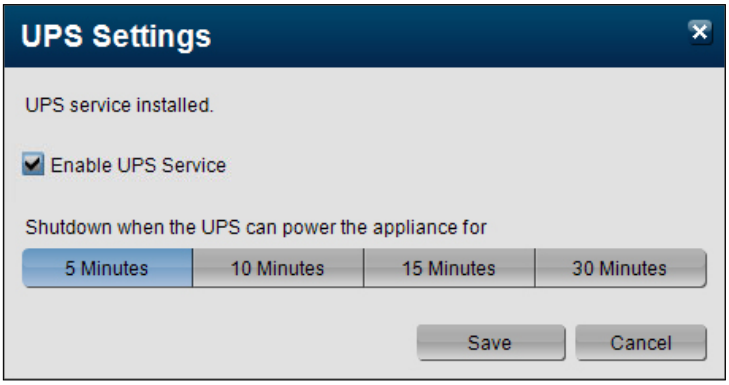


Missing UPS Support?
If **APC UPS Support** is not installed, contact 3VR Technical Support by phone at 415-513-4572 or email support@3VR.com for assistance.

5. Click Common Operations, and then click **UPS Settings**.



6. In the **UPS Settings** dialog box, check the box next to **Enable UPS Service**.



7. Set the time remaining threshold for the UPS by selecting one of the time interval buttons.

   For example, if you select **10 minutes**, the UPS shuts down the 3VR appliance when the UPS has enough battery remaining to power the system for 10 minutes.

8. Click **Save**.

2.5 License Settings and Resource Units

Certain features of VisionPoint™ VMS require licenses before you can enable them. The list of licensed features includes:

- **3VR Analytics:** Facial Surveillance, Advanced Object Tracking, License Plate Recognition, People Counting, etc.
- **IP Camera Expansion:** Enabling IP cameras on a hybrid 3VR appliance. IP cameras on NVR systems do not require a license key.

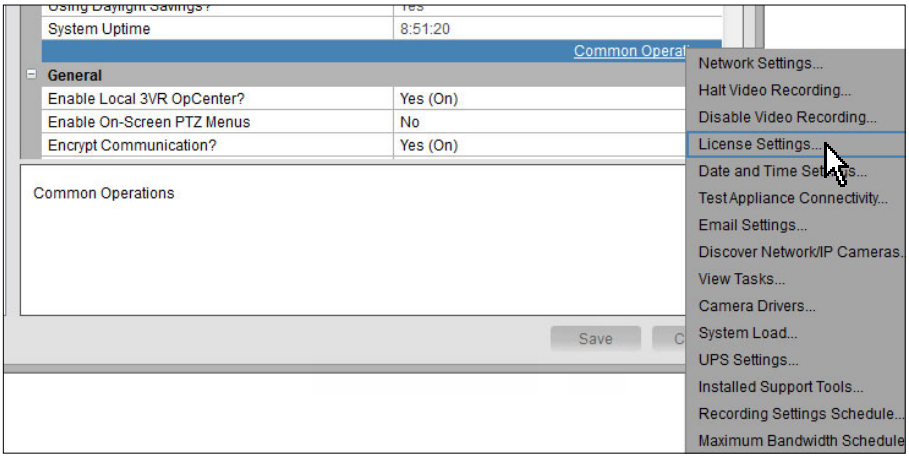
In addition to licensing, VisionPoint™ VMS keeps track of system load (memory and CPU usage) with resource units. This prevents the user from enabling too many features and overloading the system. The number of resource units is fixed and varies from model to model. Enabling features that affect system load subtracts from the number of available resource units.

Certain features, such as analytics, use both licenses and resource units when enabled.

You can check the licensing and resource unit status of your 3VR appliance from the **License Settings** dialog box:

1. In the **Configure** panel, click the appliance name in the left-hand panel to view the system settings.

2. Click Common Operations, and then click **License Settings**.

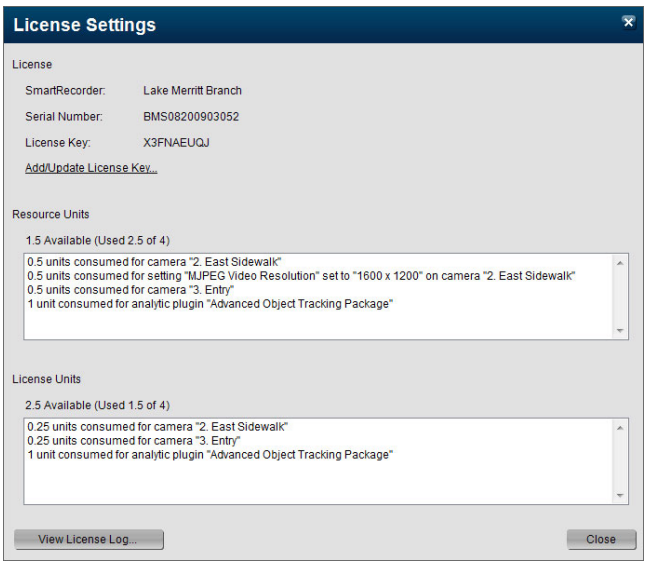


DRAFT

3. The **License Settings** dialog box displays the following information:

   - System license key (if one has been applied)
   - List of features consuming resource units and number of units used/available.
   - List of licensed features.

4. When you finish reviewing the license settings, click **Close** to return to the **Configure** panel.



3. SYSTEM STORAGE

When the available storage on a VisionPoint™ VMS server approaches 1 percent of total capacity, the server automatically trims old video first, and then, secondarily, events, to free up space.

This section explains how to configure your VMS server to efficiently use storage space, ensuring that important video surveillance is available when you need it.

The number of days of video and events that you can store on a 3VR appliance depends on a number of factors:

Built-In Storage Capacity	You can purchase 3VR appliances with a range of disk/RAID array sizes. See the current 3VR Product Overview guide (available on the 3VR web site (www.3VR.com) for more information.
Number of Cameras	3VR sells appliances that support 4, 8, 16, 24, 32, 48, 64, and 128 cameras. You can order licenses for additional IP cameras.
Camera Type	Video recorded on IP cameras consumes more storage space per minute of footage than video from analog cameras.
Continuous Recording	If VisionPoint™ VMS is set to record video continuously, storage is consumed at a higher rate than motion-based recording.
Activity Level	If continuous recording is not enabled, video is only recorded when an event occurs. As a result, cameras recording video in areas of constant activity (e.g., the main floor of a casino) generate more footage than cameras in areas that have little activity (e.g. a bank vault).
Video Recording Settings	The video resolution, frame rate, quality, and compression settings all affect the size of stored video clips.

DRAFT

3.1 System Storage: Two Approaches

Given a 3VR appliance with a fixed hard drive capacity and number of cameras, there are two opposing values that you may prioritize when configuring the remaining settings that affect system storage:

Higher Quality Video, Short-Term Storage

- Organizations using this approach value video quality over the retention of past surveillance. They set video resolution, quality, and frame rate to the highest values, and set compression to a low value to maximize quality.

Lower Quality Video, Long-Term Storage

- This approach favors the long-term preservation of surveillance over maximizing the quality of each video clip. Prioritize long-term storage over quality if your organization often revisits footage older than three months.

3.2 Best Practices for Smart Storage Consumption

Regardless of which approach you choose, the following tips help you maximize storage space without compromising important data:

Position Cameras Properly

Mount cameras in such a way that only areas of interest are shown in the camera's field of view (FOV). If the FOV includes areas of high activity that are not of interest to your organization (for example, foot traffic on the sidewalk outside of a store) many meaningless motion events will be generated, taking up valuable storage space.

Set up Motion Exclusion Zones

If the camera's FOV includes an extraneous region and it is not possible to re-position the camera, configure motion exclusion zones in System Manager to prevent events from being generated from activity in the region.

Establish a Recording Schedule

Unless your organization operates 24 hours a day, there are likely periods of high and low activity in the building. Use this variation to your advantage and configure a recording schedule of Peak and Off-Peak hours in System Manager. Once you define the schedule, configure each camera to record at a lower video resolution, quality, and frame rate during Off-Peak hours to save storage space.

Disable Continuous Recording

When **Continuous Recording** is enabled, the VMS server records video even when nothing is happening in the camera's field of view (e.g. an empty room). Free up space without missing significant events by disabling this feature.

Adjust the Motion Sensitivity Settings

Increasing the **Exclude Motion Smaller Than** and **Exclude Motion Shorter Than** thresholds can reduce the number of events generated from meaningless motion, thereby saving storage space. There is, however, a risk of missing events based on slight movements or motion that starts and stops rapidly. Adjust these values with caution.

Use Cases to Manage Important Surveillance

Events added to cases in OpCenter are excluded from the automatic trimming process. Add important events to a case as soon as you identify them to preserve the event data and associated video clip indefinitely.

DRAFT

3.3 Monitoring Storage Consumption

You can check the total storage capacity, current disk space used, and projected storage duration of a 3VR appliance in System Manager:

1. In the **Configure** panel, click the appliance name in the left-hand panel to view the system settings.

2. Locate the **Smart Storage** settings category.

   The gray fields show the current storage values, including the percentage of storage utilized and the projected video storage duration (days of video) based on the last 7 days of data.

   If you changed system or camera settings and want to refresh the storage projection, click the Reset Projections link and wait at least two business days for enough data to be gathered for the projection to be accurate.

Smart Storage	
Default Storage Time for Custom Event Types	56
Default Video Export Extension	.mp4
Minimum Days of Video	7
Normalize Sample Aspect Ratio for Exported Video	No (Off)
Special Reduced Storage Cameras	
Special Reduced Storage Duration	3
Utilization	61%
Total Disk Space	465 GB
Media Storage Used	238 GB
Database Storage Used	11 GB
Earliest Content	4/27/2011 (90 days ago)
Motion Event Storage (Days)	90
Face Event Storage (Days)	90
Imported Image Event Storage (Days)	90
Ext. Input/Alarm Storage (Days)	90
Advanced Object Storage (Days)	90
Advanced Object Storage (Days)	90
Amount of Video Currently Stored	90 days
Projected Video Storage Duration (Est)	7 days
	Reset Projections...

3.4 Storage Upgrades

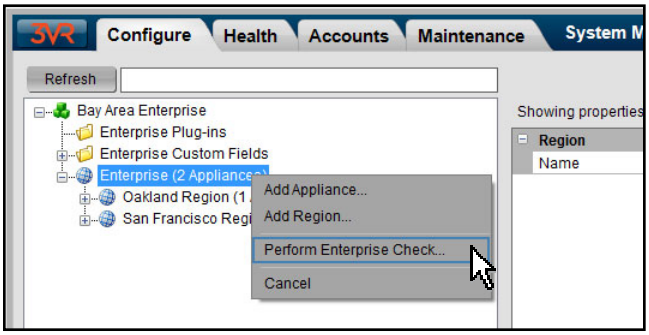
If the storage space of a 3VR system is inadequate for the your organization's needs, you can upgrade certain models of 3VR appliance to a larger storage capacity. Please refer to the chapter on "Field Upgradable Storage" in this guide for more information about this process.

DRAFT

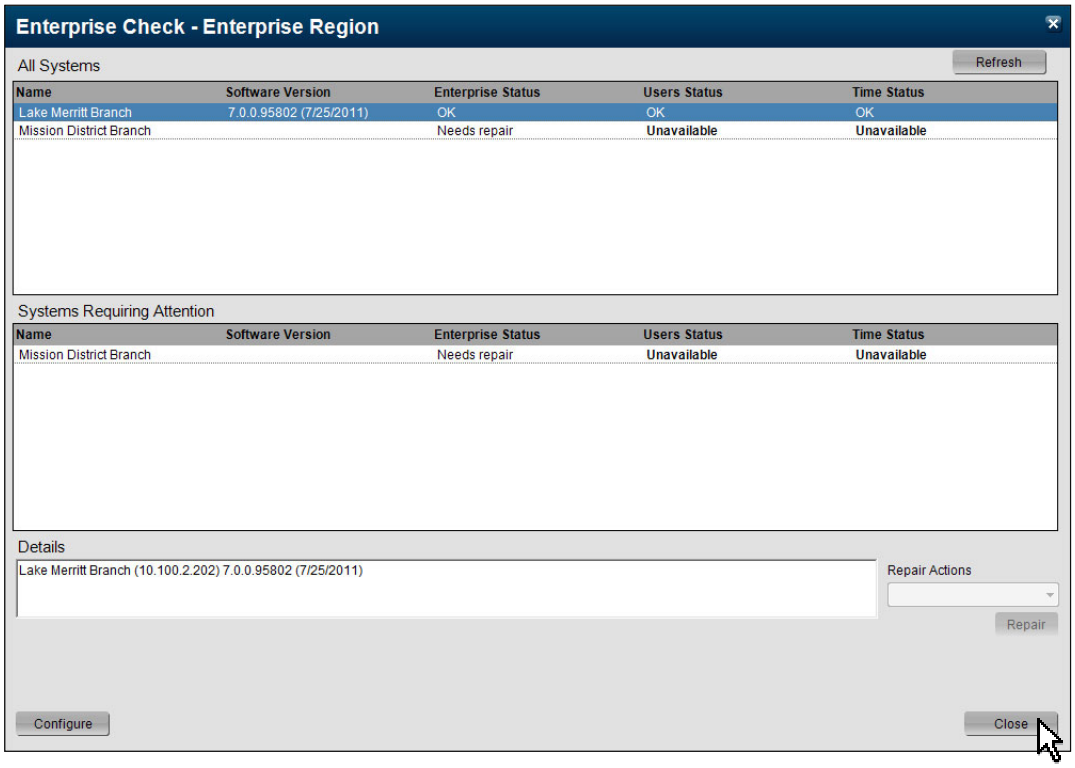
4. ENTERPRISE HEALTH CHECK

The **Check Enterprise** dialog box provides an overview of the health of the Enterprise.

1. In the **Configure** panel, right-click the Enterprise region and select **Perform Enterprise Check**.



2. The columns in the **Check Enterprise** dialog box report the following information about each VMS server on the Enterprise:



- **Name**
  The display name of the VMS server.
- **Software Version**
  The current system software version and the date the software was last updated.
- **Enterprise Status**
  The status of the connection between the VMS server and the Enterprise.
- **Users Status**
  The status of user syncing between the VMS server and the Enterprise.
- **Time Status**
  Whether or not the VMS server's date and time matches the date and time of the Enterprise.

> **More**
> To add columns for the status of Spot Monitor and ATM/Teller transactions, click **Configure**.

3. If there are problems with one or more VMS servers, select the VMS server name in the **Systems Requiring Attention** list box. The lower panel populates with details about the problem.

4. If the problem may be resolved by self-repair, the **Repair Actions** drop-down menu populates with one or more repair options. Select a repair option, and then click **Repair**.

5. To close the **Check Enterprise** dialog box, click **Close**.

5. TROUBLESHOOTING

5.1 Troubleshooting Resources

If you are experiencing a problem with a 3VR appliance or application, the following resources are available to assist you:

Installation and Resource DVD

Installation documentation is provided on the 3VR Installation and Resource DVD, included in the shipping container with every 3VR appliance.

3VR Support Portal

3VR Certified Channel Partners can access software, documentation, and FAQs/Solutions for common problems at the 3VR Support Portal, http://partners.3VR.com.

3VR Technical Support

3VR Technical Support is available for 3VR Certified Channel Partners Monday through Friday from 5 am to 6 PM Pacific Time. If you are an end user of 3VR products, please contact your 3VR reseller before contacting 3VR Technical Support directly.

3VR Technical Support Contact Information

If you are having trouble with a 3VR system or application, contact 3VR Technical Support by phone at 415-513-4572 or email support@3VR.com Monday through Friday, 5 a.m. to 6 p.m. Pacific Time (8 a.m. to 9 p.m. Eastern Time) for assistance.

DRAFT

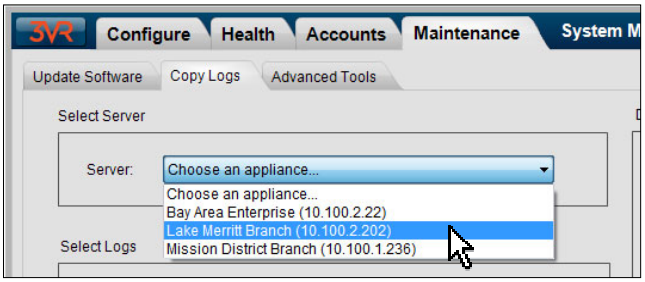
5.2 Exporting Logs

During the course of troubleshooting, 3VR Technical Support may request logs from your system. You can copy log files to disk or send them directly to 3VR Technical Support from System Manager by performing the following steps:

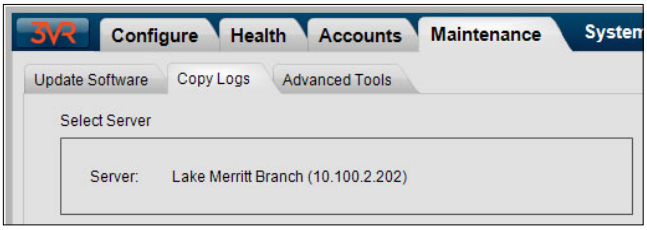
Note

Prior to uploading logs to 3VR, please contact 3VR Technical Support to open a support case. Logs submitted without an associated case will be disregarded.

1. Launch 3VR System Manager.
2. Click **Maintenance** to go the **Maintenance** panel.
3. Click the **Copy Logs** tab.
4. Specify which VMS server to copy logs from:
   - If you are connected to an Enterprise server, select a VMS server on the Enterprise from the **Server** drop-down menu:



- If you are connected to a single VMS server, you do not need to select it. The **Server** field shows read-only text with the VMS server's IP address and host name.

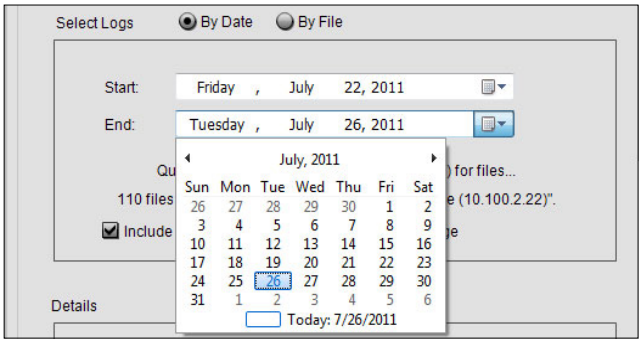


5. Choose the method for selecting log files:

   - Click **By Date** to select all logs from a specific time range.

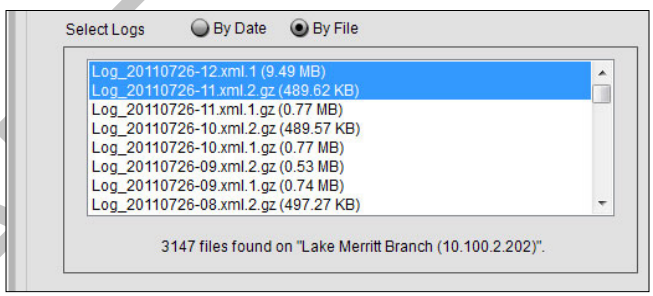
     Click to highlight the month, date, and year in the **Start** and **End** fields and press the arrow up or down keys to change the values, or click the arrow button to display a drop-down calendar.

     If the VMS server you are troubleshooting is on an Enterprise, make sure that the box next to **Include Enterprise logs from the same time range** is checked.



   - Click **By File** to choose log files by their file names.

     Select the file of interest or CTRL-click to select multiple log files.



> **Note**
> Log files are named with the date and time in the format **Log_YYYYMMDD-HH**. For example, Log_20150306-11.xml.7 contains logs from March 6th, 2015 from 10 am.

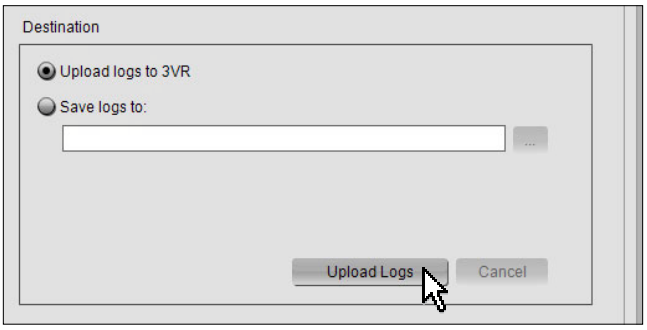
6. In the **Details** section of the **Copy Logs** panel, type the customer name in the **Customer Company Name** box.

7. Type the following information in the **Details** text box:

   - Your contact information
   - Related support case number

8. In the **Destination** section of the **Copy Logs** panel, choose a destination for the log files:

   - If you wish to upload the logs directly to 3VR Technical Support click **Upload logs to 3VR**, and then click the **Upload Logs** button.



> **Important**
> The VMS server must have a working internet connection with valid DNS settings configured in order to upload logs to 3VR.

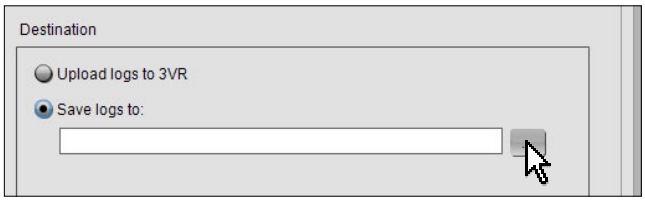
DRAFT

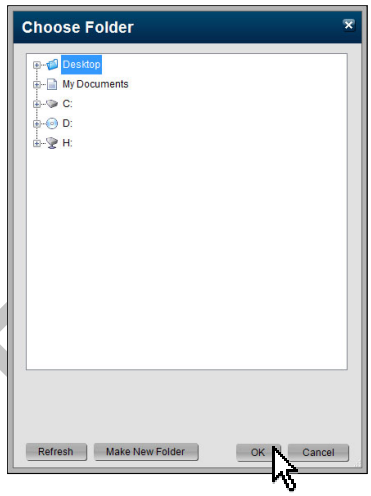
- To copy the files to your computer or a portable disk drive:

  a. **Click ( )Save logs to**, and then click the **ellipsis (...)** button.

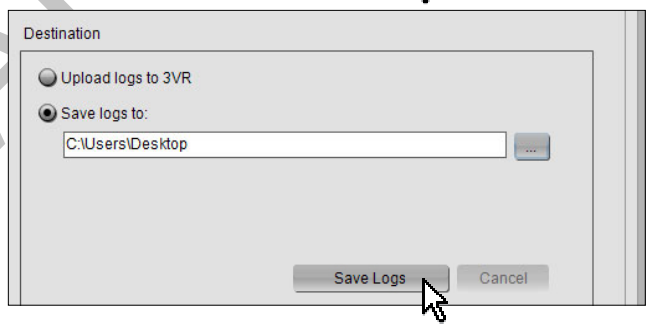
  b. Navigate to the folder where you wish to store the log files.

  c. Select the folder and click **OK**.





  d. Click the **Save Logs** button.



The system displays a message confirming that the logs were copied/uploaded.

DRAFT

Details

Log files saved to a directory or drive are stored in a zip file named using the following format:
[Unit Serial Number]-[Date Logs Were Copied]-[Time Logs Were Copied].zip

9. If you copied the logs to your computer or a USB drive, send the logs to 3VR using the following steps:

   a. Open a web browser, such as Internet Explorer or Mozilla Firefox.

   b. Navigate to http://uploadlogs.3VR.com.

   c. Click **Choose File** and select the exported log zip file.

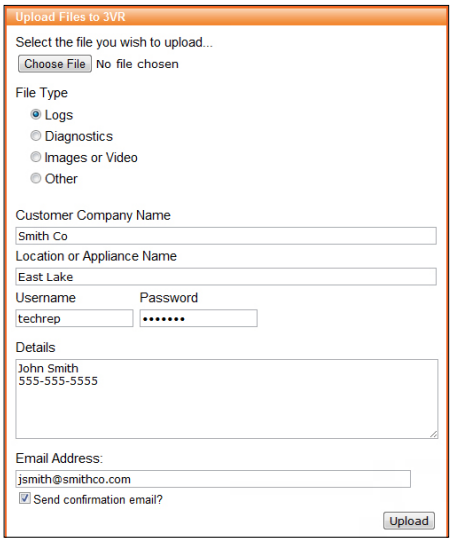
   d. Select **Logs** as the **File Type**.

   e. Type the user name **techrep**, password **3MeDeee**.

   f. Fill out the remaining fields with the details of the installation.

   g. If desired, check the box next to **Send confirmation email?** and enter your email address to receive email confirmation that the logs were uploaded.

   h. Click **Upload**. Make sure that you see the following message: "The file was successfully uploaded."



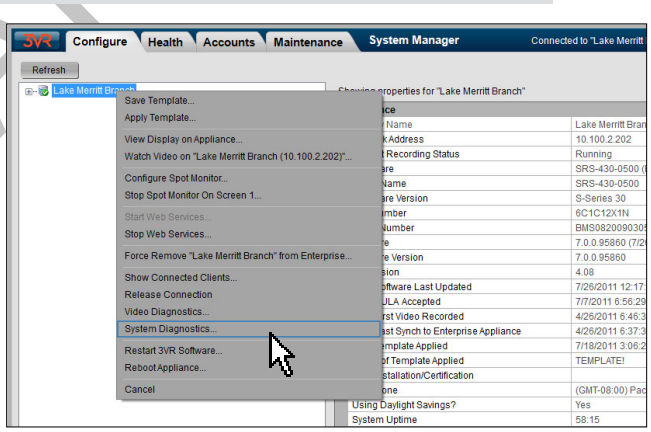
5.3 Exporting System Diagnostics

In the course of troubleshooting, 3VR Technical Support may request system diagnostics from the unit. A system diagnostics export includes all of the system and camera settings, as well as certain system health metrics. Perform the following steps to send system diagnostics to 3VR:

> **Note**
> Prior to sending diagnostics, please contact 3VR Technical Support to open a support case. Diagnostics submitted without an associated case will be disregarded.

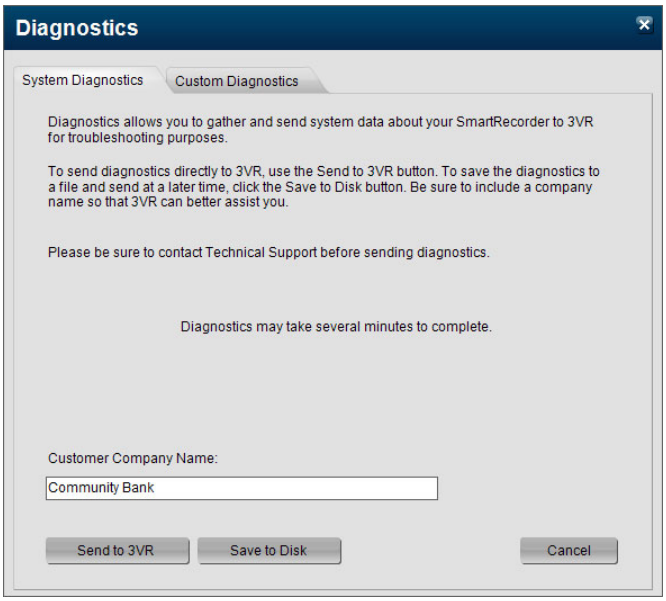
1. Launch 3VR System Manager.

2. In the **Configure** panel, right-click the system display name and select **System Diagnostics** from the menu.



DRAFT

3. In the **Diagnostics** window, type the customer name in the **Customer Company Name** box.



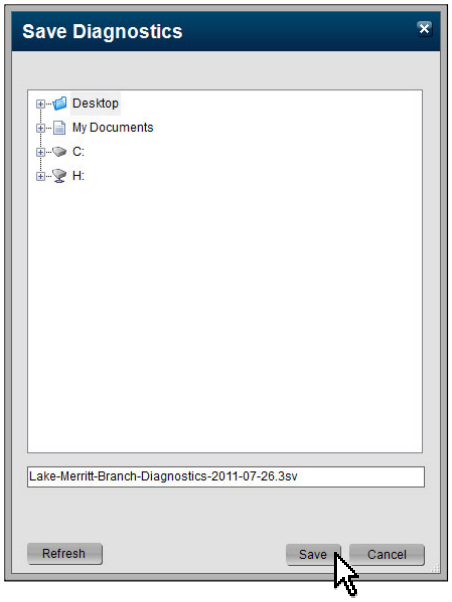
4. Choose a destination for the diagnostics export:

- If you wish to send the diagnostics directly to 3VR Technical Support, click **Send to 3VR**.
  Wait 3-5 minutes for the diagnostics to be generated and uploaded to 3VR.

  Important
  The 3VR system must have a working internet connection with valid DNS settings configured in order to send diagnostics to 3VR.

- To copy the files to your computer or a portable disk drive, click **Save to Disk.**
  Wait 3-5 minutes for the diagnostics to be generated.

  In the **Save Diagnostics** dialog box, navigate to the folder where you wish to store the diagnostics export. Select the folder and click **Save**.



DRAFT

5. If you exported the diagnostics to your computer or a USB drive, send the file to 3VR using the following steps:

   a. Open a web browser, such as Internet Explorer or Mozilla Firefox.

   b. In the address bar, type http://uploadlogs.3VR.com

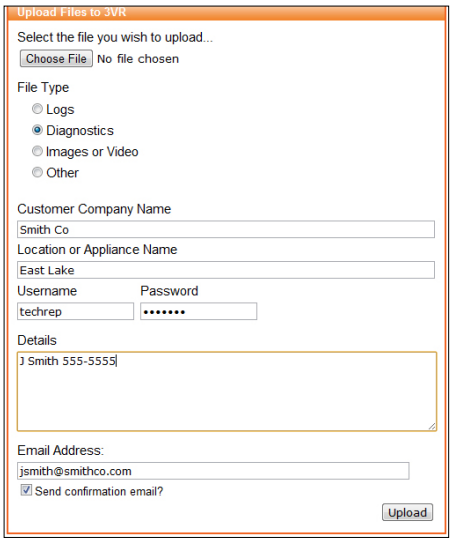
   c. Click **Choose File** and select the exported diagnostics file (extension .3sv).

   d. Select **Diagnostics** as the file type.

   e. Type the user name **techrep**, password **3MeDeee**.

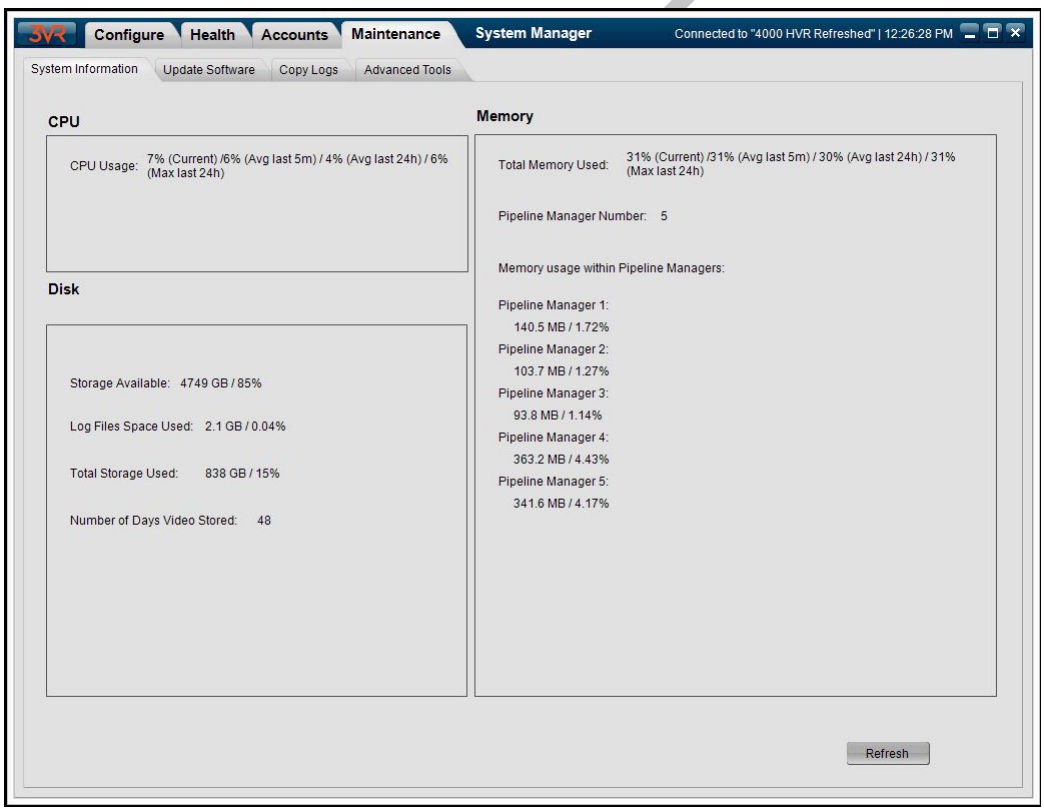
   f. Fill out the remaining fields with details of the installation.

   g. Click **Upload**. Make sure that you see the following message: "The file was successfully uploaded."



5.4 System Information (Fall Release-2015 (version 8.1.x and above) only)

The System Information tab provides a snapshot summary of the system's CPU, disk, and memory usage.



CPU

Provides a current snapshot of CPU utilization.

- Average in the last 5 minutes
- Average over the last 24 hours
- Max. over the last 24 hours

Disk

Provides information on total available storage, storage in use, and the number of days of stored video on the system. It also provides information on how much space log files use in the system.

Memory

Provides a current snapshot of memory usage.

- Average in the last 5 minutes
- Average over the last 24 hours
- Max. memory used over the last 24 hours

It also provides a summary of how many pipeline managers are running on the system and the memory used by each pipeline manager.

DRAFT

DRAFT

CHAPTER 13
Updating Software

1. UPDATING A SINGLE VMS SERVER 259
   - 1.1 Send Update Package 259
   - 1.2 Update VMS Server 260
   - 1.3 Update Client Applications 260
2. UPDATING AN ENTERPRISE - LIVE UPDATE 261
   - 2.1 Update Enterprise Server 261
   - 2.2 Update Your Client Applications 261
   - 2.3 Send Update Package to VMS Servers 262
   - 2.4 Update VMS Servers 263
   - 2.5 Update All Other Client Applications 264
3. UPDATING AN ENTERPRISE - SCHEDULED UPDATE 264
   - 3.1 Schedule Enterprise Update 264
   - 3.2 Schedule VMS Server Update 266
   - 3.3 Update Client Applications 267
4. UPDATING AN ENTERPRISE - MANAGING SCHEDULED UPDATES 267
5. UPDATING AN ENTERPRISE - MANAGING UPDATE PACKAGES 269
6. UPDATING PLUG-INS 271

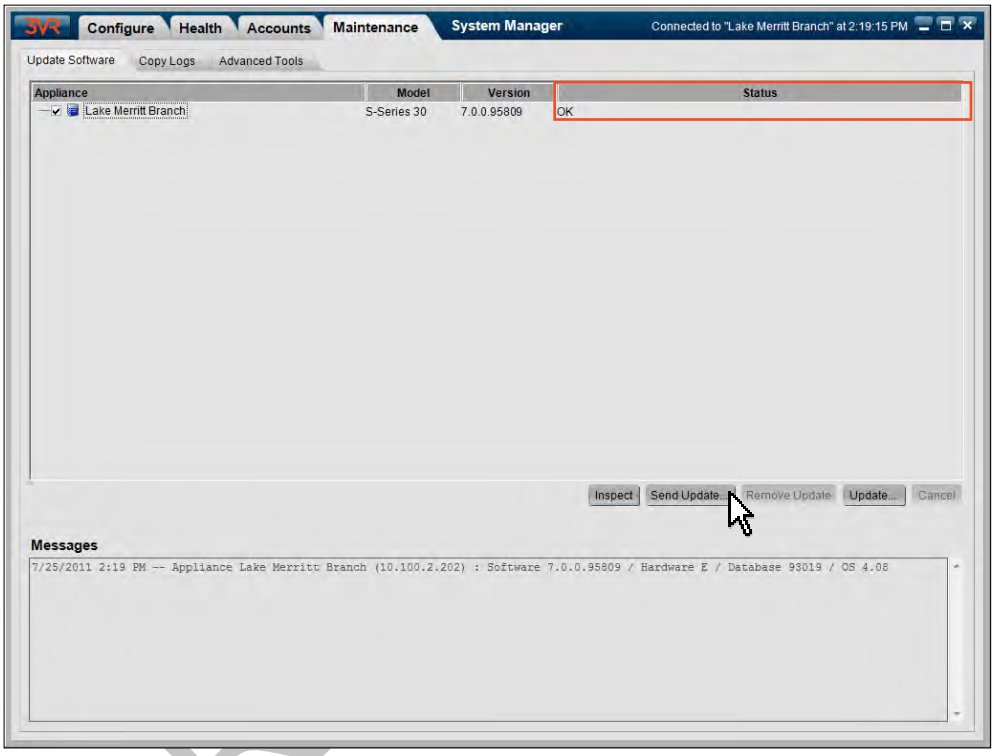
DRAFT

DRAFT

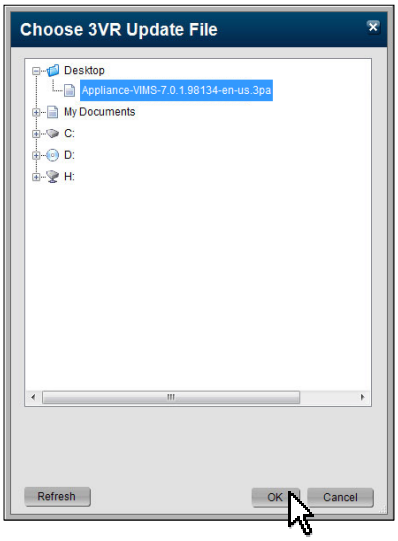
1. UPDATING A SINGLE VMS SERVER

Note
The steps in this section apply to software updates performed on a single VMS server. If you are connected to a 3VR Enterprise server and wish to update multiple VMS servers or the full Enterprise, please refer to section 2 of this chapter.

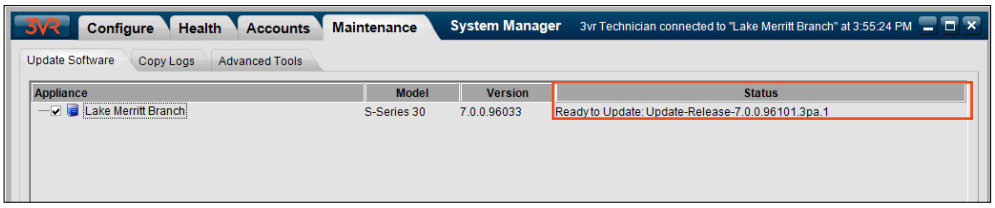
1.1 Send Update Package



1. In System Manager, click **Maintenance** to go to the **Maintenance** panel.
2. Click the **Update Software** tab.
3. Check the box next to the name of the VMS server to select it.
4. Click **Inspect**. Check the **Status** column to verify that the system is in a ready state:
   - "OK" is displayed if the system is operating normally and ready to be upgraded.
   - "Unauthorized" is displayed if the current user is not authorized to upgrade software on the selected server.
   - "Unreachable" is displayed if the system is not in a state where it can be upgraded.
5. Click **Send Update**.
6. In the **Choose 3VR Update File** window, locate the software update file, named **Appliance-VIMS-8.1.x.X.XXXXX-en-us.3pa** (where the Xs represent the software version and build number):
   - If you are connected to the 3VR appliance with a laptop or over the network, navigate to the drive on your computer where you have saved the unzipped 3VR download package. Browse to the update file and click to select it.
   - If you are connected to the 3VR appliance with a monitor, mouse, and keyboard, browse to the USB drive or CD containing the update file and click to select the file.



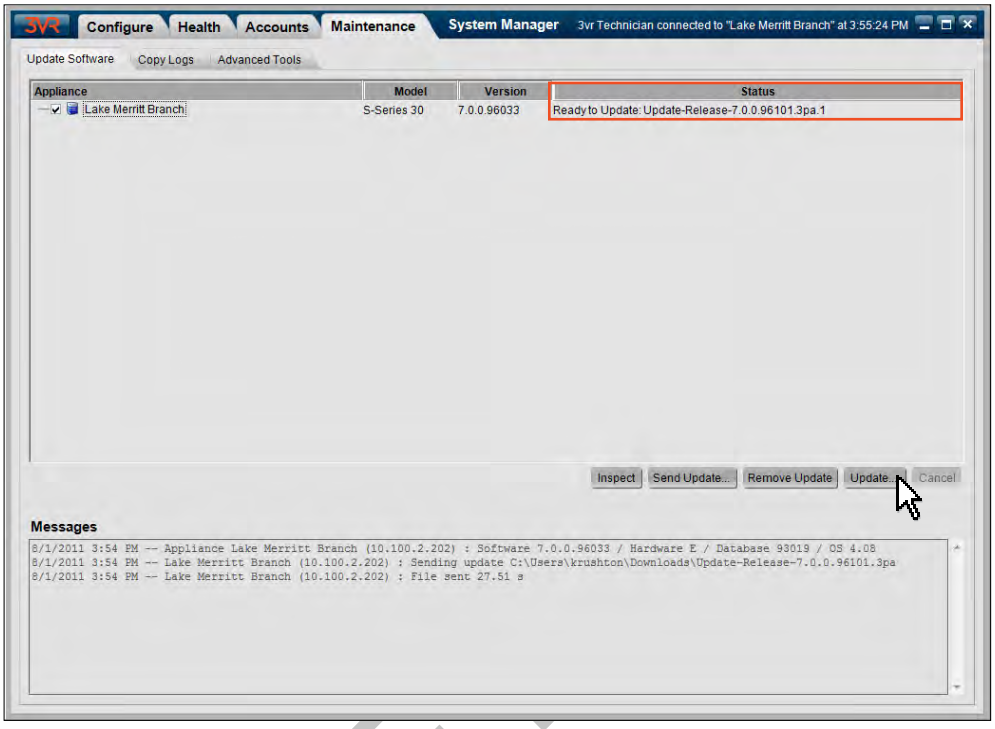
7. Click **OK**. System Manager transfers the selected update file to the VMS server. The **Status** column shows the status of the transfer as it progresses.
8. When the transfer is complete, the **Status** column for the VMS server shows "Ready to Update" with the name of the update file.



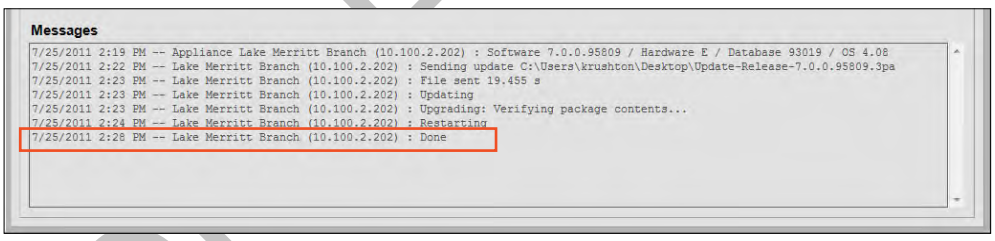
1.2 Update VMS Server

1. Click **Update**.

   The **Status** column shows the status of the update as it progresses.



2. When the update is complete, the **Messages** panel shows the VMS server's name and IP address followed by "Done."



1.3 Update Client Applications

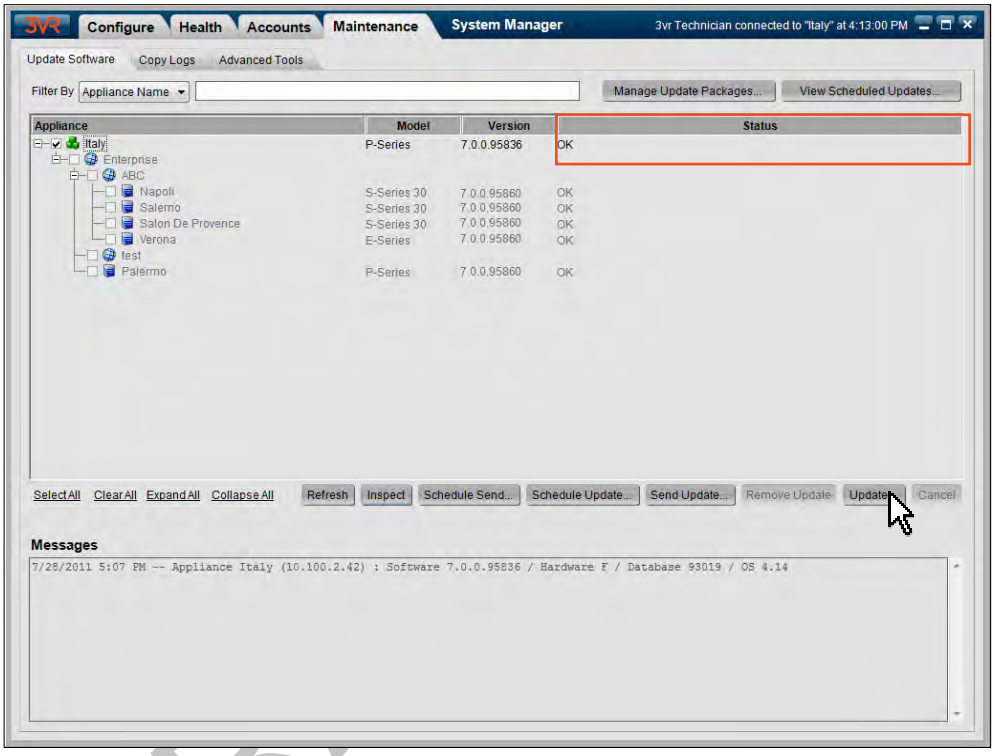
After you update the VMS server, 3VR recommends updating 3VR OpCenter, 3VR System Manager, and any other 3VR applications installed your PC using the 3VR Client Applications installation package that matches the new version. See the document *Installing and Upgrading 3VR Client Applications* for instructions.

2. UPDATING AN ENTERPRISE - LIVE UPDATE

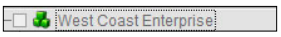
Perform the following procedure to upgrade the software on all VMS servers on a 3VR Enterprise. You should perform these steps if you wish to upgrade the Enterprise **immediately**. Please note that VMS servers are not accessible to remote users and do not record video while they are being updated. If you wish to schedule an update instead, see section 3 of this chapter.

2.1 Update Enterprise Server

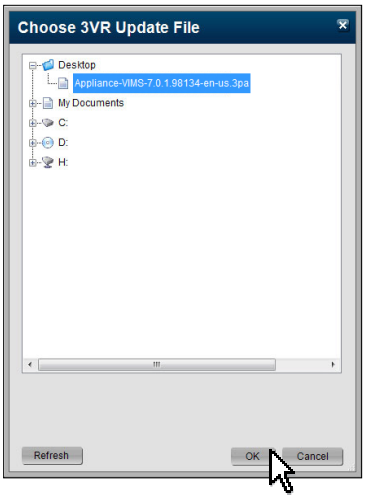
The first step in the upgrade process is to update the Enterprise server.



1. In System Manager, click **Maintenance** to go to the **Maintenance** panel.
2. Click the **Update Software** tab.
3. Check the box next to the Enterprise server. The Enterprise server is indicated by an icon with three green cubes:

4. Click **Inspect**. Check the **Status** column to verify that the system is in a ready state:
   - "OK" is displayed if the system is operating normally and ready to be upgraded.
   - "Unauthorized" is displayed if the current user is not authorized to upgrade software on the selected server.
   - "Unreachable" is displayed if the system is not in a state where it can be updated.
5. Click **Update**.
6. In the **Choose 3VR Update File** dialog box, locate the software update file, named **Appliance-VIMS-8.1.x.X.XXXXX-en-us.3pa** (where the Xs represent the software version and build number).
7. Click **OK**. After the 3VR Appliance receives the file, the update begins.
8. When the update is complete, the **Status** column displays "Done" next to the Enterprise server.
9. Close System Manager.



2.2 Update Your Client Applications

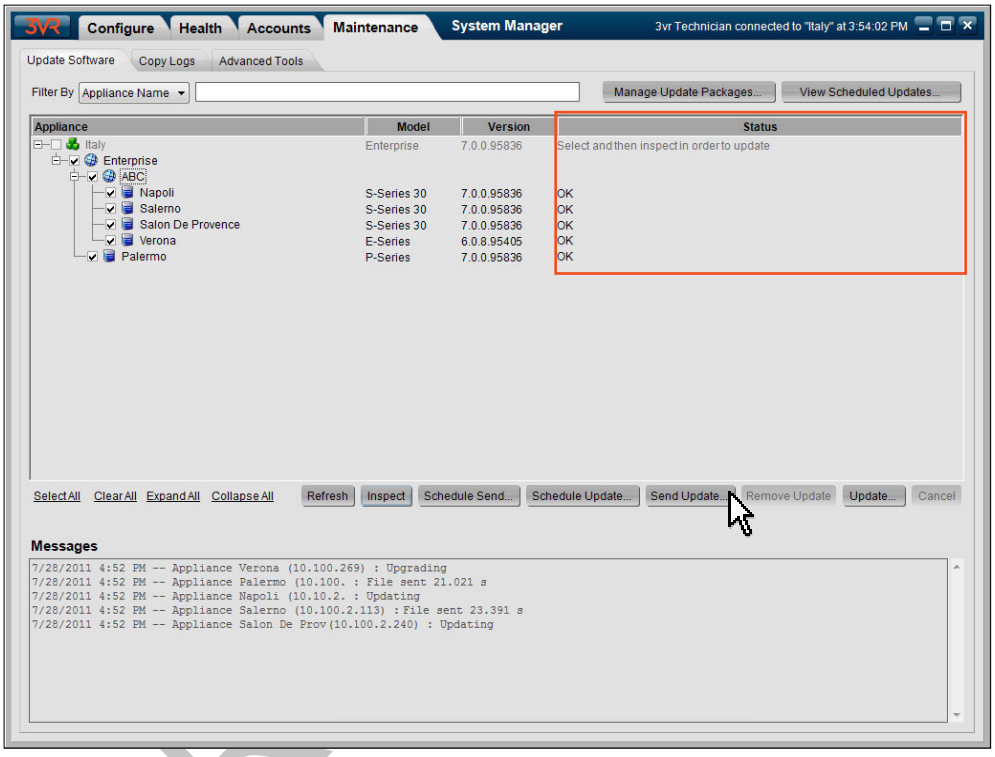
After you update the Enterprise server, 3VR recommends updating 3VR System Manager and any other 3VR applications installed on your PC using the 3VR Client Applications installation package that matches the new version of the 3VR Enterprise server. The update begins after you send the installation package files to the appliance. See the document *Installing and Upgrading 3VR Client Applications* for instructions.

Note: If you are connected to the Enterprise with a monitor, mouse, and keyboard, you may disregard this step.

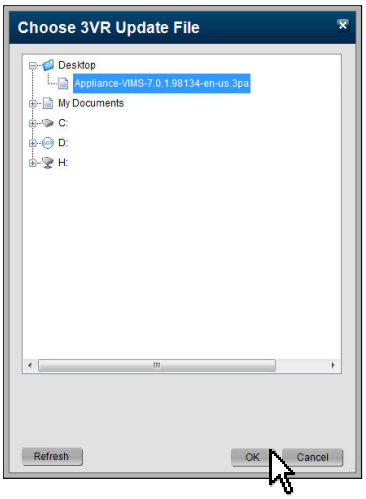
2.3 Send Update Package to VMS Servers

After updating the client applications on your PC, the next step is to transfer the update package to all of the VMS servers on the Enterprise.

1. Launch System Manager.
2. Click **Maintenance** to go to the **Maintenance** panel.
3. Click the **Update Software** tab.
4. Click Clear All to deselect the Enterprise server.
5. Click Select All to select all servers except the Enterprise.
6. Click **Inspect**. Check the **Status** column to verify that the VMS servers are in a ready state:
   - "OK" is displayed if the system is operating normally and ready to be upgraded.
   - "Unauthorized" is displayed if the current user is not authorized to upgrade software on the selected server.
   - "Unreachable" is displayed if the system is not in a state where it can be upgraded.



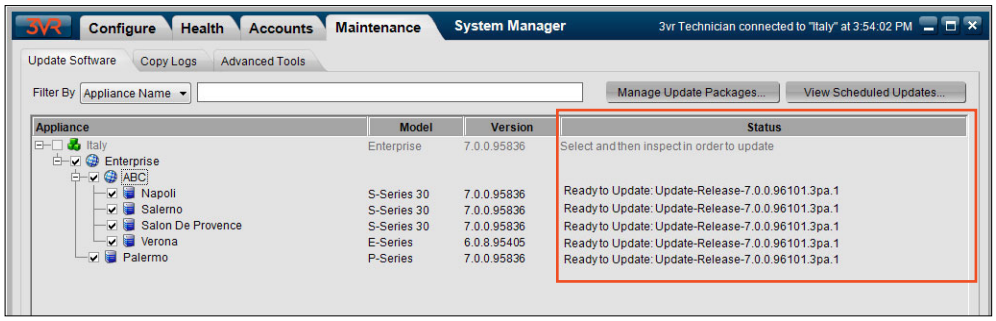
7. Click **Send Update**.
8. In the **Choose 3VR Update File** dialog box, locate the software update file, named **Appliance-VIMS-8.1.x.XXXXX-en-us.3pa** (where the Xs represent the software version and build number).



9. Click **OK**.

System Manager sends the update file to all of the VMS servers. The **Status** column shows the status of each transfer as it progresses.

When the send is complete, the **Status** column for the VMS server shows “Ready to Update” with the name of the update file for all VMS servers on the Enterprise.

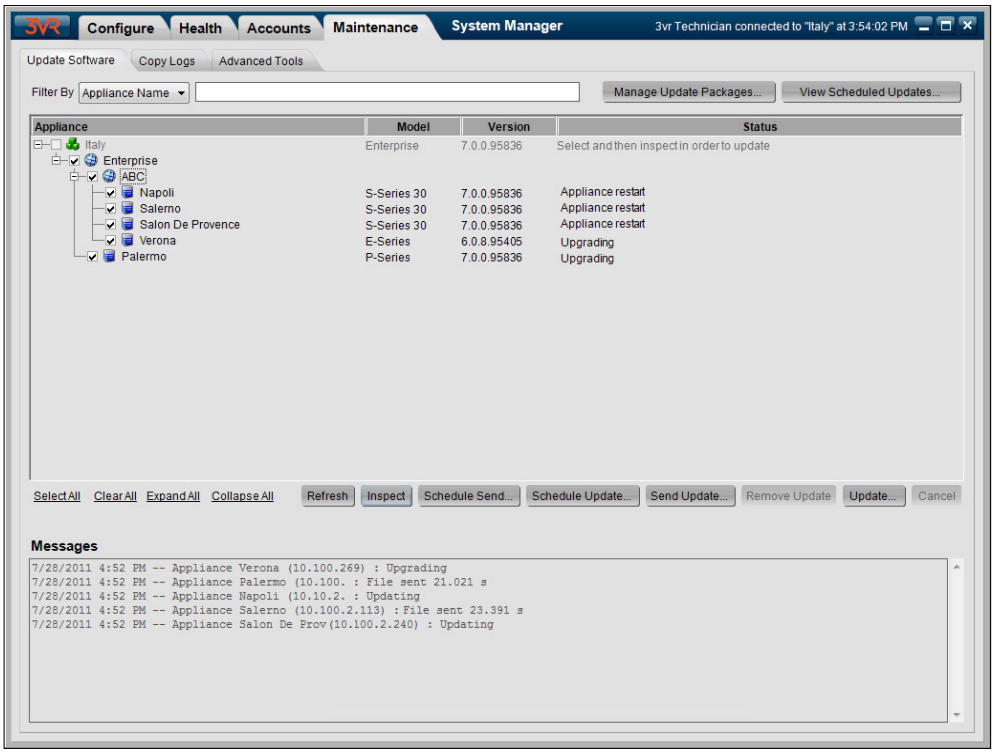


2.4 Update VMS Servers

1. Click **Update**. The update immediately begins processing on all servers.

   While the update is processing, the **Status** column shows the progress of the update for each server.

2. When the update is complete, the **Status** column displays “Done” for all servers.



2.5 Update All Other Client Applications

After you've updated the Enterprise, 3VR recommends updating 3VR OpCenter, 3VR System Manager and any other 3VR applications installed on your PCs using the 3VR Client Applications installation package that matches the new version installed on the 3VR Enterprise. See the document *Installing and Upgrading 3VR Client Applications* for instructions. 3VR recommends updating this software to take advantages of new product features.

3. UPDATING AN ENTERPRISE - SCHEDULED UPDATE

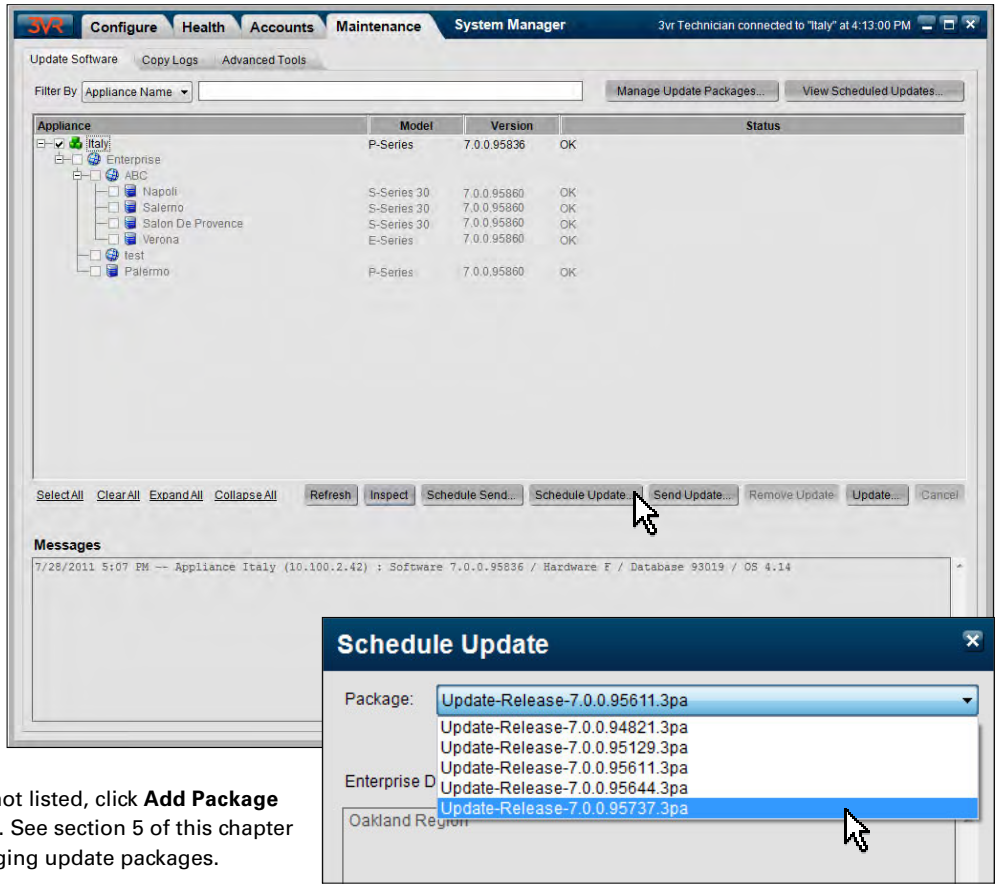
During a software update, a VMS server does not record video and cannot be accessed by remote users. Consequently, you may wish to perform a software update outside of normal business hours to minimize disruption to end users. The 3VR VisionPoint™ Enterprise server features the ability to schedule updates at a designated date and time.

Perform the following steps to schedule a software update on an Enterprise:

3.1 Schedule Enterprise Update

1. In System Manager, click **Maintenance** to go to the **Maintenance** panel.
2. Click the **Update Software** tab.
3. Check the box next to the Enterprise server. The Enterprise server is indicated by an icon with three green cubes:

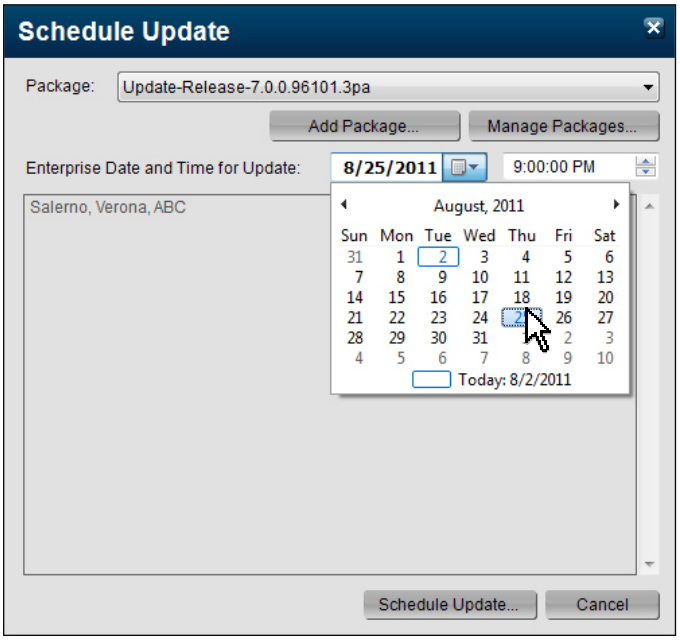
4. Click **Schedule Update**.



5. In the **Schedule Update** window, select the update package to use for the update from the **Package** drop-down menu.
   - If the update package is not listed, click **Add Package** and select the update file. See section 5 of this chapter for information on managing update packages.

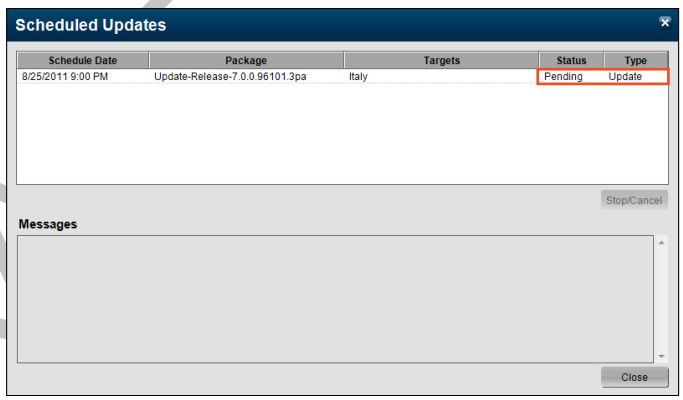
6. Specify the date and time the Enterprise update should occur.

7. Click **Schedule Update**.



8. System Manager opens the **Scheduled Updates** dialog box, showing that there is a pending update.

9. Click **Close** to return to the **Update Software** panel.



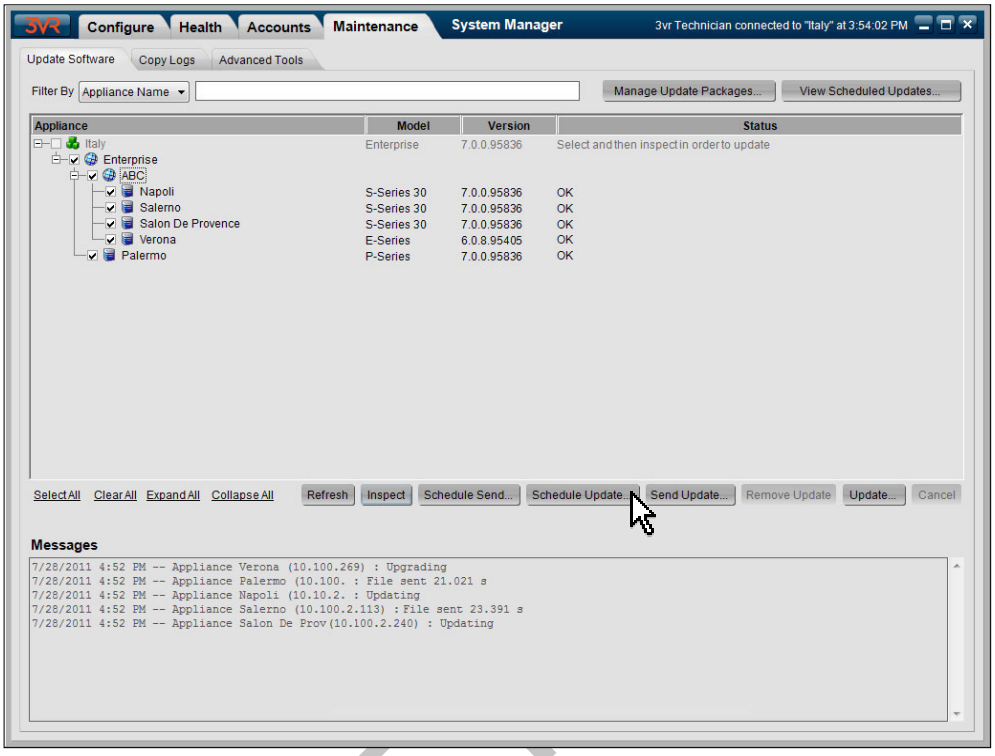
DRA

3.2 Schedule VMS Server Update

1. Click Clear All to deselect the VisionPoint™ Enterprise server.

2. Click Select All to select all servers except the Enterprise.

3. Click **Schedule Update**.

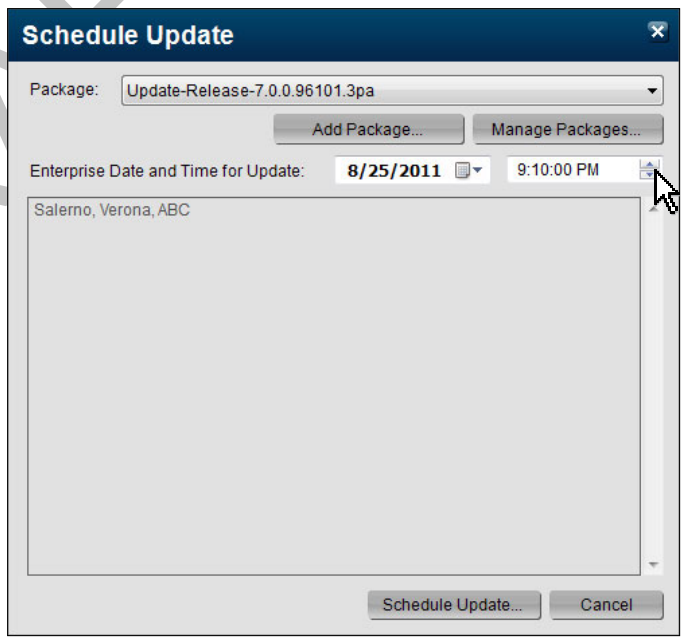


4. In the **Schedule Update** window, select the update package to use for the update from the **Package** drop-down menu.

   - If the update package is not listed, click **Add Package** and select the update file. See section 5 of this chapter for information on managing update packages.

5. Specify the date and time for the update. **You should schedule the VisionPoint™ VMS server update for 10 minutes after the Enterprise server update.** For example, if you schedule the Enterprise update for 9:00 PM, schedule the VMS server update for 9:10 PM (or later).

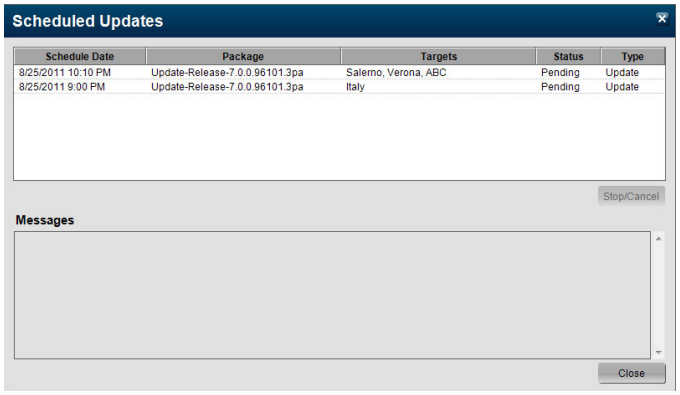
6. Click **Schedule Update**.



DRAFT

7. System Manager opens the **Scheduled Updates** dialog box, showing that there are now two pending updates, one for the Enterprise and one for its VMS servers.

8. Click **Close** to return to the **Update Software** panel.



3.3 Update Client Applications

After the scheduled updates have taken place, users who connect to the Enterprise server must update 3VR OpCenter, 3VR System Manager, and any other 3VR applications installed on their PCs using the 3VR Client Applications installation package that matches the new version. See the document *Installing and Upgrading 3VR Client Applications* for instructions.

4. UPDATING AN ENTERPRISE - MANAGING SCHEDULED UPDATES

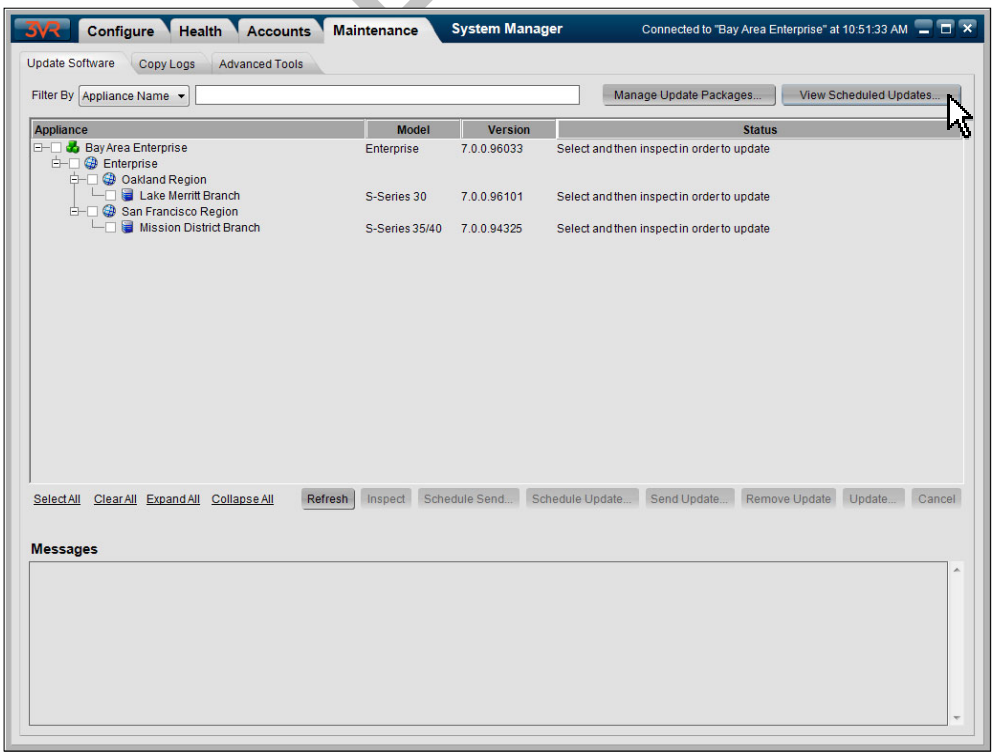
Perform the following steps to view pending and past scheduled updates:

1. In System Manager, click **Maintenance** to go to the **Maintenance** panel.

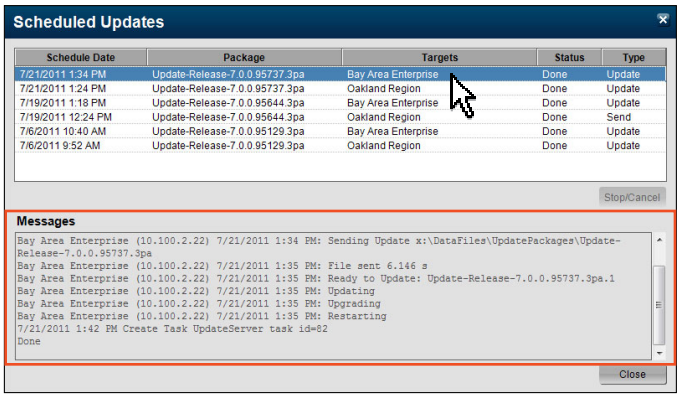
2. Click the **Update Software** tab.

3. Click **View Scheduled Updates**.

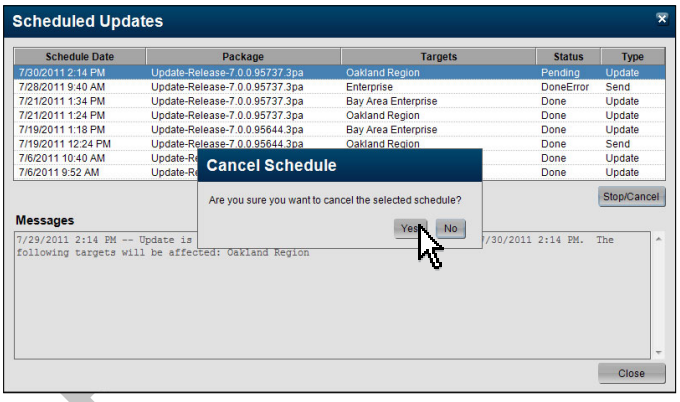
4. To view information about an update, select it from the list.



Details about the update appear in the **Messages** panel of the **Scheduled Updates** dialog box.



5. To cancel a pending update, select it from the list.
6. Click **Stop/Cancel**.
7. In the dialog box that appears, click **Yes** to confirm that you wish to cancel the scheduled update.



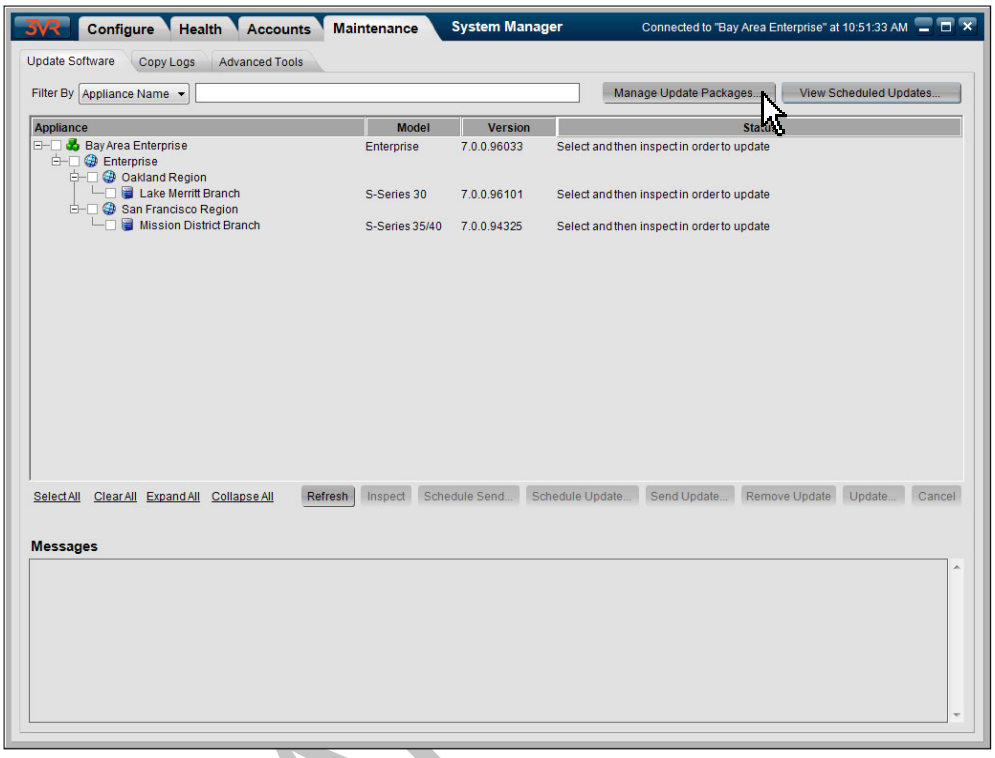
8. Click **Close** to close the **Scheduled Updates** dialog box and return to the **Update Software** tab.

DRAFT

5. UPDATING AN ENTERPRISE - MANAGING UPDATE PACKAGES

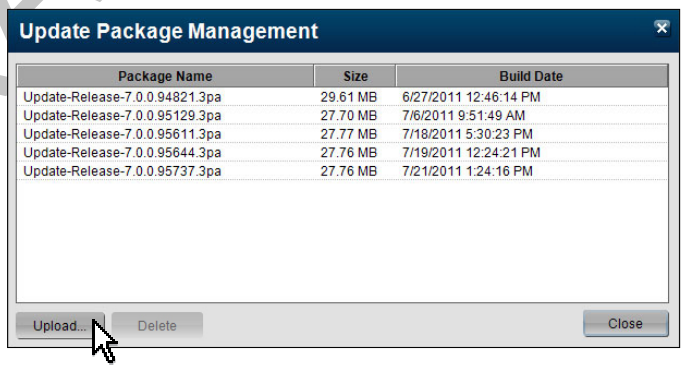
Perform the following steps to add or remove software update packages stored on a 3VR VisionPoint™ Enterprise server:

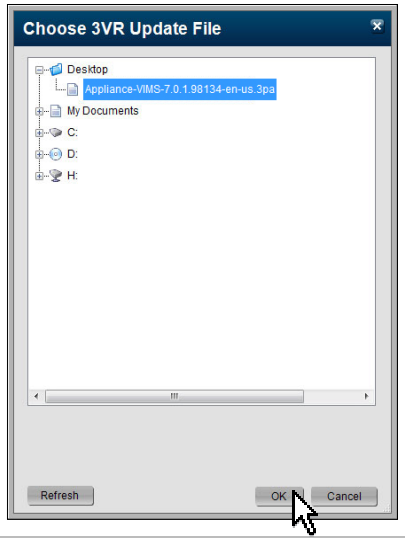
1. In System Manager, click **Maintenance** to go to the **Maintenance** panel.
2. Click the **Update Software** tab.
3. Click **Manage Update Packages**.



Adding a New Update Package

1. Click **Upload**.
2. In the **Choose 3VR Update File** dialog box, locate the software update file, named **Appliance-VIMS-8.1.x.X.XXXXX-en-us.3pa** (where the Xs represent the software version and build number).

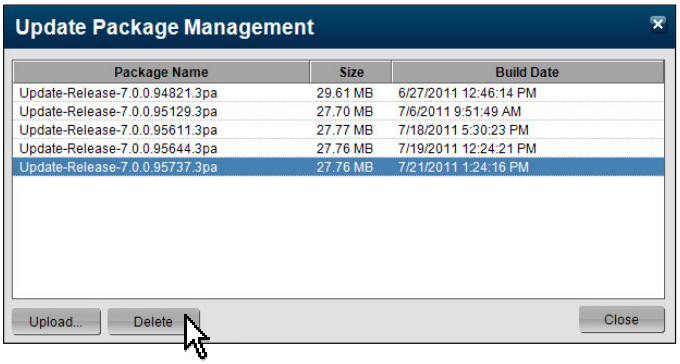




DRAFT

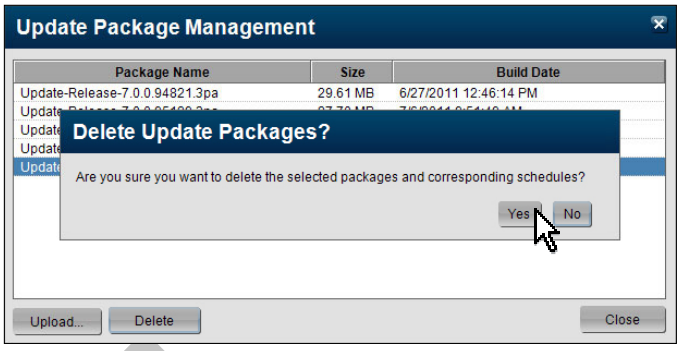
Deleting an Update Package

1. Select the package to delete.
2. Click **Delete**.



3. In the dialog box that appears, click **Yes** to confirm that you wish to delete the selected update package.

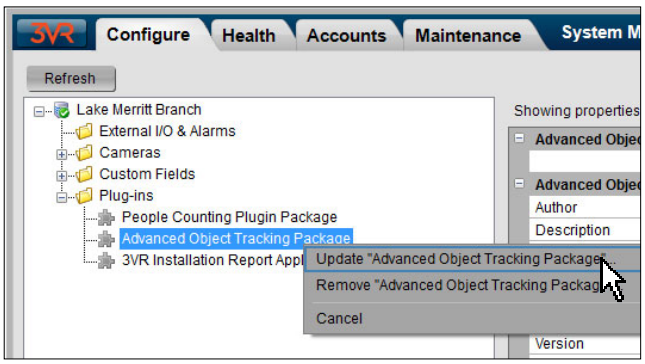
> **Warning**
> Deleting an update package also cancels any pending updates associated with the package.



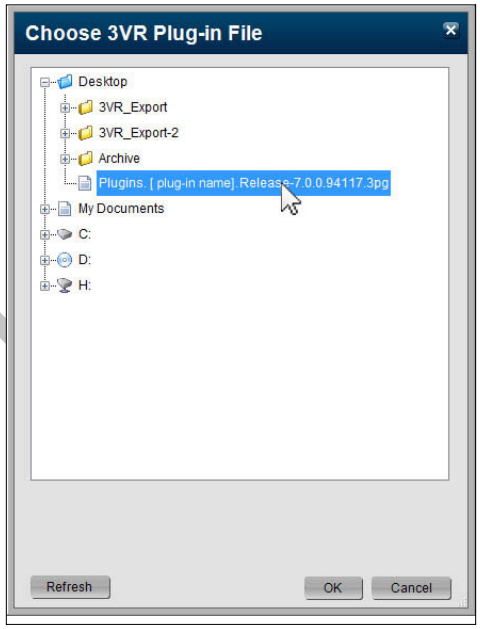
DRAFT

6. UPDATING PLUG-INS

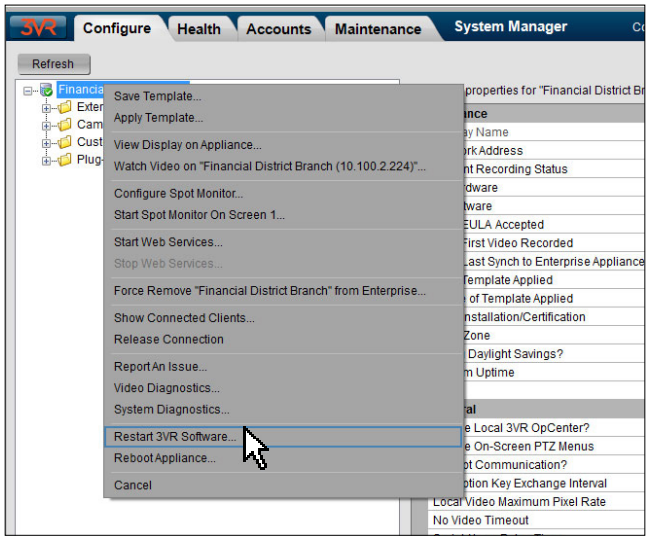
Perform the following steps to update a plug-in to a new version:



1. Launch 3VR System Manager.
2. In the **Configure** tab, click the plus sign (+) next to the system name to expand the list of configuration options.
3. Click the plus sign next to **Plug-ins** to display the list of plug-ins on the system.
4. Right-click the plug-in and select **Update "[Plug-in Name]"**.
5. In the dialog box that appears, click **Update** to acknowledge that you must restart the system software after upgrading the plug-in.
6. In the **Choose 3VR Plug-in File** dialog box, select the plug-in update file (extension .3pg).
7. Click **OK**.



8. To complete the update, right-click the system name and select **Restart 3VR Software** from the menu.
9. In the **Confirm** dialog box, click **Restart** to initiate the software restart.
10. Wait 1-2 minutes for the software to fully restart before proceeding.



DRAFT

DRAFT

CHAPTER 14
Field Upgradeable Storage

1. OVERVIEW 275
2. LIMITATIONS 275
3. BACKING UP SETTINGS 275
4. IDENTIFYING HARDWARE AND STORAGE TYPE 276
5. PLAN FOR RECORDING INTERRUPTION 277
6. BASIC PHYSICAL INSTALLATION 277
7. MODIFYING STORAGE 279
   - 7.1 5500-Series RAID - Adding a New Volume 279
   - 7.2 4000-Series and 5500-Series RAID - Replacing Existing Disks 280
   - 7.3 5500-Series Non-RAID - Adding New Disks 281
   - 7.4 4000-Series and 5500-Series Non-RAID – Replacing Existing Disks 283

DRAFT

DRAFT

1. OVERVIEW

As of version 7.2.2, 3VR supports upgrading the storage of 3VR appliances in the field. This chapter covers replacing existing drives with larger capacity drives and adding new drives to expand the storage capacity of both RAID and non-RAID 3VR appliances. (See section 4 for information about identifying your hardware model and storage type.)

Upgrading storage is a two-step process consisting of the physical installation of new drives followed by storage modification via the 3VR software. Please read through the hardware-specific instructions in section 7 for the specific model of appliance and type of upgrade you are performing before beginning the process.

If you are replacing a failed drive with another drive of the same size, please refer to the *3VR Hard Drive Replacement Guide*. The instructions in this chapter are intended only for upgrading the storage of a 3VR appliance.

Important
This information in this chapter applies only to 3VR appliances.

2. LIMITATIONS

- 3VR appliances require at least Enterprise-class hard drives with a minimum speed of 7200 RPM. Please check the Partner Support Portal or contact 3VR Technical Support for a list of currently recommended hard drive brands and models. Hard drives that have been upgraded in the field will not be covered under 3VR's hardware warranty.
- 3VR strongly recommends using new drives to upgrade storage. If you are re-purposing disks from a previous use, ensure they do not have any remaining data on them before continuing with the storage upgrade process, as old data on the disks can interfere with disk detection.

DRAFT

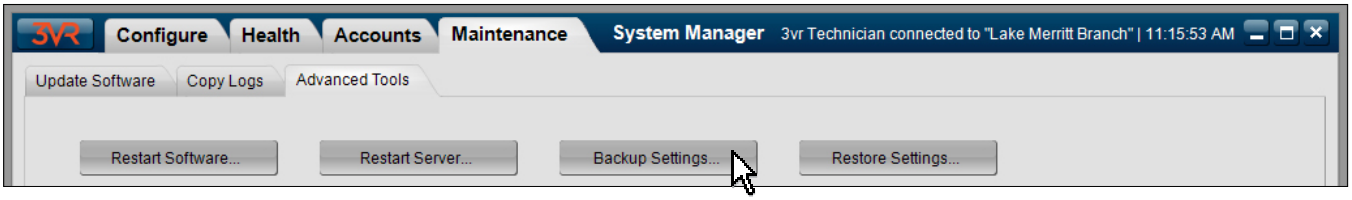
3. BACKING UP SETTINGS

When upgrading the storage on a 3VR appliance, some settings will be restored from the automatic backup files. If you are adding new drives, and not replacing existing drives, the system configuration, plug-in settings, and all media files will remain available after upgrading the storage. You will not need to restore them from the backup file.

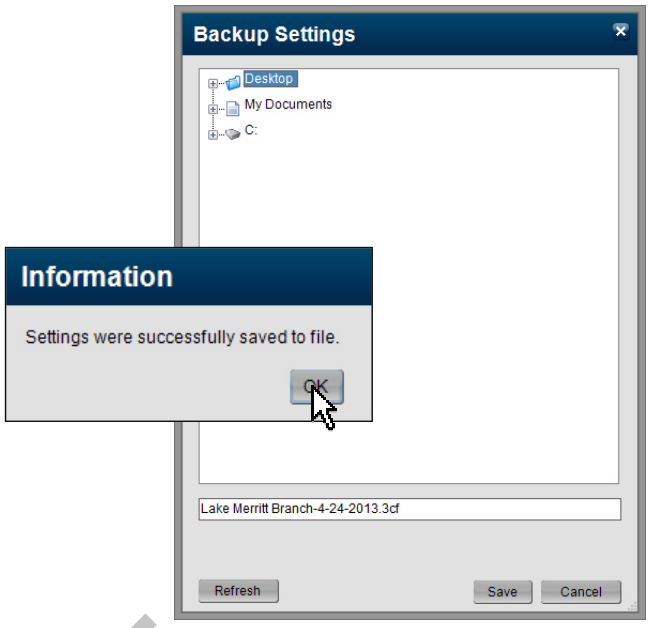
If you are replacing existing drives, the system restores configuration and system settings from its automatic backup files after the storage upgrade process is complete. All camera and system settings are restored from the automatic backup file after the upgrade with the exception of plug-in configuration and settings. Please take note of the existing plug-in configuration before beginning the upgrade and refer to plug-in specific documentation for more information about re-installing and reconfiguring plug-ins after the upgrade is complete.

As an extra safeguard, 3VR strongly recommends saving a manual settings backup file before beginning the storage upgrade process. To save a backup file:

1. Launch System Manager; connect directly to the appliance, not through the Enterprise, if applicable.
2. Navigate to the **Maintenance** tab.
3. Click **Advanced Tools**, and then click **Backup Settings**.



4. Select a location (not on the appliance itself) to save the backup file, and click **Save**.

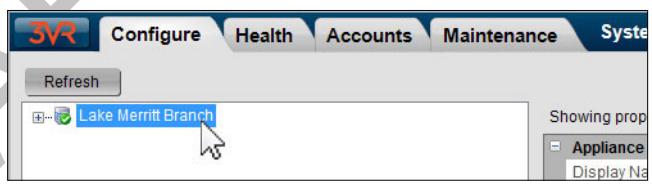


5. Wait while the settings are saved, and then click **OK**.

4. IDENTIFYING HARDWARE AND STORAGE TYPE

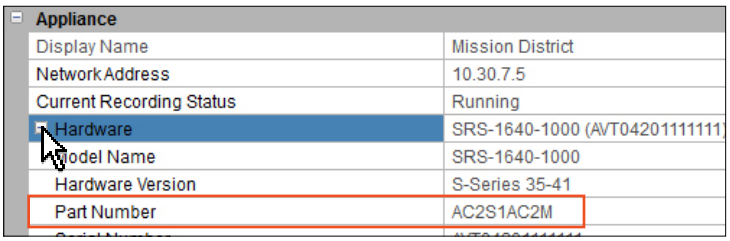
Depending on the model and storage type of the appliance, the procedure varies for replacing or adding drives and modifying storage. You can find the model and storage type of a given appliance in System Manager.

1. Launch System Manager and click on the appliance name to select it.



2. Click the plus sign next to **Hardware** in the right-hand panel to expand it.

   The **Model Name**, **Hardware Version**, **Part Number**, and **Serial Number** of the system are displayed.



3. Refer to the last two characters of the **Part Number** to find the number of disks and the storage type of the appliance.

   - A **2** in the second to last place indicates an appliance with 2 disks, and a **4** indicates an appliance with 4 disks
   - The final character will be either **M**, indicating mirrored (RAID) drives, or **N**, indicating non-mirrored (non-RAID) disks.

   Please refer to the table below for sample part numbers showing each possible configuration.

Hardware Version	RAID/Non-RAID	Sample Part Number
4000-Series	RAID	HC2X0FD**2M**
	Non-RAID	HC2X0FD**2N**
5500-Series	RAID	DD2X3FD**4M**
	Non-RAID	DD2X3FD**4N**

DRAFT

5. PLAN FOR RECORDING INTERRUPTION

When replacing an existing drive or volume with a larger one, the storage upgrade process should take about 15 minutes. During this time, the 3VR appliance will not be recording video.

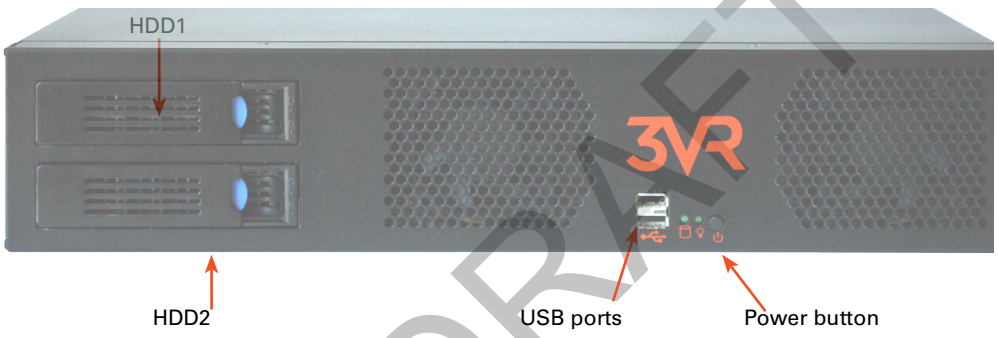
When adding new drives or volumes to a 3VR appliance, storage modification takes considerably longer than when replacing an existing drive or volume. Storage modification with new drives or volumes can take up to 30 minutes per terabyte, or up to 2 hours total. During this time, the appliance will not be recording video. Please plan ahead for this interruption in recording.

6. BASIC PHYSICAL INSTALLATION

Please contact 3VR Technical Support if you have any questions regarding the storage upgrade process. Follow the same instructions when performing installation on the 4000-Series and 5500-Series. Please note the 4000-Series is restricted to the use of its two drive bays.

Warning
It is important to read the appropriate hardware and configuration-specific storage modification instructions in section 7 **before** beginning the storage upgrade process.

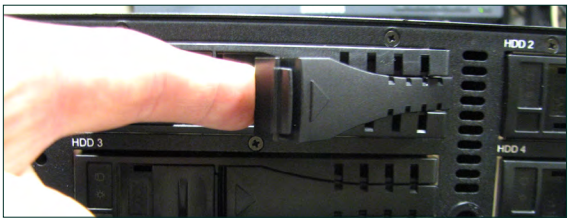
1. For the 4000-Series and 5500-Series Appliances, press the power button (4000-Series shown in the image below) once to power down the unit. Do not hold down the power button.



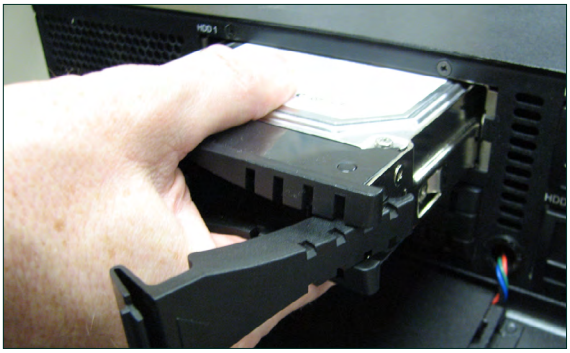
DRAFT

2. If replacing an existing drive, unlock the drive bay containing the drive you plan to replace. If adding a new drive, unlock the empty bay where you intend to install the new drive.

3. Unlatch the drive tray.



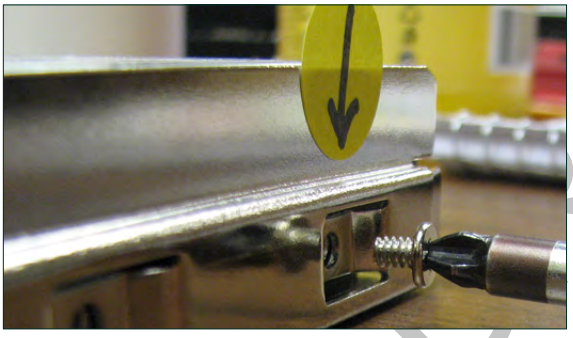
4. Slide out the drive tray.



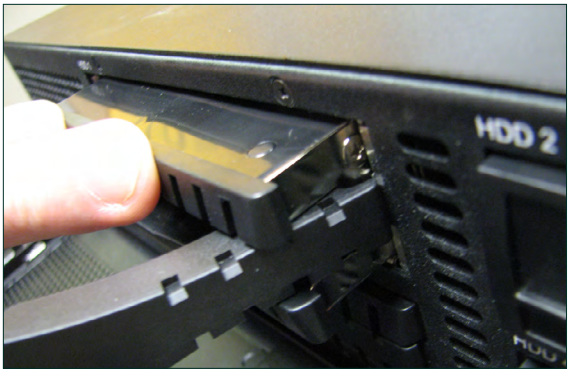
5. Remove the screws from both sides of the drive tray (four screws total).

6. If replacing an existing drive, swap out the existing hard drive for the replacement drive. If adding a new drive, place the new drive in the empty tray. In either case, ensure that the SATA interface of the new drive (inset) is positioned on the end opposite from the latch.

7. Replace the screws on the drive tray.



8. Insert the drive tray back into the drive bay and re-latch the tray.



9. Re-lock the hard drive bay.

10. Press or toggle the power button again (depending on the appliance model) to power on the unit and proceed to the appropriate step in section 7

DRAFT

7. MODIFYING STORAGE

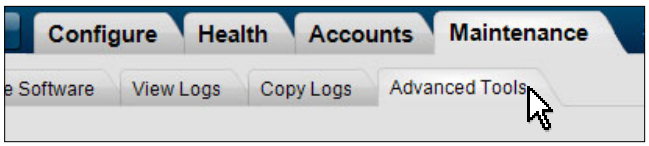
Follow the hardware-specific instructions in this section to add new drives to your 3VR appliance or replace existing drives with larger capacity drives.

7.1 5500-Series RAID - Adding a New Volume

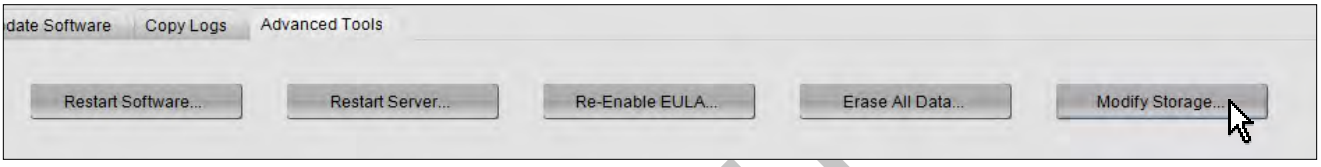
Since RAID disks mirror each other, depending on the current configuration of the appliance, you may choose either to add a new volume (two mirrored disks) or to replace an existing volume with a larger volume. This section covers adding a new volume. For more information about replacing an existing volume, continue on to section 7.2.

1. Install the new drives in the appliance according to the instructions in section 6.

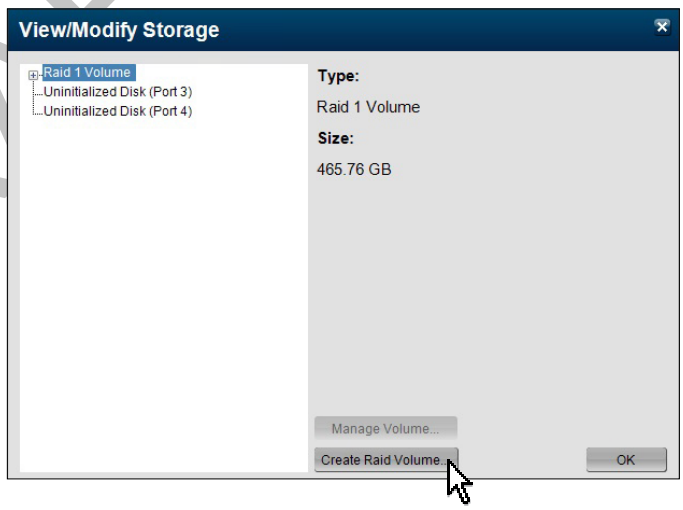
2. When the appliance boots up, launch System Manager and navigate to the **Maintenance** tab.



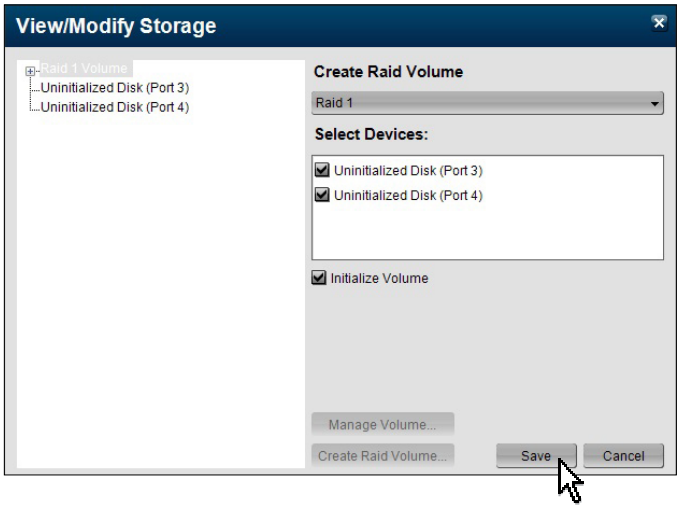
3. Click the **Advanced Tools** tab at the top, and then click **Modify Storage**.



4. Two uninitialized disks should appear in the left-hand panel of the **View/Modify Storage** dialog box. Click **Create Raid Volume**.



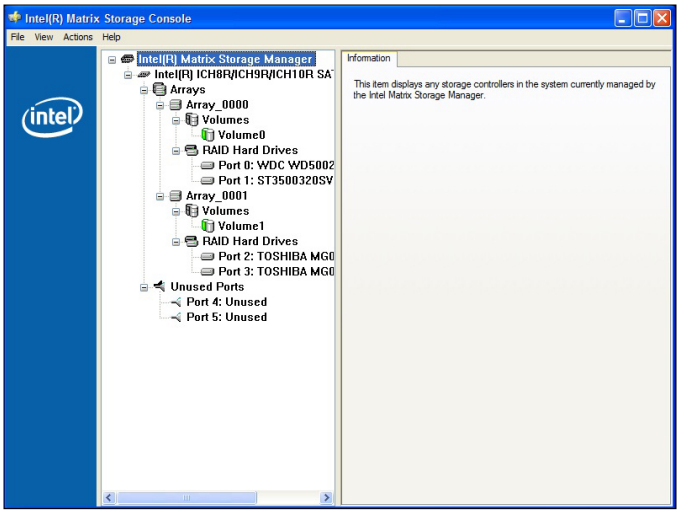
5. Check the box next to each disk name in the right-hand panel to select them, also check **Initialize Volume**.



DRAFT

6. Click **Save**, and then click **OK**.

7. Modifying the storage should take about two minutes. On a local monitor, the Intel Matrix Storage Console appears. During the automated storage expansion process, the mouse cursor may move and select a number of items on the screen. This is normal and should not be interrupted.



8. Once the RAID volume has been created, click **OK**. The system will reboot.

9. When the system returns from the reboot, the following messages appear on a local monitor.

Partitioning Disk	(less than 1 minute)
Formatting Volumes	(1-2 minutes)
Extending Database	(displays progress bar, 30 minutes per terabyte, up to 1 hour)

10. When the drive formatting is complete, the appliance automatically reboots. When the unit returns from this reboot, the storage upgrade process is complete.

11. When the storage upgrade process is complete, the appliance generates a **RAID/Disk Issue** health alert and begins rebuilding the RAID array.

DRAFT

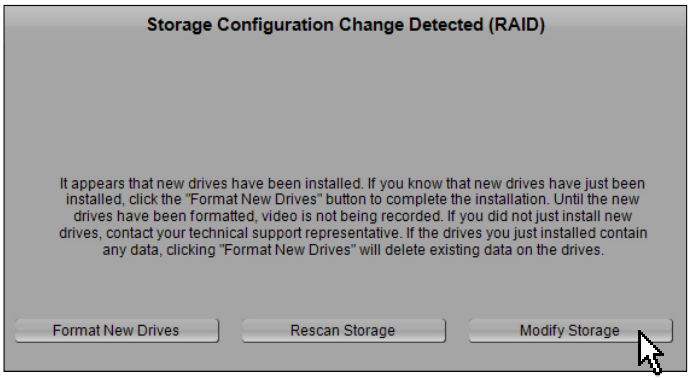
7.2 4000-Series and 5500-Series RAID - Replacing Existing Disks

1. Replace the existing drives according to the instructions in section 6.

2. If connected locally:

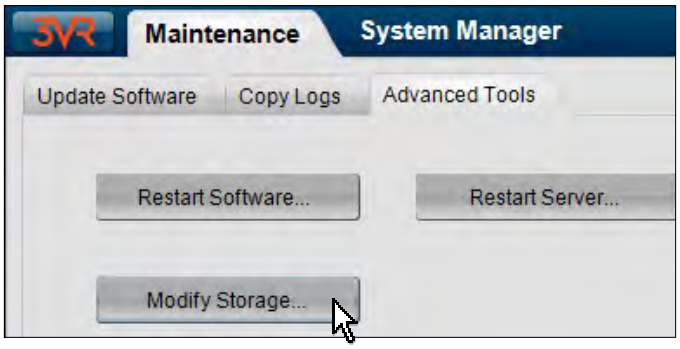
   - When the appliance boots up, a **Storage Configuration Change Detected** message appears on a locally connected monitor.

   - Click **Modify Storage**.



3. If connected remotely:

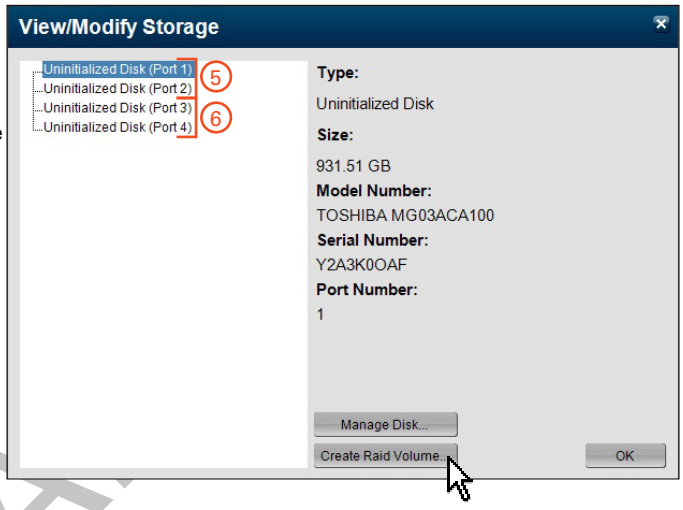
   - Launch System Manager in maintenance mode, and click the **Advanced Tools** tab.
   - Click **Modify Storage**.



4. In the **View/Modify Storage** dialog box, click **Create RAID Volume**.

5. Click **Uninitialized Disk (Port 1)** and **Uninitialized Disk (Port 2)**, to select them, and then click **Save** to create a new volume from these two disks. This process takes about two minutes.

6. When the first volume is created, click **Uninitialized Disk (Port 3)** and **Uninitialized Disk (Port 4)** to select them, and then click **Save** to create a new volume from these two disks.



7. Click **OK**. The system automatically reboots.

8. When the system returns from the reboot, the following messages appears on a local monitor (wait times in parentheses):

Partitioning Disk	(less than 1 minute)
Formatting Volumes	(1-2 minutes)
Starting Data Services	(1-2 minutes)
Creating Database	(2 minutes)

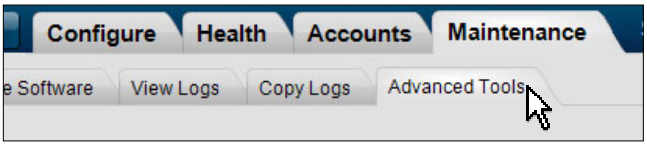
9. When this process has completed, the system automatically reboots. When the unit returns from this reboot, the storage upgrade process is complete.

10. When the storage upgrade process is complete, the appliance generates a **RAID/Disk Issue** health alert and begins rebuilding the RAID array.

7.3 5500-Series Non-RAID - Adding New Disks

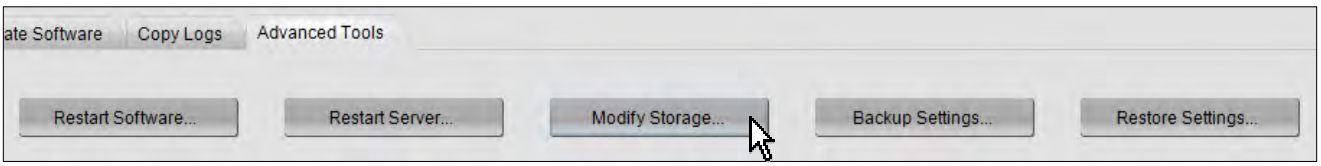
1. Install the new disk or disks, following the instructions in section 6.

2. When the appliance boots up, launch System Manager and navigate to the **Maintenance** tab. Click the **Advanced Tools** tab at the top.

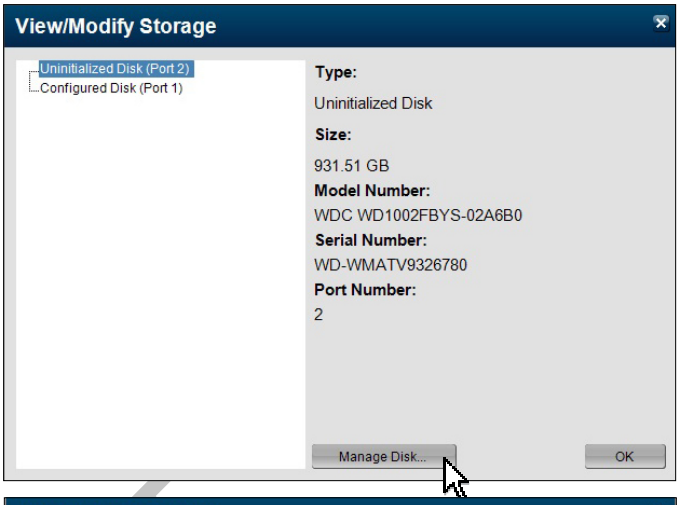


DRAFT

3. Click **Modify Storage**.

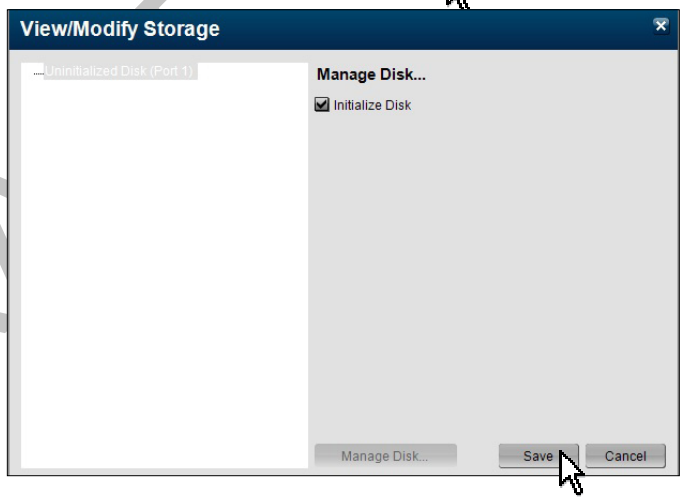


4. One or more **Uninitialized Disks** appear in the left-hand panel of the **View/Modify Storage** dialog box. Click the first uninitialized disk to highlight it, and then click **Manage Disk**.



5. Check the **Initalize Disk** box, and then click **Save**.

6. If there are remaining uninitialized disks, repeat steps 4 and 5 for each uninitialized disk. When all uninitialized disks are initialized, click **OK**.



7. Wait while the disk is formatted. This process may take up to one hour. While the drive is formatting, the following messages appear on a local monitor (wait times in parentheses):

Partitioning Disk	(less than 1 minute)
Formatting Volumes	(1-2 minutes)
Extending Database	(displays progress bar, up to 1 hour)

8. When the formatting process is complete, the appliance automatically reboots. When the unit returns from the reboot, the storage upgrade process is complete.

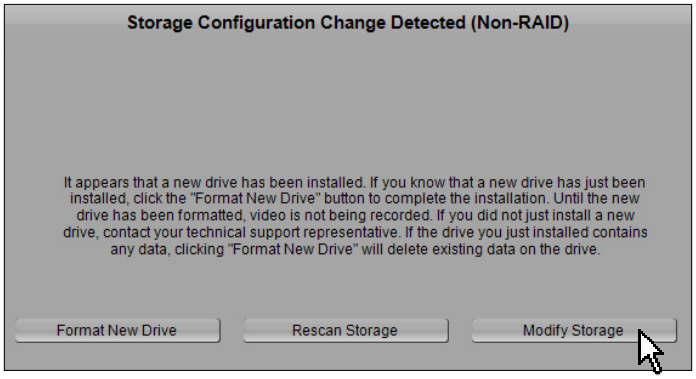
7.4 4000-Series and 5500-Series Non-RAID – Replacing Existing Disks

1. Replace disks according to the instructions in section 6.

2. If connected locally:

   - When the appliance boots up, a **Storage Configuration Change Detected** message appears.

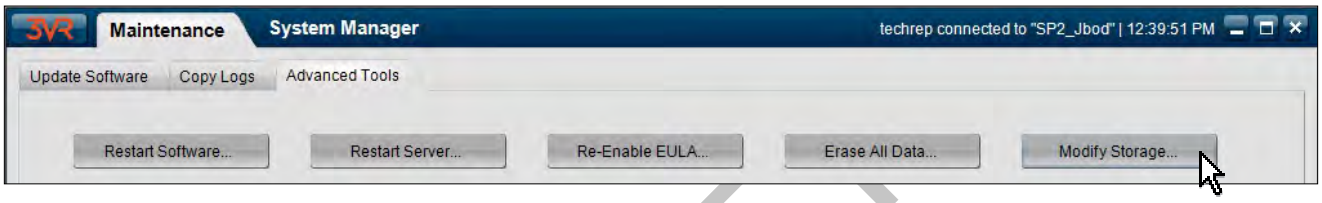
   - Click **Modify Storage**.



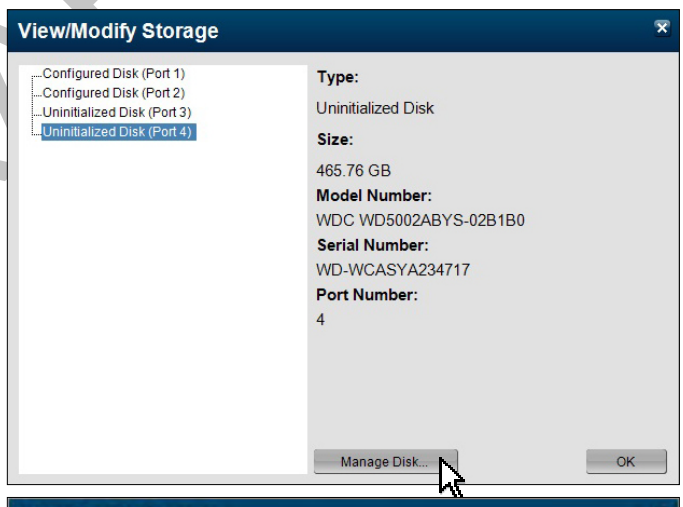
3. If connected remotely:

   - Launch System Manager in maintenance mode, and navigate to the **Advanced Tools** tab.

   - Click **Modify Storage**.



4. One or more **Uninitialized Disks** appear in the left-hand panel of the **View/Modify Storage** dialog box. Click the first uninitialized disk to highlight it, and then click **Manage Disk**.



5. Check the **Initialize Disk** box.

6. Click **Save**.

7. If there are remaining uninitialized disks, repeat steps 4 through 6 for each uninitialized disk. When all uninitialized disks are initialized, click **OK** in the confirmation window.

DRAFT

8. Wait while the new drive or drives are formatted. This process will take between five and ten minutes. While formatting is in progress, the following messages appear on a locally connected monitor (wait times in parentheses):

Partitioning Disk	(less than 1 minute)
Formatting Volumes	(1-2 minutes)
Starting Data Services	(1-2 minutes)
Creating Database	(2 minutes)

9. When formatting is complete, the system automatically reboots. When the unit returns from this reboot, the storage upgrade process is complete.

DRAFT

CHAPTER 15
Extended Storage Server

1. FUNCTIONAL OVERVIEW OF EXTENDED STORAGE SERVER 287
   1.1 About ESS 287
   1.2 Requirements 288
2. HOW TO CONFIGURE ESS 288
   2.1 Server-Side Configuration 288
   2.2 Client Configuration 290
   2.3 Health Alert 291
3. ESS INTEGRATION WITH OPCENTER AND ENTERPRISE SERVER 292
   3.1 OpCenter via Enterprise Server connecting to an Unavailable Appliance 292
   3.2 OpCenter via Enterprise Server Connecting to an Available Appliance 293
4. ESS ERROR CONDITIONS 294
   4.1 Error Conditions 294

DRAFT

DRAFT

1. FUNCTIONAL OVERVIEW OF EXTENDED STORAGE SERVER

Extended storage server (ESS) is a VMS or appliance machine that can be located on a private/public network to provide facility for other appliances/VMS servers to store and retrieve video data. You can use ESS to back up data from one or more appliances/VMS servers and place an ESS anywhere: within a private network or a public network (data center or any remote location).

1.1 About ESS

The bullet list below describes important ESS features.

- ESS can be an appliance or VMS server. It should preferably be a powerful system that contains substantial CPU power and storage.
- Provides support for 3VR clients (e.g.: OpCenter) to access data.
- Can access and view old video data captured from appliances.
- Extends the storage capabilities to beyond the local file system on the appliances.
- Minimizes data loss due to "data trimming" functionality in local appliance/VMS servers.
- Can store video data in either live or match mode.
- Enables OpCenter to access video from backups even when an appliance is not reachable.

You can use the **Client Extended Storage Setting** to perform backups based on a defined schedule. You can schedule backups immediately (for every minute), hourly, daily, or weekly. It is recommended to have bandwidth of 10 Gb or above if you need to transfer huge amounts of video data frequently between appliance(s) to the ESS. Moreover, use extra caution when choosing a system to serve as an ESS, especially on the storage side.

The local file system of an appliance will eventually lose data when disk space becomes full and "trimming" is triggered. ESS keeps the backup data until the specified threshold is reached.

ESS can support DAS (Direct Access Storage), NAS (Network Attached Storage), and SAN (Storage Area Network). For large storage (beyond 16TB or more), it is recommended to choose an NAS or SAN solution. For the SAN and NAS solution, system administrators of the ESS system need to map the network drive to a local drive of the ESS.

The ESS can act as a server and client at the same time. As an ESS, it can store data from various VMS servers. As a client, it can send its data to other Extended Storage Servers. You can use this approach to back up the data seamlessly to other high-end servers (that have more disk space) when an ESS is filled up and running short of disk space.

DRAFT

How ESS Works

In general, when an appliance is up and running, to play back video from an appliance, OpCenter connects to the appliance and requests video/audio data. In return, the appliance passes video/audio data, if that data is available in its local file system. If an appliance does not have the video/audio data, but has a backup in ESS, then the appliance gets the requested data from ESS and sends it to the 3VR client OpCenter application .

Normally, when an appliance is offline/not reachable, OpCenter is not be able to get data if it directly tries to connect to the offline appliance. However, with ESS, when OpCenter connects via Enterprise Server to an appliance that is offline, if the offline appliance's data is backed up in ESS, OpCenter can get the videos from ESS. (For OpCenter to get data for an "offline appliance," it needs to connect through Enterprise Server to play the video.)

OpCenter (via Enterprise Server) works in "normal mode" when it's initially connected to an appliance that is up and running. At the same time, it can display video from ESS for the appliances that are offline.

OpCenter (via Enterprise Server) works in "restricted mode" when it's connected to an offline appliance this is connected to an Enterprise Server. Data comes from ESS during "play back" (if the appliance data is on the ESS) and is denoted by the "E" symbol in OpCenter. During "restricted mode," only play back is allowed in OpCenter.

ESS stores server data for different appliances in different folders in order to improve data security. For security purposes, folder names are encrypted (meaning that they don't have real appliance names). A "Readme.txt" file stores the real name of the appliance. For example, for an appliance named "691aab18-bf4f-4218-af82-457acfdf965d," Extended Storage Server stores this appliance's data in a folder named "D:\newtest\ExternalStorageServer\691aab18-bf4f-4218-af82-457acfdf965d". a Readme.txt file in "D:\newtest\ExternalStorageServer\691aab18-bf4f-4218-af82-457acfdf965d" contains the real appliance name from which the data is imported in Extended Storage Server.

How the Tape Storage Feature Works (Tape Storage feature available Fall Release-2015 (8.1.x and above) only)

The tape storage feature allows you to save video to tape via the Quantum tape storage server. The basic topology is the 3VR Enterprise server connects to one or more 3VR appliances/3VR VMS servers (referred collectively here as "3VR VMS servers"). The 3VR VMS servers connect to Extended Storage Servers. Typically, a Quantum tape storage server connects to one or more Extended Storage Servers. Each Quantum server contains hard disk storage, on which it stages video from the 3VR VMS server. The hard disk on the Quantum server is mounted as a logical drive on the ESS. The Quantum server's hard disk contains two folders: "managed" and "unmanaged." Video sent to the ESS goes first to the unmanaged folder on the Quantum server. It remains in this folder until a user-defined threshold is reached. After this threshold is reached, the system places the video into a tar file and moves it into the managed folder. The Quantum server software then moves the tar files in the managed folder to tape and tracks their locations. See the *VisionPoint VMS User Manual* for information on viewing stored video.

1.2 Requirements

To use the ESS functionality, upgrade 3VR components, including the Enterprise Server, appliance (core), and ESS to the latest 3VR software version. If any of these 3VR components are on an older version of the 3VR software, users will not be able to use ESS functionality. However, using older versions of the above-specified 3VR components should have no affect on other 3VR functionality.

2. HOW TO CONFIGURE ESS

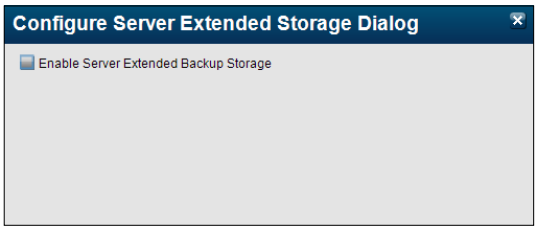
Extended Storage Server requires configuration on both the server side and the client side. ESS is the server and therefore you perform server-side configuration on the ESS side. You perform client-side configuration on the appliance/VMS server to which you plan to connect and use ESS.

DRAFT

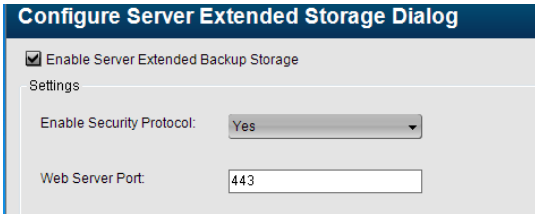
2.1 Server-Side Configuration

You can back up data to a local or shared network folder. Alternatively, you can back up to a Quantum tape storage server. The available options vary depending on the selected backup type.

1. On the ESS, launch System Manager.
2. Click on the appliance name. Then click **Common Operations** and select **Server Extended Storage Setting**. The Configure Server Extended Storage dialog box appears.
3. By default the **Enable Server Extended Backup Storage** check box is disabled. Check this box to enable ESS.



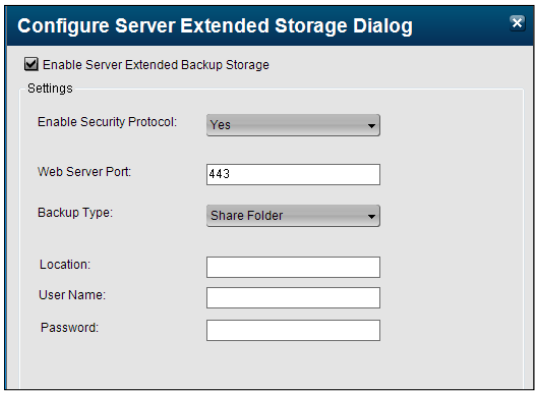
4. It's recommended to set **Enable Security Protocol** to **Yes**. Enter the correct the Web server port number as needed.



Shared or Local Folder Backup

Perform the steps below to back up to a shared or local folder.

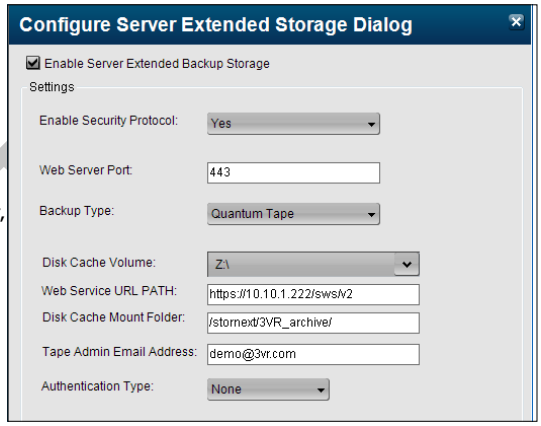
1. Select **Shared Folder** to back up to a shared, network folder. Select **Local** to back up to a local folder.



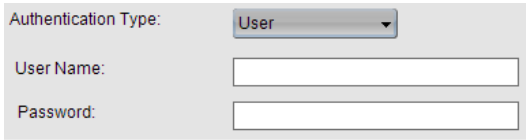
   - The local folder can be from a local file system or a mapped drive used to point to NAS or SAN servers.
   - When using the **Shared Folder** option, specify a network folder to directly store data in a network shared location (for example, D:\backups). Make sure you provide the login/password credentials to access the network drive. Also, make sure you have permission to access the network folder with the specified login and password. To access a network drive, it is recommended to run "3VR service" with administrator privileges. Be aware that the network access feature depends upon user access privileges provided or controlled by the local Windows operating system environment used for the ESS.

Quantum Tape Storage Server Backup (Fall Release-2015 (8.1.x and above) only)

Perform the steps below to back up to a Quantum tape storage server.

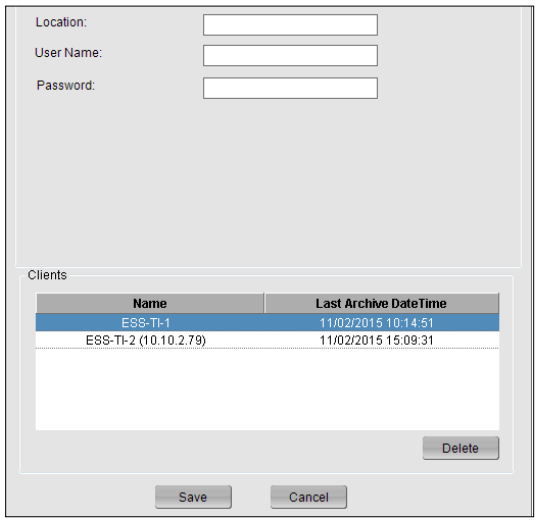


1. Select **Quantum Tape** to back up to a Quantum tape server. The Quantum tape backup features appear.
2. Select the **Z:** drive for the **Disk Cache Volume**.
3. Enter the web service URL path. Typically, this information is provided by the system integrator and is the IP address assigned to the Quantum server, along with the correct folder path.
4. Enter the disk cache mount folder path. This is the folder on the Quantum server that holds the managed and unmanaged folders. Typically, this information is also provided by the system integrator.
5. Enter the email address of the person responsible for administering the Quantum tapes in the **Tape Admin Email Address** field.
6. To use authentication, select **User** from the Authentication Type drop-down menu.



   a. Enter the username and password of a user on the Quantum server authorized to administer the system.

   - The Clients section lists appliances/VMS servers that are using ESS to store and retrieve data. An administrator can decide to delete a client's (appliance/VMS server) backup files on a destination server if that client has been inactive for a long time.

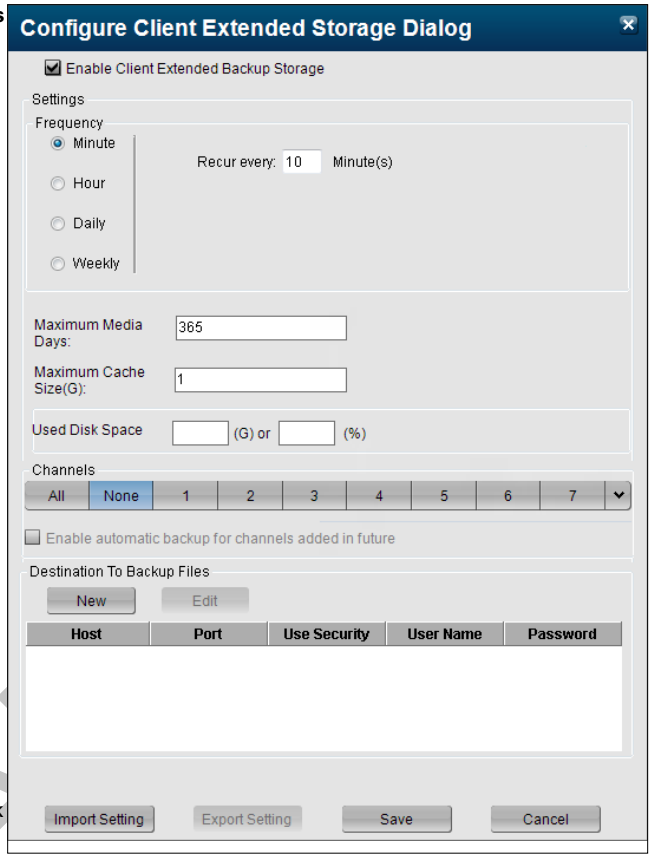


DRAFT

2.2 Client Configuration

1. From the client appliance/VMS server, launch System Manager.

2. Click on an appliance name. Then click **Common Operations** and select **Client Extended Storage Setting**.



   - The **Enable Client External Backup Storage** feature is disabled by default. Check this box to enable this feature. The associated options appear.

   - The **Frequency** options define the frequency at which video files are backed up on ESS from the client machine. You can define the frequency in terms of minutes, hours, daily, and weekly.

> **Note**
> **The system currently only supports video file backup and retrieval to and from ESS.**

   - **Maximum Media Days** defines the maximum number of days to store the video files (pertaining to the client) on the ESS. After the defined maximum number of storage days, the video content pertaining to the client is removed from ESS.

   - **Maximum cache size** defines the maximum cache space to allocate in the client. You can specify a value from 1GB to 1TB and customize it according to client storage capability.

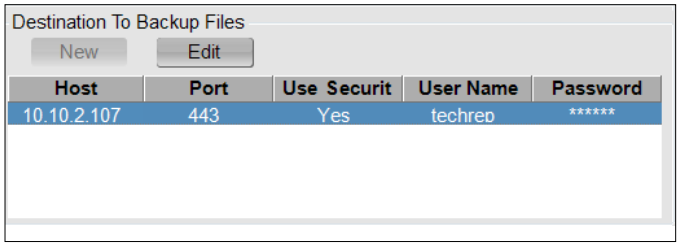
   - **Used Disk Space** specifies the maximum amount of disk space to store on the ESS.

> **Note**
> **When using tape storage, the above parameters define the thresholds for moving video from the unmanaged folder to the managed folder on the Quantum server .**

   - Select the buttons for the channels you want to back up. Select **All** to back up all channels. Optionally, check the **Enable automatic backup for channels added in the future** box to automatically back up channels added in the future.

   - Click the **Destination to Backup Files** button to define Extended Storage Server details:

     - IP address (host) of the ESS
     - Web server port number
     - Security setting
     - User credentials to access ESS.



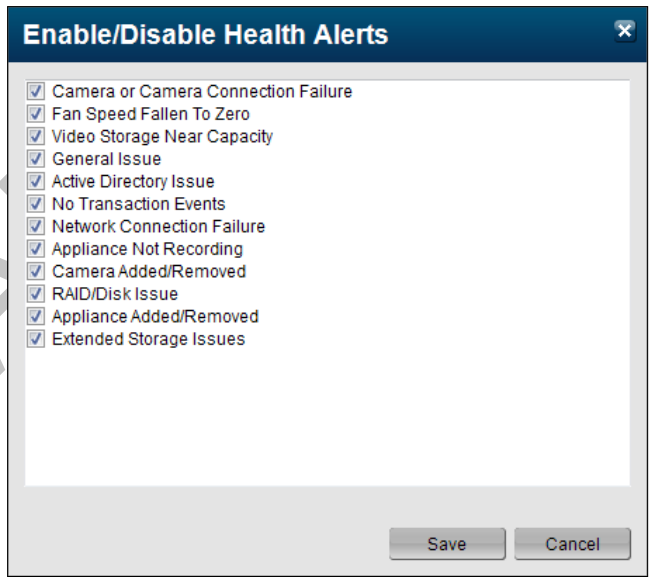
2.3 Health Alert

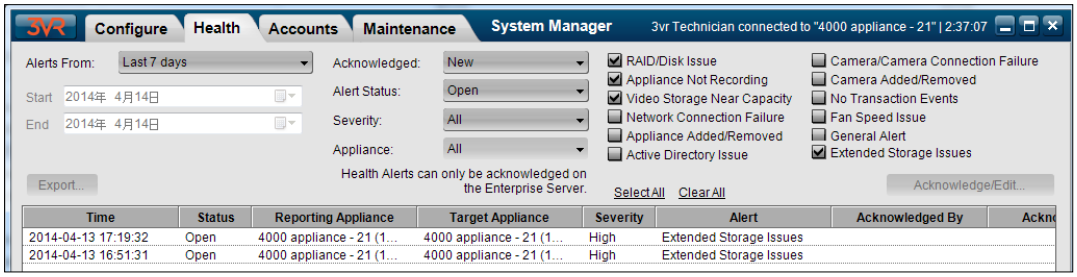
Extended Storage Server related issues can be a part of “health alert” mechanism provided by 3VR and following are the “health alerts” generated for the “Extended Storage Server” category.

- Insufficient available free space on the ESS.
- Invalid Share Folder provided for storing data.
- Invalid Backup Drive path.
- The web server ( ) cannot start.
- No request received from client for an extended period of time. (The default number of days is 30, meaning if a client did not send a request to the ESS, a health alert will be generated to remind you that you might need to delete related data of a possibly dead client.)

Perform the following steps to enable or disable health alerts:

1. Log in to System Manager as an **Administrator** or **Integrator** user.
2. Select the name of the appliance in the left panel.
3. In the right panel, scroll down to the **Health Monitoring** section and select **Enable/Disable Health Alerts**.





3. ESS INTEGRATION WITH OPCENTER AND ENTERPRISE SERVER

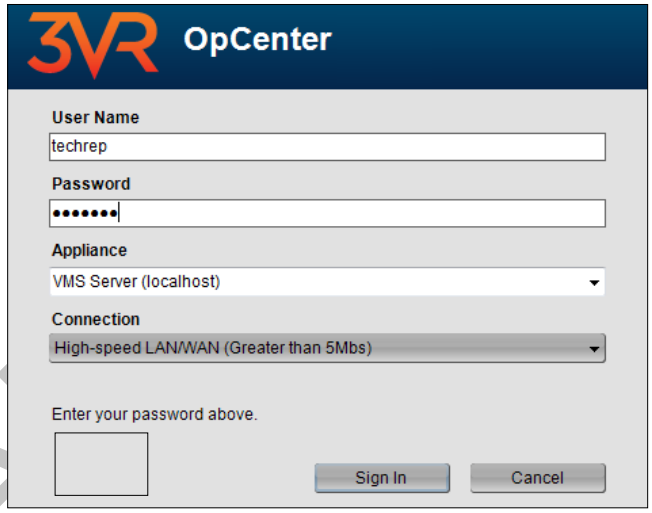
ESS integration with OpCenter helps users to watch videos in OpCenter when appliances are offline, broken, stolen, or unreachable. To watch video, OpCenter needs to be connected to the Enterprise Server. This feature is very useful when an appliance is unavailable.

3.1 OpCenter via Enterprise Server connecting to an Unavailable Appliance

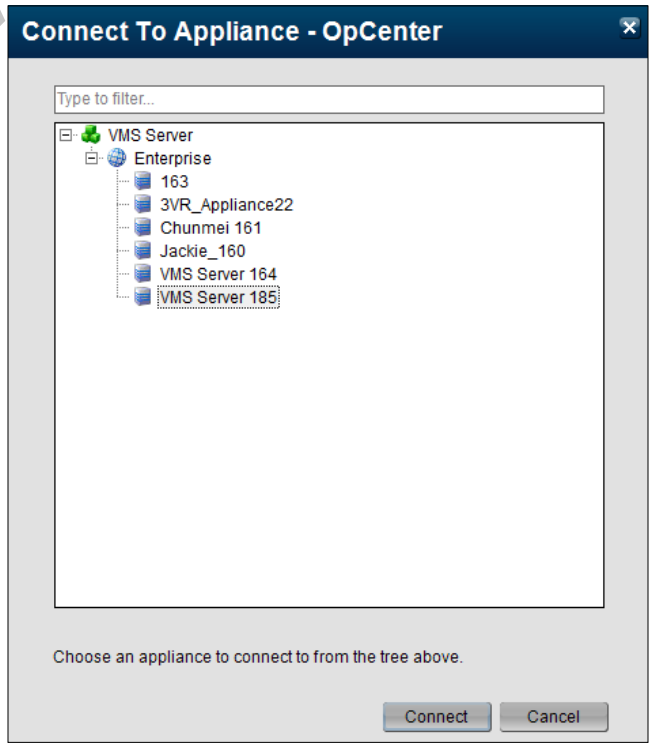
When OpCenter is connected to an unavailable/ or broken appliance via the Enterprise Server, OpCenter works in **Restricted Mode**. At this time, OpCenter gets the data from the **ESS** (if the appliance has a backup in the ESS). This is denoted by **"E"** in the OpCenter panel. While in **Restricted Mode**, OpCenter can only perform **Play Back**. Other OpCenter functions, such as, **Search** or **Export Video** are either disabled or hidden.

The following shows an example of how OpCenter operates in **Restricted Mode**:

- Log in to OpCenter via the Enterprise Server.
- Click the **Sign In** button



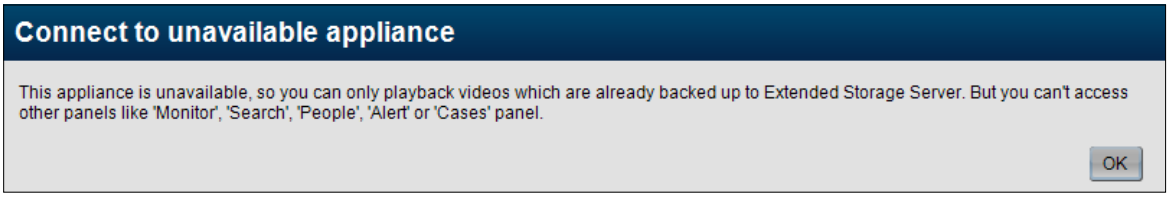
- Choose an unavailable appliance.



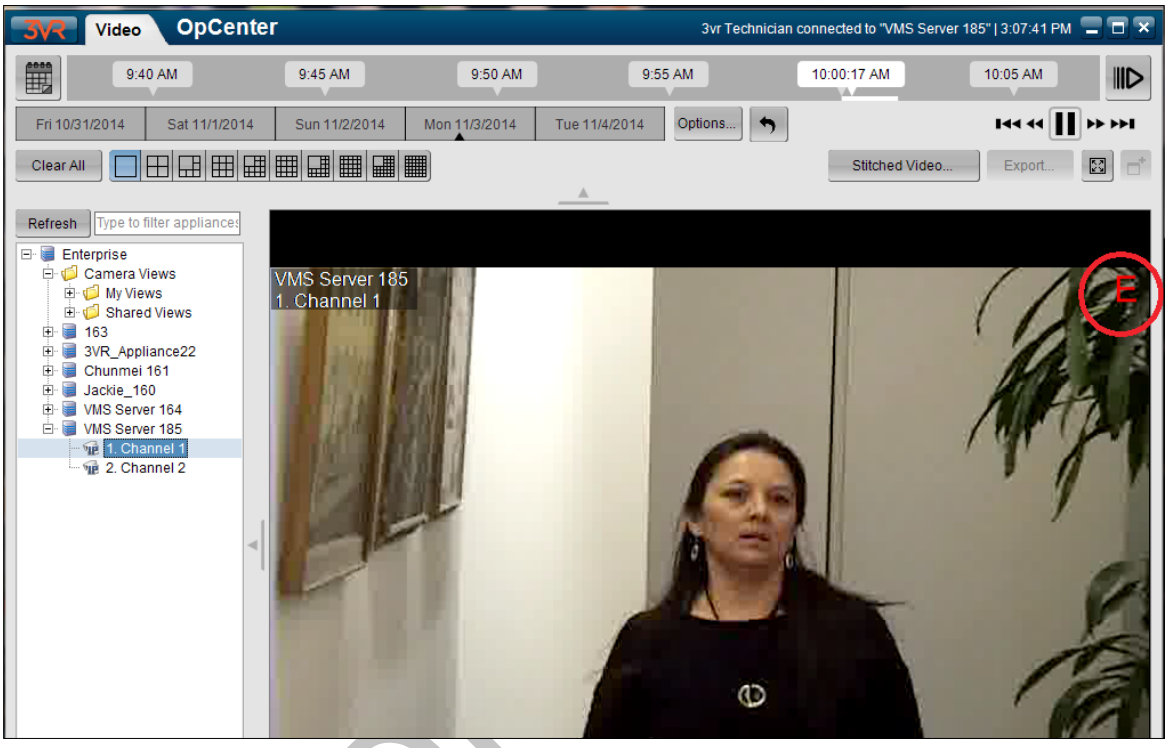
- Click the **Connect** button.

DRA

- After about 20 seconds, a warning dialog box appears.



- Drag an offline channel into OpCenter and trigger playback. A red **E** icon appears at the top -right corner of the current video box. This indicates that the video playback is coming from the ESS.

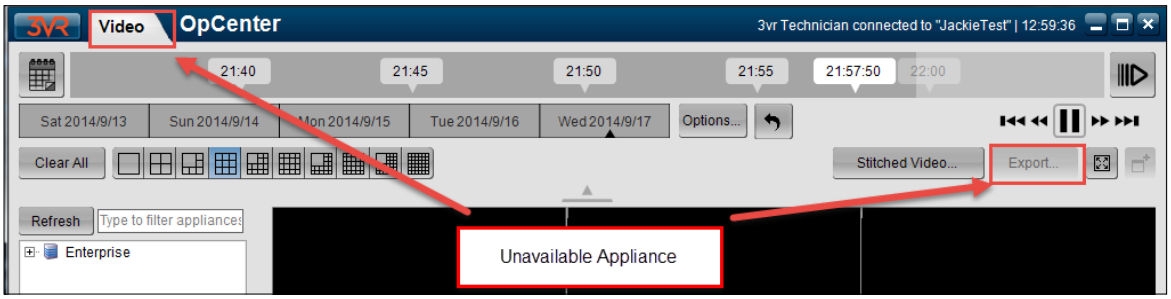


3.2 OpCenter via Enterprise Server Connecting to an Available Appliance

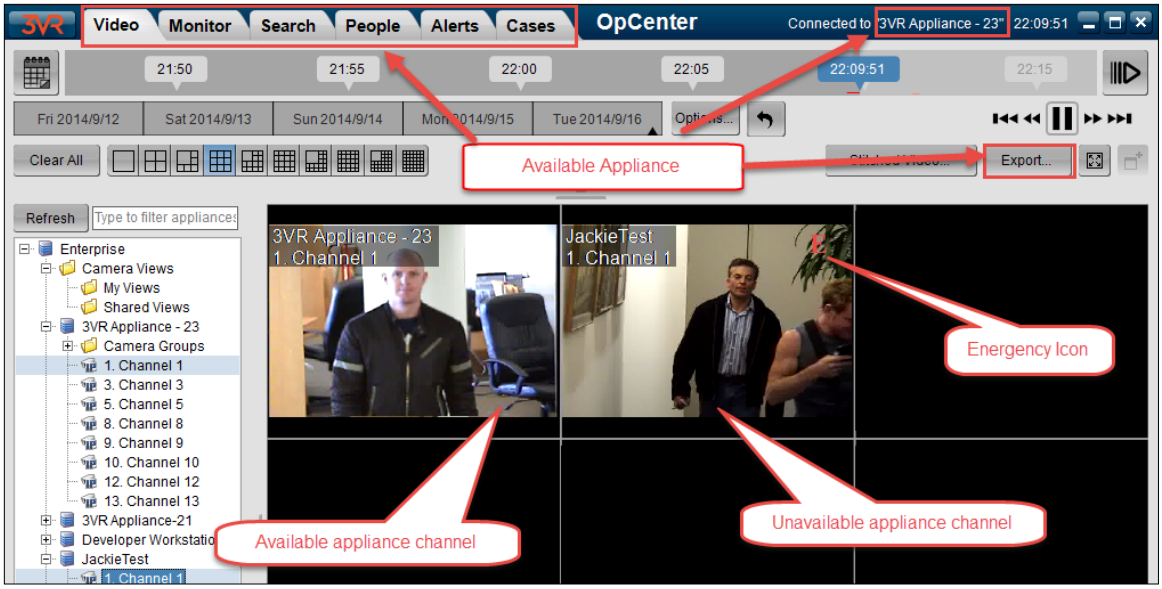
If OpCenter is connected to an available appliance via the **Enterprise Server**, OpCenter plays back video in **Normal Mode**. The **Normal Mode** OpCenter interface shows the **Export** button, as well as the panels for **Video**, **Monitor**, **Search**, **People**, **Alerts**, and **Cases**. You can play back channels from both **online** and **offline** appliances.

The following two images show the differences between OpCenter in Restricted Mode and OpCenter in Normal Mode:

- **OpCenter in Restricted Mode**:



- **OpCenter in Normal Mode**



4. ESS ERROR CONDITIONS

This section describes errors that can occur using ESS and the behaviors associated with the errors.

4.1 Error Conditions

No.	Situation	Intended Behavior
1	**Extended storage server is down**	Health alert is raised in ESS client: **"Can't connect to extended storage server [destination name]. Maybe the server appliance happens to be upgrading or rebooting. If this is not the case, make sure the server configuration in the client is correct and the Extended Storage Server is running."**
2	**Extended Storage Server Drive is near Capacity**	ESS Server triggers a health alert: **"Low disk space on drive [Drive name]. Please make sure the drive has adequate free space to continue the extended storage backup."** Please be aware there is no regular or emergency trimming in Extended Storage Server. This option advises the ESS admin to take necessary steps to clean old data from the server.
3	**Not enough free space in Extended Storage Server**	Extended Storage client triggers a health alert: **"Not enough free space for current backup. Please contact the administrator of extended storage server, or log in to System Manager to change the 'Max Storage Days' setting to a lower number of days".**
4	**Extended Storage Client is dead or not reachable**	Extended storage Server: triggers a health alert: **"Didn't receive any request from client [Hostname] for 1 month. Please log in to System Manager to trim related data if needed."** This health alert is raised when Extended Storage Client is not reachable for one month or more.
5	**Failed to save backup files in destination storage**	Problems may occur on the destination storage drive if it cannot be accessed or there is not enough free space. Extended Storage Server triggers a health alert: **"Failed to back up files to destination folder. Please make sure the destination drive {drive name} is functional and has enough free space to continue the backup".**

DRAFT

No.	Situation	Intended Behavior
6	**Failed to return to Normal Mode once connection was restored.**	Appliance may appear to be in Restricted Mode after connection has been restored. Reboot the appliance to restore full functionality.

No.	Situation	Intended Behavior
5	**Failed to save backup files in destination storage**	Problems may occur on the destination storage drive if it cannot be accessed or there is not enough free space. Extended Storage Server triggers a health alert: **"Failed to back up files to destination folder. Please make sure the destination drive {drive name} is functional and has enough free space to continue the backup."**
6	**Failed to return to Normal Mode once connection was restored.**	Appliance may appear to be in Restricted Mode after connection has been restored. Reboot the appliance to restore full functionality.

DRAFT

DRAFT

CHAPTER 16
3VR Appliance-Specific Features

1. 3VR APPLIANCE-SPECIFIC FEATURES 299
2. ALARM INTEGRATION 299
   - 2.1 Alarm Inputs 299
   - 2.2 Alarm Outputs 300
3. PHYSICAL CONNECTIONS 300
   - 3.1 4000-Series and 5500-Series 300
   - 3.2 External Adapters 301
4. ALARM INPUTS 302
   - 4.1 Configure Alarm Inputs 302
   - 4.2 Generate Test Alarm Input Event 303
5. ALARM OUTPUTS 304
   - 5.1 Configure Alarm Outputs 304
   - 5.2 Test Output Connection with External Alarm Alert Action 305
6. TROUBLESHOOTING ALARM INTEGRATION 306
   - 6.1 Review Physical Setup 306
   - 6.2 Check System Manager Configuration 306
   - 6.3 If Alarm Test Fails for All Terminal Pairs 306
7. HDMI-TO-CVBS CONVERTER 307
   - 7.1 Items in Shipping Container 307
   - 7.2 Product Diagram 307
   - 7.3 Converter Installation 307

DRAFT

DRAFT

1. 3VR APPLIANCE-SPECIFIC FEATURES

This chapter describes features that apply only to customers using 3VR appliances. These features do not apply if you are using third-party hardware.

2. ALARM INTEGRATION

This section describes how to integrate an external I/O device with a 3VR appliance.

The integration procedure varies depending on the model of appliance:

- 3VR 4000-Series and 5500-Series appliances feature an internal digital I/O board that processes both input and output signals. USB Alarm I/O devices are not compatible with 3VR appliances with integrated Alarm I/O.
- 3VR also supports the ADAM Digital I/O device (ADAM part number: A8-DI-12). This is a network device with 12 digital inputs. The device allows users to connect systems without an internal alarm board to an external alarm. Please see the ADAM Digital I/O plug-in documentation for more information. The ADAM Digital I/O device does not function with the Seproban plug-in.
- 3VR supports I/O on most ONVIF cameras.

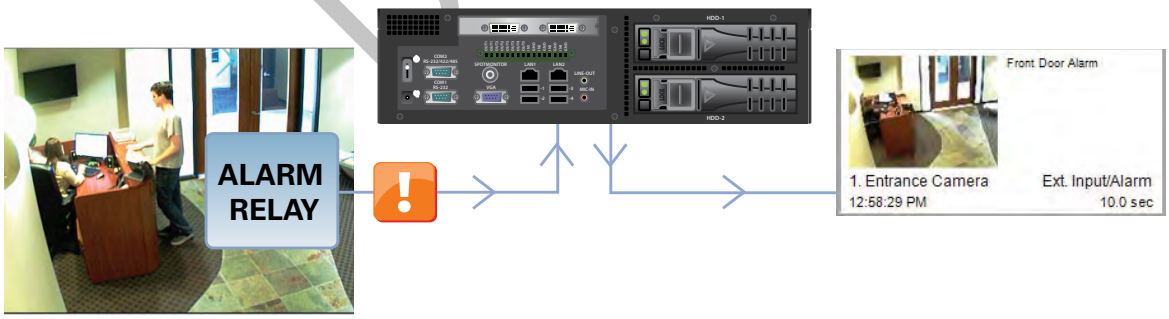
Notes

1) The most common use case for external I/O integration is an alarm system. Thus, although these instructions apply to integration with any digital I/O system, the term "alarm" is used as a catchall term in this chapter going forward.
2) External alarms are not currently supported for VMS servers running on third-party hardware. The instructions in this section apply only to 3VR appliances.
3) 3VR does not currently support the outputs on the ADAM Digital I/O device.

DRAFT

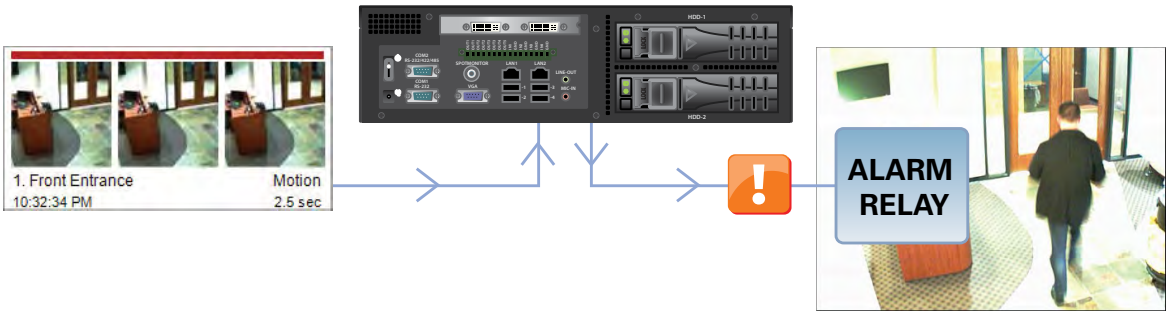
2.1 Alarm Inputs

- Alarm inputs detect dry contact closure (short condition) across the terminals.
- When the alarm system activates, the alarm input connection create an **Ext. Input/Alarm** event in 3VR OpCenter with the time of the alarm.



2.2 Alarm Outputs

- Alarm outputs are Normally Open (NO) relays that can close a circuit with a maximum rating of 220VDC/250VAC at no more than 2A.
- An alarm output connection allows the 3VR appliance to trigger the alarm in response to certain conditions (defined in the **Alerts** panel of OpCenter).



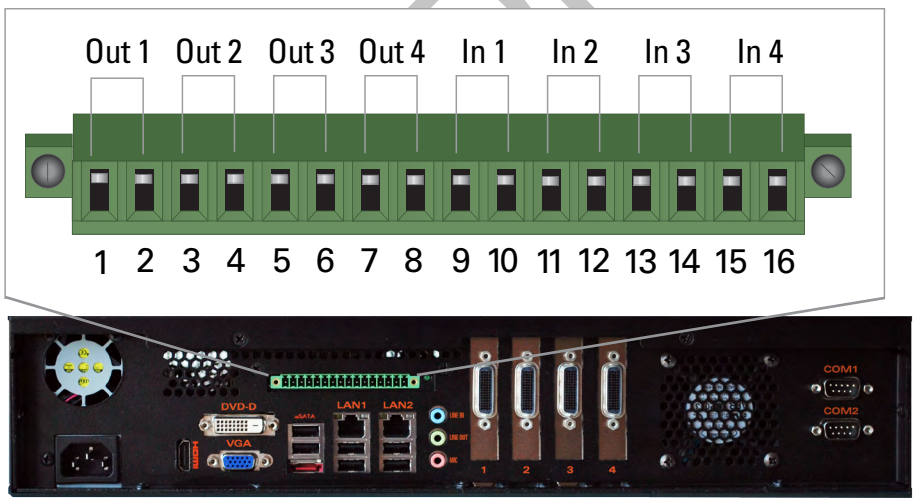
3. PHYSICAL CONNECTIONS

You wire external alarms to the 3VR appliance's built-in alarm board via an alarm connector, included with every unit.

3.1 4000-Series and 5500-Series

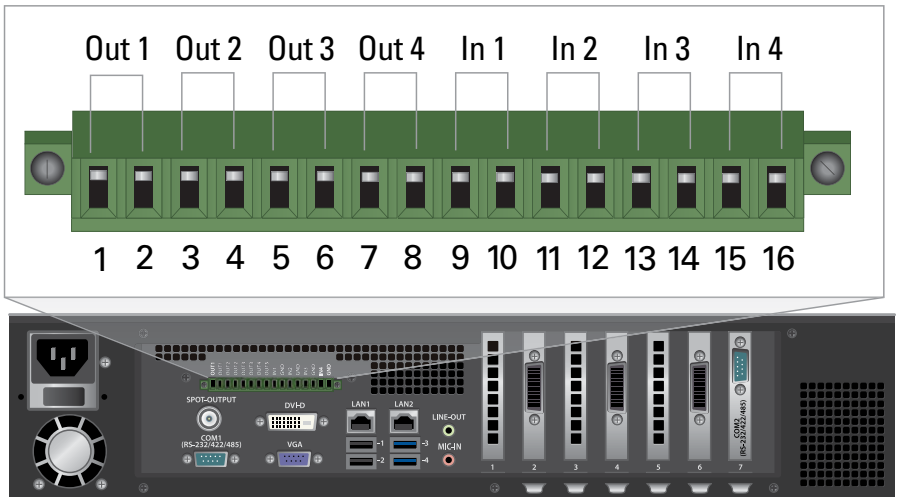
You can wire the 16-pin connector to up to 4 alarm inputs and 4 alarm outputs. The pins on the connector are arranged as shown below:

4000-Series



DRAFT

5500-Series



1. Connect each alarm input and output to a terminal pair.
2. Screw the connector into the alarm port on the back of the 3VR appliance.
3. Continue to section 4.

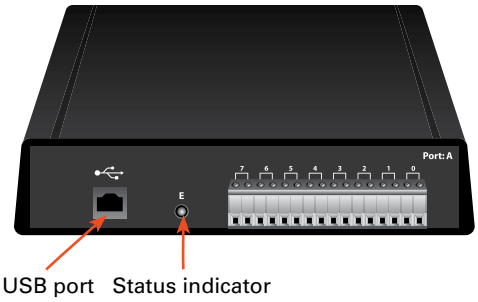
3.2 External Adapters

5500-Series appliances support the SEALEVEL SeaPORT PLC-16 USB alarm adapters. You can use this adapter to expand the number of alarm inputs or outputs beyond the number supported by the onboard hardware:

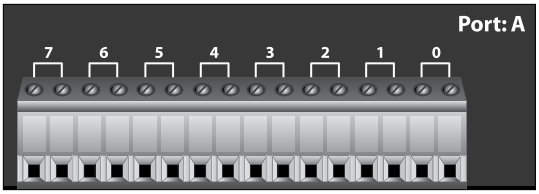
SeaPORT PLC-16

The SEALEVEL SeaPORT PLC-16 USB alarm adapter allows a 3VR system to process both input and output data from up to eight relays.

1. Connect the USB cable from the SEALEVEL device to the 3VR.
2. Verify that the yellow E (Enabled) indicator is illuminated.



Port A on the SEALEVEL is for alarm inputs.

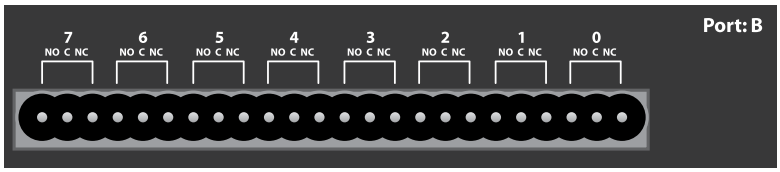


Each pair of pins (labeled 0 through 7) consists of one common pin and one alarm input pin.

3. Connect each alarm input to a common pin and its associated alarm pin.

DRAFT

Port B on the SEALEVEL connects to alarm outputs.



There are 8 SPDT outputs with 3 pins each: Normally Open (NO), Common (C), and Normally Closed (NC).

4. Connect each alarm output to a common pin and its associated Normally Open or Normally Closed pin.

5. Continue to section 4.

4. ALARM INPUTS

This section describes how to configure alarm connections in System Manager and test alarm inputs.

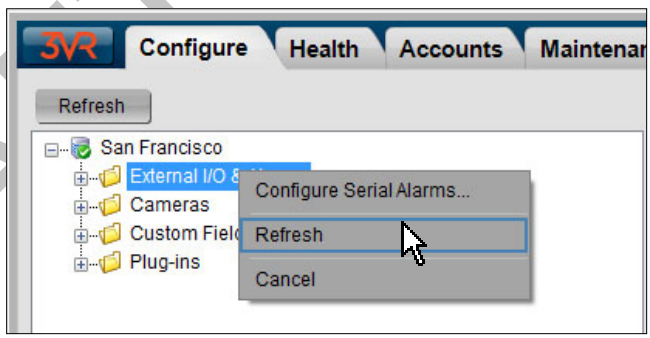
4.1 Configure Alarm Inputs

Perform the following steps to configure alarm input connections in 3VR System Manager:

1. In the **Configure** panel, click the plus sign (+) next to the system display name to expand the list of configuration options.

2. Right-click **External I/O & Alarms** and select **Refresh**.

3. In the dialog box that appears, click **Refresh** to acknowledge that the connection to the cameras will temporarily be lost while the external I/O system refreshes.

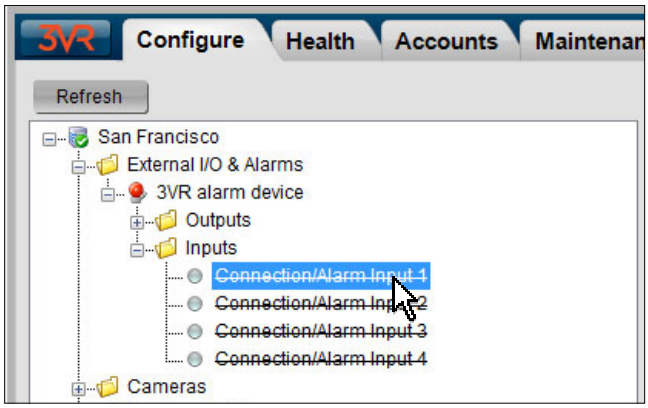


4. Click the plus sign (+) beside **External I/O & Alarms** to expand the alarms folder.

5. Click the plus sign beside **3VR alarm device**.

6. Expand the **Inputs** folder.

7. Select **Connection/Alarm Input 1**. Information about the input is displayed to the right.



8. Under the **Alarms** heading, modify the following settings as follows:

Alarm	
Active?	Yes
Name	Store Alarm
Camera	1. Channel 1
Connection/Hardware ID	1

DRAFT

- Change **Active?** to **Yes**.
- If you wish to rename the alarm, edit the **Name** setting. The alarm name appears on OpCenter event cards when the alarm is triggered.
- Select a camera to associate with this alarm from the **Camera** drop-down menu.

> **Important**
> Do not skip this step. You must associate the alarm input signal with a camera in order for alarm events to appear in 3VR OpCenter.

- The **Connection/Hardware ID field** contains the hardware address of the terminals connected to the external alarm. This field cannot be modified.

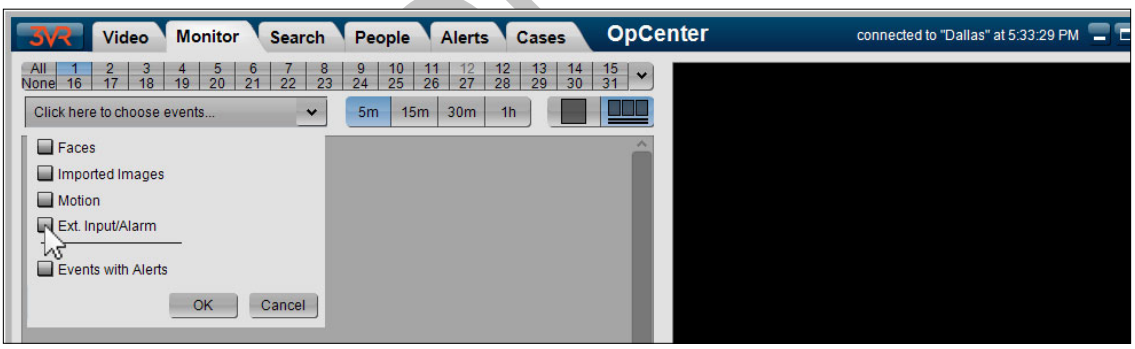
9. Click **Save** to save the configuration.
10. Right-click **External I/O & Alarms** and select **Refresh**.
11. Repeat steps 7-10 for each remaining alarm input connection.

Alarm Input Number (System Manager)	1	2	3	4	5	6	7	8
Input Port Number (SEALEVEL device)	0	1	2	3	4	5	6	7

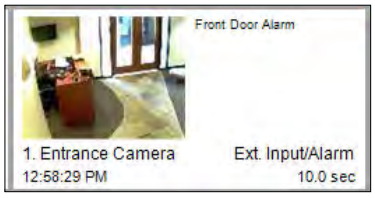
4.2 Generate Test Alarm Input Event

Perform the following steps to verify that you correctly configured an alarm input connection:

1. Generate a test alarm according to local procedure.
2. Launch 3VR OpCenter.
3. Click the **Monitor** tab to go to the **Monitor** panel.
4. Click the camera number of the camera you associated with the alarm in step 4.1.
5. Click the drop-down arrow below the camera selector to open the event type menu.



6. Check the box next to **Ext. Input Alarm**, and then click **OK**.
7. Verify that an external alarm event was generated for each alarm input connection.



> **Reference**
> See the *3VR VisionPoint™ VMS User Manual* for more information about viewing and searching for alarm events in 3VR OpCenter.

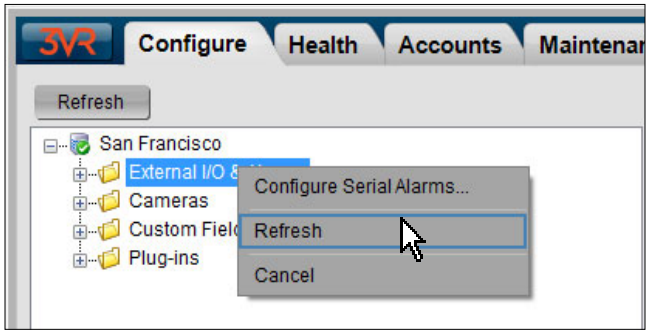
DRAFT

5. ALARM OUTPUTS

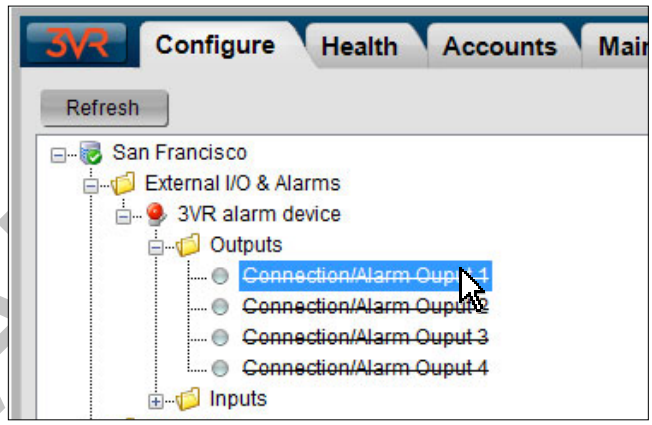
This section describes how to configure alarm output in System Manager and test the connections.

5.1 Configure Alarm Outputs

1. In the **Configure** panel, click the plus sign (+) next to the 3VR appliance name to expand the list of configuration options.
2. Right-click **External I/O & Alarms** and select **Refresh**.



3. Click the plus sign beside **External I/O & Alarms** to expand the alarms folder.
4. Click the plus sign beside **3VR alarm device.**
5. Expand the **Outputs** folder.
6. Select **Connection/Alarm Output 1**. Information about the output is displayed to the right.



7. Under the **Alarms** heading, modify the following settings:

Alarm	
Active?	Yes
Name	Vault Alarm
Normally Open?	No
Connection/Hardware ID	1

- Change **Active?** to **Yes**.
- If you wish to rename the alarm output, edit the **Name** setting.
- The **Normally Open** setting alters the default position of the relay. Unless the alarm system is wired such that a 3VR alert should cause the alarm to turn off, leave it set to **No** (the default).
- The **Connection/Hardware ID** field contains the hardware address of the terminals connected to the external alarm. This field cannot be modified.

8. Click **Save** to save the configuration.
9. Right-click **External I/O & Alarms** and select **Refresh**.
10. Repeat steps 6-9 for each additional alarm output.

Alarm Output Number (System Manager)	1	2	3	4	5	6	7	8
Output Port Number (SEALEVEL device)	0	1	2	3	4	5	6	7

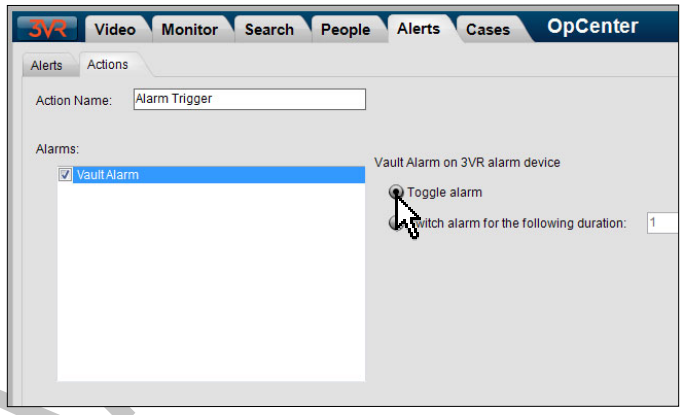
5.2 Test Output Connection with External Alarm Alert Action

Perform the following steps to verify that you correctly configured an alarm output connection:

1. Launch 3VR OpCenter.
2. Click the **Alerts** tab to go to the **Alerts** panel.
3. Click the **Actions** tab.
4. Click **New**.
5. Click **External alarm**.

In the alert action editing screen:

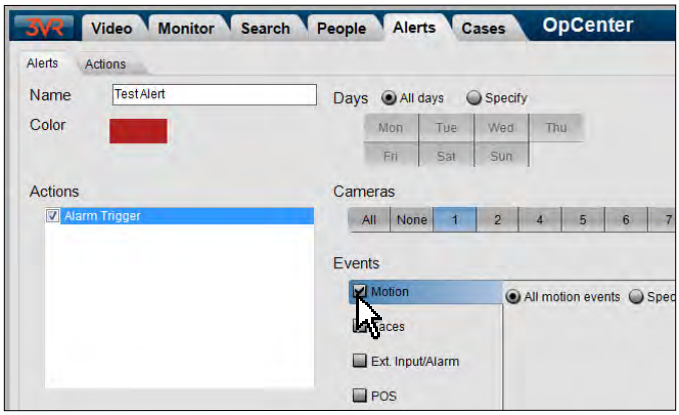
6. Type a name for the external alarm action in the **Action Name** box.
7. Select the alarm output connection you are testing from the **Alarms** panel.
8. Click **Toggle alarm**.
9. Click **Save**.



10. Click the **Alerts** tab.
11. Click **New**.

In the alert editing screen, create a test alert with the following properties:

12. Type a name for the test alert in the **Name** box.
13. Leave the **Days** and **Time** controls at their default values.
14. Under **Actions**, check the box next to the alarm trigger alert action you created in steps 6-9.
15. Select the camera number of a camera that is physically accessible to you.
16. Check the box next to **Motion**.
17. Click **Save**.



18. Walk in front of the camera number you selected in step 12. If the alarm output connection is correctly configured, the motion event that is generated by your movement will toggle the alarm.
19. If there are any additional alarm output connections, edit the alert action created in steps 6-9 so that the alert triggers on the next alarm output connection. Repeat step 18 and verify the alert action toggles the alarm again.

DRAFT

6. TROUBLESHOOTING ALARM INTEGRATION

If your alarm test does not produce the desired result, use the following steps to troubleshoot the problem.

6.1 Review Physical Setup

- Ensure that the **Connection/Alarm Input** or **Output** that you enabled in System Manager corresponds to the terminals on the alarm board or device indicated in the setup diagram.
- If you are using a SEALEVEL device, check the LEDs to verify that the device has power. If thee LEDs are unlit, the device may be defective.

6.2 Check System Manager Configuration

- Verify that you have changed the **Active?** field in the **Connection/Alarm Input** or **Output** to "Yes".
- If configuring an alarm input, make sure you have associated a camera with the **Connection/Alarm Input**.
- After reviewing the camera settings, right-click the **External I/O & Alarms** folder and select **Refresh**.

6.3 If Alarm Test Fails for All Terminal Pairs

4000-Series and 5500-Series

- Remove the green alarm connector and repeat the alarm test, touching the pins directly. If no alarm event appears, contact 3VR Technical Support for assistance.

DRAFT

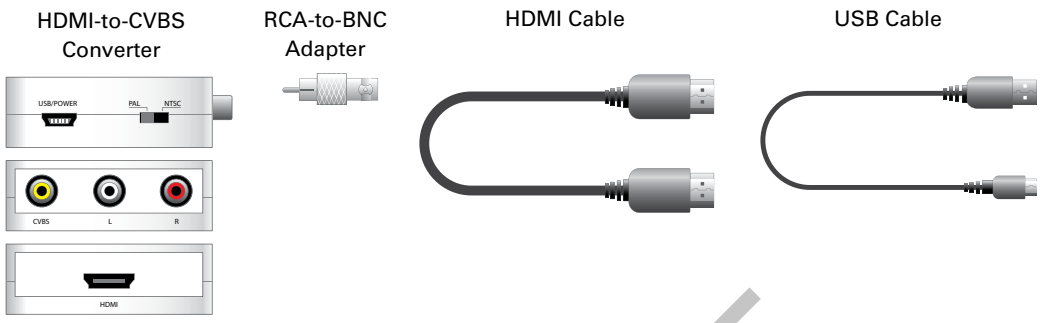
7. HDMI-TO-CVBS CONVERTER

This section describes the basic steps for installing the HDMI-to-CVBS Converter for use with the 1000-Series, 2000-Series, 3000-Series, and 4000-Series appliances. These appliances are not manufactured with a BNC Video or RCA Video output ports and require this adapter when utilizing a BNC or RCA out to monitor with your 3VR setup.

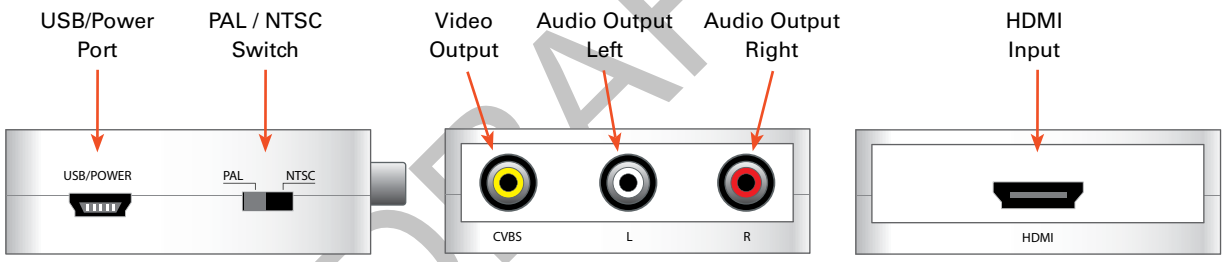
The HDMI-to-CVBS Converter converts HDMI video signals to AV composite video. This converter can also convert HDMI audio signals to FL / FR Stereo. Use the PAL / NTSC Switch to match the format of the monitor with the video output.

The converter is powered using the included USB cable and does not require an external power adapter.

7.1 Items in Shipping Container



7.2 Product Diagram



DRAFT

7.3 Converter Installation

Perform the following steps to install and configure the Converter:

20. Using the USB cable, connect the standard-sized plug into a USB port on the 3VR appliance. Connect the mini-USB plug of the cable to the HDMI-to-CVBS Converter.

21. Connect the HDMI cable from the 3VR appliance to the HDMI-to-CVBS Converter.

22. If outputting to a BNC monitor, connect the included RCA-to-BNC Adapter to the BNC cable and plug the RCA end into the port labeled Video Output.

23. The Video Output standard is NTSC in the United States. Make sure the PAL/NTSC Switch is set to NTSC.

DRAFT

APPENDIX A

Image Guidelines for Facial Surveillance

1. THE IMPORTANCE OF IMAGE QUALITY 311
   - 1.1 Key Elements in Optimizing Images for Facial Surveillance 311
2. IMAGING BACKGROUND 311
   - 2.1 Resolution 312
   - 2.2 Field of View 312
3. CAMERA PLACEMENT FOR FACIAL ANALYSIS - FOUR FACTORS 313
   - 3.1 Field of View Determines Size and Resolution of Face 313
   - 3.2 Horizontal Angle 315
   - 3.3 Vertical Angle 315
   - 3.4 Lighting Level 316
   - 3.5 Additional Considerations for Megapixel Cameras 317
4. IMAGE USE AND OPTIMIZATION FOR FACIAL ANALYSIS 318
   - 4.1 Imported Images 318
   - 4.2 CCTV Video 319
5. CONCLUSION 323

DRAFT

DRAFT

1. THE IMPORTANCE OF IMAGE QUALITY

Understanding what constitutes quality images and how to optimize the quality of images used in VisionPoint™ VMS is critical to developing viable solutions. Meeting specific requirements for VisionPoint™ facial surveillance is much more challenging than in any traditional CCTV deployment. Accordingly, many partners and users are unaccustomed to being concerned about these issues and can easily overlook them.

By understanding and optimizing image quality, you will be able to:

- Better qualify what opportunities are strong fits for 3VR VisionPoint™ VMS
- Set the appropriate level of expectations with partners and users
- Design a system that accommodates real-world conditions
- Deliver a solution that is optimally effective

1.1 Key Elements in Optimizing Images for Facial Surveillance

This appendix examines and explains the many elements that are critical to using VisionPoint™ VMS for facial surveillance. While fundamental principles apply to images from photographic cameras as well as CCTV cameras, the application will differ. The table below summarizes the key elements to provide a quick reference for future use.

DRAFT

1)	Any image, whether video or photo, requires sufficient detail. Detail is determined by (1) the level of resolution in the image and (2) the size of the person's face relative to the size of the image.
2)	The person's face must look directly towards the camera. This affects both the class of imported photos that are acceptable and how video cameras must be positioned to capture faces.
3)	Imported images must meet the requirements listed above. With the exception of mugshots and passport photos, most photos do not meet these requirements.
4)	Video cameras must be positioned specifically to capture faces. The cost may be inexpensive, but the skill is not trivial. Care must be taken to precisely position cameras to capture faces consistently.

2. IMAGING BACKGROUND

Two aspects of imaging are most important in understanding and optimizing VisionPoint™ VMS facial surveillance:

1. **Resolution**
2. **Field of view**

Without understanding the impact of these two aspects, it isn't possible to master use of VisionPoint VMS™ for either importing images or capturing video. As such, prior to analyzing facial surveillance or its application to VisionPoint™ VMS, this appendix explains these aspects and presents relevant introductory material.

2.1 Resolution

Resolution, as applied to images used in VisionPoint™ VMS, is defined as the level of visual detail in the image.

Resolution is commonly defined in two dimensions: horizontal and vertical. For instance, a frequent resolution level cited is 640 x 480 pixels. This means that there are 640 unique pixels across the image horizontally and 480 pixels down the image vertically.

The number of horizontal pixels is important for performing VisionPoint™ VMS facial surveillance because it determines the amount of detail available for performing facial analysis. Sufficient horizontal pixels are required to perform facial recognition.

One standard metric used in describing video surveillance images is the Common Intermediate Format (CIF). This is a way to quickly cite specific resolution levels that are commonly used in digital video. CIF specifies specific horizontal and vertical resolution levels.

The table below provides examples of different CIF levels.

CIF Level	Resolution	Example
QCIF (Quarter CIF)	176 x 44	
CIF	352 x 288	*Typical Internet streaming*
2CIF	704 x 240	
4CIF	704 x 576	*NTSC camera max resolution*
16CIF	1408 x 1152	*1.5 megapixel camera*

DRAFT

Industry participants commonly cite different CIF levels. These CIF levels have a significant impact on whether imported images or captured video can be used for facial analysis.

For example, an image of a person recorded with 4CIF resolution may be able to be used by VisionPoint™ VMS for facial analysis, however, the same image recorded at CIF resolution will probably not contain enough detail to be used for facial analysis unless the face is extremely large (at least a quarter of the width of the field of view). See "Camera Placement for Facial Analysis - Four Factors" on page 313 for more information and examples on field of view for facial analysis.

2.2 Field of View

Field of View is the size of an area that can be seen while looking through an imager, such as a photographic or CCTV camera. Below are two examples of images with different horizontal fields of view.

The difference in the field of view is not very significant – the one on the left is only 2 feet wider than the one on the right. However, despite this seemingly minor difference, information below shows how this makes a significant difference on the suitability of the images for facial analysis.

An image does not have a singular width for the field of view. The width of the field of view increases as the subject moves from the foreground of the image to the background.

The two major visual differences are:

1. **A subject in the foreground is in significantly clearer focus than the background.**

2. **The width of the field of view is significantly smaller in the foreground than in the background.**

The variation in the width of the field of view is a product of projecting a three-dimensional world onto a two-dimensional medium (the image). All images always exhibit this property.

This is very important because good facial analysis requires a narrow field of view (less than 4.5 feet at the point at which the subject is in best focus). So, a subject in the foreground of an image that meets the field of view requirements for facial analysis is too small if they are a step or two further away from the camera, where the field of view for the same camera placement is significantly wider. See ""Camera Placement for Facial Analysis - Four Factors" on page 313 below for more information and examples on field of view for facial analysis.

3. CAMERA PLACEMENT FOR FACIAL ANALYSIS - FOUR FACTORS

This section describes the four factors that affect facial analysis: field of view, horizontal and vertical angle, and lighting level.

3.1 Field of View Determines Size and Resolution of Face

Facial analysis requires a certain minimum resolution level to be effective. This resolution level is measured in pixels.

- 3VR requires a minimum of 35 horizontal pixels between the eyes (or about 80 - 100 horizontal pixels across the head) to perform facial analysis.

- 3VR performs analysis of all analog NTSC video at 4CIF (704 x 576 pixels)

Given these facts and the average width between eyes is 3", and the width of a head is approximately 6 - 7", an NTSC camera at 4CIF resolution can capture faces in a field of view **(FOV)** no more than about **4.5 feet**.

DRAFT

Quick Tip

Place a person standing in the foreground in optimal focus. When the person holds his/her arms stretched out from side-to-side, you should not be able to see their hands (the image should be cut off at their wrists). If you can see the person's hands in the image when the person is standing in focus in the foreground, the field of view is too wide for facial analysis.

Note

If you are looking at prerecorded images from a camera already placed, measure the width of the head, and if it is smaller than 1/7 (about 15%) of the field of view, the field of view is too wide for facial analysis.

Poor FOV

5.5 feet

Face = 1/9 of image

Maximum Acceptable FOV

4.5 feet

Face = 1/7 of image

Excellent FOV

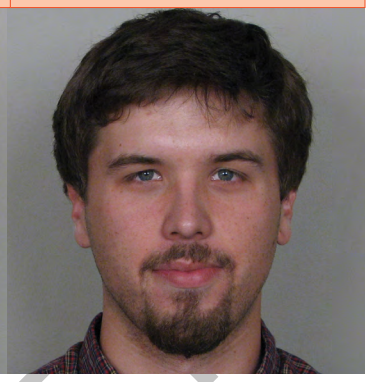
3.5 feet

Face = 1/6 of image

3.2 Horizontal Angle

Facial analysis requires a clear image of the full face, directly facing the camera - with minimal turning of the head to the left or right (horizontal angle) relative to the camera.

Quick Tip
The image must simultaneously show both ears of the subject. If one of the ears is not visible, the horizontal angle is too extreme.

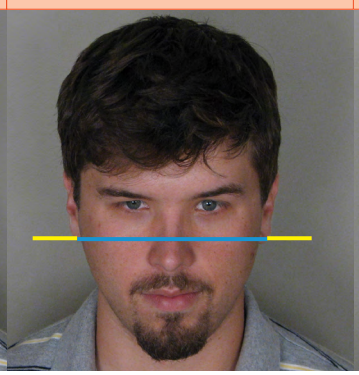
Poor Placement Horizontal angle too large Can't see both ears	Maximum Acceptable Horizontal angle marginal Some of each ear visible	Excellent Placement No horizontal angle Both ears fully visible
		

3.3 Vertical Angle

Facial analysis requires a clear image of the full face, directly facing the camera - with minimal tilting of the head up or down (vertical angle) relative to the camera.

Quick Tip
The middle of the nose should be higher than or at least the same level as the bottom of the earlobes. If the middle of the nose appears below the earlobes, the vertical angle is too high.

Cameras need to be mounted low enough or far away enough so that the vertical angle or slope does not exceed 20% above the eye level when subjects are in focus in the foreground. Given an average eye height of 5 feet, a camera 10 feet away can not be mounted higher than 20% of 10 feet (2 feet) above the eye height of 5 feet - so not higher than 5 + 2 = 7 feet. A camera 20 feet away can be mounted as high as 9 feet (20% of 20 = 4 feet above 5 feet, 4 + 5 = 9). See "Camera Positioning" on page 319 for more details.

Poor Placement Vertical angle too large Middle of nose below earlobes	Maximum Acceptable Vertical angle marginal Middle of nose at earlobes	Excellent Placement No vertical angle Middle of nose above earlobes
		

DRAFT

3.4 Lighting Level

Facial analysis requires even levels of lighting that clearly shows the detail in a face. Facial analysis requires lighting conditions that do not produce shadows and/or dark areas in the face (underexposure) and lighting conditions that do not produce glare and/or washed-out areas in the face (overexposure). A face with lots of detail visible and a wide range of dark and light pixels (referred to as "dynamic range") is required for facial analysis.

Photo A –Good Lighting. There are no areas of the face in shadow or glare. There is wide dynamic range - lots of both light and dark areas within the face, and lots of detail is visible.

Photo B –Overexposed. There are no areas of shadow, but there are significant areas with glare (notice the cheeks, nose and forehead). There is a narrower dynamic range - excessive washed-out areas with loss of detail.

Photo C –Marginally acceptable. There are some areas of the face in mild shadow and the face appears somewhat darker than desired. There is marginally acceptable dynamic range - moderate amounts of both light and dark areas within the face, and moderate amounts of detail are visible.

Photo D –Underexposed. There are substantial areas of shadow and/or not enough light. There is a narrower dynamic range - excessive dark areas with loss of detail.

Photo A –

Good lighting

Photo B –

Overexposed

Photo C –

Marginally acceptable

Photo D –

Underexposed

DRAFT

3.5 Additional Considerations for Megapixel Cameras

This section describes other factors to consider when using megapixel cameras.

Field of View

With the addition of megapixel cameras to your security solution, you can now utilize the higher resolutions available to ultimately provide a wider field of view. In essence, this allows the use of fewer cameras and more coverage while still capturing face profiles. It is extremely important to understand that the same principles still apply for facial recognition; this includes pixels in between the eyes, horizontal and vertical angles, and lighting.

The number of horizontal pixels is still the key factor in terms of performing VisionPoint™ VMS facial surveillance; the advantage of using a megapixel camera is shown in the table below.

Resolution	Megapixels	Width for Face (ft)
1024 x 768	0.7	6.5
1280 x 1024	1.3	8.0
1600 x 1200	2	10.5
2048 x 1536	3	13.5

The appearance of the field of view is obviously different with a width of 8.5'.

Pixels Between the Eyes

The same principles that apply to lower resolution cameras apply to megapixel cameras; VisionPoint™ VMS still requires 35 pixels between the eyes. However, analysis is conducted on the full megapixel frame of the camera's output. For example, with a resolution of 1280 x 1024, 3VR conducts facial analysis at 1280 x 1024 versus an analog camera at 4CIF (704 x 576).

DRAFT

4. IMAGE USE AND OPTIMIZATION FOR FACIAL ANALYSIS

VisionPoint™ can analyze faces from two primary sources:

1. *You can import digital images, such as photographs and mugshots.*
2. *You can connect CCTV cameras to a 3VR appliance and continuously analyze video.*

Best practices for each source differ significantly. The section below describes both sources.

4.1 Imported Images

You can import any image that is in a supported digital format into VisionPoint™ VMS. Supported formats include: BMP, JPEG, and GIF. VisionPoint™ VMS can only successfully analyze faces in images that meet the requirements enumerated in the previous sections (pixels between the eyes, angles, and lighting).

Passport Photos / Mugshots

Generally, passport photos and mugshots provide high-quality images for facial analysis. The angles and the lighting on these photos are generally within guidelines. Check that the number of pixels between the eyes are sufficient. VisionPoint™ VMS uses an photo import process that provides immediate feedback if the number of pixels between the eyes is insufficient.

Images from DVRs

Images from DVRs may not provide sufficient quality for facial analysis. You should qualify and set appropriate expectations. Video from DVRs is often recorded at resolutions lower than 4CIF, such as 2CIF or CIF. Because of the reduction of resolution, the field of view needed for sufficient detail increases significantly. For example, images at CIF resolution would need to have the face in focus in a field of view no wider than 2.25 feet.

Furthermore, the field of view of cameras on traditional DVRs is often 7′ to 12′, which is significantly greater than the 4.5 feet maximum field of view even if the video is recorded at 4CIF.

General Photos from Digital Cameras

Images from digital cameras may provide sufficient quality for facial analysis. To the extent that these photos exhibit the same properties as passport photos, suitability is more likely.

Photos of people in a group or performing an activity may not be suitable if the person's head is significantly tilted horizontally or vertically. This is quite common and will affect performance.

Digital cameras provide megapixel images. Given the very high resolution of these images (compared to analog photos), the width of the field of view may be very wide (as much as 20′ wide). Be careful to verify that the image has not been reduced in resolution. This is a common technique to reduce the file size of an image. However, if this is done it will significantly reduce proportionally the number of pixels between the eyes in faces in the image.

DRAFT

4.2 CCTV Video

Many existing camera positions are designed for alarm assessment and activity monitoring. You must adapt these cameras for use in facial analysis. You can use existing infrastructure for facial analysis, but you must optimize it for use in meeting the imaging guidelines enumerated in this appendix.

The remainder of this section is an important treatment of design and deployment options for CCTV video use.

Environment

First, examine the physical layout of the facility to identify natural "choke points" – areas where subjects appear within a limited field of view and are most likely to look "straight-on" toward the camera(s). Ideal choke points include entrances and hallways. The chosen areas should be free from any obstructions that might come between the camera and subject, (including transparent barriers that can create glare/reflection problems). Also, these areas should be devoid of distractions that may entice subjects to look away from the camera while passing through. Ideally, subjects should spend three seconds passing through a choke-point area.

The recommended width of a single-camera choke point is four feet, with a maximum width of 4½ feet. Areas wider than 4½ feet require multiple cameras positioned so the lines of sight slightly overlap. The degree of overlap should enable each camera to capture the full face of a subject who passes halfway between them, instead of each camera capturing only half the subject's face.

Scene lighting must be sufficient to produce a clear, sharp image. Avoid excessive background lighting, blooming, or shadowing conditions.

DRAFT

Camera Positioning

Center cameras to increase the opportunities to obtain straight-on (perpendicular) face images. In addition, set the camera at the maximum allowable distance from the subject (subject-to-lens specifications that provide a proper field of view - less than 4.5 feet, as explained in section 3). The further the distance between camera and subject, the longer the depth of field – the area within which the subject will remain in focus – thus delivering more usable 'face frames'.

Optimal full-facial recognition occurs when a camera is mounted on a vertical line that is level with (and horizontally perpendicular to), the subject's face. Harsh camera angles are detrimental, and seriously degrade the results.

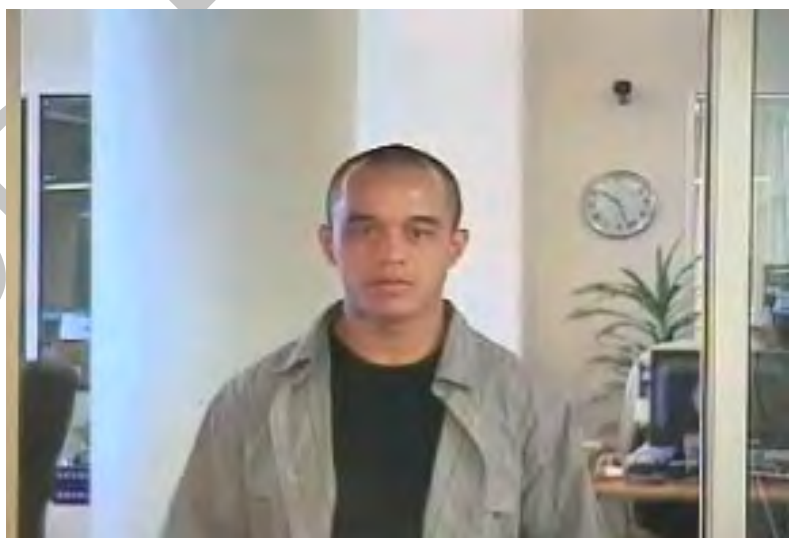
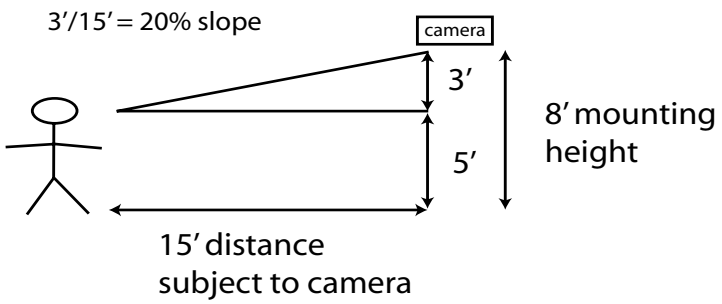


Figure 1 – Ideal Camera Positioning

While cameras are often mounted higher than the optimal face-level height, adequate face capture can occur provided the maximum vertical angle of incidence is less than a 20% slope, (see the illustration below). The greater the distance between camera and subject, the higher the camera can be mounted, while maintaining this threshold.

Determining Camera Mounting Height - No more than 20% slope to eyes in the face



The first step is to determine an average "face-height". This value is application-specific, (ie: an environment with young children requires a lower value). This example assumes an average face height of 5 feet.

The second step is to measure the "subject distance" (from lens to subject), and mounting height for the camera. In order to maintain a vertical slope of 20%, the camera can be mounted approximately .2 feet above the face height for every foot of subject distance.

Maximum Camera Mounting Height (based on average face height of 5′ and a maximum vertical slope of 20%)					
D: Distance to Subject	10′	15′	20′	25′	30′
.2 * D (20% of Distance to Subject)	2′	3′	4′	5′	6′
E: Eye Height	5′	5′	5′	5′	5′
H: Max. Mounting Height	7′	8′	9′	10′	11′

DRAFT

Simple Formula: (D x .2) + E = H

Multiply the subject distance (D) value by .2 (for 20% slope). Add the result to the eye height (E). This equals the maximum mounting height (H).

Example: assuming a 5′ eye height and 15 foot subject distance:

15′ (subject distance) x .2 (slope) = 3′

3′ + 5′ (eye height) = **8′ mounting height**

Remember, a 20% slope is a maximum number – a decreased slope provides better results, (and mounting the camera with no slope, exactly at the average face height, provides the best results).

Example: A potential entry point offers two appropriate mounting positions, one 12 feet away, the other 24 feet away. In this case, the furthest mounting location is most appropriate.

Camera/Lens Specifications

Cameras designated for face-based recording must comply with a wide range of specifications, the most important being the use of high-resolution cameras (480 TVL or greater). The camera and lens must be appropriate to the scene lighting conditions. For example, black & white low-lux or day/night camera for poorly lit areas, and super-dynamic cameras where severe backlighting can occur.

An appropriate 4′ wide field of view, (FoV), is a measurement of the focal length of the lens in relation to the object distance from the camera. While an appropriate "fixed focal length" lens can be utilized, a VariFocal Lens is strongly recommended because the selectable focal length range enables a flexible field-adjustment (fine-tuning) capability.

VariFocal Lenses are available with manual or automatic iris features. Use the automatic iris format in applications where lighting conditions may vary, for example, areas exposed to daytime sunlight.

Lens Selection

Typical VariFocal Lenses fall within the following approximate ranges: 3 to 8 millimeters (mm), 3 to 12mm, 5 to 50mm, and 20 to 100mm. The most common and least expensive are the 3 to 8mm versions, although most face capture applications require the larger size VariFocal Lenses.

Guidelines for Determining Lens Focal Length

A 4′ wide FoV requires 1.2mm per foot of distance from subject; a 4½′ wide FoV requires 1.1mm per foot.

FoV	**Distance From Object / Focal Length Needed for a Camera With 1/3″ CCD**					
	10′	20′	30′	40′	50′	60′
4.0 ft. wide	12mm	24mm	36mm	48mm	60mm	72mm
4.5 ft. wide	11mm	22mm	33mm	44mm	55mm	66mm

The estimates on the previous page assume the use of 1/3″ CCD (the most common size) camera format. Results will vary in applications using different size formats such as ½″ or ¼″. You can obtain lens calculation tools from most camera manufacturers, (online and pocket 'slide-rule' versions).

With megapixel cameras, deployment no longer requires such a large telephoto range when comparing to analog and non-megapixel IP cameras. Evidently, this depends on the particular application. Please refer to the table in the section "Field of View" on page 317 for determining the maximum width for each application.

DRAFT

3VR Face Camera Requirements Chart

1. Face Size	35 pixels between the eyes required. **Rules of thumb:** The field of view when subject is in focus must be less than 4.5 feet, or the face width must be at least 1/7 of the field of view.
2. Zoom	Zoom lens recommended: 5-50mm (5- 15% angle of view)
3. Vertical Slope	Recommended: 20% slope from eye level, (see "Camera Positioning" on page 319) Rule of thumb: the middle of the nose should be higher or at least the same level as the bottom of the earlobes.
4. Horizontal Angle	Rule of thumb: The image must simultaneously show both ears of the subject.
5. Lighting	High quality required with wide dynamic range. Well lit, no harsh shadows or glare.
6. Event Length	There must be a period of time during which the subject is in focus, large enough (face 1/7 of the field of view), well-lit, facing the camera so that both ears are visible, and the middle of the nose is above the bottom of the earlobes. Recommended: 3 seconds, (minimum 2 seconds)
7. Camera Features	B&W or color (appropriate to lighting conditions) Backlight control sometime helpful Manual or Auto-Iris Lens (as appropriate to application)
Examples	Doorways, Hallways, Entrances, Exits Queue Lines Teller Lines

DRAFT

5. CONCLUSION

Importance of Image Quality

This appendix should help you to understand and optimize image quality so that you can now:

- *Better qualify what opportunities are strong fits for 3VR VisionPoint™ VMS*
- *Set the appropriate level of expectations with partners and users*
- *Design a system that accommodates real-world conditions*
- *Deliver a solution that is optimally effective*
- *Deeper understanding of the significant advantages of utilizing megapixel cameras*

Remember the following principles as you install cameras for face recognition:

1)	Any image, whether video or photo, requires sufficient detail. Detail is determined by (1) the level of resolution in the image and (2) the size of the person's face relative to the size of the image.
2)	The person's face must look directly towards the camera. This affects both the class of imported photos that are acceptable and how video cameras must be positioned to capture faces.
3)	Imported images have to meet the requirements listed above. With the exception of mugshots and passport photos, most photos do not meet these requirements.
4)	You must position video cameras specifically to capture faces. The cost may be inexpensive, but the skill is not trivial. Take care to precisely position cameras to capture faces consistently.
5)	Megapixel cameras in your security solution allow a significantly wider field of view, but also require more storage and have a negative impact on the system performance if you do not determine a proper equilibrium.
6)	Understand that determining the maximum mounting height is not affected by the increase in resolution of megapixel cameras. You must use same formula to stay within the 20% slope specification.

DRAFT