NEC Corporation reserves the right to change the specifications, functions, or features at any time without notice.

NEC Corporation has prepared this document for use by its employees and customers. The information contained herein is the property of NEC Corporation and shall not be reproduced without prior written approval of NEC Corporation.

UNIVERGE is a trademark of NEC Corporation of America. Windows and Internet Explorer are registered trademarks of Microsoft Corporation.

Copyright 2017

NEC Corporation of America
3929 W. John Carpenter Freeway
Irving, TX 75063-9406

Communications Technology Group
# Table of Contents

## Regulatory Notice

- FCC Information ................................................................. Regulatory-1
- FCC Conditions ................................................................. Regulatory-1
- EU Conformity Statement .................................................. Regulatory-1
- Industry Canada ICES-003 Compliance ............................... Regulatory-1

## Product Liability

- Using the Equipment Safely .................................................. Product Liability-1
- Safety Considerations .......................................................... Product Liability-1
- Preventive and Cautionary Tips .......................................... Product Liability-2

## Chapter 1  Product Key Features

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>General</td>
<td>1-1</td>
</tr>
<tr>
<td>2</td>
<td>Local Monitoring</td>
<td>1-1</td>
</tr>
<tr>
<td>3</td>
<td>HDD Management</td>
<td>1-2</td>
</tr>
<tr>
<td>4</td>
<td>Recording and Playback</td>
<td>1-2</td>
</tr>
<tr>
<td>5</td>
<td>Backup</td>
<td>1-3</td>
</tr>
<tr>
<td>6</td>
<td>Alarm and Exception</td>
<td>1-3</td>
</tr>
<tr>
<td>7</td>
<td>Other Local Functions</td>
<td>1-3</td>
</tr>
<tr>
<td>8</td>
<td>Network Functions</td>
<td>1-3</td>
</tr>
</tbody>
</table>
Chapter 2 Introduction

Section 1  Front Panel ................................................................. 2-1
Section 2  USB Mouse Operation .................................................. 2-2
Section 3  Input Method Description .......................................... 2-4
Section 4  Rear Panel ................................................................. 2-5

Chapter 3 Getting Started

Section 1  Starting Up and Shutting Down the NVR ...................... 3-1
Section 2  Setting Admin Password .............................................. 3-2
Section 3  Using the Wizard for Basic Configuration .................... 3-4
Section 4  Login and Logout ......................................................... 3-11
   4.1  User Login........................................................................ 3-11
   4.2  User Logout .................................................................... 3-12
Section 5  Adding and Connecting the IP Cameras ..................... 3-13
   5.1  Activating the IP Camera.................................................... 3-13
   5.2  Adding the Online IP Cameras ......................................... 3-15
   5.3  Editing the Connected IP cameras and Configuring Customized Protocols 3-20
   5.4  Editing IP Cameras Connected to the PoE Interfaces. ............ 3-24

Chapter 4 Live View

Section 1  Live View Introduction ............................................... 4-1
Section 2  Operations in Live View .............................................. 4-1
   2.1  Using Mouse in Live View............................................... 4-2
   2.2  Quick Setting Toolbar in Live View Mode .......................... 4-3
Section 3  Adjusting Live View Settings ..................................... 4-7
Section 4  Channel-zero Encoding .............................................. 4-8
Chapter 5  PTZ Controls

Section 1  Configuring PTZ Settings ................................................................. 5-1
Section 2  Setting PTZ Presets, Patrols & Patterns ....................................... 5-2
  2.1 Customizing Presets ........................................................................ 5-2
  2.2 Calling Presets ............................................................................. 5-3
  2.3 Customizing Patrols ....................................................................... 5-4
  2.4 Calling Patrols .............................................................................. 5-6
  2.5 Customizing Patterns ..................................................................... 5-6
  2.6 Calling Patterns ............................................................................ 5-7
  2.7 Customizing Linear Scan Limit ...................................................... 5-8
  2.8 Calling Linear Scan ........................................................................ 5-9
  2.9 One-Touch Park ........................................................................... 5-10
Section 3  PTZ Control Panel .................................................................... 5-11

Chapter 6  Recording Settings

Section 1  Configuring Parameters ............................................................... 6-1
  1.1 Before You Begin .......................................................................... 6-1
  1.2 Configure Parameters .................................................................... 6-2
Section 2  Configuring Recording Schedule ............................................. 6-4
Section 3  Configuring Motion Detection Recording .................................. 6-8
Section 4  Configuring Alarm Triggered Recording .................................... 6-9
Section 5  Configuring VCA Event Recording ........................................... 6-11
Section 6  Manual Recording ................................................................... 6-13
Section 7  Configuring Holiday Recording ................................................ 6-14
Section 8  Configuring Redundant Recording ........................................... 6-16
Section 9  Configuring HDD Group for Recording .................................... 6-18
### Section 10 File Protection

10.1 Locking the Recording Files

10.2 Setting HDD Property to Read-only

### Chapter 7 Playback

#### Section 1 Playing Back Record Files

1.1 Instant Playback

1.2 Playing Back by Normal Search

1.3 Playing Back by Event Search

1.4 Playing Back by Tag

1.5 Playing Back by Smart Playback

1.6 Playing Back by System Logs

1.7 Playing Back External File

1.8 Playing Back by Sub-periods

### Chapter 8 Backup Record Files

#### Section 1 Backing Up Record Files

1.1 Quick Export

1.2 Backing Up by Normal Video Search

1.3 Backing Up by Event Search

1.4 Backing Up Video Clips

#### Section 2 Managing Backup Devices

### Chapter 9 Alarm Settings

#### Section 1 Setting Motion Detection Alarm

#### Section 2 Setting Sensor Alarms
| Section 3 | Detecting Video Loss Alarm | 9-6 |
| Section 4 | Detecting Video Tampering Alarm | 9-8 |
| Section 5 | Handling Exceptions Alarm | 9-10 |
| Section 6 | Setting Alarm Response Actions | 9-11 |
| Section 7 | Triggering or Clearing Alarm Output Manually | 9-15 |

**Chapter 10 VCA Alarm**

| Section 1 | Face Detection | 10-1 |
| Section 2 | Line Crossing Detection | 10-3 |
| Section 3 | Intrusion Detection | 10-5 |
| Section 4 | Region Entrance Detection | 10-7 |
| Section 5 | Region Existing Detection | 10-9 |
| Section 6 | Loitering Detection | 10-9 |
| Section 7 | People Gathering Detection | 10-9 |
| Section 8 | Fast Moving Detection | 10-9 |
| Section 9 | Parking Detection | 10-10 |
| Section 10 | Unattended Baggage Detection | 10-10 |
| Section 11 | Object Removal Detection | 10-10 |
| Section 12 | Audio Exception Detection | 10-11 |
| Section 13 | Sudden Scene Change Detection | 10-12 |
| Section 14 | Defocus Detection | 10-13 |
| Section 15 | PIR Alarm | 10-13 |

**Chapter 11 VCA Search**

| Section 1 | Face Search | 11-1 |
| Section 2 | Behavior Search | 11-4 |
## Chapter 12 Network Settings

**Section 1** Configuring General Settings ........................................ 12-1  
**Section 2** Configuring Advanced Settings ........................................ 12-2  
  2.1 PPPoE Settings.................................................................. 12-2  
  2.2 Configuring Cloud P2P ....................................................... 12-2  
  2.3 Configuring DDNS ............................................................ 12-3  
  2.4 Configuring NTP Server ..................................................... 12-9  
  2.5 Configuring SNMP ............................................................ 12-10  
  2.6 Configuring Remote Alarm Host .......................................... 12-11  
  2.7 Configuring Multicast ....................................................... 12-12  
  2.8 Configuring RTSP ............................................................ 12-12  
  2.9 Configuring Server and HTTP Ports .................................... 12-13  
  2.10 Configuring Email ............................................................ 12-13  
  2.11 Configuring NAT .............................................................. 12-15  

**Section 3** Checking Network Traffic ............................................. 12-19  

**Section 4** Configuring Network Detection ..................................... 12-20  
  4.1 Testing Network Delay and Packet Loss ............................... 12-20  
  4.2 Exporting Network Packet ................................................ 12-21  
  4.3 Checking the Network Status ............................................. 12-22  
  4.4 Checking Network Statistics ............................................. 12-23
Chapter 13 HDD Management

Section 1 Initializing HDDs ................................................................. 13-1
Section 2 Managing Network HDD .................................................... 13-2
Section 3 Managing HDD Group ......................................................... 13-6
  3.1 Setting HDD Groups .............................................................. 13-6
  3.2 Setting HDD Property ............................................................ 13-7
Section 4 Configuring Quota Mode .................................................... 13-8
Section 5 Checking HDD Status ....................................................... 13-10
Section 6 HDD Detection ................................................................. 13-12
Section 7 Configuring HDD Error Alarms ......................................... 13-14

Chapter 14 Camera Settings

Section 1 Configuring OSD Settings .................................................. 14-1
Section 2 Configuring Privacy Mask ................................................. 14-2
Section 3 Configuring Video Parameters .......................................... 14-3

Chapter 15 NVR Management and Maintenance

Section 1 Viewing System Information ............................................. 15-1
Section 2 Searching and Exporting Log Files ................................. 15-1
Section 3 Importing/Exporting IP Camera Information .................... 15-5
Section 4 Importing/Exporting Configuration Files ......................... 15-5
Section 5 Upgrading System .......................................................... 15-6
  5.1 Upgrading by Local Backup Device ........................................ 15-6
  5.2 Upgrading by FTP ............................................................... 15-7
Section 6 Restoring Default Settings ................................................. 15-8
Chapter 16  Miscellaneous

Section 1  Configuring General Settings  ............................................. 16-1
Section 2  Configuring DST Settings  ................................................... 16-2
Section 3  Configuring More Settings for Device Parameters .......... 16-2
Section 4  Managing User Accounts  .................................................... 16-3
  4.1  Adding a User ................................................................... 16-3
  4.2  Deleting a User ................................................................ 16-7
  4.3  Editing a User .................................................................. 16-7

Chapter 17  Troubleshooting

Section 1  Troubleshooting Issues ...................................................... 17-1

Chapter 18  List of Compatible IP Cameras

Chapter A  Glossary

Section 1  Terms and Definitions .......................................................... A-1
# List of Figures and Tables

## Chapter 2  Introduction

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>Front Panel</td>
<td>2-1</td>
</tr>
<tr>
<td>2-2</td>
<td>Control Panel Button Descriptions</td>
<td>2-1</td>
</tr>
<tr>
<td>2-3</td>
<td>Mouse Control</td>
<td>2-3</td>
</tr>
<tr>
<td>2-4</td>
<td>Soft Keyboard (1)</td>
<td>2-4</td>
</tr>
<tr>
<td>2-5</td>
<td>Soft Keyboard (2)</td>
<td>2-4</td>
</tr>
<tr>
<td>2-6</td>
<td>Soft Keyboard Description</td>
<td>2-5</td>
</tr>
<tr>
<td>2-7</td>
<td>Rear Panel without POE Interface</td>
<td>2-5</td>
</tr>
<tr>
<td>2-8</td>
<td>Rear Panel without POE Interface Description</td>
<td>2-5</td>
</tr>
<tr>
<td>2-9</td>
<td>Real Panel for 4-ch Device</td>
<td>2-6</td>
</tr>
<tr>
<td>2-10</td>
<td>Real Panel for 8-ch Device</td>
<td>2-6</td>
</tr>
<tr>
<td>2-11</td>
<td>Rear Panel with POE Interface Description</td>
<td>2-7</td>
</tr>
</tbody>
</table>

## Chapter 3  Getting Started

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-1</td>
<td>Shutdown Menu</td>
<td>3-1</td>
</tr>
<tr>
<td>3-2</td>
<td>Shutdown Attention</td>
<td>3-2</td>
</tr>
<tr>
<td>3-3</td>
<td>Setting Admin Password</td>
<td>3-3</td>
</tr>
<tr>
<td>3-4</td>
<td>Weak Password Warning</td>
<td>3-4</td>
</tr>
<tr>
<td>3-5</td>
<td>Wizard Interface</td>
<td>3-4</td>
</tr>
<tr>
<td>3-6</td>
<td>Date and Time Settings</td>
<td>3-5</td>
</tr>
<tr>
<td>3-7</td>
<td>Network Configuration for Models with POE Interface</td>
<td>3-6</td>
</tr>
<tr>
<td>3-8</td>
<td>Cloud P2P Interface</td>
<td>3-7</td>
</tr>
<tr>
<td>3-9</td>
<td>Advanced Network Parameters</td>
<td>3-8</td>
</tr>
<tr>
<td>3-10</td>
<td>HDD Management</td>
<td>3-9</td>
</tr>
<tr>
<td>3-11</td>
<td>IP Camera Management</td>
<td>3-10</td>
</tr>
<tr>
<td>3-12</td>
<td>Record Settings</td>
<td>3-11</td>
</tr>
<tr>
<td>3-13</td>
<td>Login Interface</td>
<td>3-11</td>
</tr>
</tbody>
</table>
Figure 3-14  User Account Protection ................................................................. 3-12
Figure 3-15  Log Out .................................................................................. 3-12
Figure 3-16  IP Camera Management Interface .............................................. 3-13
Figure 3-17  Activate Camera ...................................................................... 3-14
Figure 3-18  Set New Password ................................................................... 3-14
Figure 3-19  Quick Adding IP Camera Interface .............................................. 3-15
Figure 3-20  Adding IP Camera Interface ..................................................... 3-16
Figure 3-21  Selecting Multiple Channels ..................................................... 3-17
Figure 3-22  Custom Adding IP Camera Interface ........................................... 3-18
Figure 3-23  Successfully Added IP Camera ................................................... 3-19
Table 3-1  IP Camera Management Icons ................................................... 3-19
Figure 3-24  Edit the Parameters ................................................................. 3-20
Figure 3-25  Camera Network Configuration ................................................ 3-21
Figure 3-26  Camera Password Configuration ............................................. 3-22
Figure 3-27  Protocol Management Interface .............................................. 3-23
Figure 3-28  Protocol Setting ..................................................................... 3-24
Figure 3-29  List of Connected Cameras ..................................................... 3-25
Figure 3-30  Edit IP Interface Camera - Manual ........................................... 3-26

Chapter 4  Live View

Table 4-1  Live View Icons ................................................................. 4-1
Table 4-2  Mouse Operation in Live View ................................................... 4-2
Figure 4-1  Right-click Menu ................................................................. 4-3
Figure 4-2  Quick Setting Toolbar ........................................................... 4-3
Table 4-3  Quick Setting Toolbar Icons ................................................... 4-4
Figure 4-3  Digital Zoom ................................................................. 4-5
Figure 4-4  Image Settings Preset ........................................................... 4-5
Figure 4-5  Image Settings Customize ........................................................ 4-6
Figure 4-6  Live View Strategy ................................................................. 4-6
Chapter 5  PTZ Controls

Figure 5-1  PTZ Settings ................................................................. 5-1
Figure 5-2  PTZ General ................................................................. 5-2
Figure 5-3  PTZ Settings ................................................................. 5-3
Figure 5-4  PTZ Panel General ......................................................... 5-4
Figure 5-5  PTZ Settings ................................................................. 5-5
Figure 5-6  Key Point Configuration .................................................. 5-5
Figure 5-7  PTZ Panel - General ......................................................... 5-6
Figure 5-8  PTZ Settings ................................................................. 5-7
Figure 5-9  PTZ Panel - General ......................................................... 5-8
Figure 5-10 PTZ Settings ................................................................. 5-9
Figure 5-11 PTZ Panel - One Touch .................................................... 5-10
Figure 5-12 PTZ Panel - One Touch .................................................... 5-11
Figure 5-13 PTZ Panel ................................................................. 5-12
Figure 5-14 Description of PTZ Panel Icons .................................... 5-12

Chapter 6  Recording Settings

Figure 6-1  HDD General ................................................................. 6-1
Figure 6-2  HDD Advanced ............................................................. 6-2
Figure 6-3  Record Parameters .......................................................... 6-2
Figure 6-4  Record Parameters - More Settings ................................... 6-3
Figure 6-5  Sub-stream Parameters ..................................................... 6-4
Figure 6-6  Record Schedule ........................................................... 6-5
Figure 6-7  Recording Schedule Interface .......................................... 6-6
Figure 6-8  Edit Schedule ................................................................. 6-6
Figure 6-9  Draw the Schedule .......................................................... 6-7
Figure 6-10 Motion Detection - Mask .................................................. 6-8
<table>
<thead>
<tr>
<th>Figure 6-11</th>
<th>Motion Detection Handling ................................................................. 6-9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 6-12</td>
<td>Alarm Settings .................................................................................. 6-10</td>
</tr>
<tr>
<td>Figure 6-13</td>
<td>Alarm Input ....................................................................................... 6-10</td>
</tr>
<tr>
<td>Figure 6-14</td>
<td>Alarm Input Settings ......................................................................... 6-11</td>
</tr>
<tr>
<td>Figure 6-15</td>
<td>VCA Settings ..................................................................................... 6-12</td>
</tr>
<tr>
<td>Figure 6-16</td>
<td>Set Trigger Camera ........................................................................... 6-13</td>
</tr>
<tr>
<td>Figure 6-17</td>
<td>Manual Record ................................................................................... 6-14</td>
</tr>
<tr>
<td>Figure 6-18</td>
<td>Holiday Settings ............................................................................... 6-15</td>
</tr>
<tr>
<td>Figure 6-19</td>
<td>Edit Holiday Settings ....................................................................... 6-15</td>
</tr>
<tr>
<td>Figure 6-20</td>
<td>HDD General ..................................................................................... 6-16</td>
</tr>
<tr>
<td>Figure 6-21</td>
<td>HDD General - Edit ........................................................................... 6-17</td>
</tr>
<tr>
<td>Figure 6-22</td>
<td>Record Parameters ............................................................................ 6-18</td>
</tr>
<tr>
<td>Figure 6-23</td>
<td>HDD General ..................................................................................... 6-18</td>
</tr>
<tr>
<td>Figure 6-24</td>
<td>Storage Mode ................................................................................... 6-19</td>
</tr>
<tr>
<td>Figure 6-25</td>
<td>Normal Playback ............................................................................... 6-20</td>
</tr>
<tr>
<td>Figure 6-26</td>
<td>Locked File Management ................................................................... 6-21</td>
</tr>
<tr>
<td>Figure 6-27</td>
<td>Export ............................................................................................... 6-22</td>
</tr>
<tr>
<td>Figure 6-28</td>
<td>Export - Search Results .................................................................... 6-23</td>
</tr>
<tr>
<td>Figure 6-29</td>
<td>Unlock Notice ................................................................................... 6-23</td>
</tr>
<tr>
<td>Figure 6-30</td>
<td>HDD General ..................................................................................... 6-24</td>
</tr>
<tr>
<td>Figure 6-31</td>
<td>HDD General Editing ......................................................................... 6-24</td>
</tr>
</tbody>
</table>

**Chapter 7  Playback**

<table>
<thead>
<tr>
<th>Figure 7-1</th>
<th>Instant Playback Interface ................................................................. 7-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 7-2</td>
<td>Right-click Menu Under Live View ................................................... 7-2</td>
</tr>
<tr>
<td>Figure 7-3</td>
<td>Playback Calendar ............................................................................. 7-3</td>
</tr>
<tr>
<td>Figure 7-4</td>
<td>Playback Interface .......................................................................... 7-4</td>
</tr>
<tr>
<td>Figure 7-5</td>
<td>Playback Toolbar ............................................................................. 7-4</td>
</tr>
<tr>
<td>Figure 7-6</td>
<td>Playback Toolbar Buttons ................................................................ 7-5</td>
</tr>
<tr>
<td>Figure 7-7</td>
<td>Motion Search Interface ................................................................... 7-6</td>
</tr>
<tr>
<td>Figure 7-8</td>
<td>7 Interface of Playback by Event .................................................... 7-7</td>
</tr>
</tbody>
</table>
Chapter 8  Backup Record Files

Figure 8-1  Quick Export Interface ......................................................... 8-1
Figure 8-2  Quick Export Using USB1-1 .................................................. 8-2
Figure 8-3  Export Complete ................................................................. 8-2
Figure 8-4  Check Quick Export Results ............................................... 8-3
Figure 8-5  Normal Video Search for Backup ......................................... 8-4
Figure 8-6  Normal Video Search for Backup Results ............................. 8-5
Figure 8-7  Export Normal Video Search using USB Flash Drive .............. 8-6
Figure 8-8  Export Complete Dialog ...................................................... 8-6
Figure 8-9  Event Search for Backup ...................................................... 8-7
Figure 8-10 Event Search Results .......................................................... 8-8
Figure 8-11 Video Clips Export Interface ............................................... 8-9
Figure 8-12 Storage Device Management ............................................. 8-10

Chapter 9  Alarm Settings

Figure 9-1  Motion Detection Setup Interface ........................................ 9-1
Figure 9-2  Set Trigger Camera of Motion Detection .............................. 9-2
Figure 9-3  Alarm Status Interface of System Configuration .................... 9-3
Chapter 10  VCA Alarm

Figure 10-1  Face Detection ................................................................. 10-2
Figure 10-2  Set Face Detection Sensitivity ........................................ 10-3
Figure 10-3  Set Line Crossing Detection Rules .................................... 10-4
Figure 10-4  Line Draw for Line Crossing Detection ............................ 10-4
Figure 10-5  Intrusion Crossing Detection Tools ................................. 10-6
Figure 10-6  Draw Area for Intrusion Detection ................................... 10-7
Figure 10-7  Set Region Entrance Detection ....................................... 10-8
Figure 10-8  Set Audio Exception Detection Rules .............................. 10-12

Chapter 11  VCA Search

Figure 11-1  Face Search ................................................................. 11-2
Figure 11-2  Face Search Interface ................................................... 11-3
Figure 11-3  Export Files ............................................................... 11-4
Figure 11-4  Behavior Search Interface ............................................. 11-5
Chapter 12 Network Settings

Figure 12-1 Network Settings Interface ................................................................. 12-1
Figure 12-2 PPPoE Settings Interface ................................................................. 12-2
Figure 12-3 IPServer Settings Interface ............................................................ 12-3
Figure 12-4 DynDNS Settings Interface ............................................................. 12-4
Figure 12-5 PeanutHull Settings Interface ......................................................... 12-4
Figure 12-6 NO-IP Settings Interface .............................................................. 12-5
Figure 12-7 SimpleDDNS Settings Interface ..................................................... 12-5
Figure 12-8 Register Account .......................................................................... 12-6
Figure 12-9 Register New User ........................................................................ 12-7
Figure 12-10 Register Device .......................................................................... 12-8
Figure 12-11 Access Device via Client Software .............................................. 12-9
Figure 12-12 NTP Settings Interface ................................................................. 12-10
Figure 12-13 SNMP Settings Interface ............................................................. 12-11
Figure 12-14 More Settings Interface ............................................................... 12-11
Figure 12-15 Configure Multicast ................................................................. 12-12
Figure 12-16 RTSP Settings Interface ............................................................... 12-12
Figure 12-17 Host Other Settings Interface ..................................................... 12-13
Figure 12-18 Network Settings Interface ......................................................... 12-14
Figure 12-19 Email Settings Interface ............................................................. 12-14
Figure 12-20 Email Testing Message ............................................................... 12-15
Figure 12-21 UPnP™ Settings Interface ......................................................... 12-16
Figure 12-22 UPnP™ Settings Finished - Auto ................................................. 12-16
Figure 12-23 External Port Settings Dialog ..................................................... 12-17
Figure 12-24 UPnP™ Settings Finished - Manual ............................................ 12-17
Figure 12-25 External Port Settings Dialog ..................................................... 12-18
Chapter 13  HDD Management

Figure 13-1  Message Box of Uninitialized HDD .................................................. 13-1
Figure 13-2  HDD Information Interface ............................................................ 13-1
Figure 13-3  Confirm Initialization ................................................................. 13-2
Figure 13-4  Status Change to Initializing ...................................................... 13-2
Figure 13-5  Status Change to Normal .......................................................... 13-2
Figure 13-6  HDD Information Interface ........................................................ 13-3
Figure 13-7  Add NetHDD Interface .............................................................. 13-3
Figure 13-8  Add NAS Disk .......................................................................... 13-4
Figure 13-9  Add IP SAN Disk ..................................................................... 13-5
Figure 13-10 Initialize Added NetHDD ......................................................... 13-5
Figure 13-11 Storage Mode Interface ............................................................ 13-6
Figure 13-12 Reboot Attention ..................................................................... 13-6
Figure 13-13 Local HDD Settings ............................................................... 13-7
Figure 13-14 Confirm HDD Settings ............................................................. 13-7
Figure 13-15 Set HDD Property ................................................................. 13-8
Figure 13-16 Storage Mode Interface Settings ............................................. 13-9
Figure 13-17 Configure Record Quota .......................................................... 13-9
Figure 13-18 Copy Settings to Other Cameras ............................................. 13-10
Figure 13-19 View HDD Status (1) .............................................................. 13-11
Figure 13-20 View HDD Status (2) .............................................................. 13-12
Chapter 14  Camera Settings

Figure 14-1  OSD Configuration Interface .......................................................... 14-1
Figure 14-2  Privacy Mask Setting Interface ...................................................... 14-2
Figure 14-3  Set Privacy Mask Area ................................................................. 14-3
Figure 14-4  Image Settings Interface .............................................................. 14-3

Chapter 15  NVR Management and Maintenance

Figure 15-1  Device Information Interface ......................................................... 15-1
Figure 15-2  Log Search Interface .................................................................. 15-2
Figure 15-3  Log Search Results ..................................................................... 15-3
Figure 15-4  Log Details .............................................................................. 15-4
Figure 15-5  Export Log Files ......................................................................... 15-4
Figure 15-6  Import/Export Config Files .......................................................... 15-6
Figure 15-7  Local Upgrade Interface .............................................................. 15-7
Figure 15-8  FTP Upgrade Interface ............................................................... 15-8
Figure 15-9  Restore Defaults ...................................................................... 15-8

Chapter 16  Miscellaneous

Figure 16-1  General Settings Interface ......................................................... 16-1
Figure 16-2  DST Settings Interface ............................................................... 16-2
Figure 16-3  More Settings Interface ............................................................ 16-2
Figure 16-4  User Management Interface ...................................................... 16-3
Figure 16-5  Add User Menu ...................................................................... 16-4
Figure 16-6  Added User Listed in User Management Interface ................. 16-5
Figure 16-7  User Permissions Setting Interface ................................................. 16-5
Figure 16-8  User List ................................................................................. 16-7
Figure 16-9  Edit User Interface ................................................................. 16-8

Chapter 17  Troubleshooting

Figure 17-1  Windows Task Manager Interface .............................................. 17-6

Chapter 18  List of Compatible IP Cameras

Table 18-1  List of Compatible IP Cameras ..................................................... 18-2
Regulatory Notice

FCC Information

FCC compliance: This equipment has been tested and found to comply with the limits for a digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information refer to www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information refer to:

www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.
Using the Equipment Safely

These instructions are intended to ensure that the user can use the product correctly to avoid danger or property loss. The precaution measure is divided into 'Danger' and 'Warning':

**Danger**: Serious injury or death may be caused if any of these warnings are neglected.

**Warning**: Injury or equipment damage may be caused if any of these cautions are neglected.

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DANGER</strong></td>
<td>Incorrect use of the equipment may cause personal injury or death.</td>
</tr>
<tr>
<td><img src="image" alt="DANGER" /></td>
<td></td>
</tr>
<tr>
<td><strong>WARNING</strong></td>
<td>Incorrect use of the equipment may cause personal injury or a serious system fault.</td>
</tr>
<tr>
<td><img src="image" alt="WARNING" /></td>
<td></td>
</tr>
</tbody>
</table>

Safety Considerations

- **DANGER**: Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 100–240 VAC or 12 VDC according to the IEC60950-1 standard. Please refer to technical specifications for detailed information.

- **WARNING**: Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.
  - In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region. Please refer to technical specifications for detailed information.
  - Do not connect several devices to one power adapter as adapter overload may cause over-heating or a fire hazard.
  - Please make sure that the plug is firmly connected to the power socket.
  - If smoke, odor or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.
Preventive and Cautionary Tips

Before connecting and operating your device, please be advised of the following tips:

- Ensure unit is installed in a well-ventilated, dust-free environment.
- Unit is designed for indoor use only.
- Keep all liquids away from the device.
- Ensure environmental conditions meet factory specifications.
- Ensure unit is properly secured to a rack or shelf. Major shocks or jolts to the unit as a result of dropping it may cause damage to the sensitive electronics within the unit.
- Use the device in conjunction with an UPS if possible.
- Power down the unit before connecting and disconnecting accessories and peripherals.
- A factory recommended HDD should be used for this device.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the manufacturer.
**Product Key Features**

**Section 1  General**

- Connectible to network cameras, network dome and encoders.
- Connectible to the third-party network cameras like ACTI, Arecont, AXIS, Bosch, Brickcom, Canon, PANASONIC, Pelco, SAMSUNG, SANYO, SONY, Vivotek and ZAVIO, and cameras that adopt ONVIF or PSIA protocol.
- Connectible to the smart IP cameras.
- PAL/NTSC adaptive video inputs.
- Each channel supports dual-stream.
- Up to 16 network cameras can be connected.
- Independent configuration for each channel, including resolution, frame rate, bit rate, image quality, etc.
- The quality of the input and output record is configurable.

**Section 2  Local Monitoring**

- Simultaneous HDMI™ and VGA outputs.
- HDMI™ and VGA outputs at up to 1920×1080 resolution.
- Multiple screen display in live view is supported, and the display sequence of channels is adjustable.
- Live view screen can be switched in group, and manual switch and automatic cycle live view are also provided, and the interval of automatic cycle can be adjusted.
- Quick setting menu is provided for live view.
- Motion detection, video tampering, VCA (Video Content Analysis) alarm, video exception alert and video loss alert functions.
- Privacy mask.
SECTION 3 HDD MANAGEMENT

- For 8ch/16ch models, 2 SATA hard disks can be connected; For 4ch models, 1 SATA hard disk can be connected;
- Each disk with a maximum of 6TB storage capacity.
- 8 network disks (NAS/IP SAN disks) can be connected.
- Support S.M.A.R.T. and bad sector detection.
- HDD group management.
- Support HDD standby function.
- HDD property: redundancy, read-only, read/write (R/W).
- HDD quota management; different capacity can be assigned to different channel.

SECTION 4 RECORDING AND PLAYBACK

- Holiday recording schedule configuration.
- Continuous and event video recording parameters.
- Multiple recording types: manual, continuous, alarm, motion, motion | alarm, motion & alarm, and VCA.
- 8 recording time periods with separated recording types each day.
- Pre-record and post-record for alarm, motion detection for recording, and pre-record time for schedule and manual recording.
- Searching record files by events (alarm input/motion detection/VCA).
- Playback by sub-periods.
- Tag adding for record files, searching and playing back by tags.
- Locking and unlocking record files.
- Local redundant recording.
- Provide new playback interface with easy and flexible operation.
- Searching and playing back record files by camera No., recording type, start time, end time, etc.
- Smart search for the selected area in the video.
- Zooming in when playback.
- Reverse playback of multi-channel.
Supports pause, play reverse, speed up, speed down, skip forward, and skip backward when playback, and locating by dragging the mouse.

Up to 16-ch synchronous playback.

SECTION 5 BACKUP

- Export video data by USB or SATA device.
- Export video clips when playback.
- Management and maintenance of backup devices.

SECTION 6 ALARM AND EXCEPTION

- Configurable arming time of alarm input/output.
- Alarm for video loss, motion detection, VCA, video tampering, HDD full, HDD error, network disconnected, IP confliction, illegal login, abnormal record, and PoE power overload (for the models support PoE interfaces only), etc.
- Alarm triggers full screen monitoring, audio alarm, notifying surveillance center, sending email and alarm output.
- Automatic restore when system is abnormal.
- Support VCA detection alarm and VCA search.

SECTION 7 OTHER LOCAL FUNCTIONS

- Operable by front panel (depends on model) and mouse.
- Three-level user management; admin user is allowed to create many operating accounts and define their operating permission, which includes the limit to access any channel.
- Operation, alarm, exceptions and log recording and searching.
- Manually triggering and clearing alarms.
- Import and export of device configuration information.

SECTION 8 NETWORK FUNCTIONS

- 1 self-adaptive 10M/100M/1000M network interfaces are provided.
- Up to 16 independent PoE network interfaces are provided for POE series.
IPv6 is supported.
TCP/IP protocol, PPPoE, DHCP, DNS, DDNS, NTP, SADP, SMTP, SNMP, NFS, and iSCSI are supported.
TCP, UDP and RTP for unicast.
Auto/Manual port mapping by UPnPTM.
Extranet access by SimpleDDNS.
Support access by Cloud P2P.
Remote reverse playback via RTSP.
Support accessing by the platform via ONVIF.
Remote search, playback, download, locking and unlocking of the record files, and the breakpoint resume is supported for downloading files.
Remote parameters setup; remote import/export of device parameters.
Remote viewing of the device status, system logs and alarm status.
Remote keyboard operation.
Remote locking and unlocking of control panel and mouse.
Remote HDD formatting and program upgrading.
Remote system restart and shutdown.
Alarm and exception information can be sent to the remote host
Remotely start/stop recording.
Remotely start/stop alarm output.
Remote JPEG capture.
Two-way audio and voice broadcasting.
Embedded WEB server.
SECTION 1  FRONT PANEL

Figure 2-1 Front Panel and Table 2-1 Control Panel Button Descriptions provide an overview of the front panel of the Network Video Recorder system.

Table 2-1  Control Panel Button Descriptions

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power</td>
<td>POWER indicator turns green when DVR is powered up.</td>
</tr>
<tr>
<td></td>
<td>Status</td>
<td>STATUS indicator lights in red when data is being read from or written to HDD.</td>
</tr>
<tr>
<td></td>
<td>Tx/Rx</td>
<td>Tx/Rx indicator blinks green when network connection is functioning properly.</td>
</tr>
</tbody>
</table>
A regular 3-button (Left/Right/Scroll-wheel) USB mouse can also be used with this NVR. To use a USB mouse do the following:

1. Plug USB mouse into one of the USB interfaces on the front panel of the NVR.
2. The mouse should automatically be detected. If in a rare case the mouse is not detected, the possible reason may be that the two devices are not compatible. Please refer to the recommended device list from your provider.

Table 2-2 Mouse Control details the operation of the mouse.
Table 2-2  Mouse Control

<table>
<thead>
<tr>
<th>Name</th>
<th>Action</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Single-click</td>
<td>Live view: Select channel and show the quick set menu.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Menu: Select and enter.</td>
</tr>
<tr>
<td></td>
<td>Double-click</td>
<td>Live view: Switch between single-screen and multi-screen.</td>
</tr>
<tr>
<td>Left-click</td>
<td>Click and Drag</td>
<td>PTZ control: pan, tilt and zoom.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Video tampering, privacy mask and motion detection: Select target area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital zoom-in: Drag and select target area.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Live view: Drag channel/time bar.</td>
</tr>
<tr>
<td>Right-click</td>
<td>Single-click</td>
<td>Live view: Show menu.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Menu: Exit current menu to upper level menu.</td>
</tr>
<tr>
<td>Scroll-Wheel</td>
<td>Scrolling up</td>
<td>Live view: Previous screen.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Menu: Previous item.</td>
</tr>
<tr>
<td></td>
<td>Scrolling down</td>
<td>Live view: Next screen.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Menu: Next item.</td>
</tr>
</tbody>
</table>
SECTION 3    INPUT METHOD DESCRIPTION

Figure 2-2  Soft Keyboard (1)

Figure 2-3  Soft Keyboard (2)

Figure 2-4  Soft Keyboard Description provides a description of the buttons on the soft keyboard.
SECTION 4  REAR PANEL

The rear panel varies depending on the model.

Rear Panel without POE Interface

Table 2-3 Rear Panel without POE Interface Description provides an overview of the rear panel interface.

<table>
<thead>
<tr>
<th>Number</th>
<th>Item</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power Supply</td>
<td>DC 12V power supply.</td>
</tr>
<tr>
<td>2</td>
<td>Audio In</td>
<td>RCA connector for audio input.</td>
</tr>
<tr>
<td>3</td>
<td>HDMI™ Interface</td>
<td>HDMI™ video output connector.</td>
</tr>
</tbody>
</table>
Rear Panel with POE Interface

**Table 2-3 Rear Panel without POE Interface Description**

<table>
<thead>
<tr>
<th>Number</th>
<th>Item</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>LAN Network Interface</td>
<td>10 /100 /1000 Mbps self-adaptive Ethernet interface</td>
</tr>
<tr>
<td>5</td>
<td>Audio Out</td>
<td>RCA connector for audio output.</td>
</tr>
<tr>
<td>6</td>
<td>VGA Interface</td>
<td>DB9 connector for VGA output. Display local video output and menu.</td>
</tr>
<tr>
<td>7</td>
<td>USB Interface</td>
<td>Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).</td>
</tr>
<tr>
<td>8</td>
<td>Ground</td>
<td>Ground (needs to be connected when NVR starts up).</td>
</tr>
<tr>
<td>9</td>
<td>Power Switch</td>
<td>Switch for turning on/off the device.</td>
</tr>
</tbody>
</table>

**Rear Panel with POE Interface**

*Figure 2-6  Real Panel for 4-ch Device*

*Figure 2-7  Real Panel for 8-ch Device*
The 16-ch devices have both 8 and 16 independent 100 Mbps PoE network interfaces models.

Table 2-4 Rear Panel with POE Interface Description provides an overview of the rear panel interface.

<table>
<thead>
<tr>
<th>Number</th>
<th>Item</th>
<th>Function Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power Supply</td>
<td>DC 48V power supply for 4-ch device and AC 100~240V for 8-ch and 16-ch devices.</td>
</tr>
<tr>
<td>2</td>
<td>Audio In</td>
<td>RCA connector for audio input.</td>
</tr>
<tr>
<td>3</td>
<td>HDMI™ Interface</td>
<td>HDMI™ video output connector.</td>
</tr>
<tr>
<td>4</td>
<td>LAN Network Interface</td>
<td>10 /100 /1000 Mbps self-adaptive Ethernet interface</td>
</tr>
<tr>
<td>5</td>
<td>Audio Out</td>
<td>RCA connector for audio output.</td>
</tr>
<tr>
<td>6</td>
<td>VGA Interface</td>
<td>DB9 connector for VGA output. Display local video output and menu.</td>
</tr>
<tr>
<td>7</td>
<td>USB Interface</td>
<td>Universal Serial Bus (USB) ports for additional devices such as USB mouse and USB Hard Disk Drive (HDD).</td>
</tr>
<tr>
<td>8</td>
<td>Ground</td>
<td>Ground (needs to be connected when NVR starts up).</td>
</tr>
<tr>
<td>9</td>
<td>Power Switch</td>
<td>Switch for turning on/off the device.</td>
</tr>
<tr>
<td>10</td>
<td>Network Interfaces with PoE function</td>
<td>Network interfaces for the cameras and to provide power over Ethernet.</td>
</tr>
</tbody>
</table>
PROPER startup and shutdown procedures are crucial to expanding the life of the NVR.

Before you begin, check that the voltage of the extra power supply is the same as the NVR's requirement, and the ground connection is working properly.

Starting Up the NVR

1. Check that the power supply is plugged into an electrical outlet. It is **HIGHLY** recommended that an Uninterruptible Power Supply (UPS) be used in conjunction with the device. The Power indicator LED on the front panel should be red, indicating the device is receiving the power supply.

2. Turn on the power switch on the rear panel if the device starts up for the first time, or press the button on the front panel of the model support front panel buttons. The Power indicator LED should turn green indicating that the unit begins to start up.

Shutting Down the NVR

1. Enter the Shutdown menu, **Menu > Shutdown**. See Figure 3-1.

2. Click the **Shutdown** button.

3. Click the **Yes** button.
4. Turn off the power switch on the rear panel when the shutdown attention pops up (Figure 3-2).

---

**Figure 3-2  Shutdown Attention**

---

Rebooting the NVR

From the shutdown menu, you are also able to reboot the NVR.

1. Enter the Shutdown menu by clicking **Menu > Shutdown**.
2. Click the **Logout** button to lock the NVR or the **Reboot** button to reboot the NVR.

---

**SECTION 2  SETTING ADMIN PASSWORD**

For first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation.

1. Input the same password in the text field of **Create New Password** and **Confirm New Password**.
2. Click **OK** to save the password and activate the device.

For the old version device, if you update it to the new version, Figure 3-4 displays once the device starts up. You can click **YES** and follow the wizard to set a strong password.

**NOTE**

*STRONG PASSWORD RECOMMENDED* We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
Section 3 Using the Wizard for Basic Configuration

After the admin password is set, the setup wizard pops up automatically. It takes you through some basic settings of the NVR.
1. If you don’t want to use the setup wizard at that moment, click the Exit button. You can also choose to use the Setup Wizard next time by leaving the Start wizard when the device starts? checkbox checked.

2. Click the Next button to enter the Date and Time Settings interface.

3. After the time settings, click the Next button which takes you back to the Basic Network Setup Wizard interface.
4. Click the **Next** button after you configure the basic network parameters. Then you need to enter the Cloud P2P interface. Configure the Cloud P2P according to your needs.

**NOTE**

For the models have the PoE the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.
5. Click the **Next** button to enter the Advanced Network Parameter interface. You can enable PPPoE, enable DDNS, and set other ports according to your needs.
6. After configuration finishes, click the **Next** button to enter HDD Management interface.
7. To initialize the HDD, click the Init button. Initialization removes all the data saved in the HDD.

8. Click the Next button to enter the IP Camera Management interface.

9. Click Search to search. The online IP Camera and the Security status shows whether it is active or inactive. Before adding the camera, make sure the IP camera to be added is in active status.
   
   If the camera is in inactive status, click the inactive icon of the camera to set the password to activate it. You can also select multiple cameras from the list and click One-touch Activate to activate the cameras in batch.

10. Click Add to add the camera.
11. Click **Next**. Then configure the recording for the searched IP Cameras.
12. Click **OK** to complete the Setup Wizard.

**SECTION 4  LOGIN AND LOGOUT**

4.1 User Login

If NVR has logged out, you must login to the device before operating the menu and other functions.

1. Select the **User Name** in the dropdown list.
2. Input **Password**.
3. Click **OK** to log in.

---

**NOTE**

The device gets locked for 60 seconds if the admin user performs 7 failed password attempts (5 attempts for the guest/operator).

---

4.2 User Logout

After logging out, the monitor turns to the live view mode and if you want to perform some operation, you need to enter user name and password to log in again.

1. Enter the Shutdown menu. **Menu > Shutdown**.

---

**Figure 3-15 Log Out**

2. Click **Logout**.
SECTION 5  ADDING AND CONNECTING THE IP CAMERAS

5.1 Activating the IP Camera

Before adding the camera, make sure the IP camera to be added is in active status.

1. Select the Add IP Camera option from the right-click menu in live view mode or click Menu > Camera > Camera to enter the IP camera management interface.

   For the IP camera detected online in the same network segment, the Security status shows whether it is active or inactive.

   Figure 3-16  IP Camera Management Interface

2. Click the inactive icon of the camera to enter the interface to activate it. You can also select multiple cameras from the list and click the One-touch Activate to activate the cameras in batch.
3. Set the password of the camera to activate it. Checking the **Use Admin Password**, ensures the camera(s) will be configured with the same admin password of the operating NVR.

**Create New Password**: If the admin password is not used, you must create the new password for the camera and confirm it.

**STRONG PASSWORD RECOMMENDED**- **We highly recommend** you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. **And we recommend** you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to finish the activating of the IP camera. The security status of camera will be changed to **Active**.
5.2 Adding the Online IP Cameras

The main function of the NVR is to connect the network cameras and record the video received from it. Before you can get a live view or record of the video, you should add the network cameras to the connection list of the device. Before you start, ensure the network connection is valid and correct. For details on checking and configuring the network, please see Chapter 12 Section 3 - Checking Network Traffic (page 12-19) and Chapter 12 Section 4 - Configuring Network Detection (page 12-20).

Option 1

1. Click to select an idle window in the live view mode.
2. Click the icon in the center of the window to display the adding IP camera interface.

3. Select the detected IP camera and click the Add button to add it directly. You can also click the Search button to refresh the online IP camera manually.

Or you can choose to custom add the IP camera by editing the parameters in the corresponding text field and then click the Add button.
Option 2

1. Select the Add IP Camera option from the right-click menu in live view mode or click Menu > Camera > Camera to enter the IP camera management interface.

2. The online cameras with same network segment will be detected and displayed in the camera list.

3. Select the IP camera from the list and click the button to add the camera. Or you can click the One-touch Adding button to add all cameras from the list.

4. (For encoders with multiple channels only) check the checkbox Channel Port in the pop-up window, as shown in Figure 3-21 Selecting Multiple Channels. Click OK to add multiple channels.
Option 3

1. On the IP Camera Management interface, click the **Custom Adding** button to display the Add IP Camera (Custom) interface.

*Figure 3-21  Selecting Multiple Channels*
2. You can edit the IP address, protocol, management port, and other information of the IP camera to be added.

If the IP camera to be added has not been activated, you can activate it from the IP camera list on the camera management interface.

3. (Optional) Check **Continue to Add** to add other IP cameras.

4. Click **Add** to add the camera. For the successfully added IP cameras, the Security status shows the security level of the password of camera: **strong password**, **weak password** and **risk password**.
Table 3-1 provides a brief explanation of the icons depicted in Figure 3-23.

**Table 3-1  IP Camera Management Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Edit icon" /></td>
<td>Edit basic parameters of the camera</td>
</tr>
<tr>
<td><img src="image" alt="Warning icon" /></td>
<td>The camera is disconnected; you can click the icon to get the exception information of camera.</td>
</tr>
<tr>
<td><img src="image" alt="Play icon" /></td>
<td>Play the live video of the connected camera.</td>
</tr>
<tr>
<td><img src="image" alt="Upgrade icon" /></td>
<td>Upgrade the connected IP camera.</td>
</tr>
<tr>
<td><img src="image" alt="Add icon" /></td>
<td>Add the detected IP camera.</td>
</tr>
</tbody>
</table>
5.3 Editing the Connected IP cameras and Configuring Customized Protocols

After the adding of the IP cameras, the basic information of the camera lists in the page. You can configure the basic settings of the IP cameras.

1. Click the icon to edit the parameters; you can edit the IP address, protocol, and other parameters.

<table>
<thead>
<tr>
<th>Table 3-1 IP Camera Management Icons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
</tr>
<tr>
<td>![Delete icon]</td>
</tr>
<tr>
<td>![Advanced settings icon]</td>
</tr>
<tr>
<td>![Security icon]</td>
</tr>
</tbody>
</table>

Figure 3-24 Edit the Parameters
**Channel Port**: If the connected device is an encoding device with multiple channels, you can choose the channel to connect by selecting the Channel Port number from the drop-down list.

2. Click **OK** to save the settings and exit the editing interface.

**Edit Advanced Parameters**

1. Drag the horizontal scroll bar to the right side and click the icon.

![Figure 3-25 Camera Network Configuration](image)

2. From here, you can edit the network information and the password of the camera.
3. Click OK to save the settings and exit the interface.

**Configuring Customized Protocols**

To connect the network cameras which are not configured with the standard protocols, you can configure the customized protocols for them.

1. Click the **Protocol** button in the custom adding IP camera interface to enter the protocol management interface.
There are 16 customized protocols provided in the system. You can edit the protocol name and choose whether to enable the sub-stream.

2. Choose the protocol type of transmission and choose the transfer protocols.

Before customizing the protocol for the network camera, you have to contact the manufacturer of the network camera to consult the URL (uniform resource locator) for getting main stream and sub-stream.

The format of the URL is: [Type]://[IP Address of the network camera]:[Port]/[Path]. For example: rtsp://192.168.0.1:554/ch1/main/av_stream.

**Protocol Name**: Edit the name for the custom protocol.

**Enable Substream**: If the network camera does not support sub-stream or the sub-stream is not needed, leave the checkbox empty.

**Type**: The network camera adopting custom protocol must support getting stream through standard RTSP.

**Transfer Protocol**: Select the transfer protocol for the custom protocol.

**Port**: Set the port number for the custom protocol.

**Path**: Set the resource path for the custom protocol. E.g., ch1/main/av_stream.
3. Choose the protocols you just added to validate the connection of the network camera.

5.4 Editing IP Cameras Connected to the PoE Interfaces.

NOTE
This chapter is applicable only for the models with POE interface.

The PoE interfaces enables the NVR system to pass electrical power safely, along with data, on Ethernet cabling to the connected network cameras.

The POE series provides up to 16 PoE interfaces which can connect to 16 network cameras directly; and if you disable the PoE interface, you can also connect to the online network cameras. The PoE interface also supports the Plug-and-Play function.
For example, for 8-ch NVR, when you want to connect 2 online cameras and connect 6 network cameras via PoE interfaces, you must disable 2 PoE interfaces in the **Edit IP Camera** menu.

**To Add Cameras for NVR Supporting PoE Function**

Before you start, connect the network cameras via the PoE interfaces.

1. Enter the Camera Management interface: **Menu > Camera > Camera**.

2. Click the **button, and select the **Adding Method** in the drop-down list.

   - **Plug-and-Play**: Means that the camera is connected to the PoE interface, so in this case, the parameters of the camera can't be edited. The IP address of the camera can only be edited in the Network Configuration interface, see Chapter 12 Section 1 - Configuring General Settings (page 12-1) for detailed information.

   - **Manual**: You can disable the PoE interface by selecting manual while the current channel can be used as a normal channel and the parameters can also be edited.

   *The cameras connecting to the PoE interface cannot be deleted in this menu.*
Input the **IP Camera Address**, the **User Name** and **Admin Password** manually, and click **OK** to add the IP camera.

*Figure 3-30  Edit IP Interface Camera - Manual*
**Live View**

**SECTION 1   **LIVE VIEW INTRODUCTION

Live view shows you the video image received from each camera in real time. The NVR automatically enters Live View mode when powered on. It is also at the very top of the menu hierarchy, thus pressing **ESC** many times (depending on which menu you're on) brings you to the Live View mode.

**Live View Icons**

In the live view mode, there are icons (**Table 4-1**) at the upper-right of the screen for each channel, showing the status of the record and alarm in the channel, so that you can know whether the channel is recorded, or whether there are alarms occur as soon as possible.

<table>
<thead>
<tr>
<th><strong>Table 4-1 Live View Icons</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Icon</strong></td>
</tr>
<tr>
<td>![Alarm icon]</td>
</tr>
<tr>
<td>![Record icon]</td>
</tr>
<tr>
<td>![Alarm and Record icon]</td>
</tr>
<tr>
<td>![Event/Exception icon]</td>
</tr>
</tbody>
</table>

**SECTION 2   **OPERATIONS IN LIVE VIEW

In live view mode, there are many functions provided. The functions are listed below.

- **Single Screen**: showing only one screen on the monitor.
Multi-screen: showing multiple screens on the monitor simultaneously.

Auto-switch: the screen is auto switched to the next one. And you must set the dwell time for each screen on the configuration menu before enabling the auto-switch. Menu > Configuration > Live View > Dwell Time.

Start Recording: continuous record and motion detection record are supported.

Output Mode: select the output mode to Standard, Bright, Gentle or Vivid.

Add IP Camera: the shortcut to the IP camera management interface.

Playback: playback the recorded videos for current day.

2.1 Using Mouse in Live View

Table 4-2 describes the using the mouse in Live View.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common Menu</td>
<td>Quick access to the sub-menus which you frequently visit.</td>
</tr>
<tr>
<td>Menu</td>
<td>Enter the main menu of the system by right clicking the mouse.</td>
</tr>
<tr>
<td>Single Screen</td>
<td>Switch to the single full screen by choosing channel number from the drop-down list.</td>
</tr>
<tr>
<td>Multi-screen</td>
<td>Adjust the screen layout by choosing from the drop-down list.</td>
</tr>
<tr>
<td>Previous Screen</td>
<td>Switch to the previous screen.</td>
</tr>
<tr>
<td>Next Screen</td>
<td>Switch to the next screen.</td>
</tr>
<tr>
<td>Start/Stop Auto-switch</td>
<td>Enable/disable the auto-switch of the screens.</td>
</tr>
<tr>
<td>Start Recording</td>
<td>Start continuous recording or motion detection recording of all channels.</td>
</tr>
<tr>
<td>Add IP Camera</td>
<td>Enter the IP Camera Management interface, and manage the cameras.</td>
</tr>
<tr>
<td>Playback</td>
<td>Enter the playback interface and start playing back the video of the selected channel immediately.</td>
</tr>
<tr>
<td>Output Mode</td>
<td>Four modes of output supported, including Standard, Bright, Gentle and Vivid.</td>
</tr>
</tbody>
</table>

The dwell time of the live view configuration must be set before using Start Auto-switch.
If the corresponding camera supports intelligent function, the Reboot Intelligence option is included when right-clicking mouse on this camera.

---

**Figure 4-1 Right-click Menu**

![](image)

**NOTE**

The right-click menu varies according to different models, please refer to the actual GUI menu of the device.

---

### 2.2 Quick Setting Toolbar in Live View Mode

On the screen of each channel, there is a quick setting toolbar which displays when you single click the mouse in the corresponding screen.

---

**Figure 4-2 Quick Setting Toolbar**

![](image)
Table 4-3 describes the Quick Setting Toolbar icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Enable/Disable Manual Record.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Instant Playback</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Mute / Audio on</td>
</tr>
<tr>
<td>![Icon]</td>
<td>PTZ Control</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Digital Zoom</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Image Settings</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Live View Strategy</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Information</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Close</td>
</tr>
</tbody>
</table>

Instant Playback only shows the record in the last five minutes. If no record is found, it means there is no record during the last five minutes.

Digital Zoom zooms in the selected area to the full screen. Left-click and draw to select the area to zoom in, as shown in Figure 4-3.
Select the **Image Settings** icon to enter the Image Settings menu (Figure 4-4).

From here, you can set the image parameters like brightness, contrast, saturation and hue.
Select **Live View Strategy** to set strategy, including Real-time, Balanced, and Fluency.
SECTION 3  ADJUSTING LIVE VIEW SETTINGS

Live View settings can be customized according to different needs. You can configure the output interface, dwell time for screen to be shown, mute or turning on the audio, the screen number for each channel, etc.

Enter the Live View Settings interface. Menu > Configuration > Live View.

The settings available in this menu include:

- **Video Output Interface**: Designates the output to configure the settings for. Only VGA/ HDMI is selectable by default.

- **Live View Mode**: Designates the display mode to be used for Live View.

- **Dwell Time**: The time in seconds to dwell between switching of channels when enabling auto-switch in Live View.

- **Enable Audio Output**: Enables/disables audio output for the selected video output.

- **Volume**: Adjust the volume of live view, playback, and two-way audio for the selected output interface.

- **Event Output**: Designates the output to show event video.

- **Full Screen Monitoring Dwell Time**: The time in seconds to show alarm event screen.
Setting Cameras Order

1. Select a View mode in [image].

2. Select the small window, and double-click on the channel number to display the channel on the window.

3. If you do not want the camera to be displayed on the live view interface, click the corresponding [image] to stop it.

4. You can also click the [image] button to start live view for all the channels and click [image] to stop all the live view.

5. Click the Apply button to save the settings.

SECTION 4 CHANNEL-ZERO ENCODING

Sometimes you need to get a remote view of many channels in real time from web browser or CMS (Client Management System) software. In order to decrease the bandwidth requirement without affecting the image quality, channel-zero encoding is supported as an option for you.

1. Enter the Live View Settings interface. Menu > Configuration > Live View.
2. Select the **Channel-Zero Encoding** tab.

3. Check the checkbox after **Enable Channel Zero Encoding**.

4. Configure the **Frame Rate**, **Max. Bitrate Mode** and **Max. Bitrate**.
   After you set the Channel-Zero encoding, you can get a view in the remote client or web browser of 16 channels in one screen.
SECTION 1 CONFIGURING PTZ SETTINGS

Follow the procedure below to set the parameters for PTZ. Configuring of the PTZ parameters should be done before you control the PTZ camera.

1. Enter the PTZ Settings interface. Menu > Camera > PTZ.

2. Click the **RS-485 Settings** button to set the RS-485 parameters.
3. Choose the camera for PTZ setting in the Camera drop-down list.

4. Enter the parameters of the PTZ camera. All the parameters should be exactly the same as the PTZ camera parameters.

5. Click Apply to save the settings.

SECTION 2  SETTING PTZ PRESETS, PATROLS & PATTERNS

Before you begin, please make sure that the presets, patrols, and patterns are supported by PTZ protocols.

2.1 Customizing Presets

1. Enter the PTZ Control interface. Menu > Camera > PTZ.
2. Use the directional button to wheel the camera to the location where you want to set preset. The zoom and focus operations can be recorded in the preset as well.

3. Enter the preset number (1~255) in the preset text field, and click Set to link the location to the preset. Repeat the steps 2-3 to save more presets. Click Clear to clear the location information of the preset, or click Clear All to clear the location information of all the presets.

2.2 Calling Presets

This feature enables the camera to point to a specified position such as a window when an event takes place.

1. Click the PTZ button in the lower-right corner of the PTZ setting interface. Or, press the PTZ button on the front panel or click the PTZ Control icon in the quick setting bar, or select the PTZ option in the right-click menu to show the PTZ control panel.

2. Choose Camera from the drop-down list.

3. Click the button to show the general settings of the PTZ control.
2.3 Customizing Patrols

Patrons can be set to move the PTZ to different key points and have it stay there for a set duration before moving on to the next key point. The key points correspond to the presets. The presets can be set following the steps set out in Chapter 2.1 - Customizing Presets (page 5-2).

1. Enter the PTZ Control interface. **Menu > Camera > PTZ.**
2. Select a patrol number from the drop-down list of patrol.

3. Click **Set** to add key points for the patrol.

4. Configure key point parameters, such as the key point number, duration of staying for one key point, and speed of patrol. The key point corresponds to the preset. The **Key Point** number determines the order which the PTZ follows while cycling through the patrol. **Duration** refers to the time span to stay at the corresponding key point. **Speed** defines the speed at which the PTZ moves from one key point to the next.
5. Click **Add** to add the next key point to the patrol. Click **OK** to save the key point to the patrol.

You can delete all the key points by clicking **Clear** for the selected patrol, or click **Clear All** to delete all the key points for all patrols.

### 2.4 Calling Patrols

Calling a patrol makes the PTZ move according to the predefined patrol path.

1. Click the **PTZ** button in the lower-right corner of the PTZ setting interface; Or press the **PTZ** button on the front panel or click the **PTZ Control** icon in the quick setting bar, or select the **PTZ** option in the right-click menu to show the PTZ control panel.

2. Click **** to show the general settings of the PTZ control.

![Figure 5-7 PTZ Panel - General](image)

3. Select a patrol from the drop-down list and click **Call Patrol** to call it.

4. Click the **Stop Patrol** button to stop calling it.

### 2.5 Customizing Patterns

Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ movement according to the predefined path.

1. Enter the PTZ Control interface. **Menu > Camera > PTZ.**
2. Choose pattern number from the drop-down list.

3. Click the **Start** button and click corresponding buttons in the control panel to move the PTZ camera, and click the **Stop** button to stop it. The movement of the PTZ is recorded as the pattern.

### 2.6 Calling Patterns

Follow this procedure to move the PTZ camera according to predefined patterns.

1. Click the **PTZ** button in the lower-right corner of the PTZ setting interface. Or press the **PTZ** button on the front panel or click the **PTZ Control** icon in the quick setting bar, or select the **PTZ** option in the right-click menu to show the PTZ control panel.

2. Click **** to show the general settings of the PTZ control.
3. Click **Call Pattern** to call it.
4. Click **Stop Pattern** to stop calling it.

### 2.7 Customizing Linear Scan Limit

The Linear Scan can be enabled to trigger the scan in the horizontal direction in the predefined range.

*NOTE* This function is supported by certain models.

1. Enter the PTZ Control interface. **Menu > Camera > PTZ.**
2. Use the directional button to wheel the camera to the location where you want to set the limit, and click the **Left Limit** or **Right Limit** button to link the location to the corresponding limit.

   *The speed dome starts linear scan from the left limit to the right limit, and you must set the left limit on the left side of the right limit, as well the angle from the left limit to the right limit should be no more than 180°.*

### 2.8 Calling Linear Scan

*Before operating this function, make sure the connected camera supports the linear scan and is in HIKVISION protocol.*

Follow this procedure to call the linear scan in the predefined scan range.

1. Click the **PTZ** button in the lower-right corner of the PTZ setting interface; Or press the **PTZ** button on the front panel or click the **PTZ Control** icon in the quick setting bar to enter the **PTZ** setting menu in live view mode.

2. Click **∫** to show the one-touch function of the PTZ control.
3. **Click the Linear Scan button** to start the linear scan and **click the Linear Scan button again** to stop it.

   **Click the Restore button** to clear the defined left limit and right limit data. The dome needs to reboot in order for the settings to take effect.

### 2.9 One-Touch Park

Before operating this function, make sure the connected camera supports the linear scan and is in **HIKVISION** protocol.

For certain models of the speed dome, they can be configured to start a predefined park action (scan, preset, patrol and etc.) automatically after a period of inactivity (park time).

1. **Click the PTZ button** in the lower-right corner of the PTZ setting interface; Or press the PTZ button on the front panel or click the **PTZ Control icon** in the quick setting bar to enter the PTZ setting menu in live view mode.

2. **Click** to show the one-touch function of the PTZ control.
3. There are 3 one-touch park types selectable. Click the corresponding button to activate the park action.

**Park (Quick Patrol):** The dome starts patrol from the predefined preset 1 to preset 32 in order of the park time. The undefined preset will be skipped.

**Park (Patrol 1):** The dome starts move according to the predefined patrol 1 path after the park time.

**Park (Preset 1):** The dome moves to the predefined preset 1 location after the park time.

![PTZ Panel - One Touch](image)

**NOTE**

The park time can only be set through the speed dome configuration interface, by default the value is 5s.

4. Click the button again to inactivate it.

## SECTION 3  PTZ CONTROL PANEL

To enter the PTZ control panel, there are two ways supported.

- **OPTION 1:** In the PTZ settings interface, click the **PTZ** button on the lower-right corner which is next to the **Back** button.

- **OPTION 2:** In the **Live View** mode, you can press the **PTZ Control** button on the front panel or choose the **PTZ Control** icon, or select the **PTZ** option in the right-click menu. Click **Configuration** on the control panel, and you can enter the PTZ Settings interface.
In PTZ control mode, the PTZ panel will be displayed when a mouse is connected with the device. If no mouse is connected, the PTZ icon appears in the lower-left corner of the window, indicating that this camera is in PTZ control mode.

**Figure 5-13  PTZ Panel**

**Figure 5-14  Description of PTZ Panel Icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Icon</th>
<th>Description</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Direction button and the auto-cycle button" /></td>
<td>Direction button and the auto-cycle button</td>
<td><img src="image2" alt="Zoom+, Focus+, Iris+" /></td>
<td>Zoom+, Focus+, Iris+</td>
<td><img src="image3" alt="Zoom-, Focus-, Iris-" /></td>
<td>Zoom-, Focus-, Iris-</td>
</tr>
<tr>
<td><img src="image4" alt="The speed of the PTZ movement" /></td>
<td>The speed of the PTZ movement</td>
<td><img src="image5" alt="Light on/off" /></td>
<td>Light on/off</td>
<td><img src="image6" alt="Wiper on/off" /></td>
<td>Wiper on/off</td>
</tr>
<tr>
<td><img src="image7" alt="3D-Zoom" /></td>
<td>3D-Zoom</td>
<td><img src="image8" alt="Image Centralization" /></td>
<td>Image Centralization</td>
<td><img src="image9" alt="Menu" /></td>
<td>Menu</td>
</tr>
<tr>
<td><img src="image10" alt="Switch to the PTZ control interface" /></td>
<td>Switch to the PTZ control interface</td>
<td><img src="image11" alt="Switch to the one-touch control interface" /></td>
<td>Switch to the one-touch control interface</td>
<td><img src="image12" alt="Switch to the general settings interface" /></td>
<td>Switch to the general settings interface</td>
</tr>
<tr>
<td><img src="image13" alt="Previous item" /></td>
<td>Previous item</td>
<td><img src="image14" alt="Next item" /></td>
<td>Next item</td>
<td><img src="image15" alt="Start pattern / patrol" /></td>
<td>Start pattern / patrol</td>
</tr>
<tr>
<td><img src="image16" alt="Stop the patrol / pattern movement" /></td>
<td>Stop the patrol / pattern movement</td>
<td><img src="image17" alt="Exit" /></td>
<td>Exit</td>
<td><img src="image18" alt="Minimize windows" /></td>
<td>Minimize windows</td>
</tr>
</tbody>
</table>
Section 1 Configuring Parameters

Follow the procedure below to set the parameters for PTZ. The configuring of PTZ parameters should be done before you control the PTZ camera.

By configuring the parameters, you can define the parameters which affect the image quality, such as the transmission stream type, the resolution, and so on.

1.1 Before You Begin

Before you begin, perform the steps below.

1. Make sure that the HDD has already been installed. If not, please install an HDD and initialize it. (Menu > HDD > General).

2. Check the storage mode of the HDD.

Click Advanced to check the storage mode of the HDD.

If the HDD mode is Quota, please set the maximum record capacity For detailed information, see Chapter 13 Section 4 - Configuring Quota Mode (page 13-8).

If the HDD mode is Group, you must set the HDD group. For detailed information, see Chapter 6 Section 9 - Configuring HDD Group for Recording (page 6-18).
1.2 Configure Parameters

Enter the Record settings interface to configure the recording parameters: Menu > Record > Parameters.

Parameters Setting for Recording

1. Select Record tab page to configure. You can configure the stream type, the resolution, and other parameters on your demand.
2. Click More Settings to set the advanced parameters for recording and then click OK to finish editing.
Pre-record: The time you set to record before the scheduled time or event. For example, when an alarm triggered the recording at 10:00, if you set the pre-record time as 5 seconds, the camera records it at 9:59:55.

Post-record: The time you set to record after the event or the scheduled time. For example, when an alarm triggered the recording ends at 11:00, if you set the post-record time as 5 seconds, it records till 11:00:05.

Expired Time: The expired time is the longest time for a record file to be kept in the HDD, if the deadline is reached, the file will be deleted. You can set the expired time to 0, and then the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

Redundant Record: Enabling redundant record means you save the recording files in the redundant HDD. See Chapter 6 Section 8 - Configuring Redundant Recording (page 6-16).

Record Audio: Click the checkbox to enable or disable audio recording.

Video Stream: Main stream and sub-stream are selectable for recording. When you select sub-stream, you can record for a longer time with the same storage space.

3. Click Apply to save the settings.
Parameters Settings for Sub-stream

1. Enter the Sub-stream tab page.

2. Configure the parameters of the camera.

3. Click **Apply** to save the settings.

**NOTE**
- The redundant record is to decide whether you want the camera to save the recording files in the redundant HDD. You must configure the redundant HDD in HDD settings. For detailed information, see Chapter 13 3.2 - Setting HDD Property (page 13-7).
- The parameters of Main Stream (Event) are read-only.

**SECTION 2**  **CONFIGURING RECORDING SCHEDULE**

Set the recording schedule, and the camera automatically starts/stops recording according to the configured schedule.

Enter the Record Schedule interface. **Menu > Record > Schedule.**
Configure Record Schedule

1. Select Record Schedule.

Different recording types are marked in different color icons.
- **Continuous**: Scheduled recording.
- **Event**: Recording triggered by all event triggered alarm.
- **Motion**: Recording triggered by motion detection.
- **Alarm**: Recording triggered by alarm.
- **M/A**: Recording triggered by either motion detection or alarm.
- **M&A**: Recording triggered by motion detection and alarm.

2. Choose the camera you want to configure.

3. Select the check box after Enable Schedule.
4. Click **Edit** or click on the color icon under Edit and draw the schedule line on the panel.

**Edit the Schedule**

1. In the message box, you can choose the day to which you want to set schedule.

   ![Recording Schedule Interface](image)

   **Figure 6-7 Recording Schedule Interface**

   Click the **button to set the accurate time of the schedule.

2. To schedule an all-day recording, check the checkbox after the **All Day** item.

   ![Edit Schedule](image)

   **Figure 6-8 Edit Schedule**

3. To arrange other schedules, leave the **All Day** checkbox blank and set the **Start/End** time.

   ![Scheduled Recording](image)

   **Up to 8 periods can be configured for each day. And the time periods cannot be overlapped each other.**
4. Select the record type in the drop-down list.

- To enable Motion, Alarm, M | A (motion or alarm), M & A (motion and alarm) and VCA (Video Content Analysis) triggered recording and capture, you must configure the motion detection settings, alarm input settings or VCA settings as well.

- The VCA settings are only available to the smart IP cameras.

Repeat the above edit schedule steps to schedule recording for other days in the week. Click Copy to enter the Copy to interface to copy the schedule settings to other days.

5. Click Apply in the Record Schedule interface to save the settings.

**Draw the Schedule**

1. Click on the color icons. You can choose the schedule type as continuous or event.

2. Click Apply to validate the settings.
SECTION 3 CONFIGURING MOTION DETECTION RECORDING

Follow the steps in this procedure to set the motion detection parameters. In the live view mode, once a motion detection event takes place, the NVR can analyze it and perform actions to handle it. Enabling the motion detection function triggers certain channels to start recording, or triggers full screen monitoring, audio warning, notify the surveillance center and so on.

Enter the Motion Detection interface. Menu > Camera > Motion.

Configure Motion Detection

1. Choose camera you want to configure.
2. Check the checkbox after Enable Motion Detection.
3. Drag and draw the area for motion detection by mouse. If you want to set the motion detection for all the area shot by the camera, click Full Screen. To clear the motion detection area, click Clear.

4. Click Settings, and the message box for channel information displays.
5. Select the channels which you want the motion detection event to trigger recording.

6. Click **Apply** to save the settings.

7. Click **OK** to back to the upper level menu.

8. Exit the Motion Detection menu.

Edit the Motion Detection Record Schedule. For detailed information of schedule configuration, see Chapter 6 Section 2 - Configuring Recording Schedule (page 6-4).

### SECTION 4 CONFIGURING ALARM TRIGGERED RECORDING

Follow the procedure to configure alarm triggered recording.

1. Enter the Alarm setting interface. **Menu > Configuration > Alarm.**
2. Click the **Alarm Input** tab and set the alarm parameters.

- Select **Alarm Input** number and configure alarm parameters.
- Choose **N.O** (normally open) or **N.C** (normally closed) for alarm type.
- Check the checkbox for **Enable**.
- Click **Settings**.
Choose the alarm triggered recording channel.

Check the checkbox to select the channel.

Click **Apply** to save settings.

Click **OK** to back to the upper level menu.

Repeat the above steps to configure other alarm input parameters.

If the settings can also be applied to other alarm inputs, click **Copy** and choose the alarm input number.

3. Edit the **Alarm triggered record** in the Record Schedule setting interface. For detailed information of schedule configuration, see Chapter 6 Section 2 - Configuring Recording Schedule (page 6-4).

### SECTION 5  **CONFIGURING VCA EVENT RECORDING**

The event triggered recording can be configured through the menu. Then events include the motion detection, alarm and VCA events (face detection/face capture, line crossing detection, intrusion detection, region entrance detection, region exiting detection, loitering detection, people gathering detection, fast moving detection, parking detection, unattended baggage detection, object removal detection, audio loss exception detection, sudden change of sound intensity detection, and defocus detection).
1. Enter the VCA settings interface and select a camera for the VCA settings.  
   Menu > Camera > VCA.

2. Configure the detection rules for VCA events. For details, see step 2 in  
   Chapter 10 - VCA Alarm (page 10-1).

3. Click the icon to configure the alarm linkage actions for the VCA events.

4. Select the Trigger Channel tab and select one or more channels which will  
   start to record when VCA alarm is triggered.

5. Click Apply to save the settings.
6. Enter Record Schedule settings interface (Menu > Record > Schedule > Record Schedule), and set VCA as the record type. For details, see step 2 in Chapter 6 Section 2 - Configuring Recording Schedule (page 6-4).

**SECTION 6  MANUAL RECORDING**

Follow the steps to set parameters for the manual record. Using manual record, you need to manually cancel the record. The manual recording is prior to the scheduled recording.

1. Enter the Manual settings interface, Menu > Manual; or press the REC/S-HT button on the front panel.
2. Enable the **Manual Record**.
   Select **Record** on the left bar by clicking the status button before camera number to change **OFF** to **ON**.

3. Disable manual record by clicking the status button to change **ON** to **OFF**.
   The green **ON** icon means that the channel is configured in the record schedule. After rebooting, all the manual records enabled are canceled.

**SECTION 7  CONFIGURING HOLIDAY RECORDING**

Follow these steps to configure the record schedule on holidays for that year.

1. Enter the Record setting interface. **Menu > Record > Holiday**.
2. Enable Edit Holiday schedule. Click to enter the Edit interface.
Check the checkbox after Enable Holiday.
Select Mode from the drop-down list. There are three different modes for the date format to configure holiday schedule.
Set the start and end date.
Click Apply to save settings.
Click OK to exit the Edit interface.

3. Enter Record Schedule settings interface to edit the holiday recording schedule. See Chapter 6 Section 2 - Configuring Recording Schedule (page 6-4).

SECTION 8 CONFIGURING REDUNDANT RECORDING

Enabling redundant recording, which means saving the recording files not only in the R/W HDD but also in the redundant HDD, effectively enhances the data safety and reliability.

1. Enter HDD Information interface. Menu > HDD.

Figure 6-20 HDD General

2. Select the HDD and click to enter the Local HDD Settings interface.
   - Set the HDD property to Redundancy.
- Click **Apply** to save the settings.
- Click **OK** to back to the upper level menu.

**NOTE**

You must set the Storage mode in the HDD advanced settings to Group before you set the HDD property to Redundant. For detailed information, please refer to Chapter 13 3.2 - Setting HDD Property (page 13-7). There should be at least another HDD which is in Read/Write status.

3. Enter the Record setting interface. **Menu > Record > Parameters**.
   - Select the **Record** tab.
   - Click **More Settings** to enter the following interface.
- Check the checkbox of **Redundant Record**.
- Click **OK** to save settings and back to the upper level menu.

4. Repeat the above steps for configuring other channels.

**SECTION 9  CONFIGURING HDD GROUP FOR RECORDING**

You can group HDDs and save the record files in certain HDD groups.

1. Enter HDD setting interface. **Menu > HDD**.

2. Select **Advanced** on the left side menu.
Check whether the storage mode of the HDD is **Group**. If not, set it to **Group**. For detailed information, please refer to Chapter 13 Section 3 - Managing HDD Group (page 13-6).

3. Select **General** in the left side menu.

4. Click ![Icon](image) to enter editing interface.

5. Configure HDD group.
   - Choose a group number for the HDD group.
   - Click **Apply** and then in the pop-up message box, click **Yes** to save your settings.
   - Click **OK** to back to the upper level menu. Repeat the above steps to configure more HDD groups.

6. Choose the Channels which you want to save the record files in the HDD group.
   - Select **Advanced** on the left bar.
   - Choose **Group number** in the drop-down list of **Record on HDD Group**.
   - Check the channels you want to save in this group.
   - Click **Apply** to save settings.

---

**NOTE**

After having configured the HDD groups, you can configure the Recording settings following the procedure provided in Section 2 Configuring Recording Schedule on page 6-4 and Section 7 Configuring Holiday Recording on page 6-14.

---

**SECTION 10  FILE PROTECTION**

You can lock the recording files or set the HDD property to Read-only to protect the record files from being overwritten.
10.1 Locking the Recording Files

Lock File When Playback

1. Enter Playback interface. **Menu > Playback.**
2. Check the checkbox of channel(s) in the channel list and then double-click to select a date on the calendar.

![Normal Playback](image)

**NOTE**

In the multi-channel playback mode, clicking the button will lock all the record files related to the playback channels.

3. During playback, click the button to lock the current recording file.

4. Click the button to display the file management interface. Click the Locked File tab to check and export the locked files.
In the File Management interface, click to change it to to unlock the file. The file is not protected.

**Lock File When Export**

1. Enter Export setting interface. **Menu > Export**.
2. Select the channels you want to investigate by setting the checkbox to.
3. Configure the record type, file type, and start/end time.
4. Click **Search** to show the results.
5. Protect the record files.

- Find the record files you want to protect, and then click the icon which turns to , indicating that the file is locked. The record files of which the recording is still not completed cannot be locked.

- Click to change it to to unlock the file. The file is not protected.
10.2 Setting HDD Property to Read-only

1. Enter HDD setting interface. **Menu > HDD.**

   ![HDD General](image)

2. Click **to edit the HDD you want to protect.**

   ![HDD General Editing](image)

3. Set the HDD property to **Read-only.**

4. Click **OK** to save settings and back to the upper level menu.

   **NOTE**
   To edit HDD property, you need to set the storage mode of the HDD to **Group.** See Chapter 13 Section 3 - Managing HDD Group (page 13-6).
NOTE

- You cannot save any files in a Read-only HDD. If you want to save files in the HDD, change the property to R/W.

- If there is only one HDD and is set to Read-only, the NVR can't record any files. Only live view mode is available.

- If you set the HDD to Read-only when the NVR is saving files in it, then the file will be saved in next R/W HDD. If there is only one HDD, the recording will be stopped.
SECTION 1 PLAYING BACK RECORD FILES

1.1 Instant Playback

Play back the recorded video files of a specific channel in the live view mode. Channel switch is supported.

Instant Playback by Channel

Choose a channel in live view mode and click the button in the quick setting toolbar.

In the instant playback mode, only record files recorded during the last five minutes on this channel will be played back.

Figure 7-1 Instant Playback Interface
1.2 Playing Back by Normal Search

Playback by Channel

Enter the Playback interface. Using the mouse, right click a channel in live view mode and select **Playback** from the menu, as shown in Figure 7-2.

**Figure 7-2  Right-click Menu Under Live View**

![Right-click Menu Under Live View](image)

---

**NOTE**

Pressing numerical buttons will switch playback to the corresponding channels during playback process.

Playback by Time

Play back video files recorded in specified time duration. Multi-channel simultaneous playback and channel switch are supported.

1. Enter playback interface. **Menu > Playback**.
2. Check the checkbox of channel(s) in the channel list and then double-click to select a date on the calendar.
Playback Interface

You can use the toolbar in the bottom part of the Playback interface to control the playing progress.

NOTE

If there are record files for that camera in that day, in the calendar, the icon for that day is displayed as . Otherwise it is displayed as .
Click the channel(s) to execute simultaneous playback of multiple channels.

On the toolbar indicates the start/end time of the record.

On the Playback progress bar, use the mouse to click any point of the progress bar or drag the progress bar to locate specific frames. Figure 7-6 provides a brief explanation of the Playback toolbar buttons.
1.3 Playing Back by Event Search

Play back record files on one or several channels searched out by event type (e.g., alarm input, motion detection and VCA).

1. Enter the Playback interface. **Menu > Playback.**
2. Select the **Event** in the drop-down list on the top-left side.
3. Select **Alarm Input, Motion** or **VCA** as the event type.

We will use playback by VCA as an example.
4. Select the minor type of VCA from the drop-down list. For configuring the VCA recording, please refer to Chapter 6 Section 5 - Configuring VCA Event Recording (page 6-11).

5. Select the camera(s) for searching, and set the Start time and End time.

6. Click **Search** to get the search result information. You may refer to the right-side bar for the result.

7. Click the button to play back the file. Pre-play and post-play can be configured.

8. Use the toolbar in the bottom part of Playback interface to control the playing process.
You can click the << or >> button to select the previous or next event. Please refer to Figure 7-6 for the description of buttons on the toolbar.

1.4 Playing Back by Tag

Video tag allows you to record related information like people and location of a certain time point during playback. You can use video tag(s) to search for record files and position time point.

Preparing to Play Back by Tag

1. Enter Playback interface. Menu > Playback.
2. Search and play back the record file(s). Refer to Chapter 7 Section 1 - Playing Back Record Files (page 7-1) for detailed information about searching and playback of the record files.
- Click the button to add default tag.
- Click the button to add customized tag and input tag name.

A maximum of 64 tags can be added to a single video file.

3. To manage tags, click the button to enter the File Management interface and click **Tag** to manage the tags. You can check, edit, and delete tag(s).
Playing Back by Tag

1. Select the Tag from the drop-down list in the Playback interface.
2. Choose channels, edit start time and end time, and then click Search to enter Search Result interface.

![Figure 7-10 7 Tag Management Interface](image)

NOTE

You can enter keyword in the text box **Keyword** to search the tag on your command.

3. Click the button to play back the selected tag file.

You can click Back to return back to the search interface. Pre-play and post-play can be configured.

You can click the or button to select the previous or next tag. Please refer to Figure 7-6 for a description of buttons on the toolbar.

1.5 Playing Back by Smart Playback

The smart playback function provides an easy way to get through the less effective information. When you select the smart playback mode, the system analyzes the video containing the motion or VCA information, marks it with green color and plays it in the normal speed while the video without motion is played in 16-time speed. The smart playback rules and areas are configurable.
To get the smart search result, the corresponding event type must be enabled and configured on the IP camera. Here we take the intrusion detection as an example.

- Log in the IP camera by the web browser, and enable the intrusion detection by checking the checkbox. You may enter the motion detection configuration interface by **Configuration > Advanced Configuration > Events > Intrusion Detection**.

- Configure the required parameters of intrusion detection, including area, arming schedule, and linkage methods. Refer to the user manual of smart IP camera for detailed instructions.

1. Enter Playback interface. **Menu > Playback**.
2. Select **Smart** in the drop-down list on the top-left side.
3. Select a camera in the camera list.
4. Select a date in the calendar and click the ➔ button on the left toolbar to play the video file.
5. Set the rules and areas for smart search of VCA event or motion event.

**Line Crossing Detection**: Select the button and click on the image to specify the start point and end point of the line.

**Intrusion Detection**: Click the button, and specify four points to set a quadrilateral region for intrusion detection. Only one region can be set.

**Motion Detection**: Click the button and then click and draw the mouse to set the detection area manually. Click the button to set the full screen as the detection area.

6. Click to configure the smart settings.
**Skip the Non-Related Video**: The non-related video will not be played if this function is enabled.

**Play Non-Related Video at**: Set the speed to play the non-related video. Max./8/4/1 are selectable.

**Play Related Video at**: Set the speed to play the related video. Max./8/4/1 are selectable. Pre-play and post-play is not available for the motion event type.

7. Click 🕵️‍♂️ to search and play the matched video files.

8. (Optional) Click 🕵️‍♂️ to filter the searched video files by setting the target characters, including the gender and age of the human and whether he/she wears glasses.

---

**Figure 7-15 Set Result Filter**

![Figure 7-15 Set Result Filter](image)

**1.6 Playing Back by System Logs**

Play back record file(s) associated with channels after searching system logs.

1. Enter the Log Information interface. **Menu > Maintenance > Log Information.**

2. Click the **Log Search** tab to enter **Playback by System Logs**. Set search time and type and click the **Search** button.
3. Choose a log with record file and click the play button to enter Playback interface.
4. Use the toolbar in the bottom part of the Playback interface to control the playing process.
1.7 Playing Back External File

Perform the following steps to look up and play back files in the external devices.

1. Enter Tag Search interface. Menu > Playback.
2. Select the External File in the drop-down list on the top-left side. The files are listed in the right-side list. You can click the Refresh button to refresh the file list.
3. Select and click the Play button to play it back. You can adjust the playback speed by clicking ▶️ and ◀️.

1.8 Playing Back by Sub-periods

The video files can be played in multiple sub-periods simultaneously on the screens.

1. Enter Playback interface. Menu > Playback.
2. Select Sub-periods from the drop-down list in the upper-left corner of the page to enter the Sub-periods Playback interface.
3. Select a date and start playing the video file.
4. Select the Split-screen Number from the dropdown list. Up to 16 screens are configurable.
According to the defined number of split-screens, the video files on the selected date can be divided into average segments for playback. E.g., if there are video files existing between 16:00 and 22:00, and the 6-screen display mode is selected, then it can play the video files for 1 hour on each screen simultaneously.
Backup Record Files

SECTION 1 BACKING UP RECORD FILES

Export record files to backup device(s) quickly.

1.1 Quick Export

1. Enter Video Export interface. Menu > Export > Normal. Choose the channel(s) you want to back up and click the Quick Export button.

NOTE The time duration of record files on a specified channel cannot exceed one day. Otherwise, the message box “Max. 24 hours are allowed for quick export.” will pop up.

Figure 8-1 Quick Export Interface
2. Select the format of the log files to be exported. Up to nine formats are available.

3. Click **Export** to start exporting.

   ![Figure 8-2 Quick Export Using USB1-1](image)

   *NOTE*  
   Here we use USB Flash Drive and please refer to **Backing Up by Normal Video Search** on page 8-3 for more backup devices supported by the NVR.

   ![Figure 8-3 Export Complete](image)

   Stay in the Exporting interface until all record files are exported.

4. Check the backup result. The Player file **player.exe** is exported automatically during record file export.
1.2 Backing Up by Normal Video Search

You can backup the record files to various devices, such as USB devices (USB flash drives, USB HDDs, USB writer), SATA writer and e-SATA HDD.

Backup using USB flash drives and USB HDDs

2. Select the cameras to search.
3. Set search condition and click Search to enter the search result interface. The matched video files are displayed in Chart or List display mode.
4. Select video files or pictures from the **Chart** or **List** to export. Click to play the record file if you want to check it. Check the checkbox before the record files you want to back up.

 NOTE: The size of the currently selected files is displayed in the lower-left corner of the window.
5. Export the video files or picture files. Click **Export All** to export all the files. Or you can select recording files you want to back up, and click **Export** to enter Export interface.

If the inserted USB device is not recognized:
- Click the **Refresh** button.
- Reconnect the device.
- Check for compatibility from vendor.

You can also format USB flash drives or USB HDDs via the device.
Stay in the Exporting interface until all record files are exported. A pop-up message box **Export finished** displays.

**The backup of video files using USB writer or SATA writer has the same operating instructions.**
1.3 Backing Up by Event Search

Back up event-related record files using USB devices (USB flash drives, USB HDDs, USB writer), SATA writer or eSATA HDD. Quick Backup and Normal Backup are supported.

1. Enter Export interface. **Menu > Export > Event.**
2. Select the cameras to search.
3. Select the event type to alarm input, motion or VCA.

4. Set search condition and click **Search** to enter the search result interface.
   The matched video files are displayed in **Chart** or **List** display mode.

5. Select video files from the **Chart** or **List** interface to export.
6. Export the video files. Please refer to step 5 of Backing Up by Normal Video Search on page 8-3 for details.

1.4 Backing Up Video Clips

You may also select video clips in playback mode to export directly during playback, using USB devices (USB flash drives, USB HDDs, USB writer), SATA writer or eSATA HDD.

1. Enter Playback interface. Please refer to Chapter 7 section Section 1 - Playing Back Record Files (page 7-1).

2. During playback, use buttons or in the playback toolbar to start or stop clipping record file(s).

3. Click to enter the file management interface.
4. Export the video clips in playback. Please refer to step 5 of Chapter 8 section 1.2 - Backing Up by Normal Video Search (page 8-3) for details.

SECTION 2 MANAGING BACKUP DEVICES

Management of USB Flash Drives and USB HDDs

1. Enter the Export interface.
2. Conduct Backup device management.

Click **New Folder** if you want to create a new folder in the backup device. Select a record file or folder in the backup device and click the **button** if you want to delete it.

Click **Erase** if you want to erase the files from a re-writable CD/DVD. Click **Format** to format the backup device.

**NOTE**

- Click the Refresh button.
- Reconnect device.
- Check for compatibility from vendor.
SECTION 1 SETTING MOTION DETECTION ALARM

1. Enter Motion Detection interface for Camera Management and choose a camera you want to set up motion detection. **Menu > Camera > Motion.**

2. Set up detection area and sensitivity. Check **Enable Motion Detection**, and use the mouse to draw detection area(s) and drag the sensitivity bar to set sensitivity.

   ![NOTE]
   By default, the motion detection is enabled and configured in full screen. Click the button and set alarm response actions.

3. Click **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when motion alarm is triggered, and click **Apply** to save the settings.
4. Set up arming schedule of the channel.
   - Select **Arming Schedule** tab to set the arming schedule of handling actions for the motion detection.
   - Choose one day of a week and up to eight time periods which can be set within each day.
   - Click **Apply** to save the settings. Time periods shall not be repeated or overlapped.

5. Click **Handling** tab to set up alarm response actions of motion alarm (please refer to Chapter 9 Section Section 6 - Setting Alarm Response Actions (page 9-11).)

6. If you want to set motion detection for another channel, repeat the above steps or just click **Copy** in the **Motion Detection** interface to copy the above settings to it.

**SECTION 2  SETTING SENSOR ALARMS**

Set the handling action of an external sensor alarm.

1. Enter Alarm Settings of System Configuration and select an alarm input. **Menu > Configuration > Alarm.** Select **Alarm Input** tab to enter Alarm Input Settings interface.
2. Set up the handling action of the selected alarm input. Check the **Enable** checkbox and **Settings** to set up its alarm response actions.

3. Select **Trigger Channel** tab and select one or more channels which will start to record or become full-screen monitoring when an external alarm is input, and click **Apply** to save the settings.

4. Select **Arming Schedule** tab to set the arming schedule of handling actions.
Choose one day of a week. A maximum of eight time periods can be set within each day. Then click **Apply** to save the settings.

- Time periods shall not be repeated or overlapped.
- Repeat the above steps to set up arming schedule of other days of a week. You can also use Copy button to copy an arming schedule to other days.

5. Select **Linkage Action** tab to set up alarm response actions of the alarm input (please refer to Setting Alarm Response Actions on page 9-11).

6. If necessary, select **PTZ Linking** tab and set PTZ linkage of the alarm input. Set PTZ linking parameters and click **OK** to complete the settings of the alarm input.

- Please check whether the PTZ or speed dome supports PTZ linkage. One alarm input can trigger presets, patrol or pattern of more than one channel. But presets, patrols and patterns are exclusive.
7. If you want to set handling action of another alarm input, repeat the above steps. Or you can click **Copy** on the Alarm Input Setup interface and check the checkbox of alarm inputs to copy the settings to them.
SECTION 3 DETECTING VIDEO LOSS ALARM

Detect video loss of a channel and take alarm response action(s).

1. Enter Video Loss interface of Camera Management and select a channel you want to detect. **Menu > Camera > Video Loss.**
2. Set up handling action of video loss by checking **Enable Video Loss Alarm** and click the button to set up handling action of video loss.

3. Set up arming schedule of the handling actions:
   Select **Arming Schedule** tab to set the channel's arming schedule.
   Choose one day of a week and up to eight time periods can be set within each day.
   Click **Apply** button to save the settings. Time periods shall not be repeated or overlapped.
4. Select **Linkage Action** tab to set up alarm response action of video loss (please refer to **Setting Alarm Response Actions** on page 9-11).

5. Click **OK** to complete the video loss settings of the channel.

**SECTION 4 DETECTING VIDEO TAMPERING ALARM**

Trigger alarm when the lens is covered and take alarm response action(s).

1. Enter Video Tampering interface of Camera Management and select a channel you want to detect video tampering. **Menu> Camera> Video Tampering.**
2. Set the video tampering handling action of the channel. Check **Enable Video Tampering Detection**. Then, drag the sensitivity bar to set a proper sensitivity level. Use the mouse to draw an area you want to detect video tampering.

Click the **button to set up handling action of video tampering.**

3. Set arming schedule and alarm response actions of the channel.

- Click **Arming Schedule** tab to set the arming schedule of handling actions.
- Choose one day of a week and a maximum of eight time periods can be set within each day.
- Click **Apply** button to save the settings. Time periods shall not be repeated or overlapped.
4. Select **Linkage Action** tab to set up alarm response actions of video tampering alarm (please refer to Setting Alarm Response Actions on page 9-11).

5. Click **OK** to complete the video tampering settings of the channel.

**SECTION 5  HANDLING EXCEPTIONS ALARM**

Exception settings refer to the handling action of various exceptions, e.g.

- **HDD Full**: The HDD is full.
- **HDD Error**: Writing HDD error or unformatted HDD.
- **Network Disconnected**: Disconnected network cable.
- **IP Conflicted**: Duplicated IP address.
- **Illegal Login**: Incorrect user ID or password.
- **Record Exception**: No space for saving recorded files.
- **PoE Power Overload**: The power consumption of the connected cameras via the PoE interface exceeds the maximum PoE power.
Enter Exception interface of System Configuration and handle various exceptions. 
**Menu > Configuration > Exceptions.** Please refer to **Setting Alarm Response Actions** on page 9-11 for detailed alarm response actions.

---

**NOTE**

PoE Power Overload is only supported by the models with POE interface.

---

### SECTION 6  SETTING ALARM RESPONSE ACTIONS

Alarm response actions are activated when an alarm or exception occurs, including Event Hint Display, Full Screen Monitoring, Audible Warning (buzzer), Notify Surveillance Center, Upload Picture to FTP, Trigger Alarm Output and Send Email.

**Event Hint Display**

When an event or exception happens, a hint can be displayed on the lower-left corner of live view image. And you can click the hint icon to check the details. The event to be displayed is configurable.

1. Enter the Exception settings interface. **Menu > Configuration > Exceptions.**
2. Check **Enable Event Hint.**
3. Click 🌪 to set the type of event to be displayed on the image.

**Full Screen Monitoring**

When an alarm is triggered, the local monitor (VGA and HDMITM monitor) display in full screen the video image from the alarming channel configured for full screen monitoring.

If alarms are triggered simultaneously in several channels, their full-screen images will be switched at an interval of 10 seconds (default dwell time). A different dwell time can be set by going to Menu >Configuration >Live View > Full Screen Monitoring Dwell Time.

Auto-switch terminates once the alarm stops and you returned to the Live View interface.
Audible Warning
Trigger an audible beep when an alarm is detected.

Notify Surveillance Center
Sends an exception or alarm signal to remote alarm host when an event occurs. The alarm host refers to the PC installed with Remote Client.

The alarm signal will be transmitted automatically at detection mode when remote alarm host is configured. Please refer to Chapter 12 Section 2.6 - Configuring Remote Alarm Host (page 12-11) for details of alarm host configuration.

Email Linkage
Send an email with alarm information to a user or users when an alarm is detected.

Trigger Alarm Output

1. Enter Alarm Output interface. **Menu > Configuration > Alarm > Alarm Output** and select an alarm output and set alarm name and dwell time. Click **Schedule** to set the arming schedule of alarm output.

   **NOTE**
   You must select during "Trigger Channel" settings the channel(s) you want to make full screen monitoring.

   **NOTE**
   If "Manually Clear" is selected in the dropdown list of Dwell Time, you can clear it only by going to **Menu > Manual > Alarm**.

2. Set up arming schedule of the alarm output. Choose one day of a week and up to eight time periods can be set within each day. Time periods shall not be repeated or overlapped.
3. Repeat the above steps to set up arming schedule of other days of a week. You can also use **Copy** to copy an arming schedule to other days. Click **OK** to complete the video tampering settings of the alarm output number.

4. You can also copy the above settings to another channel.
SECTION 7  TRIGGERING OR CLEARING ALARM OUTPUT MANUALLY

Sensor alarm can be triggered or cleared manually. If Manually Clear is selected in the drop-down list of dwell time of an alarm output, the alarm can be cleared only by clicking Clear in the following interface.

Select the alarm output you want to trigger or clear and make related operations. Menu> Manual> Alarm.

☐ Click Trigger/Clear if you want to trigger or clear an alarm output.

☐ Click Trigger All if you want to trigger all alarm outputs.

☐ Click Clear All if you want to clear all alarm output.
### Figure 9-18  Trigger or Clear Alarm Output Manually

<table>
<thead>
<tr>
<th>Alarm Output No.</th>
<th>Alarm Name</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local-&gt;1</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Local-&gt;2</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Local-&gt;3</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Local-&gt;4</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>172.6.23.105:8000-&gt;1</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>
SECTION 1 FACE DETECTION

Face detection function detects the face as it appears in the surveillance scene, and certain actions can be taken when the alarm is triggered.

1. Enter the VCA settings interface. Menu> Camera> VCA.

2. Select the camera to configure the VCA. You can click Save VCA Picture to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Face Detection**.

4. Click `Rule Settings` to enter the face detection settings interface. Configure the trigger channel, arming schedule and linkage action for the face detection alarm. Please refer to step 3 through step 5 of Chapter 9 Section 1 - Setting Motion Detection Alarm (page 9-1) for detailed instructions.

5. Click **Rule Settings** to set the face detection rules. Click-and-drag the slider to set the detection sensitivity.

   Sensitivity: Range [1-5]. The higher the value is, the more easily the face can be detected.
6. Click **Apply** to activate the settings.

**SECTION 2**  **LINE CROSSING DETECTION**

This function can be used for detecting people, vehicles and objects which cross a set virtual line. The line crossing direction can be set as bidirectional, from left to right or from right to left. You can set the duration for the alarm response actions, such as full screen monitoring, audible warning, etc.

1. Enter the VCA settings interface. **Menu> Camera> VCA**.
2. Select the camera to configure the VCA. You can click **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Line Crossing Detection**.
4. Check the **Enable** checkbox to enable this function.
5. Click **Rule Settings** to set the line crossing detection rules.
   
   Select the direction to A<->B, A->B or A<-B.
   
   **A<->B**: Only the arrow on the B side shows; when an object going across the configured line with both direction can be detected and alarms are triggered.
   
   **A->B**: Only the object crossing the configured line from the A side to the B side can be detected.
   
   **B->A**: Only the object crossing the configured line from the B side to the A side can be detected.

   Click-and-drag the slider to set the detection sensitivity. **Sensitivity**: Range [1-100]. The higher the value is, the more easily the detection alarm can be triggered.
Click **OK** to save the rule settings and back to the line crossing detection settings interface.

![Figure 10-3 Set Line Crossing Detection Rules](image)

7. Click [ ] and set two points in the preview window to draw a virtual line. You can use the [ ] to clear the existing virtual line and re-draw it. Up to four rules can be configured.

![Figure 10-4 Line Draw for Line Crossing Detection](image)
8. Click **Apply** to activate the settings.

### SECTION 3  INTRUSION DETECTION

The Intrusion detection function detects people, vehicles, or other objects which enter and loiter in a pre-defined virtual region. Certain actions can be taken when the alarm is triggered.

1. Enter the VCA settings interface. **Menu> Camera> VCA.**
2. Select the camera to configure the VCA. You can click **Save VCA Picture** to save the captured pictures of VCA detection.
3. Select the VCA detection type to **Intrusion Detection.**
4. Check **Enable** to enable this function.
5. Click **Rule Settings** to set the intrusion detection rules. Set the following parameters.

   **Threshold**: Range [1s-10s], the threshold for the time of the object loitering in the region. When the duration of the object in the defined detection area is longer than the set time, the alarm will be triggered.

   Click-and-drag the slider to set the detection sensitivity. **Sensitivity**: Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. The higher the value is, the more easily the detection alarm can be triggered.

   **Percentage**: Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.
Click **OK** to save the rule settings and back to the line crossing detection settings interface.

7. Click ![ ] and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete drawing. Only one region can be configured.

You can use ![ ] to clear the existing virtual line and re-draw it. Up to four rules can be configured.
8. Click Apply to save the settings.

SECTION 4 REGION ENTRANCE DETECTION

Region entrance detection function detects people, vehicle or other objects which enter a pre-defined virtual region from the outside place. Certain actions can be taken when the alarm is triggered.

1. Enter the VCA settings interface. Menu> Camera> VCA.
2. Select the camera to configure the VCA. You can click Save VCA Picture to save the captured pictures of VCA detection.
3. Select the VCA detection type to Region Entrance Detection.
4. Check **Enable** checkbox to enable this function.

5. Click **Enable** to configure the trigger channel, arming schedule and linkage actions for the line crossing detection alarm.

6. Click **Rule Settings** to set the sensitivity of the region entrance detection.

   **Sensitivity**: Range [0-100]. The higher the value is, the more easily the detection alarm can be triggered.

7. Click **Draw Line** and draw a quadrilateral in the preview window by specifying four vertexes of the detection region, and right click to complete drawing. Only one region can be configured.

   You can use **Clear All** to clear the existing virtual line and re-draw it. Up to 4 rules can be configured.

---

**Figure 10-7  Set Region Entrance Detection**

![Set Region Entrance Detection](image)

---

8. Click **Apply** to save the settings.
SECTION 5  REGION EXISTING DETECTION

Region exiting detection function detects people, vehicles, or other objects which exit from a pre-defined virtual region. Certain actions can be taken when the alarm is triggered.

- Please refer to Region Entrance Detection on page 10-7 for operating steps to configure the region exiting detection.
- Up to 4 rules can be configured.

SECTION 6  LOITERING DETECTION

The Loitering detection function detects people, vehicles, or other objects which loiter in a pre-defined virtual region for some certain time. A series of actions can be taken when the alarm is triggered.

- Please refer to Intrusion Detection on page 10-5 for operating steps to configure the loitering detection.
- The Threshold [1s-10s] in the Rule Settings defines the time of the object loitering in the region. If you set the value as 5, alarm is triggered after the object loitering in the region for 5s; and if you set the value as 0, alarm is triggered immediately after the object entering the region.
- Up to 4 rules can be configured.

SECTION 7  PEOPLE GATHERING DETECTION

People gathering detection alarm is triggered when people gather around in a pre-defined virtual region. A series of actions can be taken when the alarm is triggered.

- Please refer to Intrusion Detection on page 10-5 for operating steps to configure the people gathering detection.
- The Percentage in the Rule Settings defines the gathering density of the people in the region. Usually, when the percentage is small, the alarm can be triggered when small number of people gathered in the defined detection region.
- Up to 4 rules can be configured.

SECTION 8  FAST MOVING DETECTION

Fast moving detection alarm is triggered when people, vehicles, or other objects move fast in a pre-defined virtual region. A series of actions can be taken when the alarm is triggered.
SECTION 9  PARKING DETECTION

Parking detection function detects illegal parking in places such as highway, one-way street, etc. A series of actions can be taken when the alarm is triggered.

- Please refer to Intrusion Detection on page 10-5 for operating steps to configure the parking detection.
- The Threshold[5s-20s] in the Rule Settings defines the time of the vehicle parking in the region. If you set the value as 10, alarm is triggered after the vehicle stay in the region for 10s.
- Up to 4 rules can be configured.

SECTION 10  UNATTENDED BAGGAGE DETECTION

Unattended baggage detection function detects the objects left over in the pre-defined region such as the baggage, purse, dangerous materials, etc. A series of actions can be taken when the alarm is triggered.

- Please refer to Intrusion Detection on page 10-5 for operating steps to configure the unattended baggage detection.
- The Threshold[5s-20s] in the Rule Settings defines the time of the objects left over in the region. If you set the value as 10, alarm is triggered after the object is left and stay in the region for 10s. And the Sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object left in the region can trigger the alarm.
- Up to 4 rules can be configured.

SECTION 11  OBJECT REMOVAL DETECTION

Object removal detection function detects the objects removed from the pre-defined region, such as the exhibits on display. A series of actions can be taken when the alarm is triggered.
SECTION 12 AUDIO EXCEPTION DETECTION

Audio exception detection function detects the abnormal sounds in the surveillance scene, such as the sudden increase / decrease of the sound intensity. Certain actions can be taken when the alarm is triggered.

1. Enter the VCA settings interface. **Menu> Camera> VCA.**

2. Select the camera to configure the VCA. You can click **Save VCA Picture** to save the captured pictures of VCA detection.

3. Select the VCA detection type to **Audio Exception Detection.**

4. Click **Rule Settings** to configure the trigger channel, arming schedule and linkage action for the face detection alarm.

5. Click **Rule Settings** to set the audio exception rules.

**NOTE**

- Please refer to Intrusion Detection on page 10-5 for operating steps to configure the object removal detection.
- The Threshold [5s-20s] in the Rule Settings defines the time of the objects removed from the region. If you set the value as 10, alarm is triggered after the object disappears from the region for 10s. And the Sensitivity defines the similarity degree of the background image. Usually, when the sensitivity is high, a very small object taken from the region can trigger the alarm.
- Up to 4 rules can be configured.
- Check **Audio Input Exception** to enable the audio loss detection function.

- Check the checkbox of **Sudden Increase of Sound Intensity Detection** to detect the sound steep rise in the surveillance scene. You can set the detection sensitivity and threshold for sound steep rise. **Sensitivity**: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.

  **Sound Intensity Threshold**: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

- Check the checkbox **Sudden Decrease of Sound Intensity Detection** to detect the sound steep drop in the surveillance scene. You can set the detection sensitivity[1-100] for sound steep drop.

6. Click **Apply** to activate the settings.

**SECTION 13  SUDDEN SCENE CHANGE DETECTION**

Scene change detection function detects the change of surveillance environment affected by the external factors; such as the intentional rotation of the camera. Certain actions can be taken when the alarm is triggered.
SECTION 14  DEFOCUS DETECTION

The image blur caused by defocus of the lens can be detected. Certain actions can be taken when the alarm is triggered.

- Please refer to Face Detection on page 10-1 for operating steps to configure the scene change detection.
- The Sensitivity in the Rule Settings ranges from 1 to 100, and the higher the value is, the more easily the change of scene can trigger the alarm.

SECTION 15  PIR ALARM

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector’s field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

1. Enter the VCA settings interface. Menu> Camera> VCA.
2. Select the camera to configure the VCA. You can click Save VCA Picture to save the captured pictures of VCA detection.
3. Select the VCA detection type to PIR Alarm.
4. Click Rule Settings to set the rules. Please refer to Face Detection on page 10-1 for instructions.
5. Click Apply to activate the settings.
With the configured VCA detection, the NVR supports the VCA search for the behavior analysis, face capture, people counting and heat map results.

**SECTION 1  FACE SEARCH**

When there are detected face pictures captured and saved in HDD, you can enter the Face Search interface to search the picture and play the picture related video file according to the specified conditions.

Before you begin, please refer to Chapter 10 Section 1 - Face Detection (page 10-1) for configuring the face detection.

1. Enter the Face Search interface. **Menu >VCA Search> Face Search.**
2. Select the camera (s) for the face search.
3. Specify the start time and end time for search the captured face pictures or video files.

4. Click **Search** to begin searching. The search results of face detection pictures are displayed in list or in chart format.
5. Play the face picture related video file. You can double-click on a face picture to play its related video file in the view window on the top right, or select a picture item and click ▶️ to play it. You can also click ⏸️ to stop the playing, or click ◀️ ▶️ to play the previous/next file.

6. If you want to export the captured face pictures to local storage device, connect the storage device to the device and click Export All to enter the Export interface. Click Export to export all face pictures to the storage device. Please refer to Chapter 8 - Backup Record Files (page 8-1) for the operation of exporting files.
SECTION 2  BEHAVIOR SEARCH

Behavior analysis detects a series of suspicious behaviors based on VCA detection, and certain linkage methods are enabled if the alarm is triggered.

1. Enter the Behavior Search interface. Menu >VCA Search> Behavior Search.
2. Select the camera (s) for the behavior search.
3. Specify the start time and end time for searching the matched pictures.
4. Select the VCA detection type from the drop-down list, including the line crossing detection, intrusion detection, unattended baggage detection, object removal detection, region entrance detection, region exiting detection, parking detection, loitering detection, people gathering detection and fast moving detection.

5. Click **Search** to start searching. The search results of pictures are displayed in list or in chart form.
6. Play the face picture related video file. You can double-click on a face picture to play its related video file in the view window on the top right, or select a picture item and click to play it. You can also click to stop the playing, or click < > to play the previous/next file.

7. If you want to export the captured face pictures to local storage device, connect the storage device to the device and click Export All to enter the Export interface. Click Export to export all face pictures to the storage device.

**SECTION 3  PLATE SEARCH**

You can search and view the matched captured vehicle plate picture and related information according to the plate searching conditions including the start time/end time, country and plate No.

1. Enter the Plate Search interface. **Menu > VCA Search > Plate Search.**

2. Select the camera (s) for the plate search.
3. Specify the start time and end time for searching the matched plate pictures.

4. Select the country from the drop-down list for searching the location of the vehicle plate.

5. Input the plate number in the field for search.

6. Click **Search** to start searching. The search results of detected vehicle plate pictures are displayed in list or in chart form.

   **NOTE**
   Please refer to Step 7 through step 8 of **Face Search** on page 11-1 for the operation of the search results.

**SECTION 4  PEOPLES COUNTING**

People Counting is used to calculate the number of people that entered or left a certain configured area and provide daily/weekly/monthly/annual reports for analysis.

1. Enter the People Counting interface. **Menu >VCA Search> People Counting.**
2. Select the camera for the people counting.


4. Set the statistics time.

5. Click **Counting** to start people counting statistics.

6. Click **Export** to export the statistics report in excel format.

---

**SECTION 5  HEAT MAP**

Heat map is a graphical representation of data represented by colors. The heat map function is usually used to analyze the visit times and dwell time of customers in a configured area.
1. Enter the Heat Map interface. Menu >VCA Search> Heat Map.

2. Select the camera for the heat map processing.


4. Set the statistics time.

5. Click Counting to export the report data and start heat map statistics. The results are displayed in graphics marked in different colors.
As shown in the figure above, red color block (255, 0, 0) indicates the most welcome area, and blue color block (0, 0, 255) indicates the less-popular area. You can click the Export button to export the statistics report in excel format.
Network Settings

Chapter 12

Section 1 Configuring General Settings

Network settings must be properly configured before you operate NVR over network.

1. Enter the Network Settings interface. Menu > Configuration > Network.
2. Select the General tab.

3. In the General Settings interface, configure the following settings: Working Mode, NIC Type, IPv4 Address, IPv4 Gateway, MTU and DNS Server.
   If the DHCP server is available, click the checkbox of DHCP to automatically obtain an IP address and other network settings from that server.

   ![Network Settings Interface]

   NOTE
   ❍ For the models which have the PoE or built-in switch network interfaces, the internal NIC IPv4 address should be configured for the cameras connecting to the PoE or built-in switch network interface of the NVR.
   ❍ The valid value range of MTU is 500 ~ 9676.

4. After having configured the general settings, click Apply to save the settings.
SECTION 2 CONFIGURING ADVANCED SETTINGS

2.1 PPPoE Settings

Your NVR also allows access by Point-to-Point Protocol over Ethernet (PPPoE).

1. Enter the Network Settings interface. Menu > Configuration > Network.
2. Select the PPPoE tab to enter the PPPoE Settings interface, as shown in Figure 12-2.

3. Check Enable PPPoE to enable this feature.
4. Enter User Name and Password for PPPoE access. The User Name and Password should be assigned by your ISP.
5. Click Apply to save and exit the interface.
6. After successful settings, the system asks you to reboot the device to enable the new settings, and the PPPoE dial-up is automatically connected after reboot.

You can go to Menu > Maintenance > System Info > Network interface to view the status of PPPoE connection. Please refer to Chapter 15 Section 1 - Viewing System Information (page 15-1).

2.2 Configuring Cloud P2P

Cloud P2P provides the mobile phone application and as well the service platform page to access and manage your connected NVR, which enables you to get a convenient remote access to the surveillance system.

1. Enter the Network Settings interface. Menu > Configuration > Network.
2. Select the Platform Access tab to enter the Cloud P2P Settings interface.
3. Check Enable to activate this feature.
4. If required, select the checkbox of Custom and input the Server Address.
5. To turn the Enable Stream Encryption on, select its checkbox.
6. Enter the Verification Code of the device.
7. Click **Apply** to save and exit the interface. After configuration, you can access and manage the NVR by your mobile phone on which the Cloud P2P application is installed.

### 2.3 Configuring DDNS

If your NVR is set to use PPPoE as its default network connection, you may set Dynamic DNS (DDNS) to be used for network access.

Prior registration with your ISP is required before configuring the system to use DDNS.

1. Enter the Network Settings interface. **Menu > Configuration > Network.**
2. Select the **DDNS** tab to enter the **DDNS Settings** interface.
3. Check the **DDNS** checkbox to enable this feature.
4. Select **DDNS Type**. Five different DDNS types are selectable: IPServer, DynDNS, PeanutHull, NO-IP and SIMPLEDDNS.

**IPServer:** Enter **Server Address** for IPServer.

---

!*The verification code consists of 6 capital letters and is located at the bottom of the DVR. You can also use the scanning tool of your phone to quickly get the code by scanning the QR code below.*

**DynDNS:**
- Enter **Server Address** for DynDNS (i.e. members.dyndns.org).
- In the **Device Domain Name** text field, enter the domain obtained from the DynDNS website.
- Enter the **User Name** and **Password** registered in the DynDNS website.
PeanutHull:
- Enter the **User Name** and **Password** obtained from the PeanutHull website.

**Figure 12-5  PeanutHull Settings Interface**

| Enable DDNS |  
| DDNS Type  | PeanutHull  
| Area/Country | Custom  
| Server Address |  
| Device Domain Name |  
| Status | DDNS is disabled.  
| User Name |  
| Password |  

**NO-IP**: Enter the account information in the corresponding fields.
- Enter **Server Address** for NO-IP.
- In the **Device Domain Name** text field, enter the domain obtained from the NO-IP website (www.no-ip.com).
- Enter the **User Name** and **Password** registered in the NO-IP website.
**SIMPLEDDNS:**

- Select the continent/country of the server on which the device is registered.

- The **Server Address** of the SimpleDDNS server appears by default: www.simpleddns.com.

- Enter the **Device Domain Name**. You can use the alias you registered in the SimpleDDNS server or define a new device domain name. If a new alias of the device domain name is defined in the NVR, it replaces the old one registered on the server. You can register the alias of the device domain name in the SimpleDDNS server first and then enter the alias to the **Device Domain Name** in the NVR; you can also enter the domain name directly on the NVR to create a new one.

**Register the device on the SimpleDDNS server.**

- Click **Register** to register an account if you do not have one and use the account to log in.
-- In the **Device Management** interface, click ![Register button](image) to register the device.
- Input **Device Serial No.**, **Device Domain** (Device Name) and **HTTP Port**. Click **OK** to add the device.

- **Access the Device via Web Browser or Client Software**: After having successfully registered the device on the SimpleDDNS server, you can access your device via web browser or Client Software with the Device Domain Name (Device Name).

- **Option 1 Access the Device via Web Browser**: Open a web browser, and enter `http:// www.simpleddns.com/alias` in the address bar. Alias refers to the **Device Domain Name** on the device or the **Device Name** on the SimpleDDNS server. Example: `http:// www.simpleddns.com/nvr`.

  **NOTE** If you mapped the HTTP port on your router and changed it to port No. except 80, you have to enter `http:// www.simpleddns.com/ alias:HTTP port` in the address bar to access the device.

- **OPTION 2: Access the devices via client software**: For client software, in the **Add Device** window, select **SimpleDDNS** and then edit the device information.

- **Nickname**: Edit a name for the device as you want.

- **Server Address**: www.simpleddns.com

- **Device Domain Name**: Refers to the **Device Domain Name** on the device or the Device Name on the SimpleDDNS server you created.

- **User Name**: Enter the user name of the device.
Password: Enter the password of the device.

5. Click Apply to save the settings. After setting all the required parameters for the DDNS, you can view the connecting status of the device by checking the Status information.

2.4 Configuring NTP Server

Ensure the network connection of the PC (running FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

NOTE

Refer to the user manual of the FTP server to set the FTP server on your PC and put the firmware file into the directory as required.

1. Enter the Network Settings interface. Menu >Configuration> Network.
2. Select the NTP tab to enter the NTP Settings interface, as shown in Figure 12-12.
3. Check Enable NTP to enable this feature.
4. Configure the following NTP settings:
   - **Interval**: Time interval between the two synchronizing actions with NTP server. The unit is minute.
   - **NTP Server**: IP address of NTP server.
   - **NTP Port**: Port of NTP server.
5. Click **Apply** to save and exit the interface.

**NOTE**
The time synchronization interval can be set from 1 to 10080 min, and the default value is 60 min. If the NVR is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the NVR is set up in a more customized network, NTP software can be used to establish a NTP server used for time synchronization.

### 2.5 Configuring SNMP

You can use SNMP protocol to get device status and parameters related information.

1. Enter the Network Settings interface. **Menu > Configuration > Network**.
2. Select the **SNMP** tab to enter the SNMP Settings interface, as shown in **Figure 12-13**.
3. Check **Enable SNMP** to enable this feature.
4. Configure the following SNMP settings:
   **Trap Address**: IP Address of SNMP host.
   **Trap Port**: Port of SNMP host.
5. Click **Apply** to save and exit the interface.

---

### 2.6 Configuring Remote Alarm Host

With a remote alarm host configured, the NVR sends the alarm event or exception message to the host when an alarm is triggered. The remote alarm host must have the Network Video Surveillance software installed.

1. Enter the Network Settings interface. **Menu >Configuration> Network.**
2. Select the **More Settings** tab to enter the More Settings interface, as shown in **Figure 12-14**.

---

### Figure 12-14 More Settings Interface

<table>
<thead>
<tr>
<th>Alarm Host IP</th>
<th>Alarm Host Port</th>
<th>Server Port</th>
<th>HTTP Port</th>
<th>Multicast IP</th>
<th>RTSP Port</th>
<th>Enable High-speed Dow...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>8000</td>
<td>80</td>
<td></td>
<td>554</td>
<td></td>
</tr>
</tbody>
</table>
3. Enter **Alarm Host IP** and **Alarm Host Port** in the text fields.

The Alarm Host IP refers to the IP address of the remote PC on which the Network Video Surveillance Software is installed, and the Alarm Host Port must be the same as the alarm monitoring port configured in the software.

4. Click **Apply** to save and exit the interface.

### 2.7 Configuring Multicast

The multicast can be configured to realize live view for more than 128 connections through network for the device. A multicast address spans the Class-D IP range of 224.0.0.0 to 239.255.255.255. It is recommended to use the IP address ranging from 239.252.0.0 to 239.255.255.255.

1. Enter the Network Settings interface. **Menu >Configuration> Network.**
2. Select the **More Settings** tab to enter the More Settings interface, as shown in **Figure 12-14.**
3. Set **Multicast IP**, as shown in **Figure 12-15.** When adding a device to the Network Video Surveillance Software, the multicast address must be the same as the NVR's multicast IP.

   ![Figure 12-15 Configure Multicast](image)

4. Click **Apply** to save and exit the interface.

The multicast function should be supported by the network switch to which the NVR is connected.

### 2.8 Configuring RTSP

The RTSP (Real Time Streaming Protocol) is a network control protocol designed for use in communication systems to control streaming media servers.

1. Enter the Network Settings menu. **Menu >Configuration> Network.**
2. Select the **More Settings** tab to enter the More Settings menu, as shown in **Figure 12-14.**

   ![Figure 12-16 RTSP Settings Interface](image)
3. Enter the **RTSP port** in the text field of RTSP Service Port. The default RTSP port is 554, and you can change it according to different requirements.

4. Click **Apply** to save and exit the menu.

### 2.9 Configuring Server and HTTP Ports

You can change the server and HTTP ports in the Network Settings menu. The default server port is 8000 and the default HTTP port is 80.

1. Enter the Network Settings interface. **Menu >Configuration> Network.**
2. Select the **More Settings** tab to enter the More Settings interface, as shown in **Figure 12-14.**
3. Enter new **Server Port** and **HTTP Port.**

![Figure 12-17 Host Other Settings Interface](image)

<table>
<thead>
<tr>
<th>Server Port</th>
<th>8000</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port</td>
<td>80</td>
</tr>
<tr>
<td>Multicast IP</td>
<td>239.221.2.78</td>
</tr>
</tbody>
</table>

4. Enter the **Server Port** and **HTTP Port** in the text fields. The default Server Port is 8000 and the HTTP Port is 80. You can change them according to different requirements.

5. Click **Apply** to save and exit the interface.

**NOTE**

The **Server Port** should be set to the range of 2000-65535 and it is used for remote client software access. The **HTTP port** is used for remote web browser access.

### 2.10 Configuring Email

The system can be configured to send an Email notification to all designated users if an alarm event is detected, an alarm or motion event is detected, or the administrator password is changed.

Before configuring the Email settings, the NVR must be connected to a local area network (LAN) that maintains an SMTP mail server. The network must also be connected to either an intranet or the Internet depending on the location of the e-mail accounts to which you want to send notification.

1. Enter the Network Settings interface. **Menu >Configuration> Network.**
2. Set the **IPv4 Address, IPv4 Subnet Mask, IPv4 Gateway** and the **Preferred DNS Server** in the Network Settings menu.
3. **Click Apply** to save the settings.
4. Select the **Email** tab to enter the Email Settings interface.

5. Configure the following Email settings:

   **Enable Server Authentication** (optional): Check the checkbox to enable the server authentication feature.

   **User Name**: The user account of sender’s Email for SMTP server authentication.

   **Password**: The password of sender’s Email for SMTP server authentication.

   **SMTP Server**: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

   **SMTP Port No.**: The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL (optional): Click the checkbox to enable SSL if required by the SMTP server.

**Sender**: The name of sender.

**Sender's Address**: The Email address of sender.

**Select Receivers**: Select the receiver. Up to 3 receivers can be configured.

**Receiver**: The name of user to be notified.

**Receiver's Address**: The Email address of user to be notified.

**Enable Attached Pictures**: Check the checkbox of Enable Attached Picture if you want to send email with attached alarm images. The interval is the time of two adjacent alarm images. You can also set SMTP port and enable SSL here.

**Interval**: The interval refers to the time between two actions of sending attached pictures.

6. Click **Apply** button to save the Email settings.

7. Click **Test** to test whether your Email settings work. The corresponding **Attention** message box displays. Refer to Figure 12-20. Test sends a test message to verify that the SMTP server can be reached.

---

**Figure 12-20  Email Testing Message**

---

### 2.11 Configuring NAT

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ and manual mapping.

**UPnP™**

Universal Plug and Play (UPnP™) permits the device to seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. Use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Before you begin, if you want to enable the UPnP™ function of the device, you must enable the UPnP™ function of the router to which your device is connected. When the network working mode of the device is set as multi-address, the default route of the device should be in the same network segment as that of the LAN IP address of the router.
1. Enter the Network Settings interface. Menu > Configuration > Network.
2. Select the NAT tab to enter the port mapping interface.

3. Check Enable UpnP to enable UPnP™.
4. Select the Mapping Type as Manual or Auto in the drop-down list.
   
   **Option 1 Auto:** If you select Auto, the Port Mapping items are read-only, and the external ports are set by the router automatically.
   - Select Auto in the drop-down list of Mapping Type.
   - Click Apply to save the settings.
   - Click Refresh to obtain the latest status of the port mapping.

   **Option 2 Manual:** If you select Manual as the mapping type, you can edit the external port on your demand by clicking to activate the External Port Settings dialog box.
   - Select Manual in the drop-down list of Mapping Type.
   - Click to activate the External Port Settings dialog box. Configure the external port number for server port, http port, RTSP port, and https port respectively.
- Click **Apply** button to save the settings.
- Click **Refresh** to obtain the latest status of the port mapping.

### Manual Mapping

If your router does not support the UPnP™ function, perform the following steps to map the port manually.

---

**NOTE**

- You can use the default port No., or change it according to actual requirements.
- External Port indicates the port No. for port mapping in the router.
- The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

---

**Figure 12-23  External Port Settings Dialog**

**Figure 12-24  UPnP™ Settings Finished - Manual**
Before you begin, make sure the router supports the configuration of internal port and external port in the interface of **Forwarding**.

1. Enter the Network Settings interface. **Menu > Configuration > Network**.
2. Select the **NAT** tab to enter the port mapping interface.
3. Leave the **Enable UPnP** checkbox unchecked.
4. Click  to activate the **External Port Settings** dialog box. Configure the external port number for server port, http port, RTSP port, and https port respectively.

   The value of the RTSP port No. should be 554 or between 1024 and 65535, while the value of the other ports should be between 1 and 65535 and the value must be different from each other. If multiple devices are configured for the UPnP™ settings under the same router, the value of the port No. for each device should be unique.

5. Click **OK** to save the setting for the current port and return to the upper-level menu.
6. Click **Apply** button to save the settings.
7. Enter the virtual server setting page of router; fill in the blank of Internal Source Port with the internal port value, the blank of External Source Port with the external port value, and other required contents.

   Each item should correspond with the device port, including server port, http port, RTSP port, and https port.
SECTION 3  CHECKING NETWORK TRAFFIC

You can check the network traffic to obtain real-time information of NVR such as linking status, MTU, sending/receiving rate, etc.

1. Enter the Network Traffic interface. **Menu > Maintenance > Net Detect.**
2. You can view the sending rate and receiving rate information on the interface. The traffic data is refreshed every 1 second.

SECTION 4 CONFIGURING NETWORK DETECTION

Obtain network connecting status of NVR through the network detection function, including network delay, packet loss, etc.

4.1 Testing Network Delay and Packet Loss

1. Enter the Network Traffic interface. **Menu >Maintenance >Net Detect.**
2. Click the **Network Detection** tab to enter the Network Detection menu, as shown in **Figure 12-28.**
3. Enter the destination address in the text field **Destination Address**.
4. Click **Test** to start testing network delay and packet loss. The test results pops up on the window. If the testing fails, an error message box displays as well. Refer to **Figure 12-29**.

4.2 Exporting Network Packet

By connecting the NVR to network, the captured network data packet can be exported to USB-flash disk, SATA, DVD-R/W and other local backup devices.

1. Enter the Network Traffic interface. **Menu > Maintenance >Net Detect**.
2. Click the **Network Detection** tab to enter the Network Detection interface.
3. Select the backup device from the drop-down list of Device Name, as shown in **Figure 12-30**.

Click **Refresh** if the connected local backup device cannot be displayed. When it fails to detect the backup device, please check whether it is compatible with the NVR. You can format the backup device if the format is incorrect.
4. Click **Export** button to start exporting.
5. After exporting is complete, click **OK** to finish the packet export, as shown in Figure 12-31.

Up to 1M data can be exported each time.

### 4.3 Checking the Network Status

You can also check the network status and quick set the network parameters in this interface.

1. Click the **Status** button on the lower-right corner of the page.
2. If the network is normal, the following message box displays.

If the message box displays with other information, you can click Network to show the quick setting interface of the network parameters.

4.4 Checking Network Statistics

Check the network status to obtain the real-time information of NVR.

1. Enter the Network Detection interface. Menu >Maintenance >Net Detect.
2. Choose the **Network Stat** tab.

   *Figure 12-34 Network Stat Interface*

3. Check the bandwidth of **IP Camera**, bandwidth of **Remote Live View**, bandwidth of **Remote Playback**, bandwidth of **Net Receive Idle** and bandwidth of **Net Send Idle**.

4. Click **Refresh** to get the latest status.
Section 1  Initializing HDDs

A newly installed hard disk drive (HDD) must be initialized before it can be used with your NVR.

A message box pops displays (Figure 13-1). Click Yes to initialize it immediately or you can perform the following steps to initialize the HDD.

1. Enter the HDD Information interface. Menu > HDD> General.

2. Select HDD to be initialized.

3. Click the Init button.
4. Select **OK** to start initialization.

5. After the HDD has been initialized, the status of the HDD changes from **Uninitialized** to **Normal**.

Initializing the HDD erases all data on it.

**SECTION 2**  **MANAGING NETWORK HDD**

You can add the allocated NAS or disk of IP SAN to NVR, and use it as network HDD.
1. Enter the HDD Information interface. **Menu > HDD >General.**

![HDD Information Interface](image)

2. Click **Add** to enter the Add NetHDD interface, as shown in **Figure 13-7.**

![Add NetHDD Interface](image)

3. Add the allocated NetHDD.

4. Select the type as **NAS** or **IP SAN**.

5. Configure the NAS or IP SAN settings.

   **Add NAS disk:**
   - Enter the **NetHDD IP** address in the text field.
   - Click **Search** to search the available NAS disks.
   - Select the **NAS** disk from the list shown below. Or you can just manually enter the directory in the text field of NetHDD Directory.
   - Click **OK** to add the configured NAS disk. Up to 8 NAS disks can be added.
Add IP SAN:
- Enter the NetHDD IP address in the text field.
- Click Search to search the available IP SAN disks.
- Select the IP SAN disk from the list shown below.
- Click OK to add the selected IP SAN disk. Up to 1 IP SAN disk can be added.
6. After having successfully added the NAS or IP SAN disk, return to the HDD Information menu. The added NetHDD displays in the list.

   **NOTE**  If the added NetHDD is uninitialized, please select it and click the Init button for initialization.
3.1 Setting HDD Groups

Multiple HDDs can be managed in groups. Video from specified channels can be recorded onto a particular a HDD group through HDD settings.

1. Enter the Storage Mode interface. Menu > HDD > Advanced.
2. Set the Mode to Group, as shown in Figure 13-11.

3. Click Apply and the Attention box (Figure 13-12) displays.

4. Click Yes to reboot the device to activate the changes.
5. After reboot of device, enter the HDD Information interface. Menu > HDD > General.
6. Select HDD from the list and click  to enter the Local HDD Settings interface, as shown in Figure 13-13.
7. Select the Group number for the current HDD. The default group number for each HDD is 1.

8. Click OK to confirm the settings.

9. In the pop-up Attention box (Figure 13-14), click Yes to finish the settings.

3.2 Setting HDD Property

The HDD property can be set to redundancy, read-only or read/write (R/W). Before setting the HDD property, please set the storage mode to Group (refer to step 1-4 of Setting HDD Groups on page 13-6).

An HDD can be set to read-only to prevent important recorded files from being overwritten when the HDD becomes full in overwrite recording mode.
When the HDD property is set to redundancy, the video can be recorded both onto the redundancy HDD and the R/W HDD simultaneously so as to ensure high security and reliability of video data.

1. Enter the HDD Information interface. **Menu > HDD > General.**
2. Select **HDD** from the list and click the icon to enter the Local HDD Settings interface, as shown in **Figure 13-15.**

   ![Figure 13-15 Set HDD Property](image)

3. Set the HDD property to **R/W, Read-only, or Redundancy.**
4. Click **OK** to save the settings and exit the interface.
5. In the HDD Information menu, the HDD property will be displayed in the list.

   **NOTE** At least 2 hard disks must be installed on your NVR when you want to set a HDD to Redundancy, and there is one HDD with R/W property.

### SECTION 4  CONFIGURING QUOTA MODE

Each camera can be configured with allocated quota for the storage of recorded files.

1. Enter the Storage Mode interface. **Menu > HDD > Advanced.**
2. Set the **Mode** to **Quota**, as shown in **Figure 13-16.** (The NVR must be rebooted to enable the changes to take effect.)
3. Select a camera for which you want to configure quota.

4. Enter the storage capacity in the text fields of **Max. Record Capacity (GB)**, as shown in **Figure 13-17**.

5. You can copy the quota settings of the current camera to other cameras if required. Click **Copy** to enter the **Copy Camera** menu, as shown in **Figure 13-18**.
6. Select the camera(s) to be configured with the same quota settings. You can also click the checkbox of IP Camera to select all cameras.

7. Click **OK** to finish the Copy settings and return back to the Storage Mode interface.

8. Click **Apply** to apply the settings.

   **NOTE**
   If the quota capacity is set to 0, then all cameras will use the total capacity of HDD for record.

**SECTION 5  CHECKING HDD STATUS**

You may check the status of the installed HDDs on NVR so as to take immediate action in case of HDD failure.

**Checking HDD Status in HDD Information Interface**

1. Enter the HDD Information interface. **Menu > HDD > General**.

2. Check the status of each HDD which is displayed on the list, as shown in **Figure 13-19**.
Checking HDD Status in HDD Information Interface

1. Enter the System Information interface. **Menu >Maintenance > System Info.**

2. Click the **HDD** tab to view the status of each HDD displayed on the list, as shown in **Figure 13-20.**

**NOTE** If the status of HDD is Normal or Sleeping, it works normally. If the status is Uninitialized or Abnormal, please initialize the HDD before use. And if the HDD initialization is failed, please replace it with a new one.
SECTION 6 HDD DETECTION

The device provides the HDD detection function such as the adopting of the S.M.A.R.T. and the Bad Sector Detection technique. The S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a monitoring system for HDD to detect and report on various indicators of reliability in the hopes of anticipating failures.


1. Select the HDD to view its S.M.A.R.T information list, as shown in Figure 13-21.
The related information of the S.M.A.R.T. monitoring system is shown on the interface.

You can choose the self-test types as Short Test, Expanded Test or the Conveyance Test. Click start to start the S.M.A.R.T. HDD self-evaluation.

If you want to use the HDD even when the S.M.A.R.T. checking fails, check the checkbox of the Continue to use the disk when self-evaluation is failed item.

**Bad Sector Detection**

1. Click the Bad Sector Detection tab.
2. Select the HDD No. in the dropdown list you want to configure, and choose All Detection or Key Area Detection as the detection type.
3. Click Detect to start the detection.
Click **Error info** to see the detailed damage information. You can also pause/resume or cancel the detection.

**SECTION 7  CONFIGURING HDD ERROR ALARMS**

You can configure the HDD error alarms when the HDD status is **Uninitialized** or **Abnormal**.

1. Enter the Exception interface. **Menu > Configuration > Exceptions**.
2. Select the **Exception Type** to **HDD Error** from the drop-down list.
3. Click the checkboxes below to select the HDD error alarm type(s), as shown in **Figure 13-23**.

---

**NOTE**

The alarm type can be selected to: Audible Warning, Notify Surveillance Center, Send Email and Trigger Alarm Output. Please refer to Chapter 9 Section 6 - Setting Alarm Response Actions (page 9-11).
4. When Trigger Alarm Output is selected, you can also select the alarm output to be triggered from the list below.

5. Click Apply to save the settings.
SECTION 1 CONFIGURING OSD SETTINGS

You can configure the OSD (On-screen Display) settings for the camera, including date/time, camera name, etc.

1. Enter the OSD Configuration interface. **Menu > Camera > OSD.**
2. Select the camera to configure OSD settings.
3. Edit the **Camera Name** in the text field.
4. Configure the **Display Name**, **Display Date** and **Display Week** by clicking the checkbox.
5. Select the **Date Format**, **Time Format** and **Display Mode**.

You can use the mouse to click and drag the text frame on the preview window to adjust the OSD position.

7. Click **Apply** to apply the settings.
SECTION 2 CONFIGURING PRIVACY MASK

You are allowed to configure the four-sided privacy mask zones that cannot be viewed by the operator. The privacy mask can prevent certain surveillance areas to be viewed or recorded.

1. Enter the Privacy Mask Settings interface. **Menu > Camera > Privacy Mask.**
2. Select the camera to set privacy mask.
3. Click the checkbox of **Enable Privacy Mask** to enable this feature.

4. Use the mouse to draw a zone on the window. The zones will be marked with different frame colors. Up to 4 privacy mask zones can be configured and the size of each area can be adjusted.

5. Clear the configured privacy mask zones on the window by clicking the corresponding **Clear Zone 1-4** icons on the right side of the window, or click **Clear All** to clear all zones.
6. Click **Apply** to save the settings.

### SECTION 3 CONFIGURING VIDEO PARAMETERS

1. Enter the Image Settings interface. **Menu > Camera > Image.**
2. Select the camera to set image parameters.
3. Click on the arrow to change the value of each parameter.
4. Click **Apply** to save the settings.
**SECTION 1  VIEWING SYSTEM INFORMATION**

1. Enter the System Information interface. **Menu > Maintenance > System Info.**
2. You can click the **Device Info, Camera, Record, Alarm, Network** and **HDD** tabs to view the system information of the device.

---

**SECTION 2  SEARCHING AND EXPORTING LOG FILES**

The operation, alarm, exception and information of the NVR can be stored in log files, which can be viewed and exported at any time.

1. Enter the Log Search interface. **Menu > Maintenance > Log Information.**
2. Set the log search conditions to refine your search, including the **Start Time**, **End Time**, **Major Type** and **Minor Type**.

3. Click **Search** to start search log files.

4. The matched log files are displayed as in **Figure 15-3**. Up to 2000 log files can be displayed each time.
5. Click the button of each log or double-click it to view its detailed information, as shown in Figure 15-4. Click the button to view the related video files if available.
6. If you want to export the log files, click the Export button on the Search Result interface to enter the Export menu, as shown in Figure 15-5.
7. Select the backup device from the drop-down list by Device Name.

8. Select the format of the log files to be exported. Up to nine formats are selectable.

9. Click Export to export the log files to the selected backup device.
   Click New Folder to create new folder in the backup device, or click Format to format the backup device before log export.

---

**NOTE**

Please connect the backup device to NVR before operating log export.

---

**SECTION 3 IMPORTING/EXPORTING IP CAMERA INFORMATION**

The information of added IP camera can be generated into an excel file and exported to the local device for backup, including the IP address, manage port, password of admin, etc. The exported file can be edited on your PC, like adding or deleting the content, and copy the setting to other devices by importing the excel file into it.

1. Enter the camera management interface. Menu > Camera > IP Camera Import/Export.

2. Click the IP Camera Import/Export tab and the content of detected plugged external device appears.

3. Click Export to export configuration files to the selected local backup device.

4. To import a configuration file, select the file from the selected backup device and click Import. After the importing process is completed, you must reboot the NVR.

---

**SECTION 4 IMPORTING/EXPORTING CONFIGURATION FILES**

The configuration files of the NVR can be exported to local device for backup; and the configuration files of one NVR can be imported to multiple NVR devices if they are to be configured with the same parameters.

2. Click **Export** to export configuration files to the selected local backup device.

3. To import a configuration file, select the file from the selected backup device and click **Import**. After the import process is completed, you must reboot the NVR.

   After having finished the import of configuration files, the device reboots automatically.

SECTION 5  UPGRADING SYSTEM

The firmware on your NVR can be upgraded by local backup device or remote FTP server.

5.1 Upgrading by Local Backup Device

1. Connect your NVR with a local backup device where the update firmware file is located.

2. Enter the Upgrade interface. **Menu >Maintenance >Upgrade**.
3. Click the **Local Upgrade** tab to enter the local upgrade menu, as shown in Figure 15-7.

![Local Upgrade Interface](image)

4. Select the update file from the backup device.
5. Click **Upgrade** to start upgrading.
6. After the upgrading is complete, reboot the NVR to activate the new firmware.

### 5.2 Upgrading by FTP

Ensure the network connection of the PC (running FTP server) and the device is valid and correct. Run the FTP server on the PC and copy the firmware into the corresponding directory of your PC.

Refer to the user manual of the FTP server to set the FTP server on your PC and put the firmware file into the directory as required.

1. Enter the Upgrade interface. **Menu >Maintenance >Upgrade**.
2. Click the **FTP** tab to enter the local upgrade interface, as shown in Figure 15-8.
3. Enter the **FTP Server Address** in the text field.
4. Click **Upgrade** to start upgrading.
5. After upgrading is complete, reboot the NVR to activate the new firmware.

**SECTION 6  RESTORING DEFAULT SETTINGS**

1. Enter the Default interface. **Menu > Maintenance > Default.**

2. Select the restoring type from the following three options.
   - **Restore Defaults:** Restore all parameters, except the network (including IP address, subnet mask, gateway, MTU, NIC working mode, default route, server port, etc.) and user account parameters, to the factory default settings.
   - **Factory Defaults:** Restore all parameters to the factory default settings.
   - **Restore to Inactive:** Restore the device to the inactive status.
3. Click **OK** to restore the default settings. The device will reboot automatically after restoring to the default settings.
SECTION 1 CONFIGURING GENERAL SETTINGS

You can configure the BNC output standard, VGA output resolution, mouse pointer speed through the Menu > Configuration > General interface.

1. Enter the General Settings interface. Menu > Configuration > General.
2. Select the General tab.

3. Configure the following settings:
   - **Language**: The default language used is English.
   - **Resolution**: Select the resolution for the video output, which must be the same with the resolution of the monitor screen.
   - **Time Zone**: Select the time zone.
   - **Date Format**: Select the date format.
   - **System Date**: Select the system date.
   - **System Time**: Select the system time.
   - **Mouse Pointer Speed**: Set the speed of mouse pointer; four levels are configurable.
Enable Wizard: Enable/disable the Wizard when the device starts up.
Enable Password: Enable/disable the use of the login password.

4. Click Apply to save the settings.

SECTION 2 CONFIGURING DST SETTINGS

1. Enter the General Settings interface. Menu >Configuration >General.
2. Choose DST Settings tab.

You can check the checkbox before the Auto DST Adjustment item.
Or you can manually check the Enable DST checkbox, and then choose the date of the DST period.

SECTION 3 CONFIGURING MORE SETTINGS FOR DEVICE PARAMETERS

1. Enter the General Settings interface. Menu >Configuration >General.
2. Click the More Settings tab to enter the More Settings interface, as shown in Figure 16-3.

3. Configure the following settings:
**Device Name**: Edit the name of NVR.

**Device No.**: Edit the serial number of NVR. The Device No. can be set in the range of 1~255, and the default No. is 255. The number is used for the remote and keyboard control.

**Auto Logout**: Set timeout time for menu inactivity. E.g., when the timeout time is set to 5 Minutes, then the system will exit from the current operation menu to live view screen after 5 minutes of menu inactivity.

**Menu Output Mode**: You can choose the menu display on different video output. By default, only HDMITM /VGA is selectable.

4. Click **Apply** to save the settings.

**SECTION 4 MANAGING USER ACCOUNTS**

There is a default account in the NVR: Administrator. The Administrator user name is admin and the password is set when you start the device for the first time. The Administrator has the permission to add and delete users and configure user parameters.

4.1 **Adding a User**

1. Enter the User Management interface. **Menu > Configuration > User.**

*Figure 16-4  User Management Interface*
2. Click the Add button to enter the Add User interface.

3. Enter the information for new user, including **User Name**, **Password**, **Confirm**, **Level** and **User's MAC Address**.

   **Password**: Set the password for the user account.

   **Level**: Set the user level to **Operator** or **Guest**. Different user levels have different operating permission.
   - **Operator**: The Operator user level has permission of Two-way Audio in Remote Configuration and all operating permission in Camera Configuration by default.
   - **Guest**: The Guest user has no permission of Two-way Audio in Remote Configuration and only has the local/remote playback in the Camera Configuration by default.

   **User's MAC Address**: The MAC address of the remote PC which logs onto the NVR. If it is configured and enabled, it only allows the remote user with this MAC address to access the NVR.

   **NOTE**: STRONG PASSWORD RECOMMENDED- We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Click **OK** to save the settings and go back to the User Management interface. The added new user displays on the list, as shown in Figure 16-6.

   ![Figure 16-6  Added User Listed in User Management Interface](image)

5. Select the user from the list and then click the button to enter the Permission settings interface, as shown in Figure 16-7.

   ![Figure 16-7  User Permissions Setting Interface](image)

6. Set the operating permission of **Local Configuration**, **Remote Configuration**, and **Camera Configuration** for the user.
Local Configuration

**Local Log Search:** Searching and viewing logs and system information of NVR.

**Local Parameters Settings:** Configuring parameters, restoring factory default parameters and importing/exporting configuration files.

**Local Camera Management:** The adding, deleting and editing of IP cameras.

**Local Advanced Operation:** Operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

**Local Shutdown Reboot:** Shutting down or rebooting the NVR.

Remote Configuration

**Remote Log Search:** Remotely viewing logs that are saved on the NVR.

**Remote Parameters Settings:** Remotely configuring parameters, restoring factory default parameters and importing/exporting configuration files.

**Remote Camera Management:** Remote adding, deleting and editing of the IP cameras.

**Remote Serial Port Control:** Configuring settings for RS-232 and RS-485 ports.

**Remote Video Output Control:** Sending remote button control signal.

**Two-Way Audio:** Realizing two-way radio between the remote client and the NVR.

**Remote Alarm Control:** Remotely arming (notify alarm and exception message to the remote client) and controlling the alarm output.

**Remote Advanced Operation:** Remotely operating HDD management (initializing HDD, setting HDD property), upgrading system firmware, clearing I/O alarm output.

**Remote Shutdown/Reboot:** Remotely shutting down or rebooting the NVR.

Camera Configuration

**Remote Live View:** Remotely viewing live video of the selected camera (s).

**Local Manual Operation:** Locally starting/stoping manual recording and alarm output of the selected camera (s).

**Remote Manual Operation:** Remotely starting/stoping manual recording and alarm output of the selected camera (s).

**Local Playback:** Locally playing back recorded files of the selected camera (s).

**Remote Playback:** Remotely playing back recorded files of the selected camera (s).
Local PTZ Control: Locally controlling PTZ movement of the selected camera(s).

Remote PTZ Control: Remotely controlling PTZ movement of the selected camera(s).

Local Video Export: Locally exporting recorded files of the selected camera(s).

7. Click **OK** to save the settings and exit interface.

---

4.2 Deleting a User

1. Enter the User Management interface. **Menu > Configuration >User.**
2. Select the user to be deleted from the list, as shown in **Figure 16-8.**

![User List](image)

3. Click the **** icon to delete the selected user account.

4.3 Editing a User

For the added user accounts, you can edit the parameters.

1. Enter the User Management interface. **Menu > Configuration >User.**
2. Select the user to be edited from the list, as shown in **Figure 16-8.**
3. Click the **** icon to enter the Edit User interface, as shown in **Figure 16-9.**
4. Edit the corresponding parameters.

**Operator and Guest** - You can edit the user information, including user name, password, permission level and MAC address. Check the checkbox of Change Password if you want to change the password, and input the new password in the text field of Password and Confirm. A strong password is recommended.

**Admin** - You are only allowed to edit the password and MAC address. Check the checkbox of Change Password if you want to change the password, and the input the correct old password, and the new password in the text field of Password and Confirm.
5. Click **OK** to save the settings and exit the menu.

6. For the Operator or Guest user account, click the **✓** button on the user management interface to edit the permission.
SECTION 1  TROUBLESHOOTING ISSUES

- No image displayed on the monitor after starting up normally.

  **Possible Reasons:**
  
  - No VGA or HDMITM connections.
  - Connection cable is damaged.
  - Input mode of the monitor is incorrect.
  
  1. Verify the device is connected with the monitor via HDMITM or VGA cable. If not, please connect the device with the monitor and reboot.
  2. Verify the connection cable is good. If there is still no image display on the monitor after rebooting, please check if the connection cable is good, and change a cable to connect again.
  3. Verify Input mode of the monitor is correct. Please check the input mode of the monitor matches with the output mode of the device (e.g. if the output mode of NVR is HDMITM output, then the input mode of monitor must be the HDMITM input). And if not, please modify the input mode of monitor.
  4. Check if the fault is solved by the step 1 to step 3. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.

- There is an audible warning sound "Di-Di-Di-DiDi" after a new bought NVR starts up.

  **Possible Reasons:**
  
  - No HDD is installed in the device.
  - The installed HDD has not been initialized.
  - The installed HDD is not compatible with the NVR or is broken-down.
  
  1. Verify at least one HDD is installed in the NVR. If not, please install the compatible HDD. Please refer to the "Quick Operation Guide" for the HDD installation steps.

    If you don't want to install a HDD, select **Menu >Configuration > Exceptions**, and uncheck the **Audible Warning** checkbox of HDD Error.
2. Verify the HDD is initialized.
   Select Menu >HDD >General.
   If the status of the HDD is "Uninitialized", please check the checkbox of corresponding HDD and click the Init button.

3. Verify the HDD is detected or is in good condition.
   Select Menu >HDD >General.
   If the HDD is not detected or the status is "Abnormal", please replace the dedicated HDD according to the requirement.

4. Check if the fault is solved by the step 1 to step 3. If it is solved, finish the process.
   If not, please contact the engineer from our company to do the further process.

- The status of the added IP camera displays as "Disconnected" when it is connected through Private Protocol. Select Menu >Camera >Camera >IP Camera to get the camera status.

**Possible Reasons:**

Network failure, and the NVR and IP camera lost connections.

The configured parameters are incorrect when adding the IP camera.

Insufficient bandwidth.

1. Verify the network is connected.
   Enter the Network Traffic interface. Menu > Maintenance >Net Detect. Click the Network Detection tab to enter the Network Detection menu Enter the destination address in the text field of Destination Address. Click Test button to start testing network delay and packet loss. The testing result pops up on the window. If there exists return information and the time value is little, the network is normal.

2. Verify the configuration parameters are correct.
   Select Menu > Camera > Camera >IP Camera. Verify the following parameters are the same with those of the connected IP devices, including IP address, protocol, management port, user name and password.

3. Verify the whether the bandwidth is enough.
   Select Menu >Maintenance > Net Detect > Network Stat. Check the usage of the access bandwidth, and see if the total bandwidth has reached its limit.

4. Check if the fault is solved by the step 1 to step 3. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.
The IP camera frequently goes online and offline and the status of it displays as "Disconnected".

Possible Reasons:

The IP camera and the NVR versions are not compatible.

Unstable power supply of IP camera.

Unstable network between IP camera and NVR.

Limited flow by the switch connected with IP camera and NVR.

1. Verify the IP camera and the NVR versions are compatible.
   - Enter the IP camera Management interface Menu > Camera > Camera > IP Camera, and view the firmware version of connected IP camera.
   - Enter the System Info interface Menu > Maintenance > System Info > Device Info, and view the firmware version of NVR.

2. Verify power supply of IP camera is stable.
   - Verify the power indicator is normal.
   - When the IP camera is offline, please try the ping command on PC to check if the PC connects with the IP camera.

3. Verify the switch is not flow control.
   - Check the brand, model of the switch connecting IP camera and NVR, and contact with the manufacturer of the switch to check if it has the function of flow control. If so, please turn it down.

4. Check if the fault is solved by the step 1 to step 3. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.

No monitor connected with the NVR locally and when you manage the IP camera to connect with the device by web browser remotely, of which the status displays as Connected. And then you connect the device with the monitor via VGA or HDMITM interface and reboot the device, there is black screen with the mouse cursor.

Connect the NVR with the monitor before startup via VGA or HDMITM interface, and manage the IP camera to connect with the device locally or remotely, the status of IP camera displays as Connect.

Possible Reasons:

After connecting the IP camera to the NVR, the image is output via the main spot interface by default.

1. Enable the output channel.
2. Select Menu > Configuration > Live View > View, and select video output
interface in the drop-down list and configure the window you want to view.

- The view settings can only be configured by the local operation of NVR.
- Different camera orders and window-division modes can be set for different output interfaces separately, and digits like "D1" and "D2" stand for the channel number, and "X" means the selected window has no image output.

3. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.

Live view stuck when video output locally.

Possible Reasons:

Poor network between NVR and IP camera, and there exists packet loss during the transmission.

The frame rate has not reached the real-time frame rate.

1. Verify the network between NVR and IP camera is connected. Enter the Network Traffic interface. Menu > Maintenance > Net Detect.
   Click the Network Detection tab to enter the Network Detection menu.
   Enter the destination address in the text field of Destination Address.
   Click Test button to start testing network delay and packet loss. The testing result pops up on the window. If there exists return information and the time value is little, the network is normal.

2. Verify the frame rate is real-time frame rate. Select Menu > Record > Parameters > Record, and set the Frame rate to Full Frame.

3. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.

Live view stuck when video output remotely via the Internet Explorer or platform software.

Possible Reasons:

Poor network between NVR and IP camera, and there exists packet loss during the transmission.

Poor network between NVR and PC, and there exists packet loss during the transmission.

The performances of hardware are not good enough, including CPU, memory, etc.

1. Verify the network between NVR and IP camera is connected.
Enter the Network Traffic interface. **Menu > Maintenance > Net Detect.**

Click the **Network Detection** tab to enter the Network Detection menu.

Enter the destination address in the text field of **Destination Address**.

Click **Test** button to start testing network delay and packet loss. The testing result pops up on the window. If there exists return information and the time value is little, the network is normal.

2. Verify the network between NVR and PC is connected.

Open the **cmd** window in the **Start** menu, or you can press **windows+R** shortcut key to open it.

Use the ping command to send large packet to the NVR, execute the command of "**ping 192.168.0.0 -I 1472 -f**" (the IP address may change according to the real condition), and check if there exists packet loss.

![NOTE](image)

*Simultaneously press Ctrl and C to exit the ping command.*

3. Verify the hardware of the PC is good enough. Simultaneously press **Ctrl, Alt and Delete** to enter the windows task management interface, as shown in **Figure 17-1**.
Select the **Performance** tab; check the status of the CPU and Memory. If the resource is not enough, please end some unnecessary processes.

4. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.

When using the NVR to get the live view audio, there is no sound or there is too much noise, or the volume is too low.

**Possible Reasons:**

Cable between the pickup and IP camera is not connected well; impedance mismatches or incompatible.

The stream type is not set as "**Video & Audio**".

The encoding standard is not supported with NVR.

1. Verify the cable between the pickup and IP camera is connected well; impedance matches and compatible.
Log in the IP camera directly, and turn the audio on, check if the sound is normal. If not, please contact the manufacturer of the IP camera.

2. Verify the setting parameters are correct. Select Menu > Record > Parameters > Record, and set the Stream Type as "Audio & Video".

3. Verify the audio encoding standard of the IP camera is supported by the NVR. NVR supports G722.1 and G711 standards, and if the encoding parameter of the input audio is not one of the previous two standards, you can log in the IP camera to configure it to the supported standard.

4. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.

The image gets stuck when NVR is playing back by single or multi-channel.

Possible Reasons:

Poor network between NVR and IP camera, and there exists packet loss during the transmission.

The frame rate is not the real-time frame rate.

The NVR supports up to 16-channel synchronize playback at the resolution of 4CIF, if you want a 16-channel synchronize playback at the resolution of 720p, the frame extracting may occur, which leads to a slight stuck.

1. Verify the network between NVR and IP camera is connected.


   Click the Network Detection tab to enter the Network Detection menu. Enter the destination address in the text field of Destination Address. Click Test button to start testing network delay and packet loss. The testing result pops up on the window. If there exists return information and the time value is little, the network is normal.

   2. Verify the frame rate is real-time frame rate. Select Menu > Record > Parameters > Record, and set the Frame Rate to "Full Frame".

   3. Verify the hardware can afford the playback. Reduce the channel number of playback. Select Menu > Record > Encoding > Record, and set the resolution and bit rate to a lower level.

   4. Reduce the number of local playback channel. Select Menu > Playback, and uncheck the checkbox of unnecessary channels.

   5. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.
No record file found in the NVR local HDD, and prompt "No record file found".

Possible Reasons:

The time setting of system is incorrect.

The search condition is incorrect.

The HDD is error or not detected.

1. Verify the system time setting is correct. Select Menu > Configuration > General > General, and verify the "Device Time" is correct.
2. Verify the search condition is correct. Select "Playback", and verify the channel and time are correct.
3. Verify the HDD status is normal. Select Menu > HDD > General to view the HDD status, and verify the HDD is detected and can be read and written normally.
4. Check if the fault is solved by the above steps. If it is solved, finish the process. If not, please contact the engineer from our company to do the further process.
List of Compatible IP Cameras

- For the list, our company holds right to interpret.
- ONVIF compatibility means the camera can be supported both when it uses the ONVIF protocol and its private protocols. Only ONVIF is supported refers to the camera can only be supported when it uses the ONVIF protocol. Only AXIS is supported refers to the function can only be supported when it uses the AXIS protocol.

Table 18-1 provides a list of compatible IP Cameras.
### Table 18-1 List of Compatible IP Cameras

<table>
<thead>
<tr>
<th>IP Camera Manufacturer or Protocol</th>
<th>Model</th>
<th>Version</th>
<th>Max. Resolution</th>
<th>Sub-stream</th>
<th>Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTI</td>
<td>TCM4301-10D-X-00063</td>
<td>AID-310-V4.12.08-AC</td>
<td>1280×1024</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>TCM5311-11D-X-00023</td>
<td>AID-310-V4.12.09-AC</td>
<td>1280×960</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>TCM3401-40L-X-00027</td>
<td>AID-220-V3.13.16-AC</td>
<td>1280×1024</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>ARECONT</td>
<td>AV8151DN</td>
<td>65172</td>
<td>1600×1200</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>AV1305M</td>
<td>65175</td>
<td>1280×1024</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>AV2125</td>
<td>65143</td>
<td>1600×1200</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>AV2815</td>
<td>65220</td>
<td>1920×1080</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>AV3105M</td>
<td>65175</td>
<td>1920×1080</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>AV3105</td>
<td>65175</td>
<td>1920×1080</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>M1114</td>
<td>5.09.1</td>
<td>1024×640</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td>AXIS</td>
<td>M5011 (ONVIF compatibility)</td>
<td>5.21</td>
<td>704×576</td>
<td>√ (Only AXIS is supported)</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>M5014 (ONVIF compatibility)</td>
<td>5.21.1</td>
<td>1280×800</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>P3301 (ONVIF compatibility)</td>
<td>5.11.2</td>
<td>758×576</td>
<td>√</td>
<td>√ (Only AXIS is supported)</td>
</tr>
<tr>
<td></td>
<td>P3304 (ONVIF compatibility)</td>
<td>5.20</td>
<td>1440×900</td>
<td>√</td>
<td>√ (Only AXIS is supported)</td>
</tr>
<tr>
<td></td>
<td>P3343 (ONVIF compatibility)</td>
<td>5.20.1</td>
<td>800×600</td>
<td>√</td>
<td>√ (Only AXIS is supported)</td>
</tr>
<tr>
<td></td>
<td>P3344 (ONVIF compatibility)</td>
<td>5.20.1</td>
<td>1440×900</td>
<td>√</td>
<td>√ (Only AXIS is supported)</td>
</tr>
<tr>
<td></td>
<td>P5532</td>
<td>5.15</td>
<td>720×576</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>Q404</td>
<td>5.02</td>
<td>720×576</td>
<td>√</td>
<td>x</td>
</tr>
<tr>
<td>Bosch (ONVIF compatibility)</td>
<td>AutoDome Jr 800HD</td>
<td>39500-450</td>
<td>1920×1080</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>NBC 265 P</td>
<td>07500-453</td>
<td>1280×720</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Domino NBN-921-P</td>
<td>10500-453</td>
<td>1280×720</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>Brickcom</td>
<td>FB-130NP (ONVIF compatibility)</td>
<td>V3.1.0.8</td>
<td>1280×1024</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>CB-500AP (ONVIF compatibility)</td>
<td>V3.2.1.3</td>
<td>1920×1080</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>WFB-100AP</td>
<td>V3.1.0.9</td>
<td>1280×800</td>
<td>x</td>
<td>√</td>
</tr>
<tr>
<td>IP Camera Manufacturer or Protocol</td>
<td>Model</td>
<td>Version</td>
<td>Max. Resolution</td>
<td>Sub-stream</td>
<td>Audio</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------</td>
<td>---------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>Canon</td>
<td>VB-M6000</td>
<td>V1r 1.0.0</td>
<td>1280×960</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Canon</td>
<td>VB-516000D</td>
<td>V1r 1.0.0</td>
<td>1280×960</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Canon</td>
<td>VB-N7000F</td>
<td>V1r 1.0.0</td>
<td>1280×960</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HLNT</td>
<td>HLC-WAD</td>
<td>V1.0.40</td>
<td>1920×1200</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>DS-2CD1013F-E</td>
<td>V3.1.0 build 1311202</td>
<td>2560×1920</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7113F-ED</td>
<td>V3.1.0 build 1311202</td>
<td>2560×1920</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7113F-EZ</td>
<td>V3.1.0 build 1311202</td>
<td>2560×1920</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD8113F-E</td>
<td>V4.0.3 build 120913</td>
<td>2560×1920</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD8113F-E</td>
<td>V4.0.3 build 120913</td>
<td>2560×1920</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD8414F-E</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD1014F-ED</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>DS-2CD7214F-EZH</td>
<td>V3.1.0 build 1311202</td>
<td>2048×1536</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Network Video Recorder Configuration Guide
<table>
<thead>
<tr>
<th>IP Camera Manufacturer or Protocol</th>
<th>Model</th>
<th>Version</th>
<th>Max. Resolution</th>
<th>Sub-stream</th>
<th>Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>D5-2CD2112-E</td>
<td>V5.1.2 build 40116</td>
<td>1280 x 960</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-F</td>
<td>V5.1.2 build 40116</td>
<td>1280 x 960</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD5112-EI</td>
<td>V5.1.2 build 40116</td>
<td>1280 x 960</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD5112-FI</td>
<td>V5.1.2 build 40116</td>
<td>1280 x 960</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-E</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-EZ</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-E</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-EZ</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-E</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-EZ</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-E</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD0112-EZ</td>
<td>V5.1.2 build 131202</td>
<td>1280 x 720</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3I</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>D5-2CD2112-3F</td>
<td>V5.1.2 build 40116</td>
<td>2048 x 1536</td>
<td>✓</td>
<td>x</td>
</tr>
<tr>
<td>IP Camera Model</td>
<td>Version</td>
<td>Max. Resolution</td>
<td>Sub-stream</td>
<td>Audio</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>DS-2CD210F-3E</td>
<td>V5.1.3 build 140117</td>
<td>1280x960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD4011F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD211F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD211F-3E/2.8-12mm</td>
<td></td>
<td>2000x1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD411F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD211F-3E/2.8-12mm</td>
<td></td>
<td>2000x1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD22F-3E</td>
<td>V5.1.3 build 140117</td>
<td>1920x1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD42F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD42F-3E/2.8-12mm</td>
<td></td>
<td>1920x1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD424F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD424F-3E/2.8-12mm</td>
<td></td>
<td>1920x1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD224F-3E</td>
<td>V5.1.3 build 140117</td>
<td>1920x1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD23F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD433F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD433F-3E/2.8-12mm</td>
<td>V5.1.3 build 140117</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD233F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD433F-3E/2.8-12mm</td>
<td></td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD233F-3E/3.6mm</td>
<td></td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD212F-3E</td>
<td>V5.1.3 build 140117</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD411F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD411F-3E/2.8-12mm</td>
<td></td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD212F-3E</td>
<td>V5.1.3 build 140117</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD412F-3E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-2CD412F-3E/2.8-12mm</td>
<td></td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD412F-3E/3.6mm</td>
<td></td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD212F-3E</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD212F-3E/2.8-12mm</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD412F-3E</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD412F-3E/2.8-12mm</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD412F-3E/3.6mm</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD212F-3E</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD233F-3E</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD233F-3E/2.8-12mm</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD233F-3E/3.6mm</td>
<td>V5.1.0 build 131202</td>
<td>2048x1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD8021F</td>
<td>V2.0.0 build 690522</td>
<td>704x470</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DS-2CD8112F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Camera Manufacturer or Protocol</td>
<td>Model</td>
<td>Version</td>
<td>Max. Resolution</td>
<td>Sub-stream</td>
<td>Audio</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------</td>
<td>---------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>DS-2CD831F</td>
<td></td>
<td>V3.1.0</td>
<td>704×576</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DS-2CD831FF2</td>
<td></td>
<td>V3.1.0</td>
<td>704×576</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DS-2CD831F2</td>
<td></td>
<td>V3.1.0</td>
<td>704×576</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DS-2CD831F2-E</td>
<td></td>
<td>V3.1.0</td>
<td>704×576</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DS-2CD831F2-E2</td>
<td></td>
<td>V3.1.0</td>
<td>704×576</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DS-2CD831F2-E2-E</td>
<td></td>
<td>V3.1.0</td>
<td>704×576</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DS-2CD831F2-E2-E2</td>
<td></td>
<td>V3.1.0</td>
<td>704×576</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DS-2CD9121</td>
<td>V3.4.2 build 12103</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>iDS-2CD9121</td>
<td>V3.4.2 build 12103</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9121A</td>
<td>V3.5.0 build 13005</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9121A</td>
<td>V3.6.1 build 14013</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD91211</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD91211</td>
<td>V3.6.1 build 14013</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.6.1 build 14013</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>DS-2CD9122</td>
<td>V3.5.0 build 130012</td>
<td>1500×1000</td>
<td>✓</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>IP Camera Manufacturer or Protocol</td>
<td>Model</td>
<td>Version</td>
<td>Max. Resolution</td>
<td>Sub-stream</td>
<td>Audio</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------</td>
<td>---------</td>
<td>----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>D8-2DF5174-A/D/A3/D3 AF/A3F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8-2DE5174-A/A3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8-2DE5174-A AE</td>
<td>V5.1.0 build 131203</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DE5174-A EE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8-2DE5174-A AE</td>
<td>V5.1.0 build 131203</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF5174-A EE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8-2DE5174-A EE</td>
<td>V5.1.0 build 131203</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF5174-A EE</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DM1-5722 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>D8-2DF1-5702 D8-2DF1-572 D8-2DM1-5702 D8-2DM1-572 D8-2DF1-5722</td>
<td></td>
<td>1280x720</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>IP Camera Manufacturer or Protocol</td>
<td>Model</td>
<td>Version</td>
<td>Max. Resolution</td>
<td>Sub-stream</td>
<td>Audio</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------</td>
<td>----------------------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>D8-2DF1-514</td>
<td>D8-2DF1-514</td>
<td>V3.2.0 build131223</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>D8-2DF1-114</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>D8-2DF1-402</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>D8-2DF1-402N</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D8-22CN2005</td>
<td>D8-22CN2005</td>
<td>V3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-22CN3006</td>
<td>D8-22CN3006</td>
<td>V3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-22DN2005</td>
<td>D8-22DN2005</td>
<td>v3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-22DN3006</td>
<td>D8-22DN3006</td>
<td>V3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-22CN2007</td>
<td>D8-22CN2007</td>
<td>v3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-22CN3007</td>
<td>D8-22CN3007</td>
<td>V3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-22DN2007</td>
<td>D8-22DN2007</td>
<td>V3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-22DN3007</td>
<td>D8-22DN3007</td>
<td>V3.0.2 build130926</td>
<td>1280x960</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6501HFI</td>
<td>D8-6501HFI</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6504HFI</td>
<td>D8-6504HFI</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6501HFI-Sata</td>
<td>D8-6501HFI-Sata</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6504HFI-Sata</td>
<td>D8-6504HFI-Sata</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6501HFI-Sata</td>
<td>D8-6501HFI-Sata</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6504HFI-Sata</td>
<td>D8-6504HFI-Sata</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6501HCI</td>
<td>D8-6501HCI</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6504HCI</td>
<td>D8-6504HCI</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6501HCI-Sata</td>
<td>D8-6501HCI-Sata</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6504HCI-Sata</td>
<td>D8-6504HCI-Sata</td>
<td>V1.0.1 build130607</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6501HFI</td>
<td>D8-6501HFI</td>
<td>V1.0.1 build 131202</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>D8-6502HFI</td>
<td>D8-6502HFI</td>
<td>V1.0.1 build 131202</td>
<td>704x576</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>IP Camera Manufacturer or Protocol</td>
<td>Model</td>
<td>Version</td>
<td>Max. Resolution</td>
<td>Sub-stream</td>
<td>Audio</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------</td>
<td>---------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
<tr>
<td>NEC D5-0500HFPL</td>
<td>V1.0.4 build 150115</td>
<td>1020-1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NEC D5-0600HFPL/NEC D5-0601HFPL</td>
<td>V1.0.4 build 150115</td>
<td>1020-1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SW152(ONVIF compatibility)</td>
<td>Application:1.66 Image data:1.05</td>
<td>800-900</td>
<td>✓</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>WV-SC338(ONVIF compatibility)</td>
<td>Application:1.66 Image data:1.05</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SW155(ONVIF compatibility)</td>
<td>Application:1.66 Image data:1.05</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SW316(ONVIF compatibility)</td>
<td>Application:1.66 Image data:1.03</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SP105(ONVIF compatibility)</td>
<td>Application:1.66 Image data:1.03</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-VF112(ONVIF compatibility)</td>
<td>Application:1.66 Image data:1.03</td>
<td>640-240</td>
<td>✓</td>
<td></td>
<td>×</td>
</tr>
<tr>
<td>WV-SP102(ONVIF compatibility)</td>
<td>Application:1.66 Image data:1.03</td>
<td>640x480</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SP559(ONVIF compatibility)</td>
<td>Application:1.30 Image data:1.21</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SW559(ONVIF compatibility)</td>
<td>Application:1.30 Image data:1.21</td>
<td>1020-1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SW255(ONVIF compatibility)</td>
<td>Application:1.20 Image data:1.21</td>
<td>1020-1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SW355(ONVIF compatibility)</td>
<td>Application:1.20 Image data:1.04</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SW352(ONVIF compatibility)</td>
<td>Application:1.20 Image data:1.04</td>
<td>800-900</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-VF342(ONVIF compatibility)</td>
<td>Application:1.06 Image data:1.06</td>
<td>800-900</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-VF312(ONVIF compatibility)</td>
<td>Application:1.06 Image data:1.06</td>
<td>800-900</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-VF346(ONVIF compatibility)</td>
<td>Application:1.06 Image data:1.06</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SP900H</td>
<td>Application:1.34 Image data:1.06</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>WV-SP936H</td>
<td>Application:1.06 Image data:1.06</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>PELCO D1118</td>
<td>1.0.0-20120327-2.9310-A1.1552</td>
<td>1280-960</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DE30ND-AX3V3-U2</td>
<td>1.0.0-20120327-2.9081-A1.1552</td>
<td>1920-1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DX30ND-ACF2HE3</td>
<td>1.0.0-20120327-2.9080-A1.1552</td>
<td>2048-1536</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SAMSUNG (ONVIF compatibility)</td>
<td>SNB-5080D</td>
<td>V3.10_130416</td>
<td>1280-1024</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SANYO VCC-HD2500P</td>
<td>2.0.0-02(110318-00)</td>
<td>1920-1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SANYO VCC-HD1500P</td>
<td>2.0.0-02(110318-00)</td>
<td>1920-1080</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Network Video Recorder Configuration Guide 18-9
<table>
<thead>
<tr>
<th>Manufacturer or Protocol</th>
<th>Model</th>
<th>Version</th>
<th>Max. Resolution</th>
<th>Sub-stream</th>
<th>Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>SONY</td>
<td>VCC-HD400IP</td>
<td>2.03-02(010312-00)</td>
<td>1920×1080</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>SNC-CHZ20</td>
<td>1.50.00</td>
<td>1920×1080</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>SNC-8H124(ONVIF compatibility)</td>
<td>1.73.00</td>
<td>1280×720</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>SNC-EP680(ONVIF compatibility)</td>
<td>1.53.00</td>
<td>1920×1080</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>SNC-DH120T(Only ONVIF is supported)</td>
<td>1.50.00</td>
<td>2048×1536</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>Nivoteex</td>
<td>IP7133</td>
<td>0030a</td>
<td>640×480</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>FD8134(ONVIF compatibility)</td>
<td>0107a</td>
<td>1280×960</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>IP8161(ONVIF compatibility)</td>
<td>0104a</td>
<td>1600×1200</td>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>IP8331(ONVIF compatibility)</td>
<td>0102a</td>
<td>640×480</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>IP8332(ONVIF compatibility)</td>
<td>0103b</td>
<td>1280×800</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>ZAVIO</td>
<td>D5110</td>
<td>MG.1.6.05P9</td>
<td>1280×1024</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>F3106</td>
<td>MG.1.6.03P9</td>
<td>1280×1024</td>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>F3110</td>
<td>MG.1.6.01</td>
<td>1280×720</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>F3206</td>
<td>MG.1.6.02P4F</td>
<td>1920×1080</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>F531E</td>
<td>LM.1.6.1S8P10</td>
<td>640×480</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>
# Glossary

## Appendix A

### Section 1  Terms and Definitions

The following terms are used in this document. The term or acronym is listed as well as the associated definition. The terms are listed in alphabetical order.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDNS</td>
<td>Dynamic DNS is a method, protocol or network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a domain name server to change, in real time (ad-hoc) the active DNS configuration of its configured host names, addresses or other information stored in DNS.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol (DHCP) is a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.</td>
</tr>
<tr>
<td>Dual Stream</td>
<td>Dual stream is a technology used to record high resolution video locally while transmitting a lower resolution stream over the network. The two streams are generated by the DVR, with the main stream having a maximum resolution of 4CIF and the sub-stream having a maximum resolution of CIF.</td>
</tr>
<tr>
<td>HDD</td>
<td>Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.</td>
</tr>
<tr>
<td>HTTP</td>
<td>Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.</td>
</tr>
<tr>
<td>Hybrid DVR</td>
<td>A hybrid DVR is a combination of a DVR and NVR.</td>
</tr>
<tr>
<td>NTP</td>
<td>Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.</td>
</tr>
<tr>
<td>NTSC</td>
<td>Acronym for National Television System Committee. NTSC is an analog television standard used in such countries as the United States and Japan. Each frame of an NTSC signal contains 525 scan lines at 60Hz.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NVR</td>
<td>Acronym for Network Video Recorder. An NVR can be a PC-based or embedded system used for centralized management and storage for IP cameras, IP Domes and other DVRs.</td>
</tr>
<tr>
<td>PAL</td>
<td>Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast television systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.</td>
</tr>
<tr>
<td>PPPoE</td>
<td>PPPoE, Point-to-Point Protocol over Ethernet, is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.</td>
</tr>
<tr>
<td>PTZ</td>
<td>Acronym for Pan, Tilt, Zoom. PTZ cameras are motor driven systems that allow the camera to pan left and right, tilt up and down and zoom in and out.</td>
</tr>
<tr>
<td>USB</td>
<td>Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.</td>
</tr>
</tbody>
</table>
Network Video Recorder
Configuration Guide

NEC Corporation of America
ISSUE 1.0