

AO

TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS

PROPOSTA COMERCIAL

PREGÃO ELETRÔNICO: 012/2026

PROCESSO: 2025/000002770-00

OBJETO: Registro de preços para aquisição remunerada, sob demanda, de solução de videomonitoramento IP, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

DADOS DA EMPRESA		
Razão Social: Teltex Tecnologia S.A.		
CNPJ: 73.442.360/0003-89		
Inscrição Estadual: 083.483.89-6		
Inscrição Municipal: 4679988		
Endereço: Rod. Gov. Mário Covas, SN, KM 279, Sala 79, Jacury, Serra/ES, CEP 29161-230		
Telefone: (11) 3840-6400		
E-mail: licitacoes@teltex.com.br		
DADOS BANCÁRIOS		
Banco: Santander (033)	Agência: 1064	Conta Corrente: 130036631
DADOS DO REPRESENTANTE LEGAL PARA ASSINATURA CONTRATO		
Nome: Valmor Fernandes Rosa Filho (brasileiro, administrador, casado)		
Cargo: Diretor Presidente		
RG: 60.347.955-49 SSP/RS		
CPF: 553.691.380-87		
E-mail: juridico@teltex.com.br		

ITEM	DESCRIÇÃO	MARCA	MODELO	QTD.	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
1	Fornecimento de Câmera Tipo 1 – Câmera IP Bullet com Detecção Facial e Vídeo Estruturado	1. Hikvision 2. Teltex	1. DS-2CD3666G2T-IZS (2,7 - 13,5mm) + DS-1260ZJ + HS-TF-L2(STD)/256G (modelo 256 GB) 2. Acessórios Necessários	400	2.540,00	1.016.000,00
2	Fornecimento de Câmera Tipo 2 – Câmera IP Dome com entrada de alarme e microfone embutido	1. Hikvision 2. Teltex	1. DS-2CD3566G2-IS + DS-1280ZJ-DM46 (BLACK) + HS-TF-L2 512G (modelo 512 GB) 2. Acessórios Necessários	90	2.000,00	180.000,00
3	Fornecimento de Câmera Tipo 3 – Câmera IP com lentes fixas para monitoramento visual em 180°	1. Hikvision 2. Teltex	1. DS-2CD2387G2P-LSU/SL (4mm) + DS-1280ZJ-DM55 + DS-1678ZJ (Junction Box) + HS-TF-L2 512G (modelo 512 GB) 2. Acessórios Necessários	90	2.650,00	238.500,00

4	Fornecimento de Câmera Tipo 4 – Câmera multimódulo com panorâmico 180° e PTZ	1. Hikvision 2. Teltex	1. DS-2SF8C425MXG1-ELWY/26(F0) + DS-1603ZJ-Pole-P + DS-1678ZJ + HS-TF-L2(STD)/256G (modelo 256 GB) 2. Acessórios Necessários	6	17.000,00	102.000,00
5	Fornecimento de NVR Tipo 1 – NVR de 128 Canais	1. Hikvision 2. Teltex	1. DS-96128NXI-S16 2. Acessórios Necessários	2	210.000,00	420.000,00
6	Fornecimento de NVR Tipo 2 – NVR de 64 Canais	1. Hikvision 2. Teltex	1. DS-9664NXI-S16R(STD) 2. Acessórios Necessários	6	105.500,00	633.000,00
7	Fornecimento de NVR Tipo 3 – NVR de 16 Canais	1. Hikvision 2. Teltex	1. DS-9616NI-M8 2. Acessórios Necessários	60	6.500,00	390.000,00
8	Fornecimento de HD 6TB 24/7 para CFTV	Western Digital	WD8002PURP	154	2.700,00	415.800,00
9	Instalação de Câmera Tipo 1	Teltex	Teltex	400	520,00	208.000,00
10	Instalação de Câmera Tipo 2	Teltex	Teltex	90	700,00	63.000,00
11	Instalação de Câmera Tipo 3	Teltex	Teltex	90	890,00	80.100,00
12	Instalação de Câmera Tipo 4	Teltex	Teltex	6	1.140,00	6.840,00
13	Instalação NVR Tipo 1 - 128 canais	Teltex	Teltex	2	1.840,00	3.680,00
14	Instalação NVR Tipo 2 - 64 canais	Teltex	Teltex	6	1.740,00	10.440,00
15	Instalação NVR Tipo 3 - 16 canais	Teltex	Teltex	60	964,00	57.840,00
16	Instalação HD 6TB	Teltex	Teltex	154	175,00	26.950,00
17	Fornecimento de Videowall 2x3	1. LG 2. Ellan 3. Hikvision 4. Triunfo 5. Intelbras 6. WJ 7. Teltex	1. LG - 55VM5J-H 2. 1KPW3255 - Ellan + OGCW1006 - Ellan 3. HIKVISION - DS-6908UDI(C)(STD) 4. BKS2-12350P + Triunfo + UV02 - Triunfo 5. CH 2005 6. CALHA 0020 (Calhas com 4, 6, 8, 10 e 12 tomadas com fixação para 19". Tomadas padrão brasileiro (NBR 14136) 2P + T (10A e 20A) 250V. Cabo constituído de 3 via PP 2,5 m de Comprimento (10A e 20A) com plug) 7. Acessórios Necessários	1	44.000,00	44.000,00

18	Fornecimento de Videowall 2x2	1. LG 2. Ellan 3. Hikvision 4. Triunfo 5. Intelbras 6. WJ Moreira 7. Teltex	1. LG - 55VM5J-H 2. 1KPW2255 - Ellan + OGDW2008 - ELLAN 3. HIKVISION - DS-6904UDI@ 4. BKS2-12350P - Triunfo + UV02 - Triunfo 5. CH 2005 6. CALHA 0020 (Calhas com 4, 6, 8, 10 e 12 tomadas com fixação para 19". Tomadas padrão brasileiro (NBR 14136) 2P +T (10A e 20A) 250V. Cabo constituído de 3 via PP 2,5 m de Comprimento (10A e 20A) com plug) 7. Acessórios Necessários	1	34.000,00	34.000,00
19	Instalação de Videowall 2x3	Teltex	Teltex	1	5.000,00	5.000,00
20	Instalação de Videowall 2x2	Teltex	Teltex	1	4.300,00	4.300,00
VALOR TOTAL OFERTADO (R\$)						3.939.450,00

VALOR TOTAL DA PROPOSTA: R\$ 3.939.450,00 (TRÊS MILHÕES, NOVECIENTOS E TRINTA E NOVE MIL, QUATROCENTOS E CINQUENTA REAIS)

DAS EXIGÊNCIAS DA PROPOSTA:

Validade da proposta: 60 (sessenta) dias.

Observação: Estão inclusos nos preços supramencionados todos os custos diretos e indiretos, inclusive de embalagens, transportes ou fretes, e ainda os resultantes da incidência de quaisquer tributos, contribuições ou obrigações decorrentes da legislação trabalhista, fiscal e previdenciária a que estiver sujeito.

Declaro que possuo capacidade operacional e técnica para atendimento a todos os requisitos deste Edital e seus anexos.

Serra/ES, 27 de fevereiro de 2026

FELIPE PINHEIRO
VITORINO:34649238
862

Assinado de forma digital por
FELIPE PINHEIRO
VITORINO:34649238862
Dados: 2026.02.27 13:16:08 -03'00'

TELTEX TECNOLOGIA S.A.

Felipe Pinheiro Vitorino

Procurador

RG 32.949.497-1 SSP/SP

CPF 346.492.388-62

AO
TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAPÁ

DECLARAÇÕES EM GERAL

PREGÃO ELETRÔNICO: 012/2026

PROCESSO: 2025/000002770-00

OBJETO: Registro de preços para aquisição remunerada, sob demanda, de solução de videomonitoramento IP, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

FELIPE PINHEIRO VITORINO, portador da cédula de identidade RG sob o nº 32.949.497-1 SSP/SP e inscrito no CPF/MF sob o nº 346.492.388-62, brasileiro, solteiro, coordenador de licitações, com endereço comercial na Rua França Pinto, 1089, Vila Mariana, São Paulo/SP, CEP 04016-034, como representante devidamente constituído da empresa **TELTEX TECNOLOGIA S.A.**, inscrita no CNPJ nº 73.442.360/0003-89, com Inscrição Estadual nº 083.483.89-6 e Inscrição Municipal nº 4679988, situada na Rodovia Governador Mário Covas, SN, KM 279, Sala 79, Jacuhy, Serra/ES, CEP 29161-230, e-mail licitacoes@teltex.com.br e telefone (11) 3840-6400, doravante denominado Licitante, em atendimento ao disposto no edital do Pregão Eletrônico nº 012/2026, **DECLARA**, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

- a) A proposta anexa foi elaborada de maneira independente pelo Licitante, e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 012/2026, por qualquer meio ou por qualquer pessoa;
- b) A intenção de apresentar a proposta anexa não foi informada a, discutido com ou recebido de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 012/2026, por qualquer meio ou por qualquer pessoa;
- c) Que não tentou, por qualquer meio ou qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 012/2026 quanto a participar ou não da referida licitação;
- d) Que o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado a ou discutido com qualquer outro participante potencial ou de fato do Pregão Eletrônico nº 012/2026 antes da adjudicação do objeto da referida licitação;
- e) Que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer integrante do Tribunal de Justiça do Amazonas antes da abertura oficial das propostas; e
- f) Que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Serra/ES, 27 de fevereiro de 2026

FELIPE PINHEIRO
VITORINO:3464923886
2

Assinado de forma digital por
FELIPE PINHEIRO
VITORINO:34649238862
Dados: 2026.02.27 14:25:04 -03'00'

TELTEX TECNOLOGIA S.A.

Felipe Pinheiro Vitorino

Procurador

RG 32.949.497-1 SSP/SP

CPF 346.492.388-62



PROCURAÇÃO

OUTORGANTE:

TELTEX TECNOLOGIA S/A, inscrita no CNPJ nº 73.442.360/0001-17, com Inscrição Estadual nº 131.271.080.112 e Inscrição Municipal nº 6.952.415-7, localizada na Rua França Pinto, 1089, Andar 1 e 2, Bairro Vila Mariana, São Paulo/SP, CEP 04016-034, e-mail juridico@teltex.com.br e telefone (11) 3840-6400, neste ato representada pelo seu Diretor Presidente, Sr. **VALMOR FERNANDES ROSA FILHO**, portador da cédula de identidade RG nº 60.347.955-49 SSP/RS e inscrito no CPF/MF sob o nº 553.691.380-87, brasileiro, casado, administrador de empresas, com endereço residencial na Avenida Iraí, 407, Ap. 171, Indianópolis, São Paulo/SP, CEP 04082-001.

OUTORGADO:

FELIPE PINHEIRO VITORINO, portador da cédula de identidade RG nº 32.949.497-1 SSP/SP e inscrito no CPF/MF sob o nº 346.492.388-62, brasileiro, solteiro, coordenador de licitações, com endereço comercial na Rua França Pinto, 1089, Bairro Vila Mariana, São Paulo/SP, CEP 04016-034.

PODERES:

Através do presente instrumento particular de mandato, o Outorgante constitui como seu procurador o Outorgado, a quem confere poderes para representá-lo, incluindo todas as filiais, em todo e qualquer processo licitatório, em todas as modalidades de licitação previstas em lei (concorrência, concurso, leilão, pregão presencial ou eletrônico e diálogo competitivo) e em qualquer esfera administrativa (municipal, estadual, distrital ou federal), perante quaisquer órgãos e repartições da administração pública direta ou indireta, empresas públicas, podendo praticar todos os atos necessários à participação e à defesa dos interesses da outorgante em licitações, incluindo, mas não se limitando a: formular, assinar e protocolar propostas de preços, documentos de habilitação e demais documentos pertinentes; participar de sessões públicas; formular ofertas e lances, verbais ou escritos, durante as sessões públicas; impugnar editais e solicitar esclarecimentos; formular e interpor recursos administrativos, apresentar contrarrazões, realizar pedidos de reconsideração e esclarecer diligências.

A presente procuração é outorgada por 12 (doze) meses a contar da data de assinatura.

São Paulo/SP, 12 de novembro de 2025

Assinado digitalmente por:
VALMOR FERNANDES ROSA
FILHO
CPF: 553.691.380-87
Certificado emitido por 11º
TABELIÃO DE NOTAS DA
CAPITAL - SÃO PAULO/SP
Data: 17/11/2025 15:31:36 -03:00

Reconheço a assinatura de VALMOR FERNANDES
ROSA FILHO (553.691.380-87) em 17/11/2025
15:31:45 -03:00, São Paulo/São Paulo

Valmor Fernandes Rosa Filho
Em Testemunho da verdade
SÃO PAULO/SP, 17/11/2025 15:31:45 -03:00
PAULO AUGUSTO RODRIGUES CRUZ-TABELIÃO
11º TABELIÃO DE NOTAS DA CAPITAL - SÃO
PAULO/SP
Código de validação:
ERN76ZUAMUJKWA4XAED
Data: 17/11/2025 15:31:45 -03:00



REPÚBLICA FEDERATIVA DO BRASIL

ESTADO DE SÃO PAULO

SECRETARIA DA SEGURANÇA PÚBLICA

INSTITUTO DE IDENTIFICAÇÃO RICARDO GUMBLETON DAUNT

8000-2

PROIBIDO PLASTIFICAR



Felipe Pinheiro Vitorino

ASSINATURA DO TITULAR

CARTEIRA DE IDENTIDADE

REGISTRO
GERAL

32.949.497-1

DATA DE
EXPEDIÇÃO 10/JUL/2008

NOME

FELIPE PINHEIRO VITORINO

FILIAÇÃO

JOSE CARLOS VITORINO

E

DEOLINDA PINTO PINHEIRO
VITORINO

NATURALIDADE

S. PAULO -SP

DATA DE NASCIMENTO

31/JUL/1987

DOC ORIGEM

SÃO PAULO SP
BELA VISTA

CN:LV.A154/FLS.181V/N.093034

CPF

346492388/62

ASSINATURA DO DIRETOR

LEI Nº 7.116 DE 29/08/83



Network Camera

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

Please scan the following QR code to obtain the "**Safety Instruction**" of the product, and read it carefully. These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.



Figure 1-1 Safety Instruction

Contents

Chapter 1 Overview	1
1.1 Configuration Process	1
1.2 Firmware Update	1
1.3 System Requirement	1
Chapter 2 Device Activation and Accessing	3
2.1 Activate the Device via SADP	3
2.2 Activate the Device via Browser	3
2.3 Login	4
2.3.1 Plug-in Installation	4
2.3.2 Admin Password Recovery	5
2.3.3 Illegal Login Lock	6
Chapter 3 Live View	7
3.1 Live View Parameters	7
3.1.1 Start and Stop Live View	7
3.1.2 Aspect Ratio	7
3.1.3 Live View Stream Type	7
3.1.4 Select the Third-Party Plug-in	7
3.1.5 Light	8
3.1.6 Count Pixel	8
3.1.7 Start Digital Zoom	8
3.1.8 Auxiliary Focus	8
3.1.9 Lens Initialization	9
3.1.10 Lens Parameters Adjustment	9
3.1.11 Conduct 3D Positioning	11
3.2 Set Transmission Parameters	11
Chapter 4 Video and Audio	13

4.1 Video Settings	13
4.1.1 Stream Type	13
4.1.2 Video Type	13
4.1.3 Resolution	13
4.1.4 Bitrate Type and Max. Bitrate	14
4.1.5 Video Quality	14
4.1.6 Frame Rate	14
4.1.7 Video Encoding	14
4.1.8 Smoothing	16
4.2 Audio Settings	16
4.2.1 Audio Encoding	17
4.2.2 Audio Input	17
4.2.3 Audio Output	17
4.2.4 Environmental Noise Filter	17
4.3 Two-way Audio	17
4.4 ROI	18
4.4.1 Set ROI	18
4.5 Set Target Cropping	19
4.6 Display Info. on Stream	19
4.7 Display Settings	19
4.7.1 Scene Mode	20
4.7.2 Image Parameters Switch	25
4.7.3 Video Standard	26
4.7.4 Local Video Output	26
4.8 OSD	26
4.9 Set Privacy Mask	27
4.10 Overlay Picture	27
Chapter 5 Video Recording and Picture Capture	28

5.1 Storage Settings	28
5.1.1 Memory Card	28
5.1.2 Set FTP	30
5.1.3 Set NAS	31
5.1.4 eMMC Protection	32
5.1.5 Set Cloud Storage	32
5.2 Video Recording	33
5.2.1 Record Automatically	33
5.2.2 Record Manually	35
5.2.3 Playback and Download Video	35
5.3 Capture Configuration	36
5.3.1 Capture Automatically	36
5.3.2 Capture Manually	36
5.3.3 View and Download Picture	37
Chapter 6 Event and Alarm	38
6.1 Set Motion Detection	38
6.1.1 Expert Mode	38
6.1.2 Normal Mode	39
6.2 Set Video Tampering Alarm	40
6.3 Set Alarm Input	41
6.4 Set Exception Alarm	42
6.5 Set Video Quality Diagnosis	42
6.6 Set Audio Exception Detection	43
6.7 Set Defocus Detection	44
6.8 Set Scene Change Detection	44
Chapter 7 Arming Schedule and Alarm Linkage	45
7.1 Set Arming Schedule	45
7.2 Linkage Method Settings	45

7.2.1 Trigger Alarm Output	46
7.2.2 FTP/NAS/Memory Card Uploading	47
7.2.3 Send Email	47
7.2.4 Notify Surveillance Center	48
7.2.5 Trigger Recording	48
7.2.6 Flashing Light	48
7.2.7 Audible Warning	49
7.2.8 Alarm Server	50
Chapter 8 Network Settings	51
8.1 TCP/IP	51
8.2 Access to Device via Domain Name	52
8.3 Access to Device via PPPoE Dial Up Connection	53
8.4 SNMP	53
8.5 Set IEEE 802.1X	54
8.6 Set QoS	54
8.7 HTTP(S)	55
8.8 Multicast	56
8.8.1 Multicast Discovery	56
8.9 RTSP	56
8.10 Set SRTP	57
8.11 Bonjour	57
8.12 WebSocket(s)	58
8.13 Port Mapping	58
8.13.1 Set Auto Port Mapping	58
8.13.2 Set Manual Port Mapping	58
8.13.3 Set Port Mapping on Router	59
8.14 RTCP	60
8.15 Wireless Dial	60

8.15.1 Set Wireless Dial	60
8.15.2 Wireless Expert Settings	61
8.16 WLAN AP (Access Point)	63
8.16.1 Set WLAN AP	63
8.16.2 Access to Device via AP	64
8.17 Traffic Shaping	65
8.18 Data Monitoring	65
8.19 Wi-Fi	65
8.19.1 Connect Device to Wi-Fi	66
8.20 Set ISUP	66
8.21 Access Camera via Hik-Connect	67
8.21.1 Enable Hik-Connect Service on Camera	67
8.21.2 Set Up Hik-Connect	68
8.21.3 Add Camera to Hik-Connect	69
8.22 Set Open Network Video Interface	70
8.23 Set SDK Service	70
Chapter 9 System and Security	71
9.1 System Settings	71
9.1.1 View Device Information	71
9.1.2 Time and Date	71
9.1.3 Set RS-232	72
9.1.4 Set RS-485	73
9.1.5 Set Live View Connection	73
9.1.6 Location Settings	73
9.1.7 External Device	74
9.1.8 View Open Source Software License	74
9.1.9 Wiegand	74
9.2 User and Account	74

9.2.1 Set User Account and Permission	74
9.2.2 Simultaneous Login	75
9.2.3 Online Users	75
9.3 Maintenance	75
9.3.1 Restart	75
9.3.2 Upgrade	75
9.3.3 Restore and Default	76
9.3.4 Import and Export Configuration File	76
9.3.5 Search and Manage Log	77
9.3.6 Search Security Audit Logs	77
9.3.7 SSH	77
9.3.8 Export Diagnose Information	78
9.3.9 Diagnosis	78
9.4 Security	80
9.4.1 Set IP Address Filter	80
9.4.2 Set MAC Address Filter	80
9.4.3 Control Timeout Settings	81
9.4.4 Certificate Management	81
9.4.5 TLS	84
Chapter 10 VCA Resource	85
10.1 Set Open Platform	85
10.2 General Settings	86
10.2.1 Set Camera Info	86
10.2.2 Metadata	86
10.2.3 AcuSearch	87
10.3 Smart Event	87
10.3.1 Set Intrusion Detection	88
10.3.2 Set Line Crossing Detection	89

10.3.3 Set Region Entrance Detection	91
10.3.4 Set Region Exiting Detection	92
10.3.5 Set Unattended Baggage Detection	94
10.3.6 Set Object Removal Detection	95
10.3.7 Set Loitering Detection	97
10.3.8 Set People Gathering Detection	98
10.3.9 Set Fast Moving Detection	99
10.3.10 Set Parking Detection	101
10.4 Face Capture	102
10.4.1 Set Face Capture	102
10.4.2 Overlay and Capture	103
10.4.3 Face Capture Algorithms Parameters	104
10.4.4 Set Shield Region	106
10.5 People Management	107
10.5.1 Regional People Counting	107
10.5.2 Overlay and Capture	113
10.5.3 Advanced Settings	113
10.6 People Counting	114
10.6.1 Set People Counting Rule	114
10.7 Road Traffic	116
10.7.1 Set Vehicle Detection	116
10.7.2 Set Mixed-Traffic Detection Rule	119
10.7.3 Overlay and Capture	121
10.7.4 Import or Export Blocklist & Allowlist	123
10.7.5 Advanced Parameters Configuration	124
10.8 AI Open Platform	124
10.8.1 Set AI Open Platform	124
10.8.2 Set Rules	125

Chapter 11 EPTZ	129
11.1 Patrol	129
11.2 Auto-Tracking	129
Appendix A. FAQ	131

Chapter 1 Overview

1.1 Configuration Process

This section briefly explains the software configuration process of the network camera. Please set up the device according to the actual situation.

General Configuration Process

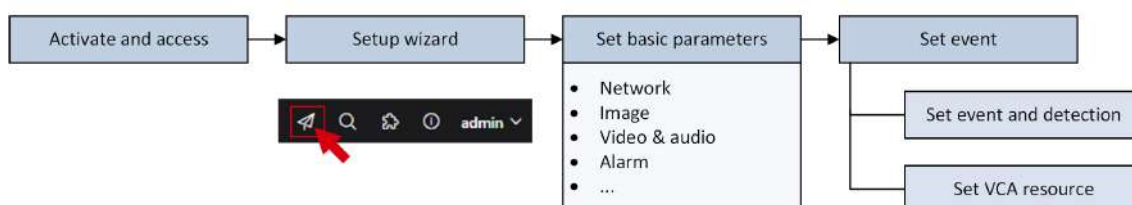


Figure 1-1 General Configuration Process

- **Activate and access device via web browser.** You should set a login password (for **admin** user) to activate the device when access the device via network. Open the web browser and enter the IP address. The default IP address of the device is 192.168.1.64.
- Follow the **Wizard** or click  on the web page to quickly set the device parameters.
- Set the basic parameters, including network, image, video and audio, alarm, etc.
- Set event and detection rules. You can set basic **event and detection** rules or **allocate VCA resources** for deep learning function.

1.2 Firmware Update

For better user experience, we recommend you to update your device to the latest firmware. Please get the latest firmware package from the official website or the local technical expert. For more information, please visit the official website: <https://www.hikvision.com/en/support/download/firmware/>.

For the upgrading settings, refer to **Upgrade**.

1.3 System Requirement

Your computer should meet the requirements for proper visiting and operating the product.

Operating System	Microsoft Windows XP SP1 and above version
CPU	2.0 GHz or higher
RAM	1G or higher
Display	1024×768 resolution or higher
Web Browser	For the details, see <u>Plug-in Installation</u>

Chapter 2 Device Activation and Accessing

To protect the security and privacy of the user account and data, you should set a login password to activate the device when access the device via network.



Note

Refer to the user manual of the software client for the detailed information about the client software activation.

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access www.hikvision.com to get SADP software to install.

Steps

1. Connect the device to network using the network cable.
2. Run SADP software to search the online devices.
3. Check **Device Status** from the device list, and select **Inactive** device.
4. Create and input the new password in the password field, and confirm the password.



Caution

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.

5. Click **OK**.

Device Status changes into **Active**.

6. **Optional:** Change the network parameters of the device in **Modify Network Parameters**.

2.2 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

1. Connect the device to the PC using the network cables.
2. Change the IP address of the PC and device to the same segment.



Note

The default IP address of the device is 192.168.1.64. You can set the IP address of the PC from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.

3. Input **192.168.1.64** in the browser.
4. Set device activation password.



Caution

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: 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.

5. Click **OK**.
6. Input the activation password to log in to the device.
7. **Optional:** Go to **Configuration** → **Network** → **Network Settings** → **TCP/IP** to change the IP address of the device to the same segment of your network.

2.3 Login

Log in to the device via Web browser.

2.3.1 Plug-in Installation

Certain operating systems and web browsers may restrict the display and operation of the device function. You should install a plug-in or complete certain settings to ensure normal display and operation. For detailed restricted function, refer to the actual device.

Operating System	Web Browser	Operation
Windows	• Internet Explorer 10+ • Google Chrome 57 and earlier version • Mozilla Firefox 52 and earlier version	Follow pop-up prompts to complete plug-in installation.
	• Google Chrome 57+ • Mozilla Firefox 52+ • Edge 89+	Click  to download and install plug-in.
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+	Plug-in installation is not required. Go to Configuration → Network → Network Service → WebSocket(s) to enable WebSocket or WebSockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.



Note

- The device only supports Windows and Mac OS system, and does not support Linux system.
 - To improve the user experience on certain devices, it's recommended to use a more advanced web browser for access. Please refer to the actual device or product specification.
 - Certain device models do not support Internet Explorer web browser.
-

2.3.2 Admin Password Recovery

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page after completing the account security settings.

You can reset the password by setting the security question or email.



Note

When you need to reset the password, make sure that the device and the PC are on the same network segment.

Security Question

You can set the account security during the activation. Or you can go to **Configuration → System → User Management**, click **Account Security Settings**, select the security question and input your answer.

You can click **Forget Password** and answer the security question to reset the admin password when access the device via browser.

Email

You can set the account security during the activation. Or you can go to **Configuration → System → User Management**, click **Account Security Settings**, input your email address to receive the verification code during the recovering operation process.

2.3.3 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.

Go to **Maintenance and Security → Security → Login Management**, and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

When your login attempts with the wrong password reach the set times, the device is locked.

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Live View

It introduces the live view parameters, function icons and transmission parameters settings.

3.1 Live View Parameters

The supported functions vary depending on the model.

3.1.1 Start and Stop Live View

Click **Live View**. Click  to start live view. Click  to stop live view.

3.1.2 Aspect Ratio

Aspect Ratio is the display ratio of the width to height of the image.

-  refers to 4:3 window size.
-  refers to 16:9 window size.
-  refers to original window size.
-  refers to self-adaptive window size.
-  refers to original ratio window size.

3.1.3 Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to **Stream Type**.

3.1.4 Select the Third-Party Plug-in

When the live view cannot display via certain browsers, you can change the plug-in for live view according to the browser.

Steps

1. Click **Live View**.
2. Click  to select the plug-in.
 - When you access the device via Internet Explorer, you can select Webcomponents or QuickTime.
 - When you access the device via the other browsers, you can select Webcomponents, QuickTime or MJPEG.

3.1.5 Light

Click  to turn on or turn off the illuminator.



Caution

For the device with laser:

- DO NOT stare at operating light source. May be harmful to the eyes.
 - If appropriate shielding or eye protection is not available, turn on the light only at a safe distance or in the area that is not directly exposed to the light.
 - When assembling, installing or maintaining the device, DO NOT turn on the light, or wear eye protection.
-

3.1.6 Count Pixel

It helps to get the height and width pixel of the selected region in the live view image.

Steps

1. Click  to enable the function.
2. Drag the mouse on the image to select a desired rectangle area.
The width pixel and height pixel are displayed on the bottom of the live view image.

3.1.7 Start Digital Zoom

It helps to see a detailed information of any region in the image.

Steps

1. Click  to enable the digital zoom.
2. In live view image, drag the mouse to select the desired region.
3. Click in the live view image to back to the original image.

3.1.8 Auxiliary Focus

It is used for motorized device. It can improve the image if the device cannot focus clearly.

For the device that supports ABF, adjust the lens angle, then focus and click ABF button on the device. The device can focus clearly.

Click  to focus automatically.

Note

- If the device cannot focus with auxiliary focus, you can use **Lens Initialization** , then use auxiliary focus again to make the image clear.
 - If auxiliary focus cannot help the device focus clearly, you can use manual focus.
-

3.1.9 Lens Initialization

Lens initialization is used on the device equipped with motorized lens. The function can reset lens when long time zoom or focus results in blurred image. This function varies according to different models.

Click  to operate lens initialization.

3.1.10 Lens Parameters Adjustment

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the device. In live view interface, you can click the direction control buttons to control the pan/tilt movement, and click the zoom/focus/iris buttons to realize lens control.

Note

- Supported PTZ functions may vary according to different camera models.
 - For the devices which support lens movements only, the direction buttons are invalid.
-

Direction Control



Click and hold the direction button to pan/tilt the device.

Zoom

- Click  , and the lens zooms in.
- Click  , and the lens zooms out.

Focus

- Click  , then the lens focuses near and the nearby object gets clear.
- Click  , then the lens focuses far and the distant object gets clear.

Iris

- When the image is too dark, click  to enlarge the iris.
- When the image is too bright, click  to stop down the iris.

PTZ Speed

- Slide  to adjust the speed of the pan/tilt movement.

PTZ Lock

PTZ lock means to disable the zoom, focus and PTZ rotation functions of the corresponding channel, so that to reduce the target missing caused by PTZ adjustment.



Note

The function is only supported by certain device models.

Click  to lock the PTZ operation, or click  to unlock it.

PTRZ Adjustment

PTRZ is an abbreviation for pan, tilt, rotate and zoom. It means the movement options of the device. In the interface, you can use the control buttons to adjust the movement of the device, such as device panning, tilting, rotating, and zooming.



Note

The function is only supported by certain device models.

Go to **Configuration** → **PTZ** → **PTRZ** .

Control Panel

	Click and hold the directional button to pan/tilt the device.
•  • 	Click and hold the button to adjust rotating position.

Auto Recovery

Click  , the device will correct the rotating position automatically to make the live view image positive. Make sure the **Self-Test Status** is **Initialized**.



Note

- Go to **Configuration → PTZ → PTZ** to view the **Self-Test Status**.
- If you want to initialize PTZ and enable PTZ self-check manually, go to **Configuration → PTZ → PTZ** and click **Self-Test**, then the PTZ is initialized.

Refer to **Lens Parameters Adjustment** for more detailed settings of lens adjustment.

3.1.11 Conduct 3D Positioning

3D positioning is to relocate the selected area to the image center.

Steps

1. Click  to enable the function.
2. Select a target area in live image.
 - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
 - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
 - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
3. Click the button again to turn off the function.

3.2 Set Transmission Parameters

The live view image may be displayed abnormally according to the network conditions. In different network environments, you can adjust the transmission parameters to solve the problem.

Steps

1. Go to **Configuration → Local → Live View Parameters**.
2. Set the transmission parameters as required.

Protocol

TCP

TCP ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. It is suitable for the stable network environment.

UDP

UDP is suitable for the unstable network environment that does not demand high video fluency.

MULTICAST

MULTICAST is suitable for the situation that there are multiple clients. You should set the multicast address for them before selection.



Note

For detailed information about multicast, refer to ***Multicast***.

HTTP

HTTP is suitable for the situation that the third-party needs to get the stream from the device.

Playing Performance

Shortest Delay

The device takes the real-time video image as the priority over the video fluency.

Balanced

The device ensures both the real-time video image and the fluency.

Fluent

The device takes the video fluency as the priority over real-time. In poor network environment, the device cannot ensure video fluency even the fluency is enabled.

Custom

You can set the frame rate manually. In poor network environment, you can reduce the frame rate to get a fluent live view. But the rule information may not display.

3. Click **Save**.

Chapter 4 Video and Audio

This part introduces the configuration of video and audio related parameters.

4.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.

Go to setting page: **Configuration → Video/Audio → Video** .

4.1.1 Stream Type

For device supports more than one stream, you can specify parameters for each stream type.

Main Stream

The stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission.

Sub Stream

The stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

Other Streams

Streams other than the main stream and sub stream may also be offered for customized usage.

4.1.2 Video Type

Select the content (video and audio) that should be contained in the stream.

Video Stream

Only video content is contained in the stream.

Video&Audio

Video content and audio content are contained in the composite stream.

4.1.3 Resolution

Select video resolution according to actual needs. Higher resolution requires higher bandwidth and storage.

4.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but mosaic may occur on the image.

Variable Bitrate

It means that the device automatically adjust the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

4.1.5 Video Quality

When **Bitrate Type** is set as Variable, video quality is configurable. Select a video quality according to actual needs. Note that higher video quality requires higher bandwidth.

4.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).

A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

4.1.7 Video Encoding

It stands for the compression standard the device adopts for video encoding.



Note

Available compression standards vary according to device models.

H.264

H.264, also known as MPEG-4 Part 10, Advanced Video Coding, is a compression standard. Without compressing image quality, it increases compression ratio and reduces the size of video file than MJPEG or MPEG-4 Part 2.

H.264+

H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.264+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



Note

When H.264+ is enabled, **I Frame Interval** is not configurable.

H.265

H.265, also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2, is a compression standard. In comparison to H.264, it offers better video compression at the same resolution, frame rate and image quality.

H.265+

H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.265+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



Note

When H.265+ is enabled, **I Frame Interval** is not configurable.

I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.

In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

SVC

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.

The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.

SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able to decode high quality video stream.

MPEG4

MPEG4, referring to MPEG-4 Part 2, is a video compression format developed by Moving Picture Experts Group (MPEG).

MJPEG

Motion JPEG (M-JPEG or MJPEG) is a video compression format in which intraframe coding technology is used. Images in a MJPEG format are compressed as individual JPEG images.

Profile

This function means that under the same bitrate, the more complex the profile is, the higher the quality of the image is, and the requirement for network bandwidth is also higher.

4.1.8 Smoothing

It refers to the smoothness of the stream. The higher the value of the smoothing is, the better the fluency of the stream will be, though, the video quality may not be so satisfactory. The lower the value of the smoothing is, the higher the quality of the stream will be, though it may appear not fluent.

4.2 Audio Settings

It is a function to set audio parameters such as audio encoding, environment noise filtering.

Go to the audio settings page: **Configuration → Video/Audio → Audio** .



Only certain camera models support the function.

4.2.1 Audio Encoding

Select the audio encoding compression of the audio.

4.2.2 Audio Input



- Connect the audio input device as required.
 - The audio input display varies with the device models.
-

LineIn	Set Audio Input to LineIn when the device connects to the audio input device with the high output power, such as MP3, synthesizer or active pickup.
MicIn	Set Audio Input to MicIn when the device connects to the audio input device with the low output power, such as microphone or passive pickup.

4.2.3 Audio Output



Connect the audio output device as required.

It is a switch of the device audio output. When it is disabled, all the device audio cannot output. The audio output display varies with the device modes.

4.2.4 Environmental Noise Filter

Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

4.3 Two-way Audio

It is used to realize the two-way audio function between the monitoring center and the target in the monitoring screen.

Before You Start

- Make sure the audio input device (pick-up or microphone) and audio output device (speaker) connected to the device is working properly. Refer to specifications of audio input and output devices for device connection.
- If the device has built-in microphone and speaker, two-way audio function can be enabled directly.

Steps

1. Click **Live View**.
2. Click  on the toolbar to enable two-way audio function of the camera.
3. Click , disable the two-way audio function.

4.4 ROI

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression. The technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

4.4.1 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video coding type. ROI is supported when the video coding type is H.264 or H.265.

Steps

1. Go to **Configuration → Video/Audio → ROI**.
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** and click  to draw ROI region on the live view.



Note

Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.

5. Input the **Area Name** and **ROI Level**.
6. Click **Save**.



Note

The higher the ROI level is, the clearer the image of the detected region is.

7. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

4.5 Set Target Cropping

You can crop the image, transmit and save only the images of the target area to save transmission bandwidth and storage.

Steps

1. Go to **Configuration → Video/Audio → Target Cropping** .
2. Check **Enable** and set **Third Stream** as the **Stream Type**.



Note

After enabling target cropping, the third stream resolution cannot be configured.

3. Select a **Cropping Resolution**.

A red frame appears in the live view.

4. Drag the frame to the target area.
5. Click **Save**.



Note

- Only certain models support target cropping and the function varies according to different camera models.
 - Some functions may be disabled after enabling target cropping.
-

4.6 Display Info. on Stream

The information of the objects (e.g. human, vehicle, etc.) is marked in the video stream. You can set rules on the connected rear-end device or client software to detect the events including line crossing, intrusion, etc.

Before You Start

This function is supported in smart events. Go to **VCA** , select **Smart Event** and click **Next** to enable **Smart Event**.

Steps

1. Go to **Configuration → Video/Audio → Display Info. on Stream** .
2. Check **Enable Dual-VCA**.
3. Click **Save**.

4.7 Display Settings

It offers the parameter settings to adjust image features.

Go to **Configuration → Image → Display Settings** .

Click **Default** to restore settings.

4.7.1 Scene Mode

There are several sets of image parameters predefined for different installation environments. Select a scene according to the actual installation environment to speed up the display settings.

Image Adjustment

By adjusting the **Brightness**, **Saturation**, **Contrast** and **Sharpness**, the image can be best displayed.

Exposure Settings

Exposure is controlled by the combination of iris, shutter, and photo sensibility. You can adjust image effect by setting exposure parameters.

In manual mode, you need to set **Exposure Time**, **Gain** and **Slow Shutter**.

Focus

It offers options to adjust the focus mode.

Focus Mode

Auto

The device focuses automatically as the scene changes. If you cannot get a well-focused image under auto mode, reduce light sources in the image and avoid flashing lights.

Semi-auto

The device focuses once after the PTZ and lens zooming. If the image is clear, the focus does not change when the scene changes.

Manual

You can adjust the focus manually on the live view page.

Day/Night Switch

Day/Night Switch function can provide color images and black/white images in day and night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The image is black/white or colorful and the supplement light will be enabled to ensure clear live view image at night.



Note

Only certain device models support the supplement light and colorful image.

Auto

The camera switches between the day mode and the night mode according to the light condition of environment.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.

Triggered by alarm input

You can set **Triggering Status** as **Day** or **Night**. For example, if the **Triggering Status** is **Night**, the mode turns into **Night** when the device receives alarm input signal.

Triggered by video

The camera switches between the day mode and the night mode according to the light condition of environment. This mode is applicable when the device supports road traffic and vehicle detection.



Note

- Day/Night Switch function varies according to models.
 - You can turn on the smart supplement light for better image effect. For supplement light settings, refer to ***Supplement Light Settings***.
-

Supplement Light Settings

You can set supplement light and refer to the actual device for relevant parameters.

Smart Supplement Light

Smart supplement light avoids over exposure when the supplement light is on.

Supplement Light Mode

When the device supports supplement light, you can select supplement light mode.

IR Supplement Light

IR light is enabled.

White Light

White light is enabled.

Mixed Light

Both IR light and white light are enabled.

Smart

When you select this mode after enabling certain smart events or motion detection, in the night state, the default supplement light mode is IR supplement light mode. When the alarm is triggered, the white light is enabled and the device captures the target. After the alarm ends, the supplement light mode will switch to IR supplement light mode.

Only device models with IR and white light or hybrid supplement light with IR and white light support this function.

Off

Supplement light is disabled.



Note

The supplement light mode may vary according to different device models.

Brightness Adjustment Mode

Auto

The brightness adjusts according to the actual environment automatically.

Manual

You can drag the slider or set value to adjust the brightness.

BLC

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set as **Custom**, you can draw a red rectangle on the live view image as the BLC area.

WDR

The WDR (Wide Dynamic Range) function helps the camera provide clear images in environment with strong illumination differences.

When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.



Note

When WDR is enabled, some other functions may be not supported. Refer to the actual interface for details.



Figure 4-1 WDR

HLC

When the bright area of the image is over-exposed and the dark area is under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright area and brighten the dark area, so as to achieve the light balance of the overall picture.

White Balance

White balance is the white rendition function of the camera. It is used to adjust the color temperature according to the environment.



Figure 4-2 White Balance

DNR

Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

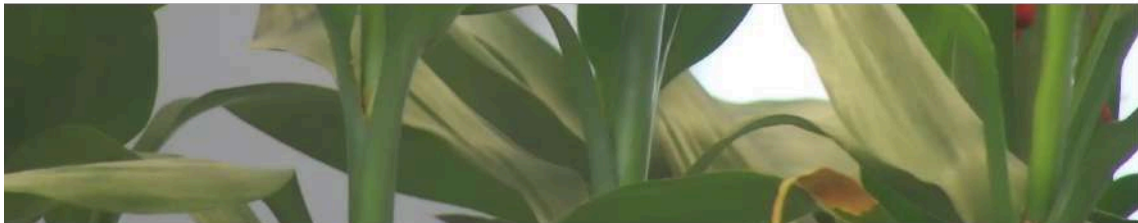
Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

Expert

Set the DNR level for both space DNR and time DNR to control the noise reduction degree. The higher level means stronger reduction degree.



DNR Off



DNR On

Figure 4-3 DNR

Defog

You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.



Defog Off



Defog On

Figure 4-4 Defog

EIS

Increase the stability of video image by using jitter compensation technology.

Gray Scale

You can choose the range of the **Gray Scale** as [0-255] or [16-235].

Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.



Note

The video recording will be shortly interrupted when the function is enabled.

Rotate

When this function is enabled, the live view will rotate 90° counterclockwise. For example, 1280 × 720 is rotated to 720 × 1280.

Enabling this function can change the effective range of monitoring in the vertical direction.



Note

This function is supported under certain settings.

Lens Distortion Correction

For device equipped with motorized lens, image may appear distorted to some extent. Enable this function to correct the distortion.



Note

- This function is only supported by certain device equipped with motorized lens.
 - The edge of image will be lost if this function is enabled.
-

4.7.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

Go to image parameters switch setting page: **Configuration** → **Image** → **Display Settings** → **Image Parameters Switch** , and set parameters as needed.

Set Scheduled-switch

Switch the image to the linked scene mode automatically in certain time periods.

Steps

1. Check **Scheduled-switch**.
2. Select and configure the corresponding time period and linked scene mode.



Note

For Linked Scene configuration, refer to **Scene Mode** .

3. Click **Save**.

4.7.3 Video Standard

Video standard is an ability of a video card or video display device that defines the amount of colors that are shown and the resolution. The two most common video standard used are NTSC and PAL. In NTSC, 30 frames are transmitted each second. Each frame is made up of 525 individual scan lines. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines. Select video signal standard according to the video system in your country/region.

4.7.4 Local Video Output

If the device is equipped with video output interfaces, such as BNC, CVBS, HDMI, and SDI, you can preview the live image directly by connecting the device to a monitor screen.

Select the output mode as ON/OFF to control the output.

4.8 OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, color, and text overlay displayed on video stream.

Go to OSD setting page: **Configuration → Image → OSD Settings** . Set the corresponding parameters, and click **Save** to take effect.

Character Set

Select character set for displayed information. If Korean is required to be displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

Display

Set camera name, date, week, and their related display formats.

Format Settings

Set OSD parameters, such as **Display Mode**, **OSD Size**, **Font Color**, and **Alignment**.

Text Overlay

Set customized overlay text on image.

4.9 Set Privacy Mask

The function blocks certain areas in the live view to protect privacy. No matter how the device moves, the blocked scene will never be seen.

Steps

1. Go to **Configuration → Image → Privacy Mask**.
2. Check **Enable**.
3. Click . Drag the mouse in the live view to draw a closed area.
 - Drag the corners of the area** Adjust the size of the area.
 - Drag the area** Adjust the position of the area.
 - Click**  Clear all the areas you set.
4. Click **Add** to add a privacy mask and set **Region Name** and **Mask Type**.
5. Click **Save**.

4.10 Overlay Picture

Overlay a customized picture on live view.

Before You Start

The picture to overlay has to be in BMP format with 24-bit, and the maximum picture size is 128 × 128 pixel.

Steps

1. Go to **Configuration → Image → Picture Overlay**.
2. Check **Enable**.
3. Click **Upload** to select a picture and open it.

The picture with a red rectangle will appear in live view after successfully uploading.
4. Drag the red rectangle to adjust the picture position.
5. Click **Save**.

Chapter 5 Video Recording and Picture Capture

This part introduces the operations of capturing video clips and snapshots, playback, and downloading captured files.

5.1 Storage Settings

This part introduces the configuration of several common storage paths.

5.1.1 Memory Card

You can view the capacity, free space, status, type, and property of the memory card. Encryption of memory card is supported to ensure data security.

Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.

Steps

1. Go to **Configuration** → **Storage** → **Storage Management** → **HDD Management** .
2. Select the memory card.



Note

If an **Unlock** button appears, you need to unlock the memory card first. See [**Detect Memory Card Status**](#) for details.

-
3. Click **Format** to initialize the memory card.

When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.

4. **Optional:** Encrypt the memory card.

- 1) Click **Encrypted Format**.
- 2) Set the encryption password.
- 3) Click **OK**.

When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.



Note

Keep your encryption password properly. Encryption password cannot be found if forgotten.

-
5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

- Insert an encrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.
- You need to know the correct encryption password of the memory card.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management**.
2. Select the memory card.



Note

If an **Unlock** button appears, you need to unlock the memory card first. See [***Detect Memory Card Status***](#) for details.

3. Verify the encryption password.
 - 1) Click **Parity**.
 - 2) Enter the encryption password.
 - 3) Click **OK**.

When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.



Note

If the encryption password is forgotten and you still want to use this memory card, see [***Set New or Unencrypted Memory Card***](#) to format and set the memory card. All existing contents will be removed.

4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

The device detects the status of Hikvision memory card. You receive notifications when your memory card is detected abnormal.

Before You Start

The configuration page only appears when a Hikvision memory card is installed to the device.

Steps

1. Go to **Configuration → Storage → Storage Management → Memory Card Detection**.
2. Click **Status Detection** to check the **Remaining Lifespan** and **Health Status** of your memory card.

Remaining Lifespan

It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.

Health Status

It shows the condition of your memory card. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.



Note

It is recommended that you change the memory card when the health status is not "good".

-
3. Click **R/W Lock** to set the permission of reading and writing to the memory card.
 - Add a Lock
 - a. Select the **Lock Switch** as ON.
 - b. Enter the password.
 - c. Click **Save**
 - Unlock
 - If you use the memory card on the device that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of users.
 - If you use the memory card (with a lock) on a different device, you can go to **HDD Management** to unlock the memory card manually. Select the memory card, and click **Unlock**. Enter the correct password to unlock it.
 - Remove the Lock
 - a. Select the **Lock Switch** as OFF.
 - b. Enter the password in **Password Settings**.
 - c. Click **Save**.



Note

- Only admin user can set the **R/W Lock**.
- The memory card can only be read and written when it is unlocked.
- If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.

-
4. Set **Arming Schedule** and **Linkage Method**. See [Set Arming Schedule](#) and [Linkage Method Settings](#) for details.
 5. Click **Save**.

5.1.2 Set FTP

You can configure the FTP server to save images which are captured by events or a timed snapshot task.

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration → Event → Alarm Setting → FTP**.
2. Configure FTP settings.

Server Address and Port

The FTP server address and corresponding port.

User Name and Password

The FTP user should have the permission to upload pictures.

If the FTP server supports picture uploading by anonymous users, you can check **Anonymous** to hide your device information during uploading.

Directory Structure

The saving path of snapshots in the FTP server.

3. **Optional:** Check **Upload Picture** to enable uploading snapshots to the FTP server.

Picture Filing Interval

For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

Picture Name

Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.

4. **Optional:** Check **Enable Automatic Network Replenishment**.



Note

Upload to FTP/Memory Card/NAS in Linkage Method and **Enable Automatic Network Replenishment** should be both enabled simultaneously.

5. Click **Test** to verify the FTP server.
6. Click **Save**.

5.1.3 Set NAS

Take network server as network disk to store the record files, captured images, etc.

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration → Storage → Storage Management → Net HDD**.
2. Click **Add**.
3. Set **Mounting Type**.

Mounting Type

Select file system protocol according to the operation system.

Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.

4. Set the **Server Address** and **File Path** for the disk.

Server Address

The IP address of the network disk.

File Path

The saving path of network disk files.

5. Click **Test** to check whether the network disk is available.
6. Click **OK** to finish the steps to add a Net HDD.
7. **Optional:** Configure the Net HDD.

Edit Click  to edit the parameter setting.

Delete Delete the Net HDD.

- Click .
- Select the Net HDD, click **Delete**.

8. Click **Save**.

5.1.4 eMMC Protection

It is to automatically stop the use of eMMC as a storage media when its health status is poor.



Note

The eMMC protection is only supported by certain device models with an eMMC hardware.

Go to **Configuration → System → System Settings → System Service** for the settings.

eMMC, short for embedded multimedia card, is an embedded non-volatile memory system. It is able to store the captured images or videos of the device.

The device monitors the eMMC health status and turns off the eMMC when its status is poor. Otherwise, using a worn-out eMMC may lead to device boot failure.

5.1.5 Set Cloud Storage

It helps to upload the captured pictures and data to the cloud. The platform requests picture directly from the cloud for picture and analysis. The function is only supported by certain models.

Steps



Caution

If the cloud storage is enabled, the pictures are stored in the cloud video manager firstly.

1. Go to **Configuration → Storage → Storage Management → Cloud Storage** .
2. Check **Enable**.
3. Set basic parameters.

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.
Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

4. Click **Test** to test the configured settings.
5. Click **Save**.

5.2 Video Recording

This part introduces the operations of manual and scheduled recording, playback, and downloading recorded files.

5.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

Select **Trigger Recording** in event settings for each record type except **Continuous**. See [**Event and Alarm**](#) for details.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .
2. Check **Enable**.
3. Select a record type.



Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

When motion detection is enabled and trigger recording is selected as linkage method, object movement is recorded.

Alarm

When alarm input is enabled and trigger recording is selected as linkage method, the video is recorded after receiving alarm signal from external alarm input device.

Motion | Alarm

Video is recorded when motion is detected or alarm signal is received from the external alarm input device.

Motion & Alarm

Video is recorded only when motion is detected and alarm signal is received from the external alarm input device.

Event

The video is recorded when configured event is detected.

4. Set schedule for the selected record type. Refer to **Set Arming Schedule** for the setting operation.
5. Set the advanced recording parameters.

Overwrite

Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos.

Pre-record

The time period you set to record before the scheduled time.

Post-record

The time period you set to stop recording after the scheduled time.

Stream Type

Select the stream type for recording.



Note

When you select the stream type with higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

Recording Expiration

The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they can not be recovered.

6. Click **Save**.

5.2.2 Record Manually

Steps

1. Go to **Configuration → Local**.
2. Set the **Video Size** and **Video Saving Path** for recorded video files.
3. Click **Save**.
4. Click  in the live view interface to start recording. Click  to stop recording.

What to do next

View the recorded video files.

Go to **Configuration → Local** and click **Open** behind **Video Saving Path** to open the saving path and view the files.

5.2.3 Playback and Download Video

You can search, playback, clip and download the videos stored in the local storage or network storage.

Steps

1. Go to **Playback → Video**.
2. Set search condition and click **Search**.
The matched video files showed on the timing bar.
3. Click  to play the video files.
 - Click  to play video files in full screen. Press **ESC** to exit full screen.
 - Click  to stop video playback for all channels.
4. **Optional:** Click  to clip video files. Click  again to stop clipping video files



Note

Go to **Configuration → Local → Clip Saving Path**, view and change the saving path of clipped video files.

-
5. **Optional:** Click  on the playback interface to download files.



Note

Go to **Configuration → Local → Downloaded File Saving Path**, view and change the saving path of downloaded video files.

5.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

5.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to **Event and Alarm** for event settings.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Picture Capture**.
2. Set capture schedule. Refer to **Set Arming Schedule** for configuring schedule time.

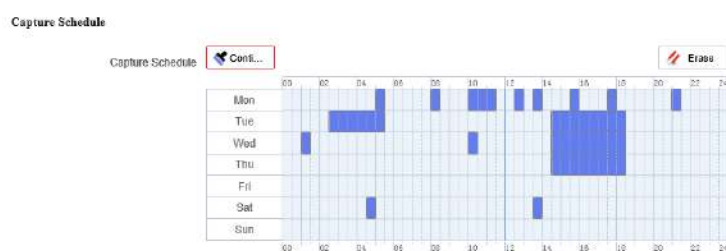


Figure 5-1 Set Capture Schedule

3. Set the capture type.

Scheduled

Capture a picture at the configured time interval.

Event-Triggered

Capture a picture when an event is triggered.

4. Set the **Format, Resolution, Quality, Interval, and Capture Number**.



Note

The resolution of the captured picture is the same as the resolution of the captured picture stream. You can select **Stream Type** in **Advanced**.

5. Click **Save**.

5.3.2 Capture Manually

Steps

1. Go to **Configuration → Local**.

2. Set the **Image Format** and saving path to for snapshots.

JPEG

The picture size of this format is comparatively small, which is better for network transmission.

BMP

The picture is compressed with good quality.

3. Click **Save**.
4. Click  near the live view or play back window to capture a picture manually.

5.3.3 View and Download Picture

You can search, view and download the pictures stored in the local storage or network storage.

Steps

1. Go to **Playback → Picture**.
2. Set search condition and click **Search**.
The matched pictures showed in the file list.
3. Download the pictures.
 - Select the pictures then click **Download** to download them.
 - Click **Download This Page** to download the pictures of this page.
 - Click **Download All** to download all the pictures.



Note

Go to **Configuration → Local → Playback Capture Saving Path**, view and change the saving path of captured pictures when playback.

Chapter 6 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm. Certain events may not be supported by certain device models.

6.1 Set Motion Detection

It helps to detect the moving objects in the detection region and trigger the linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Motion Detection**.
2. Check **Enable**.
3. **Optional**: Highlight to display the moving object in the image in green.
 - 1) Check **Enable Dynamic Analysis for Motion**.
 - 2) Go to **Configuration → Local**.
 - 3) Set **Rules** to **Enable**.
4. Select mode in **Configuration**, and set rule region and rule parameters.
 - For the information about normal mode, see **Normal Mode**.
 - For the information about expert mode, see **Expert Mode**.
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see **Set Arming Schedule**. For the information about linkage methods, see **Linkage Method Settings**.
6. Click **Save**.

6.1.1 Expert Mode

You can configure different motion detection parameters for day and night according to the actual needs.

Steps

1. Select **Expert Mode** in **Configuration**.
2. Set parameters of expert mode.

Scheduled Image Settings

OFF

Image switch is disabled.

Auto-Switch

The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

Scheduled-Switch

The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

Sensitivity

The higher the value of sensitivity is, the more sensitive the motion detection is. If scheduled image settings is enabled, the sensitivity of day and night can be set separately.

3. Select an **Area** and click . Click and drag the mouse on the live image and then release the mouse to finish drawing one area.



Figure 6-1 Set Rules

4. Click  to clear all the areas.
5. Click **Save**.
6. **Optional:** Repeat above steps to set multiple areas.

6.1.2 Normal Mode

You can set motion detection parameters according to the device default parameters.

Steps

1. Select **Normal Mode** in **Configuration**.
2. Set the **Sensitivity** of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to **0**, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle. This function allows alarm triggering by specified target types (human and vehicle).



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

4. Click  . Click and drag the mouse on the live image, and then right click the mouse to finish drawing one area.
5. **Optional:** Click  to clear all the areas.
6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6.2 Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Video Tampering** .
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
4. Click  and drag the mouse in the live view to draw the area.

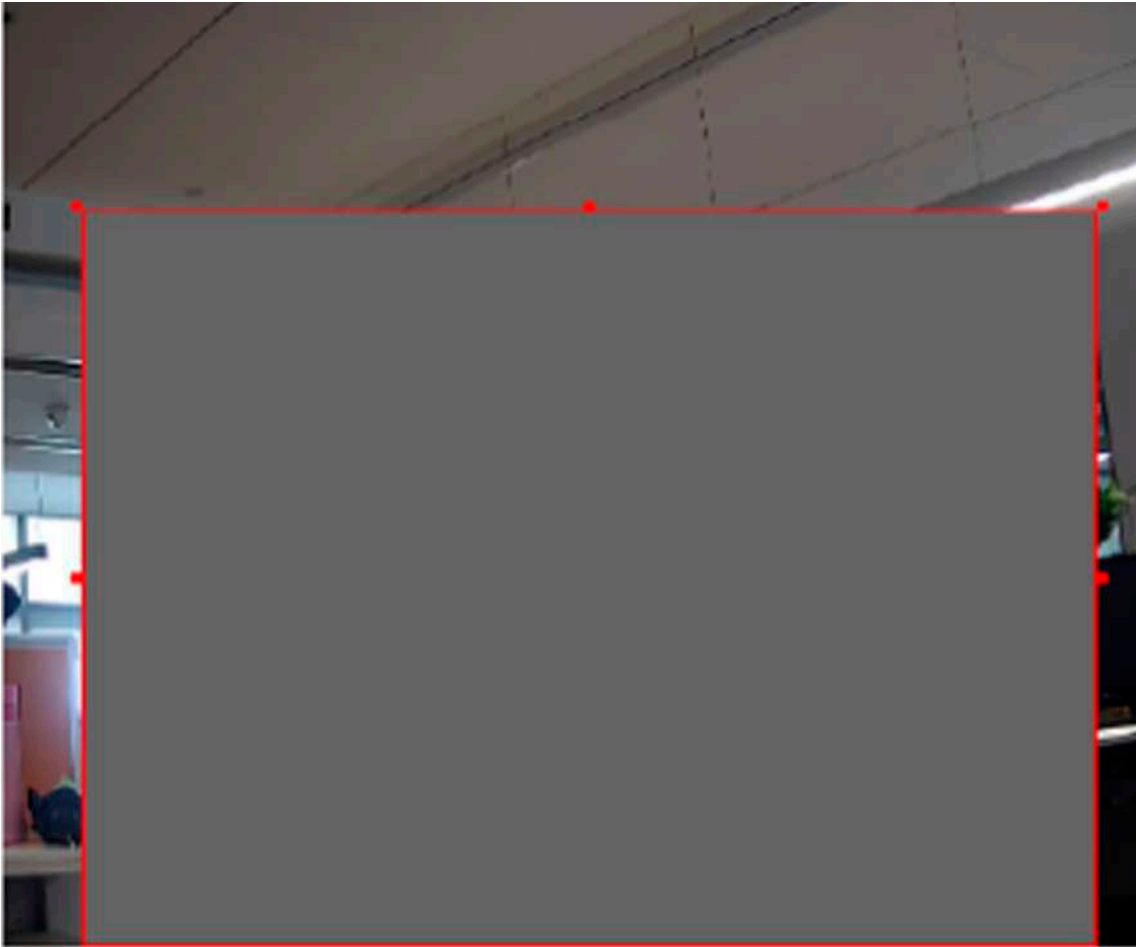


Figure 6-2 Set Video Tampering Area

5. **Optional:** Click  to delete all the drawn areas.
6. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
7. Click **Save**.

6.3 Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start



Note

This function is only supported by certain models.

Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Configuration → Event → Event and Detection → Alarm Input** .
2. Select an **Alarm Input NO.** and click  to set alarm input.
3. Select **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Check **Enable Alarm Input Handling**.
5. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
6. Click **Copy to...** to copy the settings to other alarm input channels.
7. Click **Save**.

6.4 Set Exception Alarm

Exception such as network disconnection can trigger the device to take corresponding action.

Steps

1. Go to **Configuration → Event → Event and Detection → Exception** .
2. Select **Exception Type**.

HDD Full

The HDD storage is full.

HDD Error

Error occurs in HDD.

Network Disconnected

The device is offline.

IP Address Conflicted

The IP address of current device is same as that of other device in the network.

Illegal Login

Incorrect user name or password is entered.

3. Refer to **Linkage Method Settings** for setting linkage method.
4. Click **Save**.

6.5 Set Video Quality Diagnosis

When the video quality of the device is abnormal and the alarm linkage is set, the alarm will be triggered automatically.

Steps

1. Go to **Configuration → Event → Event and Detection → Video Quality Diagnosis** .
2. Select **Diagnosis Type**.
3. Set the corresponding parameters.

Alarm Detection Interval

The time interval to detect the exception.

Sensitivity

The higher the value is, the more easily the exception will be detected, and the higher possibility of misinformation would be.

Alarm Delay Times

The device uploads the alarm when the alarm reaches the set number of times.

4. Check the selected diagnosis type, and the related type will be detected.
5. Set arming schedule. See **Set Arming Schedule** .
6. Set linkage method. See **Linkage Method Settings** .
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with models.

6.6 Set Audio Exception Detection

Audio exception detection function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

Steps

1. Go to **Configuration → Event → Event and Detection → Audio Exception Detection** .
2. Select one or several audio exception detection types.

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.



Note

- The lower the sensitivity is, the more significant the change should be to trigger the detection.
 - The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
-

Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage methods.
4. Click **Save**.



Note

The function is only supported by certain models. The actual function varies according to different models.

6.7 Set Defocus Detection

The blurred image caused by lens defocus can be detected. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Defocus Detection**.
 2. Check **Enable**.
 3. Set **Sensitivity**. The higher the value is, the more easily the defocus image can trigger the alarm. You can adjust the value according to the actual environment.
 4. For the linkage method settings, refer to **Linkage Method Settings**.
 5. Click **Save**.
-



Note

The function is only supported by certain models. The actual display varies with models.

6.8 Set Scene Change Detection

Scene change detection function detects the change of the scene. Some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Event and Detection → Scene Change Detection**.
 2. Click **Enable**.
 3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
 4. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
 5. Click **Save**.
-



Note

The function is only supported by certain models. The actual display varies with models.

Chapter 7 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

7.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. **Optional:** Click **Arming Schedule and Linkage Method** in the related event interface.
2. Click **Edit** behind **Arming Schedule**.
3. Click **Draw**, and drag the time bar to draw desired valid time.



Note

- Each cell represents 30 minutes.
 - Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
 - Up to 8 periods can be configured for one day.
4. Click **Erase**, and drag the time bar to clear selected valid time.
 5. Click **OK** to save the settings.



Figure 7-1 Set Arming Schedule

7.2 Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

7.2.1 Trigger Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps

1. Go to **Configuration → Event → Alarm Setting → Alarm Output** .
2. Set alarm output parameters.

Automatic Alarm For the information about the configuration, see [Automatic Alarm](#) .

Manual Alarm For the information about the configuration, see [Manual Alarm](#) .

Manual Alarm

You can trigger an alarm output manually.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click  to set alarm parameters.

Alarm Name

Custom a name for the alarm output.

2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click  to set alarm parameters.

Alarm Name

Custom a name for the alarm output.

Delay

It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see [Set Arming Schedule](#) .
3. **Optional:** Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

7.2.2 FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refer to [Set FTP](#) to set the FTP server.

Refer to [Set NAS](#) for NAS configuration.

Refer to [Set New or Unencrypted Memory Card](#) for memory card storage configuration.

7.2.3 Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refer to [Set Email](#) .

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated recipients if an alarm event is detected.

Before You Start

Set the DNS server before using the Email function. Go to **Configuration → Network → Network Settings → TCP/IP** for DNS settings.

Steps

1. Go to email settings page: **Configuration → Event → Alarm Setting → Email** .
2. Set email parameters.
 - 1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
 - 2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
 - 3) Set the **E-mail Encryption**.
 - When you select **TLS**, and disable **STARTTLS**, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
 - When you select **TLS** and check **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the **SMTP Port** should be set as 25.



Note

If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.

- 4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Picture**. The notification email has a certain number of attached alarm pictures about the event with configurable image capturing interval.



Note

The number of alarm pictures may vary according to different device models and different events.

- 5) Input the recipient's information, including the recipient's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

7.2.4 Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

7.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event. For recording settings, refer to [Video Recording and Picture Capture](#).

7.2.6 Flashing Light

After enabling **Flashing Light** and setting the **Flashing Light Alarm Output**, the light flashes when an alarm event is detected.

Set Flashing Alarm Light Output

When events occur, the flashing light on the device can be triggered as an alarm.

Steps

1. Go to **Configuration → Event → Alarm Setting → Flashing Alarm Light Output**.
2. Set **Flashing Duration** and **Flashing Frequency**.

Flashing Duration

The time that the flashing lasts when one alarm happens.

Flashing Frequency

The rate at which the light flashes. High frequency, medium frequency, low frequency, and normally on are selectable.

3. Set the arming schedule. See [Set Arming Schedule](#) for details.

4. Click **Save**.



Note

Only certain device models support the function.

7.2.7 Audible Warning

After enabling **Audible Warning** and setting **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when an alarm happens.

For audible alarm output settings, refer to [Set Audible Alarm Output](#).



Note

The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Alarm Setting → Audible Alarm Output**.

2. Select **Sound Type** and set related parameters.

- Select **Prompt** and set the alarm times you need.
- Select **Warning** and its contents. Set the alarm times you need.
- Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Set → Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.

3. **Optional**: Click **Test** to play the selected audio file on the device.

4. Set arming schedule for audible alarm. See [Set Arming Schedule](#) for details.

5. Click **Save**.



Note

The function is only supported by certain device models.

7.2.8 Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTPS, or ISUP data transmission.

Set Alarm Server

Steps

1. Go to **Configuration → Event → Alarm Setting → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol**.



Note

HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

-
4. Click **Test** to check if the IP or host is available.
 5. Click **Save**.

Chapter 8 Network Settings

8.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration** → **Network** → **Network Settings** → **TCP/IP** for parameter settings.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.



Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.



Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address**, **IPv6 Subnet**, **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

Domain Name Settings

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.



Note

DHCP should be enabled for the dynamic domain name to take effect.

8.2 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name. The DDNS service of the device only supports HTTPS.

Before You Start

Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps

1. Refer to **TCP/IP** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Network Settings → DDNS**.
3. Check **Enable** and select **DDNS Type**.

DynDNS

Dynamic DNS server is used for domain name resolution.

NO-IP

NO-IP server is used for domain name resolution.

4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to **Port Mapping** for port mapping settings.
6. Access the device.

By Browsers

Enter the domain name in the browser address bar to access the device.

By Client Software Add domain name to the client software. Refer to the client manual for specific adding methods.

8.3 Access to Device via PPPoE Dial Up Connection

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps

1. Go to **Configuration → Network → Network Settings → PPPoE** .
2. Check **Enable**.
3. Set the PPPoE parameters.

Dynamic IP

After successful dial-up, the dynamic IP address of the WAN is displayed.

User Name

User name for dial-up network access.

Password

Password for dial-up network access.

Confirm

Input your dial-up password again.

4. Click **Save**.
5. Access the device.

By Browsers Enter the WAN dynamic IP address in the browser address bar to access the device.

By Client Software Add the WAN dynamic IP address to the client software. Refer to the client manual for details.



Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to **[Access to Device via Domain Name](#)** for detail information.

8.4 SNMP

You can set the SNMP (Simple Network Management Protocol) to get device information in network management.

Before You Start

Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to **Configuration → Network → Network Settings → SNMP**.
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.



Note

The SNMP version you select should be the same as that of the SNMP software.

And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

-
3. Configure the SNMP settings.
 4. Click **Save**.

8.5 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X.

Go to **Configuration → Network → Network Settings → 802.1X**, and enable the function.

Select protocol and version according to router information. User name and password of server are required.



Note

- If you set the **Protocol** to **EAP-TLS**, select the **Client Certificate** and **CA Certificate**.
 - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
-

8.6 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.



Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Network Settings → QoS**.
2. Set **Video/Audio DSCP**, **Event/Alarm DSCP** and **Management DSCP**.



Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.

3. Click **Save**.

8.7 HTTP(S)

HTTP is an application-layer protocol for transmitting hypermedia documents. HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Network Service → HTTP(S)**.
 2. Enter **HTTP Port**.
-



Note

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter `http://192.168.1.64:81` in the browser for login.

3. Check **Enable** in **HTTPS**.
-



Note

You can click **TLS Settings** to set the TLS version that the device supports. Refer to for details.

4. Enter **HTTPS Port**.
5. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
6. Select **Server Certificate**.
7. Set **Web Authentication**.

Authentication

Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

8. Click **Save**.

8.8 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Go to **Configuration → Network → Network Service → Multicast** for the multicast settings.

IP Address

It stands for the address of multicast host.

8.8.1 Multicast Discovery

Go to **Configuration → Network → Network Settings → TCP/IP** to enable this function.

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

8.9 RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

Steps

1. Go to **Configuration → Network → Network Service → RTSP**.

2. Enter **Port**.

3. Set **Multicast** parameters.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

4. Set **RTSP Authentication**.

Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to

the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

5. Click **Save**.

8.10 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

Steps

1. Go to **Configuration → Network → Network Service → SRTP**.
2. Enter the **Port** number.
3. Set **Multicast** parameters.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

4. Select **Server Certificate**.
5. Select **Encrypted Algorithm**.
6. Click **Save**.



Note

- Only certain device models support this function.
 - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
-

8.11 Bonjour

It is an implementation of zero-configuration networking (zeroconf), a group of technologies that includes service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

Go to **Configuration → Network → Network Service → Bonjour** to enable the function, and click **Save**.

After enabling the function, the device spread and receive service information in local area network.

8.12 WebSocket(s)

WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

Go to **Configuration → Network → Network Service → WebSocket(s)** to set parameters, and click **Save**.

WebSocket

TCP-based full-duplex communication protocol port for plug-in free preview via HTTP protocol.

WebSockets

TCP-based full-duplex communication protocol port for plug-in free preview via HTTPS protocol.

8.13 Port Mapping

By setting port mapping, you can access devices through the specified port.

Steps

1. Go to **Configuration → Network → Network Service → NAT**.
2. Select the port mapping mode.

Auto Port Mapping Refer to [Set Auto Port Mapping](#) for detailed information.

Manual Port Mapping Refer to [Set Manual Port Mapping](#) for detailed information.

3. Click **Save**.

8.13.1 Set Auto Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.



Note

UPnP™ function on the router should be enabled at the same time.

8.13.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.

2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

8.13.3 Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding** → **Virtual Servers**, and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

108M Wireless Router
Model No.: TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- + Network
- + Wireless
- Advanced Settings ---
- + DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- + Security
 - Static Routing
 - Dynamic DNS
- Maintenance ---
- + System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☒
2	8000	192.168.10.23	ALL	☒
3	554	192.168.10.23	ALL	☒
4	8200	192.168.10.23	ALL	☒
5	81	192.168.10.24	ALL	☒
6	8001	192.168.10.24	ALL	☒
7	555	192.168.10.24	ALL	☒
8	8201	192.168.10.24	ALL	☒

Common Service Port: ID

Figure 8-1 Port Mapping on Router

Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

8.14 RTCP

The device relies on RTCP (Real-time Transport Control Protocol) to deliver packets sequentially to provide a reliable delivery mechanism and to provide services for flow control or congestion control.

Go to **Configuration → Network → Network Service → RTCP** and check **Enable** to enable the function.

8.15 Wireless Dial

Data of audio, video and image can be transferred via 3G/4G wireless network.

Note

The function is only supported by certain device models.

8.15.1 Set Wireless Dial

The built-in wireless module offers dial-up access to the Internet for the device.

Before You Start

Get a SIM card, and activate 3G/4G services. Insert the SIM card to the corresponding slot.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial**.
2. Check to enable the function.
3. Go to **Dial Parameters** to configure and save the parameters.
4. Click **Settings** behind **Dial Plan**. See [Set Arming Schedule](#) for detailed information.
5. View the **Dial Status**.

Click Refresh Refresh the dial status.

Click Disconnect Disconnect the 3G/4G wireless network.

When the **Dial Status** turns to **Connected**, it means a successful dial.

6. Access the device via the **IP Address** of the computer in the network.
 - Input the IP address in the browser to access the device.
 - Add the device in client application. Select **IP/Domain**, and input IP address and other parameters to access the device.

7. Optional: You can view 4G SIM card information and network carrier information.



Note

For certain device models working on **Performance Mode** or **Proactive Mode**, the wireless mode can be upgraded. If necessary, please upgrade the wireless mode under the guidance of a professional.

- 8. Optional:** Click **Re-Camp** to reconnect the device to wireless network manually. The device will maintain airplane mode for 10 seconds and then connects to network automatically.
- 9. Optional:** Check **Enable** to enable **Auto Re-Camp**, and then set the **Re-Camp Interval**. The device will reconnect to the wireless network at set **Re-Camp Interval** automatically.
-



Note

The function may vary according to different device models.

8.15.2 Wireless Expert Settings

Wireless expert settings provide more details of the 3G/4G wireless network to which the device connects and help the professionals troubleshoot potential network issues.

Cell Radio Frequency Parameters

Cell radio frequency parameters provides the current wireless network information to which the device is connected.

Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** to view cell radio frequency parameters.

Network Info

It displays the current cellular network information. You can click **Refresh** to view the frequency information of different cells.

Radio Frequency Fluctuation

It records the fluctuation of the cellular network to which the device has connected during the past 7 days. Click **Export Report** and set and confirm the encryption password to export the fluctuation report.

Lock Band

You can lock a set of bands that get the device faster data rates to improve the network speed.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings → Lock Band**.
2. Check **Enable**.

3. Click **Add** and enter the band.



Note

- The band you enter should be B + number or N + number. For example, you can enter B1 or N1.
- Up to five bands are supported.

4. **Optional:** Click  to delete the selected band. You can also click **Clear All** to clear the list.

Capture Baseband Packet

This function can capture the protocol interaction packet to help the professionals to locate the communication failures between 4G module and the base station.

Steps



Note

This function is reserved for the professionals and technical support staff.

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings**.
2. Click **Configuration** behind **Capture Baseband Packet** to enter the setting interface.
3. Check **Enable** to enable this function.
4. Set capture duration and the saving path. The saving path depends on the actual storage method of the device. You can click **Delete Captured Packet Under This Path** to delete the captured packet.
5. Click **Save**.
6. Click **Start Capturing Packet** to capture the baseband packet.
7. **Optional:** Click **Stop Capturing** to stop the capturing process.
8. After the capturing is completed, click **Export Captured Packet** to save the report.

Speed Test

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings**.
2. Click **Configuration** behind **Speed Test** to enter the setting interface.
3. Select the default server or enter the server address. You can follow the steps below to get the nearby server address.



Note

You can follow the steps below to get the nearby server address.

- a. Visit this website to get the nearby server address: <https://www.speedtest.net/speedtest-servers-static.php>.
 - b. Select and copy the URL of the nearby speed test station and paste it in **Server Address**.
-

4. Click **Speed Test** to start the test.

You can view the speed details after the test is completed. You can also click **Export Speed Test Result**.

8.16 WLAN AP (Access Point)

The device can be used as a wireless access point with the WLAN AP function. You can connect your phone or PC to the device AP, so as to access to the device and configure the parameters via your phone or PC.



Note

The function is only supported by certain device models.

8.16.1 Set WLAN AP

Steps

1. Go to **Configuration → Network → Network Settings → WLAN AP**.
2. Select the WLAN AP mode.

On

The function is enabled.

Maintenance Mode

The WLAN AP function is automatically turned on for 5 minutes after the device is cold booted (by turning the switch on the device to **ON**), after which the WLAN AP function is turned off if the device's 4G communication is normal, and remains on if the device's 4G communication is abnormal.

Off

The function is disabled.

3. Set the related parameters.

SSID

For certain device models, the default SSID of the device is named as "Hik-Serial Number".

For certain device models, the default SSID of the device is named as "Default SSID" on the device label.

You can define it as needed.

Security Mode

WPA2-personal mode is supported.

Encryption Type

AES and **TKIP** are selectable.

Password

The password for wireless connection via the device AP. The default password is the nine-digit serial number of the camera. Please change the default password and set a strong password after logging in for the first time.



Caution

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 **Save**.



Note

The function may vary according to different device models.

What to do next

You can connect your mobile phone or PC to the AP.

8.16.2 Access to Device via AP

You can access to the device via the device AP when the device cannot connect to the network.

Steps

1. Go to **Configuration** → **Network** → **Network Settings** → **WLAN AP** to enable WLAN AP function.

For certain device models, the WLAN AP function is automatically turned on for 5 minutes after the device is cold booted (by turning the switch on the device to **ON**), after which the WLAN AP function is turned off if the device's 4G communication is normal, and remains on if the device's 4G communication is abnormal.

2. Search the device WLAN AP in the WLAN list of your phone or PC.

3. Enter the password and connect your mobile phone or PC to the AP.



Note

- The AP name is SSID ("Hik-Serial Number" by default). The password is serial number by default. The serial number can be obtained from **Configuration** → **System** → **System Settings** → **Basic Information**.
- For certain device models, the AP name is the "Default SSID" on the device label.

4. Enter the IP address in the browser.



Note

The default IP of the device AP is 192.168.8.1.

Result

The connected devices will be displayed in the **Connected Device** interface.

8.17 Traffic Shaping

Traffic shaping is used to shape and smooth video data packet before transmission.

It helps to improve latency and reduce packet loss caused by network congestion and ensure the video quality as well. Shaping level is configurable.

8.18 Data Monitoring

You can view and manage the SIM card data or wired network data used by the device. SIM card data is the data service provided by network carriers; wired network data is usually provided through a 4G router.

Steps

1. Go to **Configuration → Network → Network Settings → Data Monitoring**.
2. Check **Enable**.
3. Set the following parameters according to your data plan.

Plan Type

Daily, Monthly, or Annually can be selected.

Data Plan

Enter the amount of usable data and select the unit.

Pre-Alarm Threshold

When the used data reaches the set percentage of data plan, the device sends an alarm message, and shows notification on the OSD or pop-up window.

4. Select **Normal Linkage**.

If **Send Email** or **Notify Surveillance Center** is selected, the device sends an alarm message by Email or to surveillance center when the used data reaches the threshold.

5. Click **Save**.



Note

The function varies with different device models.

8.19 Wi-Fi

Connect the device to wireless network by setting Wi-Fi parameters.



Note

This function is only supported by certain device models.

8.19.1 Connect Device to Wi-Fi

Before You Start

Refer to the user manual of wireless router or AP to set SSID, key, and other parameters.

Steps

1. Go to TCP/IP settings page: **Configuration → Network → Network Settings → TCP/IP**.
2. Select **Wlan** to set the parameters. Refer to **TCP/IP** for detailed configuration.



Note

For stable use of Wi-Fi, it is not recommended to use DHCP.

3. Go to Wi-Fi settings page: **Configuration → Network → Network Service → Wi-Fi**.
4. Set and save the parameters.
 - 1) Check to enable Wi-Fi function.
 - 2) Click **Refresh** to view and select the available wireless router or AP, or click **+** to add it manually.
 - 3) Select or input a **SSID**, which should be the same as that of wireless router or AP.

The parameters of the network is automatically shown in **Wi-Fi**.
 - 4) Select the **Network Mode** as **Manage**.
 - 5) Select the **Security Mode** according to your needs, and the parameters should be the same as those of the wireless network connection you set on the router or AP.
 - 6) Click **Save**.

What to do next

Go to TCP/IP settings page: **Configuration → Network → Network Settings → TCP/IP**, and click **Wlan** to check the **IPv4 Address** and log in the device.

8.20 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Platform Access → ISUP**.
2. **Optional:** Select an access center.
3. Check **Enable**.
4. Select a protocol version and enter related parameters.
5. Click **Save**.

Register status turns to **Online** when the function is correctly set.

8.21 Access Camera via Hik-Connect

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.

Before You Start

Connect the camera to network with network cables.

Steps

1. Get and install Hik-Connect application by the following ways.
 - Visit <https://appstore.hikvision.com> to download the application according to your mobile phone system.
 - Visit the official site of our company. Then go to **Support** → **Tools** → **Hikvision App Store**.
 - Scan the QR code below to download the application.



Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit <https://appstore.hikvision.com/static/help/index.html> to refer to the troubleshooting.
- Visit <https://appstore.hikvision.com/>, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

-
2. Start the application and register for a Hik-Connect user account.
 3. Log in after registration.
 4. In the app, tap "+" on the upper-right corner and then scan the QR code of the camera to add the camera. You can find the QR code on the camera or on the cover of the Quick Start Guide of the camera in the package.
 5. Follow the prompts to set the network connection and add the camera to your Hik-Connect account.

For detailed information, refer to the user manual of the Hik-Connect app.

8.21.1 Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

Before You Start

You need to activate the camera before enabling the service.

Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Platform Access → Hik-Connect .**
3. Check **Enable**.
4. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
5. Create a verification code or change the old verification code for the camera.



Note

The verification code is required when you add the camera to Hik-Connect service.

6. Save the settings.

Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.



Note

The verification code is required when you add the camera to Hik-Connect service.

5. Click and read "Terms of Service" and "Privacy Policy".
6. Confirm the settings.

8.21.2 Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
 - Visit <https://appstore.hikvision.com> to download the application according to your mobile phone system.
 - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store .**
 - Scan the QR code below to download the application.



Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit <https://appstore.hikvision.com/static/help/index.html> to refer to the troubleshooting.
- Visit <https://appstore.hikvision.com/>, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

-
2. Start the application and register for a Hik-Connect user account.
 3. Log in after registration.

8.21.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.

Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

-
5. Input the verification code of your camera.

Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

-
6. Tap **Connect to a Network** button in the popup interface.
 7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection

Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)

Wired Connection

Connect the camera to the router with a network cable and tap **Connected** in the result interface.



Note

The router should be the same one which your mobile phone has connected to.

8. Tap **Add** in the next interface to finish adding.

For detailed information, refer to the user manual of the Hik-Connect app.

8.22 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Platform Access → Open Network Video Interface** .
2. Check **Enable**.
3. Select an authentication mode.
 - If you select **Digest**, the device only supports digest authentication.
 - If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication.
4. Click **Add** to configure the Open Network Video Interface user.
5. Click **Save**.
6. **Optional**: Repeat the steps above to add more Open Network Video Interface users.
7. **Optional**: Manage the user.
 - Click to delete the selected Open Network Video Interface user.
 - Click to modify the selected Open Network Video Interface user.

8.23 Set SDK Service

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

Steps

1. Go to **Configuration → Network → Platform Access → SDK Service** .
2. Set **SDK Service** parameters.
 - 1) Check **Enable** to add the device to the client software with SDK protocol.
 - 2) Enter the **Port** number.
3. Set **Enhanced SDK Service** parameters.
 - 1) Check **Enable** to add the device to the client software with SDK over TLS protocol.
 - 2) **Optional**: Click **TLS Settings** to enable the TLS version that the device supports. Refer to [TLS](#) for details.
 - 3) Enter the **Port** number.
 - 4) Select a server certificate to make sure the data transmission security. You can click **Certificate Management** to add a certificate. Refer to [Certificate Management](#) for details.
4. Click **Save**.

Chapter 9 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

9.1 System Settings

9.1.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration → System → System Settings → Basic Information** to view the device information.

9.1.2 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

Synchronize Time Manually

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Select **Manual Time Sync.**.
4. Choose one time synchronization method.
 - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
 - Click **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

Set NTP Server

You can use NTP server when accurate and reliable time source is required.

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.

3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.



Note

Server Address is NTP server IP address.

5. Click **Test** to test server connection.
6. Click **Save**.

Synchronize Time by Satellite



Note

This function varies depending on different devices.

Steps

1. Enter **Configuration → System → System Settings → Time Settings**.
2. Select **Satellite Time Sync**.
3. Set **Interval**.
4. Click **Save**.

Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → Time Settings**.
2. Check **Enable**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

9.1.3 Set RS-232

RS-232 can be used to debug device or access peripheral device. RS-232 can realize communication between the device and computer or terminal when the communication distance is short.

Before You Start

Connect the device to computer or terminal with RS-232 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-232**.
2. Set RS-232 parameters to match the device with computer or terminal.
3. Click **Save**.

9.1.4 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

Before You Start

Connect the device and computer or terminal with RS-485 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-485**.
2. Set the RS-485 parameters.



Note

You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.

9.1.5 Set Live View Connection

It controls the remote live view connection amount.

Live view connection controls the maximum live view that can be streamed at the same time.

Enter **Configuration → System → System Settings → System Service** to set the upper limit of the remote connection number.

9.1.6 Location Settings

Location displays and uploads the current longitude and latitude of the device.

Auto Uploading

Check **Enable** and set **Location Upload Interval**.

The device will upload its location at the set interval. You can also click **Refresh** to upgrade the device location manually.

Manual Settings

Check **Enable** and set **Location Upload Interval**. Enter the longitude and latitude of the device and click **Save**.

The device will upload the set location at the set interval.



Note

This function may vary according to different device models.

9.1.7 External Device

For the device supporting external devices, including the supplement light, wiper on the housing, the LED light, and heater, you can control them via the Web browser when it is used with the housing. External devices vary with models.

9.1.8 View Open Source Software License

On the top-right corner, click  and select **Open Source Software Description** to download the license. You can view the license in the editor.

9.1.9 Wiegand



Note

This function is only supported by certain camera models.

Check **Enable** and select the protocol. The default protocol is SHA-1 26bit.

If enabled, the recognized license plate number will be output via the selected Wiegand protocol.

9.2 User and Account

9.2.1 Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.



Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

Steps

1. Go to **Configuration → System → User Management → User Management**.
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

Administrator

The administrator has the authority to all operations and can add users and operators and assign permission.

User

Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

Modify Select a user and click  to change the password and permission.

Delete Select a user and click  .



Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

9.2.2 Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management → Online Users** , click **General**, and set **Simultaneous Login**.

9.2.3 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

9.3 Maintenance

9.3.1 Restart

You can restart the device via browser.

Go to **Maintenance and Security → Maintenance → Restart** , and click **Restart**.

9.3.2 Upgrade

Before You Start

You need to obtain the correct upgrade package.



Caution

DO NOT disconnect power during the process, and the device restarts automatically after upgrade.

Steps

1. Go to **Maintenance and Security → Maintenance → Upgrade**.
2. Choose one method to upgrade.

Firmware Locate the exact path of the upgrade file.

Firmware Directory Locate the directory which the upgrade file belongs to.

3. Click  to select the upgrade file.
4. Click **Upgrade**.

9.3.3 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps

1. Go to **Maintenance and Security → Maintenance → Backup and Restore**.
2. Click **Restore** or **Default** according to your needs.

Restore Reset device parameters, except user information, IP parameters and video format to the default settings.

Default Reset all the parameters to the factory default.



Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

9.3.4 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

Steps

1. Export configuration file.
 - 1) Go to **Maintenance and Security → Maintenance → Backup and Restore → Backup**.
 - 2) Click **Export** and input the encryption password to export the current configuration file.
 - 3) Set the saving path to save the configuration file in local computer.
2. Import configuration file.
 - 1) Access the device that needs to be configured via web browser.
 - 2) Go to **Maintenance and Security → Maintenance → Backup and Restore → Reset**.
 - 3) Click  to select the saved configuration file.
 - 4) Input the encryption password you have set when exporting the configuration file.

5) Click **Import**.

9.3.5 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Maintenance and Security → Maintenance → Log**.
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

The matched log files will be displayed on the log list.

4. **Optional:** Click **Export** to save the log files in your computer.

9.3.6 Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Steps



Note

This function is only supported by certain camera models.

1. Go to **Maintenance and Security → Maintenance → Security Audit Log**.
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

The log files that match the search conditions will be displayed on the Log List.

4. **Optional:** Click **Export** to save the log files to your computer.

9.3.7 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Maintenance and Security → Maintenance → Device Debugging**, and click **Settings** of **SSH**. You can edit the number of the port. Click **Save**.



Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

9.3.8 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Maintenance and Security** → **Maintenance** → **Device Debugging** → **Diagnose Information** . Click **Export**. In the pop-up window, check desired diagnose information and click **Export** to export corresponding diagnose information of the device.

9.3.9 Diagnosis

For the device that supports 4G network, diagnosis can help get the communication packet and the device power and network information for future maintenance and troubleshooting.

Capture Device Packet

This function is reserved for the professionals and is used to get the communication packet between the device and the external device for future problem diagnosis and debugging.

Steps



Note

This function is reserved for the professionals and technical support staff.

1. Go to **Maintenance and Security** → **Maintenance** → **Device Debugging** , and click **Settings** of **Capture Device Packet**.
2. Check **Enable** to enable this function.

Capture Device Packet

After the capture packet function is enabled, recording will stop automatically. Recording will recover after the capture packet function is disabled.

Enable

Capture Duration *

1

min

Save Captured Packet to

EMMC/2

Delete Captured Packet Under This Path

NIC Type

Wired Network

Wireless Dial/PPPoE

IP

0.0.0.0

Port No.

0

Auto Capture

After this function is enabled, the device packet will be captured when wakeup happens.

Packet Capturing Status

Save

Start Capturing Packet

Export Captured Packet

Figure 9-1 Capture Device Packet

3. Set **Capture Duration** according to your need.
4. Select the packet saving path.

Note

- a. The saving path option is subject to the actual storage method of the device.
- b. You can click **Delete Captured Packet Under This Path** to delete the saved packet file(s).

5. Set NIC type, IP, and port.
6. **Optional:** You can select **Auto Capture** and the device packet will be captured when wakeup happens.
7. Click **Save**.
8. Click **Start Capturing Packet**.

9. After the capturing is completed, click **Export Captured Packet** to save the report.

Export Device Info

Go to **Maintenance and Security → Maintenance → Device Debugging → Export Device Info** , you can click **Export** to export device information, such as voltage, current, power, 4G data.

9.4 Security

You can improve system security by setting security parameters.

9.4.1 Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

Steps

1. Go to **Maintenance and Security → Security → IP Address Filter** .

2. Check **Enable**.

3. Select the type of IP address filter.

Blocklist IP addresses in the list cannot access the device.

Allowlist Only IP addresses in the list can access the device.

4. Edit the IP address filter list.

Add Add a new IP address or IP address range to the list.



Modify the selected IP address or IP address range in the list.



Delete the selected IP address or IP address range in the list.

5. Click **Save**.

9.4.2 Set MAC Address Filter

MAC address filter is a tool for access control. You can enable the MAC address filter to allow or forbid the visits from the certain MAC addresses.

Steps

1. Go to **Maintenance and Security → Security → MAC Address Filter** .

2. Check **Enable**.

3. Select the type of MAC address filter.

Blocklist MAC addresses in the list cannot access the device.

Allowlist Only MAC addresses in the list can access the device.

4. Edit the MAC address filter list.

Add Add a new MAC address to the list.



Modify the selected MAC address in the list.



Delete the selected MAC address in the list.

5. Click **Save**.

9.4.3 Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Maintenance and Security** → **Security** → **Login Management** → **Control Timeout Settings** to complete settings.

9.4.4 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.



Note

The function is only supported by certain device models.

Server Certificate/Client Certificate



Note

The device has default self-signed server/client certificate installed. The certificate ID is **default**.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security** → **Security** → **Certificate Management**.
2. Click **Create Self-signed Certificate**.
3. Input certificate information.



Note

The input certificate ID cannot be the same as the existing ones.

4. Click **Save** to save and install the certificate.

The created certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain functions, the function name is shown in the column **Functions**.

5. Optional: Click **Property** to see the certificate details.

Install Self-signed Request Certificate

You can send the self-signed certificate to a trusted third-party for the signature, and install the certificate to the device.

Before You Start

Create a self-signed certificate first. See [**Create and Install Self-signed Certificate**](#) for instructions.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management**.
2. Select a self-signed certificate from the **Server/Client Certificate** list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **Save**.

The certificate request details are displayed in a pop-up window.

6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
 - 1) Click **Import**.
 - 2) Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existed ones.

-
- 3) Click  to select the certificate file.
 - 4) Select **Self-signed Request Certificate**.
 - 5) Click **Save**.

The imported certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain function, the function name is shown in the column **Functions**.

9. Optional: Click **Property** see the certificate details.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management**.
2. Click **Import** in the **Server/Client Certificate** list.

3. Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existed ones.

4. Click to select the certificate file.

5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

Independent Key If your certificate has an independent key, select this option.
Browse to select the private key and input the private-key password.

PKCS#12 If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **Save**.

The imported certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain function, the function name is shown in the column **Functions**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security** → **Security** → **Certificate Management** .

2. Click **Import** in the **CA Certificate** list.

3. Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existing ones.

4. Click to select the certificate file.

5. Click **Save**.

The imported certificate is displayed in the **CA Certificate** list.

If the certificate is used by certain functions, the function name is shown in the **Functions** column.

Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.



Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

9.4.5 TLS

The Transport Layer Security (TLS) protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. TLS settings are effective for HTTP(S) and enhanced SDK service.

Go to **Maintenance and Security → Security → TLS** , and enable the desired TLS protocol. Click **Save**.



Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

Chapter 10 VCA Resource

VCA resource is a collection of smart functions supported by the device.

10.1 Set Open Platform

HEOP (Hikvision Embedded Open Platform) allows you to install the application for the third-party to develop and run its function and service. For the device supporting HEOP, you can follow the steps to import and run smart applications.

Steps

1. Go to **VCA** interface.



Note

Before installing the application, make sure that the application you want to install fits the following conditions.

- Each application has its own exclusive name.
- The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
- The memory and computing power of the application is less than that available memory and computing power of the device.

2. Click **Import Application** and browse your local path to select an application package and import.
3. Click **Import License** and browse your local path to select a license file and import.
4. **Optional:** Set application.

Click	Enable or disable the application.
Click	Delete the application.
Click	Export log.
Click	Browse a local path and import an application package to update the application.
Click	Clear memory fragmentation and free up more memory to enable more smart applications.
View details	Select an application and click on it to show the details on the page.

10.2 General Settings

Set the general parameters which are related to the smart applications.

Go to **VCA → Set Application → General Settings** to set the following parameters.

Camera Info.

For camera information settings, refer to **Set Camera Info** .

FTP

For FTP settings, refer to **Set FTP** .

Email

For Email settings, refer to **Set Email** .

Alarm Output

For alarm output settings, refer to **Automatic Alarm** .

Audible Alarm Output

For audible alarm output settings, refer to **Set Audible Alarm Output** .

Alarm Server

For alarm server settings, refer to **Alarm Server** .

Metadata

For metadata settings, refer to **Metadata** .

10.2.1 Set Camera Info

Customize specific information for the device. It may help identify a certain device when multiple devices are under management.

Go to **VCA → Set Application → General Settings → Camera Info** to set **Device No.** and **Camera Info**.

10.2.2 Metadata

Metadata is the raw data that the device collects before algorithm processing. It is often used for the third party integration.

Go to **VCA → Set Application → General Settings → metadata Settings** to enable metadata uploading of the desired function.



This function may vary according to different camera models.

Smart Event

The metadata of the smart event includes the target ID, target coordinate, time, etc.

Face Capture

The metadata of face capture includes the rule information, target ID, target coordinate, time information, etc. The camera detects the whole image by default. If the area is configured in the face capture settings, the camera detects the configured area.

10.2.3 AcuSearch

The device transmits the POS information of the target to network video recorder after detecting the target. It is to achieve accurate and quick search on the connected network video recorder.

Before You Start

- Make sure the connected network video recorder (NVR) supporting AcuSearch to do with the function.
- After the function is enabled, the ongoing smart application will be disabled while **Smart Event** or **Multi-Target-Type Detection** will be enabled.
- The function is only supported by certain models. The actual display varies with the models.

Steps

1. Enable the function for the device.
2. Set the function on the connected network video recorder.
 - 1) Enable AcuSearch function for the selected channel (refer to the configured camera device) on the network video recorder.
 - 2) Click the AcuSearch button on the playback page of the network video recorder.
 - 3) Click a target on a network video recorder to search for pictures that contain the target.
 - 4) Click a picture to play a video before and after that moment.



Refer to the *User Manual* of NVR for the actual settings on NVR.

10.3 Smart Event



- For certain device models, you need to enable the smart event function on **VCA** page first to show the function configuration page.
 - The function varies according to different models.
-

10.3.1 Set Intrusion Detection

It is used to detect objects entering and loitering in a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Intrusion Detection**.
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Threshold

Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missed.

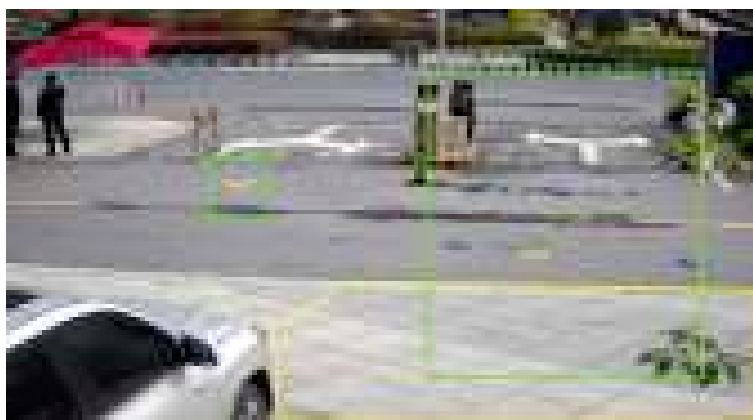


Figure 10-1 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.

10.3.2 Set Line Crossing Detection

It is used to detect objects crossing a predefined virtual line. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection line. Click  and a line with an arrow appears in the live view. Drag the line to the location on the live view as desired.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional:** Click  to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Direction

It stands for the direction from which the object goes across the line.

A<->B: The object going across the line from both directions 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.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

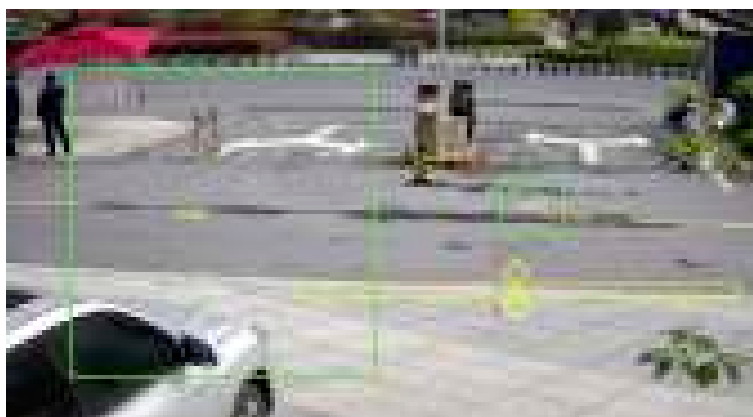


Figure 10-2 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.

10.3.3 Set Region Entrance Detection

It is used to detect objects entering a predefined virtual region from the outside place. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Region Entrance Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

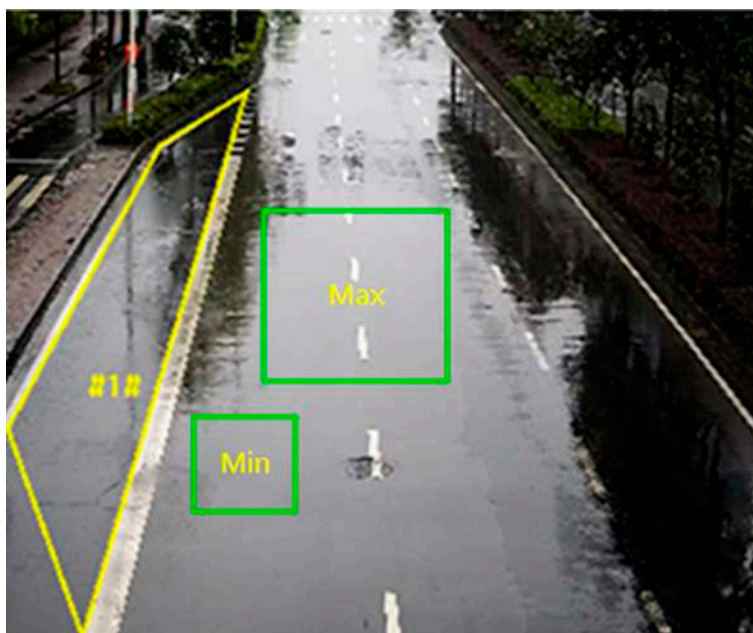


Figure 10-3 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.

10.3.4 Set Region Exiting Detection

It is used to detect objects exiting from a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Region Exiting Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.

3) **Optional:** Click  to delete all the setting areas.

4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

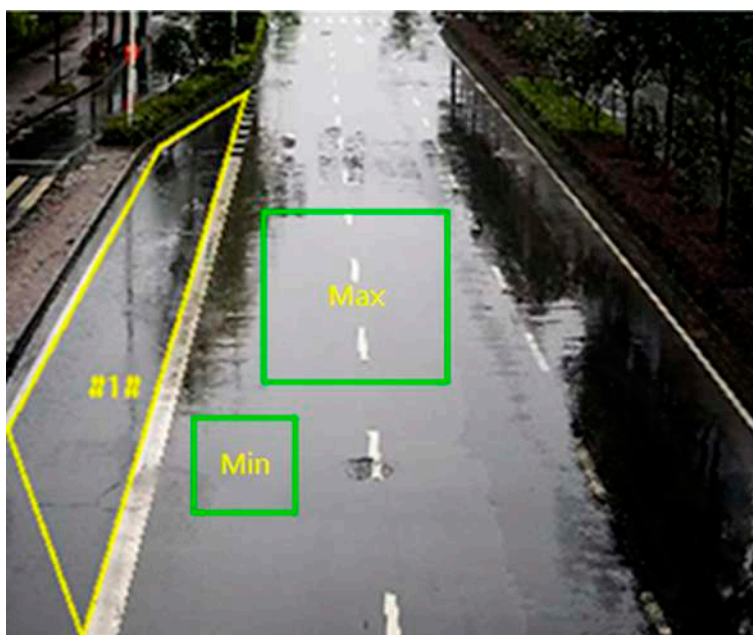


Figure 10-4 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to [Set Arming Schedule](#) . For the linkage method settings, refer to [Linkage Method Settings](#) .
7. Click **Save**.

10.3.5 Set Unattended Baggage Detection

It is used to detect the objects left over in the predefined region. Linkage methods can be triggered after the object is left and stays in the region for a set time period.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Unattended Baggage Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set parameters.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold

It stands for the time of the objects left in the region. Alarm is triggered after the object is left and stays in the region for the set time period.

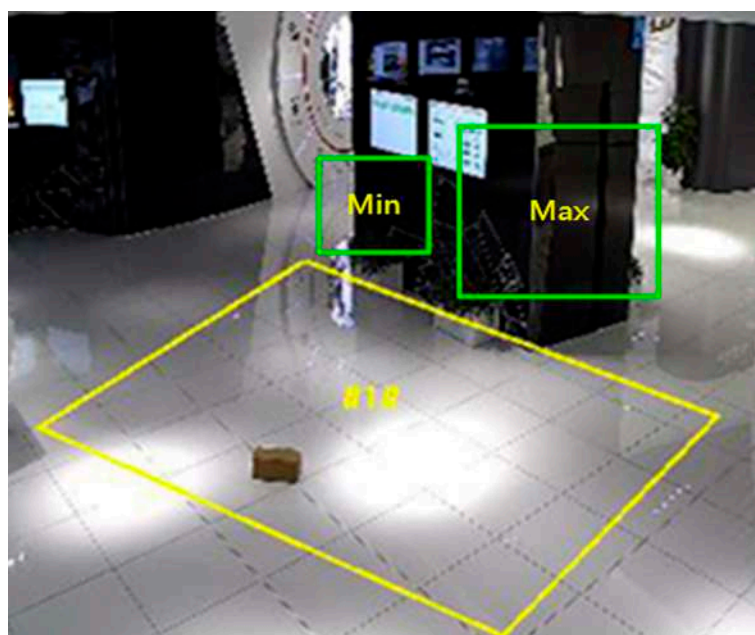


Figure 10-5 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.6 Set Object Removal Detection

It detects whether the objects are removed from the predefined detection region, such as the exhibits on display. If it occurs, the device can take linkage actions and the staff can take measures to reduce property loss.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.

2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.

3) **Optional:** Click  to delete all the setting areas.

4. Set parameters.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold

The threshold for 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.

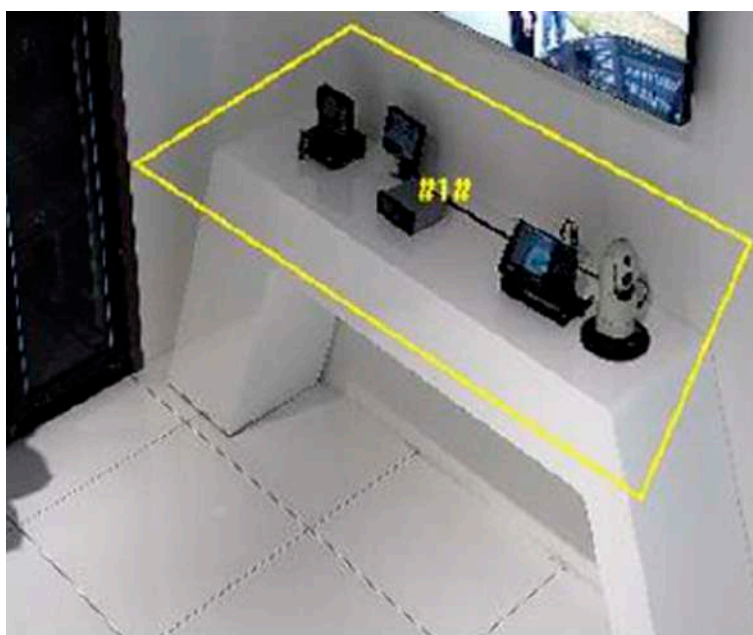


Figure 10-6 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6. For the arming schedule settings, see **Set Arming Schedule** . For the linkage method settings, see **Linkage Method Settings** .

7. Click **Save**.



The function is only supported by certain models. The actual display varies with the models.

10.3.7 Set Loitering Detection

It detects whether there is any target loitering in a predefined area. If the time that the target loiters in the set region reaches the set threshold, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Loitering Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set rules.

Threshold

Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

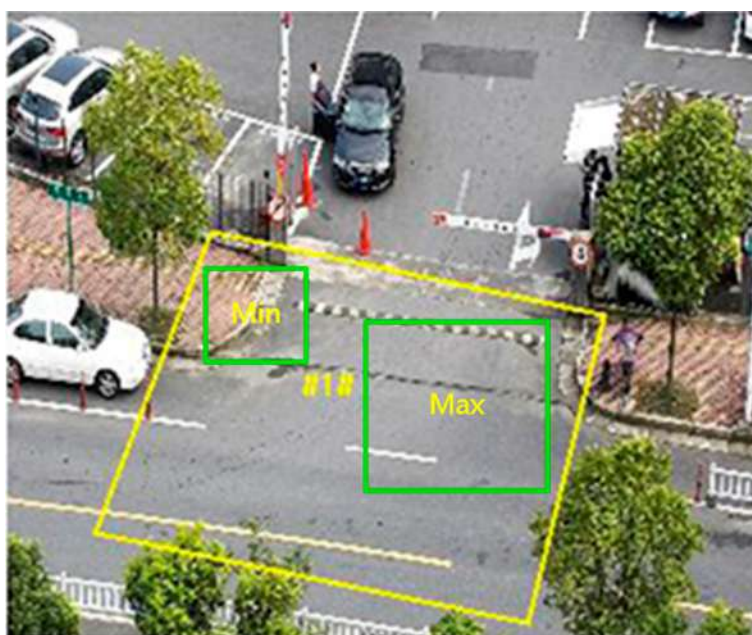


Figure 10-7 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.8 Set People Gathering Detection

It detects the people density in a predefined area. If the people density exceeds the set percentage, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → People Gathering Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) **Optional:** Click  to delete all the setting areas.

4. Set rules.

Percentage

It stands for the percentage of people in the predefined area. When the people percentage in the live view exceeds the set value, the device will trigger an alarm.

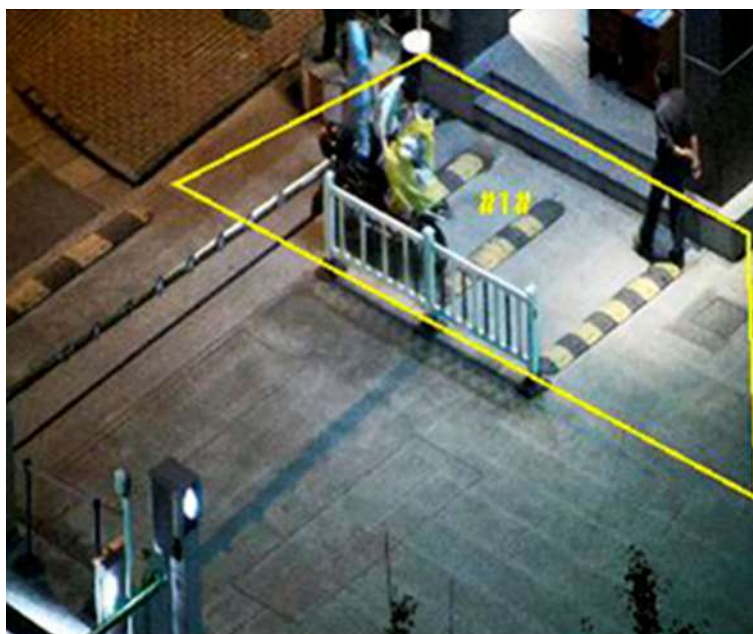


Figure 10-8 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings**
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.9 Set Fast Moving Detection

When there are targets moving at a high speed in a predefined area, the device will take linkage actions and trigger an alarm.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Fast Moving Detection** .
2. Check **Enable**.

3. Click **Add** to add a rule and set a detection area.

- 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
- 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
- 3) **Optional:** Click  to delete all the setting areas.

4. Set Rules.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.



Figure 10-9 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.10 Set Parking Detection

It detects parking violation in a predefined area. When the parking time exceeds a set threshold, the device can take linkage actions. It is applicable in expressway and one-way street.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Parking Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set rules.

Threshold

Threshold stands for the threshold for the parking time in the region. If the parking time exceeds the threshold, an alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the part of an acceptable target that enters the pre-defined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target part that goes across the pre-defined region. ST stands for the complete target. The higher the value of sensitivity is, the more easily the alarm can be triggered.

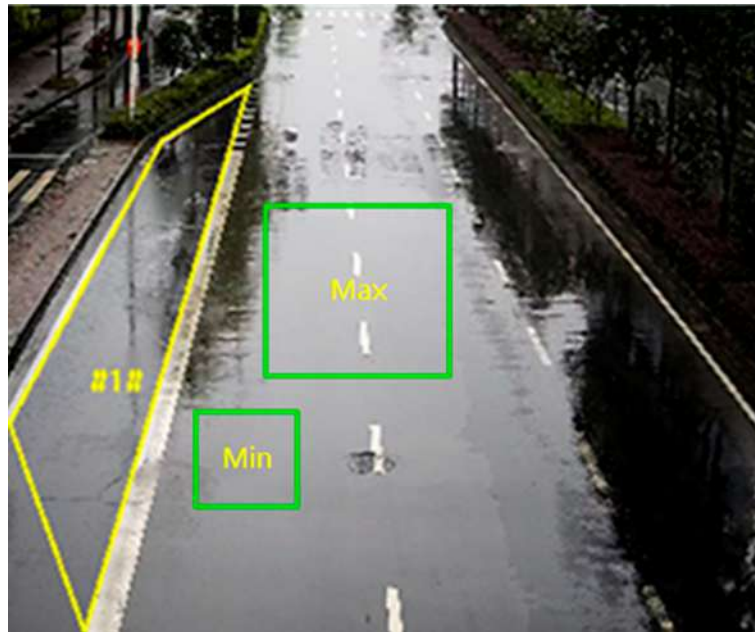


Figure 10-10 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings**
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.4 Face Capture

The device can capture the face that meets the rules in the configured rule area, and the captured picture will be uploaded.



Note

- For certain device models, you need to enable this function on **VCA** page first.
 - The function is only supported by certain device models.
-

10.4.1 Set Face Capture

The face that appears in the configured area can be captured.

Before You Start

- Go to **VCA** and select the application. Select **Face Capture** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Face Capture**.

Steps

1. Go to **VCA** → **Set Application** → **Face Capture** → **Rule** .
2. Check **Enable** to enable the rule settings.
3. Click  to draw the detection area you want the face capture to take effect. Draw area by left-clicking end-points in the live view window, and right-clicking to finish the area drawing. It is recommended that the drawn area occupies 1/2 to 2/3 of the live view image.
4. Draw pupil distance.

Min. Pupil Distance

Click  to draw the minimum pupil distance. If the pupil distance of the face in the video image is smaller than the minimum pupil distance, the face will not be detected.

Max. Pupil Distance

Click  to draw the maximum pupil distance. If the pupil distance of the face in the video image is larger than the maximum pupil distance, the face will not be detected.

You can also input the value of distance in the text field.

5. **Optional:** For shield region settings, refer to [Set Shield Region](#) .
6. For the arming schedule settings, refer to [Set Arming Schedule](#) . For the linkage method settings, refer to [Linkage Method Settings](#) .
7. Click **Save**.
8. For overlay and capture settings, refer to [Overlay and Capture](#) . For advanced parameters settings, refer to [Face Capture Algorithms Parameters](#) .

Result

You can view and download captured pictures in **Playback** → **Picture** . Refer to [View and Download Picture](#) for details.

10.4.2 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Display VCA info. on Stream

Display smart information on stream, including the target and rules information.

Display Target info. on Alarm Picture

Overlay the alarm picture with target information.

Background Picture Settings

Comparing to target picture, background picture is the scene image which offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to the surveillance center, check **Background Upload**. For some devices, you can also check **Face Picture** to upload the captured face picture.

Target Picture Settings

Custom, Head Shot, Half-Body Shot and Full-Body Shot are selectable.



Note

If you select **Custom**, you can customize **width**, **head height** and **body height** as required.

You can check **Fixed Picture Height** to set the picture height.

Face Beautification

Check **Face Beautification** and adjust the beautification level as needed.



Note

Face Beautification slightly adjusts the captured face pictures and reduces facial noise.

Face Enhancement

Check **Face Enhancement** and the device is able to capture better and clearer face pictures when it is dark.

Text Overlay

You can check desired items and adjust their order to display on captured pictures.

See [Set Camera Info](#) to set **Device No.** and **Camera Info**.

10.4.3 Face Capture Algorithms Parameters

It is used to set and optimize the parameters of the algorithm library for face capture function.

Version

It stands for the current algorithm version.

Capture Parameters

Best Shot

The best shot after target leaves the detection area.

Capture Threshold

It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.

Quick Shot

When the face picture grading value is higher than the quick shot threshold, the face picture will be captured and uploaded. Otherwise, the picture with the highest grading value that reaches the max. capture interval will be selected for upload.

Quick Shot Threshold

It stands for the quality of face to trigger quick shot.

Max. Capture Interval

It refers to the max. time occupation for one quick shot.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area.

Remove Duplicated Faces

This function can help filter out repeated captures of certain face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity value is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

The time from when each face picture is added to the duplicates removing library until when it is deleted.

Face Exposure

Check the checkbox to enable the face exposure.

Reference Brightness

The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value you set. The higher the value, the brighter the face is.

Min. Duration

The minimum duration of the camera exposures the face.



Note

If the face exposure is enabled, please make sure the WDR function is disabled, and the manual iris is selected.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture. If the detected face stays in the scene for a time shorter than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.



Note

The face filtering time (longer than 0 s) may increase the possibility of the actual capture times less than the set value above.

Facial Posture Filter

Facial posture filter can filter out face of certain postures. The figure on the right of the slider stands for the posture angle which is acceptable in the face capture action. Click ⓘ to display the diagram illustrating the face turning direction when setting up this filter.

Upload Feature

Feature stands for the feature information the algorithm can tell from face pictures. Check the function to upload the information.

Restore Parameters

Restore Defaults

Click **Restore** to restore all the settings in advanced configuration to the factory default.

10.4.4 Set Shield Region

The shield region allows you to set the specific region in which the set smart function rule is invalid.

Steps

1. Select **Shield Region**.
2. Click  to draw shield region. Repeat this step above to set more shield regions.
3. **Optional:** Select and click on the drawn region, then click  to delete the selected drawn region.
4. **Optional:** Click  to delete all drawn regions.
5. Click **Save**.

10.5 People Management

People management is used to detect and analyze people number and changes in a predefined region. It can be applied to the entrances and exits, supermarkets, etc.



Note

- For certain device models, you need to enable **People Management** on **VCA** page first.
 - The function is only supported by certain device models.
-

10.5.1 Regional People Counting

It counts people in a predefined area and detects people number changes and crowded situation. When the people number exception or waiting time exception occurs, the device can trigger an alarm.

Refer to **Set People Density** to set people density detection.

Refer to **Set People Exception Detection** to set people exception detection.

Refer to **Waiting Time Exception Detection** to set waiting time exception detection.

Set People Density

This function detects the level of people density in the set rule region.

Before You Start

- Go to **VCA → Select Application**, select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule**.
2. Click **Add** to add a rule and set its name.
3. Set a rule.

+ Add

Rule 1 ×

*Rule Name Rule 1

*Alarm Interval 5 sec

*First Alarm Delay 5 sec

Alarm Times Per Exception ☒

*Alarm Times 1

People Number OSD ☒

Figure 10-11 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.



Note

People density alarm does not support **Alarm Times Per Exception**, **Alarm Interval** and **First Alarm Delay** settings.

- Click  to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.



Note

- Up to 8 regions can be set at the same time.
 - Try not to overlap the regions.
- Check **People Density Alarm** to enable the function.

People Density Alarm

① People Density Alarm ☒

Upload Type

Scheduled Uploading ☒

Statistics Cycle

People Quantity Change Upload ☐

Congestion Level Upload ☐

Density Level

Level	Number of...	Custom Name
1		
2		
3		

Figure 10-12 People Density Alarm

Scheduled Uploading

The device uploads people density information within the set statistics cycle.

People Quantity Change Upload

The device uploads the people quantity change information if there is any change in the set rule region.

Congestion Level Upload

The device uploads the congestion information when there is any change of congestion level in the set rule region.

Density Level

Number of People

The range for each level by inputting the lower limit of the number of people in the set rule region.

Custom Name

The name of the level.



Note

- Set the **Number of People** before the **Custom Name**.
- Up to three levels can be configured. The density increases from level 1 to level 3.

6. Set arming schedule. See [Set Arming Schedule](#) .

7. Set linkage method. See [Linkage Method Settings](#) .

8. Click **Save**.

9. **Optional:** Set text overlay. For detailed settings, refer to [Overlay and Capture](#) .
10. **Optional:** View version and set filtering condition. For detailed settings, refer to [Advanced Settings](#) .

Set People Exception Detection

This function detects the number of people in the set rule region and an alarm is triggered when the situation meets the alarm-triggering condition.

Before You Start

- Go to **VCA → Select Application** , select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

- Go to **VCA → Set Application → People Management → Regional People Counting → Rule** .
- Click **Add** to add a rule and set its name.
- Set a rule.

The screenshot shows the 'Set Rules' configuration interface. At the top, there is a dashed box with a '+ Add' button. Below it, a red box highlights 'Rule 1' with a close icon. The configuration fields are as follows:

- * Rule Name: Rule 1
- * Alarm Interval: 5 sec
- * First Alarm Delay: 5 sec
- Alarm Times Per Exception: ☒
- * Alarm Times: 1
- People Number OSD: ☒

Figure 10-13 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Alarm Times Per Exception

It refers to the alarm times after an alarm is triggered. If you do not check it and set the times, the device will keep sending alarms.

Alarm Interval

Within the set **Alarm Interval**, the same alarm will not be uploaded.

First Alarm Delay

When the first alarm is triggered, the alarm will be uploaded after a set time period.

- Click  to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.



Note

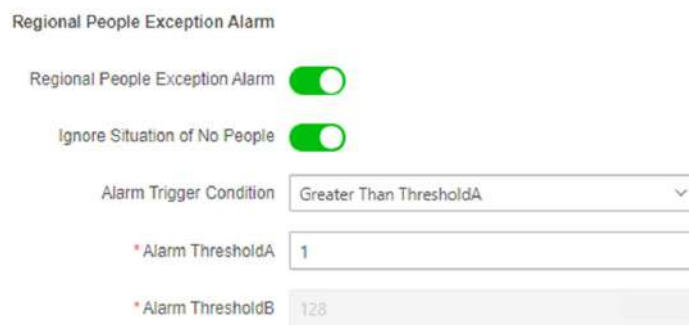
- Up to 8 regions can be set at the same time.
- Try not to overlap the regions.

- Check **Regional People Exception Alarm**, and set **Alarm Trigger Condition** and **Alarm Threshold**.



Note

- After enabling **Ignore Situation of No People**, the device will not trigger an alarm when there is no people in the region.
 - This function can filter the potential alarm condition under which the value is less than the set **Alarm Threshold** and no people in the region.
-



Regional People Exception Alarm

Regional People Exception Alarm ☒

Ignore Situation of No People ☒

Alarm Trigger Condition Greater Than ThresholdA

* Alarm ThresholdA

* Alarm ThresholdB

Figure 10-14 Regional People Exception Alarm

- Set arming schedule. See [Set Arming Schedule](#) .
- Set linkage method. See [Linkage Method Settings](#) .
- Click **Save**.
- Optional:** Set text overlay. For detailed settings, refer to [Overlay and Capture](#) .
- Optional:** View version and set filtering condition. For detailed settings, refer to [Advanced Settings](#) .

Waiting Time Exception Detection

This function detects the waiting time of the set rule region and an alarm is triggered when the waiting time meets the alarm-triggering condition.

Before You Start

- Go to **VCA → Select Application** , select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule** .
2. Click **Add** to add a rule and set its name.
3. Set a rule.

+ Add

Rule 1 ×

*Rule Name Rule 1

*Alarm Interval 5 sec

*First Alarm Delay 5 sec

Alarm Times Per Exception ☒

*Alarm Times 1

People Number OSD ☒

Figure 10-15 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Alarm Times Per Exception

It refers to the alarm times after an alarm is triggered. If you do not check it and set the times, the device will keep sending alarms.

Alarm Interval

Within the set **Alarm Interval**, the same alarm will not be uploaded.

First Alarm Delay

When the first alarm is triggered, the alarm will be uploaded after a set time period.



Note

Dwell time exception alarm supports **Alarm Times Per Exception**, **Alarm Interval** and **First Alarm Delay** settings only on the condition that the **Alarm Trigger Condition** is **Greater Than Threshold A**.

- Click  to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.



Note

- Up to 8 regions can be set at the same time.
- Try not to overlap the regions.

- Check **Dwell Time Exception Alarm**, and set **Alarm Trigger Condition** and **Alarm Threshold**.

Dwell Time Exception Alarm

 Dwell Time Exception Alarm ☒

Alarm Trigger Condition Greater Than ThresholdA 

* Alarm ThresholdA 300 sec

* Alarm ThresholdB 3600 sec

Figure 10-16 Dwell Time Exception Alarm

- Set arming schedule. See [Set Arming Schedule](#) .
- Set linkage method. See [Linkage Method Settings](#) .
- Click **Save**.
- Optional:** Set text overlay. For detailed settings, refer to [Overlay and Capture](#) .
- Optional:** View version and set filtering condition. For detailed settings, refer to [Advanced Settings](#) .

10.5.2 Overlay and Capture

Go to **VCA → People Management → Overlay & Capture** . Check the information you want to overlay on the captured pictures. You can also click   to adjust the order.

10.5.3 Advanced Settings

Set the advanced parameters for people management function and click **Save**.

Version

It stands for the current algorithm version.

Algorithm Mode

Select a mode according to the installation scene.

Filter

Target Size

It stands for the size of the target detection window. A target larger than this pixel can be counted as a real target. It can remove the false alarm of a certain fixed target.

Displacement

It stands for target displacement or the target width. A target will not be counted if its displacement is less than the set percentage.

Min. Waiting Duration

Waiting time shorter than the set value will be filtered.

Confidence

The higher the threshold is, the more difficult a target will be detected, but the higher the accuracy is.



Note

The filtering settings should be operated by the professionals. The filter settings can adjust the algorithm for detection to change the detection range, sensitivity, etc.

10.6 People Counting

People counting is used to calculate the number of people entering or exiting an area.



Note

- For certain device models, you need to enable **People Counting** on **VCA** page first.
 - The function is only supported by certain device models.
-

10.6.1 Set People Counting Rule

After setting the detection rules and algorithm parameters, the device calculates the number of people entering or exiting in the rule area, triggers linkage actions and uploads data automatically.

Before You Start

- Go to **VCA** and select the application. Select **People Counting** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Counting**.

Steps

1. Go to **VCA** → **Set Application** → **People Counting** → **Rule** .
2. Check **Enable** to enable the function.
3. Click **Add** to add a detection area.
4. Click  to draw the polygon detection area (count area). Left-click end-points in the live view window, and right-click to finish the drawing.
5. Click  to draw the detection line. The arrow shows entering direction, you can click  to change the direction.



Note

In order to improve the counting accuracy, please draw the detection area according to the following rules.

- The detection area needs to cover the people entering and exiting access.
- The detection line must be completely contained within the red detection area and perpendicular to the path of the person passing through.

6. **Optional:** Adjust the detection area and detection line.

Click  Clear the selected detection area or line.

Click  Clear all detection areas and lines.

7. **Optional:** Repeat the above steps to draw up to 3 detection areas and corresponding detection lines.

8. Set people counting parameters.

OSD Overlay Content

Select the counting data type to be displayed in the live view image from the drop-down list, and adjust the display position of people counting data in the live view image.



Note

OSD overlay only counts the number of the person on the current day. The data will be cleared automatically when the device restarts or at the daily reset time.

Daily Reset Time

The device clears the data in 00:00 each day by default. You can select a time point through the drop-down list. After selecting, the counting data will be automatically cleared at this time point every day.

You can click **Manual Reset** to manually trigger a data reset and clear the current people counting data.

9. Click **Save**.

10. Set arming schedule. See [Set Arming Schedule](#) .

11. Set linkage method. See [Linkage Method Settings](#) .

12. Click **Save**.

13. **Optional:** Set people counting data uploading parameters.

Click **Data Upload** to enter the interface. Click **Save** after finishing the settings.

Real-Time Data Uploading

Send the real-time data to the platform.

Upload Data Periodically

Set the **Data Statistics Cycle**, and the passenger flow counting data will be uploaded to the platform at intervals according to the **Data Statistics Cycle**.

14. **Optional:** Set people counting advanced parameters.

Click **Advanced** to enter the interface. Click **Save** after finishing the settings.

Version

It stands for the current algorithm version.

Clear Storage Data

Clear all people counting data stored in the device. This function must be used with caution.

Result

- If the target crosses the detection area along the entering direction and crosses the detection line, then it is counted as the entering number.
- If the target crosses the detection area along the exiting direction and crosses the detection line, then it is counted as the exiting number.

10.7 Road Traffic

Vehicle Detection and Mixed-Traffic Detection are available for the road traffic monitoring. The device captures the passing motor vehicles and non-motor vehicles and uploads the relevant information together with the captured pictures.



Note

- For certain device models, you need to select **Road Traffic** on **VCA** page first.
 - The function is only supported by certain device models.
-

10.7.1 Set Vehicle Detection

The vehicles that enter the set lane can be detected and the picture of the vehicle and its license plate can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

- Go to **VCA** and select the application. Select **Road Traffic** and click **Next** to enable the function.
- Make sure the device is installed properly.
- Make sure the image parameters are properly configured.
- Make sure the captured license plate picture is clear enough.

Steps

1. Go to **VCA** → **Set Application** → **Road Traffic** → **Rule** , and select **Vehicle Detection** as detection type.
2. Check **Enable**.
3. Select the operating mode.

Entrance/Exit

The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in the entrance/exit.

City Street

The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in the city street.

Alarm Input

It means the input alarm will trigger a license plate capture and recognition action.



Note

- When **Alarm Input** is selected, the alarm input A<-1 will automatically be assigned to trigger vehicle detection and its alarm type is always NO.
- If the A<-1 alarm input is used to trigger vehicle detection, it cannot be used for other basic events.
- When **Alarm Input** is selected and saved, previously configured linkage method for A<-1 will be canceled.

4. Select the total number of lanes.

5. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.

The blue detection line is the trigger line of the license plate, which is mainly used in the **Entrance/Exit** scene to improve the capture efficiency. It is recommended to put it in the lower middle of the screen to make sure that the full-size car with the plate can pass it.

6. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.



Note

Only 1 license plate can be captured at one time for each lane.

7. Select **Area** and **Country/Region**.

8. Set the detection mode.

Vehicle Priority

The device will detect the vehicle scale first, then catch the plate out to make the analysis. It will get the better accuracy but sometimes it will lose some results in the not-satisfied installation scenario.

License Plate & Vehicle

In license plate & vehicle mode, the device detects license plate and vehicle simultaneously and it uploads the alarm information and the captured pictures.



Note

It is recommended to select **Vehicle Priority** mode if there are no issues on installation and supplement light. After the issues of plate recognition are carried out, you can switch the mode to **License Plate & Vehicle** mode.

9. Check **Remove Duplicated License Plates** and set the **Time Interval**. The default time interval is 4 minutes.

10. Click **Save**.

11. Go to **Arming Schedule and Linkage Method**. You can set the arming schedule and linkage method independently for blocklist, allowlist and other list, and you should set them one by one.

Target Type **Blocklist** Allowlist Others

Arming Schedule

Arming Schedule **Edit**

Linkage Method

Direction ☒ All ☐ Forward ☐ Reverse

Notify Surveillance ... ☒

Upload to FTP/Mem... ☒

Trigger Alarm Output ☒ Select All

☒ A->1 ☒ A->2

Save

Figure 10-17 Arming Schedule and Linkage Method

- 1) Click to select the blocklist, allowlist and other list.
- 2) Set the arming schedule. Refer to [***Set Arming Schedule***](#) for details.
- 3) Set the linkage method. Check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

Direction

Only the vehicles moving as the selected direction can trigger the selected linkage methods.

All

All means that the vehicles in all moving directions will be considered. It is highly recommended to choose **All** if there is no special use.

Forward

Forward means that the vehicle moves toward the camera.

Reverse

Reverse means that the vehicle moves away from the camera.

Wiegand Linkage

The device can send reports to the third-party platform via the Wiegand protocol. Make sure the device supports Wiegand interface and the device is connected by Wiegand interface carefully.

Make sure the Wiegand is enabled and the protocol is properly configured in the system settings. Refer to **Wiegand** for details.

Enable **Wiegand Linkage** and select the wiegand interface connected to the external device.

The linkage will be triggered only when the detected vehicle driving direction is the same as the configured direction.

12. Go to **Road Traffic → Overlay & Capture** to set the image parameters and text overlay of the captured pictures. Refer to **Overlay and Capture** for details.
13. Import or export the license plate blocklist and allowlist. Refer to **Import or Export Blocklist & Allowlist** for details.

10.7.2 Set Mixed-Traffic Detection Rule

The motor vehicles and non-motor vehicles that enter the set lane can be detected, and the picture of targets can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

- Go to **VCA** and select the application. Select **Road Traffic** and click **Next** to enable the function.
- Make sure the device is installed properly.
- Make sure the image parameters are properly configured.

Steps

1. Go to **VCA → Set Application → Road Traffic → Rule** , and select **Mixed-traffic Detection** as detection type.
2. Check **Enable**.
3. Select the total number of lanes.
4. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.

The blue detection line is the trigger line of the license plate, which is mainly used in the **Entrance/Exit** scene to improve the capture efficiency. It is recommended to put it in the lower middle of the screen to make sure that the full-size car with the plate can pass it.

5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.



Note

Only 1 license plate can be captured at one time for each lane.

-
6. Select **Area** and **Country/Region**.
 7. Check **Remove Duplicated License Plates** and set the **Time Interval**. The default time interval is 4 minutes.
 8. Click **Save**.

9. Go to **Arming Schedule and Linkage Method**. You can set the arming schedule and linkage method independently for blocklist, allowlist and other list, and you should set them one by one.

Target Type ☒ Blocklist ☐ Allowlist ☐ Others

Arming Schedule

Arming Schedule

Linkage Method

Direction ☒ All ☐ Forward ☐ Reverse

Notify Surveillance ... ☒

Upload to FTP/Mem... ☒

Trigger Alarm Output ☒ Select All

☒ A->1 ☒ A->2

Figure 10-18 Arming Schedule and Linkage Method

- 1) Click to select the blocklist, allowlist and other list.
- 2) Set the arming schedule. Refer to **Set Arming Schedule** for details.
- 3) Set the linkage method. Check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

Direction

Only the vehicles moving as the selected direction can trigger the selected linkage methods.

All

All means that the vehicles in all moving directions will be considered. It is highly recommended to choose **All** if there is no special use.

Forward

Forward means that the vehicle moves toward the camera.

Reverse

Reverse means that the vehicle moves away from the camera.

Wiegand Linkage

The device can send reports to the third-party platform via the Wiegand protocol.

Make sure the device supports Wiegand interface and the device is connected by Wiegand interface carefully.

Make sure the Wiegand is enabled and the protocol is properly configured in the system settings. Refer to **Wiegand** for details.

Enable **Wiegand Linkage** and select the wiegand interface connected to the external device.

The linkage will be triggered only when the detected vehicle driving direction is the same as the configured direction.

10. Go to **Road Traffic → Overlay & Capture** to set the image parameters and text overlay of the captured pictures. Refer to **Overlay and Capture** for details.
11. Import or export the license plate blocklist and allowlist. Refer to **Import or Export Blocklist & Allowlist** for details.

10.7.3 Overlay and Capture

You can set the image parameters of the captured images in vehicle detection and mixed-traffic detection.

Go to **VCA** and select **Road Traffic**.

Go to **VCA → Set Application → Road Traffic → Overlay & Capture** .



Note

The function varies according to different device models.

Picture Type ☒ License Plate/Target Close-up ☐ Vehicle ☒ Background

Picture Quality

Restriction Type ☒ Picture Quality ☐ Picture Size

Picture Quality 80

* Picture Size 1024 Kb

Picture Resolution 2560*1440

FTP Host

FTP Picture Name ☒ Default ☐ Custom

Picture Name IP_Channel No_Time_Type.jpg

Text Overlay

Text Overlay ☒

Font Color

Background Color

Text Overlay

Text Overlay	To Be Selected	Selected
	☐ Type	☐ Type Sort

Save

Figure 10-19 Overlay & Capture

Picture Quality

The larger the value is, the clearer the picture is, but larger storage space is also required.

Picture Size

The larger the value is, the larger the storage space is needed. And the level of network transmission requirement is also higher.

Picture Resolution

The captured background picture resolution.

Picture Capture Interval

The camera supports continuously trigger the alarm and upload captured picture each interval.

Check **Capture Interval** and set the interval.

FTP Picture Name

You can set the naming rule for captured pictures in vehicle detection and mixed-traffic detection in the FTP server.

Select **Default** to use the default rule.

Select **Custom**, select information for the picture name, and click   to adjust the order of picture name parameters. If **Capture Time** is not selected in custom mode, the captured picture triggered by the same vehicle later will replace the captured picture before due to the same picture name.



Note

For more information about FTP settings, refer to [**Set FTP**](#).

Text Overlay

You can overlay camera, device or vehicle information on the captured image and click   to adjust the order of overlay texts.

Set the font color and background color by selecting the color box, and click the desired color in the pop-up palette or the drop-down box.

10.7.4 Import or Export Blocklist & Allowlist

You can import and export the blocklist and allowlist as desired, and check the list content in this interface.

Steps

1. Click **Import** to import the selected file.
2. Click  to open the PC local directory.
3. Find the blocklist & allowlist file and click to select it. Click **Open** to confirm.



Note

- The file to import should corresponds with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.
- The file should be in the .xls format and the cell format should be Text.

-
4. Click **Import** to import the selected file.
 5. Click **Export All** to export the license plate list.
 6. **Optional:** Click **Add** to add a license plate and set its related information one by one.
 7. **Optional:** Click  to select the filtering type. **All Types**, **Wiegand CardID**, **License Plate No.** and **Type** are selectable. As for **Type**, you can select **Keywords** to define the specific filtering type. Click **Search** to view the results.
 8. **Optional:** You can select a plate No. and click  to delete a plate from the blocklist or allowlist.
 9. **Optional:** You can select a plate No. and click  to edit the related information of the license plate from the blocklist or allowlist.

10.7.5 Advanced Parameters Configuration

Go to **VCA** and select the application. Enter the application configuration interface and click **Advanced** to set advanced parameters. Click **Save** after finishing the configuration.



Note

The function varies according to different device models.

Version

It stands for the current algorithm version.

Overlay Intelligent Information

Overlay the related intelligent information or POS information in the video.

10.8 AI Open Platform

AI Open Platform is to generate a model library based on the training material provided by the user, then load the model library into the device and allow user to configure tasks and rules. When a target in the scene is detected to trigger the rules, the device can take linkage actions, which can realize personalized smart applications.



Note

- The function is only supported by certain device models.
 - For certain device models, you need to enable **AI Open Platform** on **VCA** page first.
-

10.8.1 Set AI Open Platform

Steps

1. Go to **VCA → Set Application → AI Open Platform** .



Note

- Specific smart functions are supported for configuration via the AI Open Platform, such as hard hat detection, coal mine safety detection, etc.
 - After selecting a specific function, the device will load the model package of the corresponding function.
 - The function varies according to different device models, please refer to the actual device.
-
- For **Hard Hat Detection**, it detects targets in the set detection area who do not wear the hard hat and triggers an alarm.
 - For **Coal Mine Safety Detection**, you should go to **VCA → Set Application → Coal Mine Safety Management** and enable the function. In coal mine scenarios, it detects targets such as persons and mine cars in the detection area, detects if the belt deviates from the idlers, and if

the person not wears a hard hat. It triggers an alarm according to the set rules for coal mine safety detection.

2. **Optional:** Add a model into **Model Library**. Select the **Model Library** and related **Label File** from the local path, then set the **Model Name**. The model types are as follows.

Detection Model

Detects a specific target in the live view and provides the detection result and coordinate position of the target.

Classification Model

Classifies pictures or targets with attributes.

Mixed Model

Detects targets in the live view and classifies them.



Note

Max. Number of Model Packages refers to the maximum number of model packages that the device supports.

3. Select a model and enable it.

4. Select an **Analysis Mode**.

Live Video Analysis	The device analyzes the live video to realize target detection and result uploading.

Scheduled Capture Analysis	The device captures based on the set Auto-Switch Interval to analyze the captured picture and upload results.

5. **Optional:** Enable **Overlay Target Frame** and **Rule Overlay** according to your needs.

Overlay Target Frame	Overlay the alarm picture with target frame.

Rule Overlay	Overlay the alarm picture with rule information.

6. Set the arming schedule and linkage method. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .

7. Set rules for the linked channel. Refer to **Set Rules** for details.

8. Click **Save**.

10.8.2 Set Rules

Set rules for the linked channel.

Before You Start

Make sure the related model in **VCA → AI Open Platform** is selected, and the task configuration is finished.

Steps

1. Click **Linked Channel** to select a channel in **Channel Management**.
2. Click  of the linked channel to set rules.

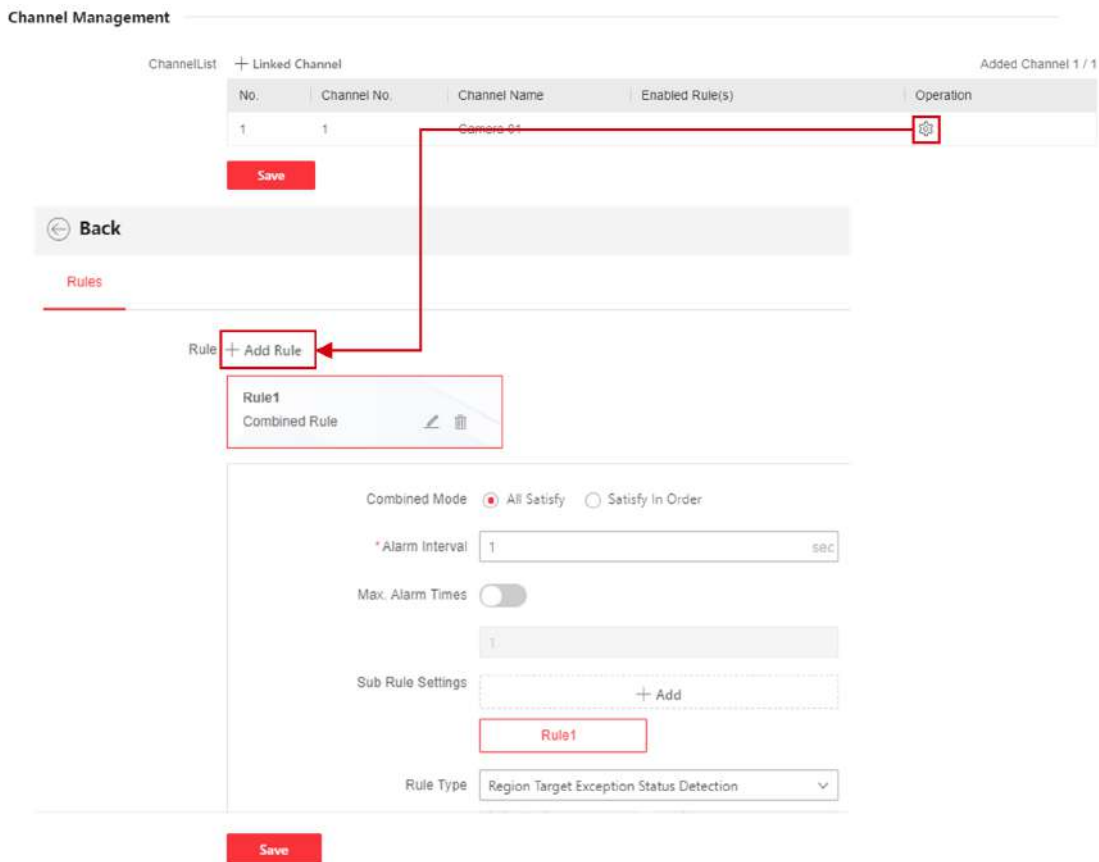


Figure 10-20 Set Rules

3. Click **Add Rule**. Select the rule and click  to rename the rule and select the rule type.

Region Target Exception Status Detection

Detects and counts the number of the target in the predefined virtual rule area, and compares it with the setting rule. When satisfying the triggering condition, it will trigger the alarm.

Line Crossing Target Detection

Detects if any targets crossing the predefined virtual rule line and triggers the alarm when detects.

Full Analysis Rule

Detects and analyzes all targets in the predefined virtual rule area.

Line Crossing Target Counting

Detects and counts the number of the target crossing the predefined virtual rule line.

Region Target Number Counting

Detects and counts the number of the target in the predefined virtual rule area.

Combined Rule

Supports **Region Target Exception Status Detection** and **Line Crossing Target Detection** in the predefined virtual rule area. You can set **Combined Mode** as **All Satisfy** or **Satisfy In Order** for the detection order.



Note

Rule types vary according to different model packages, please refer to the actual device.

4. Set the detection rule and draw rule area or line.
 - Draw a rule area: click  to draw a convex area in the live view window, left click the end-points in the live view window to define the boundary of the set rule area, and right click to finish drawing.
 - Draw a rule line: click  and a line with an arrow appears in the live video. Drag the line to the location in the live view window as desired.
5. Set rule parameters.

Object

The detection target type of the model.

Attribute

The detection target property of the model.

Duration

The duration of the status. The alarm will be triggered when the set time duration is reached.

Alarm Interval

During the set alarm interval, alarms of the same type only trigger one notification.

Sensitivity

The higher the value of sensitivity is, the easier the alarm can be triggered. If the sensitivity value is too large, the false alarm may be produced easier. Please set it according to the actual situation.

Max. Alarm Times

The maximum number of times an alarm can be triggered in the status that triggers the alarm.

Counting Interval

The time interval for counting.

Algorithm Validity

When the confidence threshold given by the algorithm is greater than or equal to the set validity, an alarm is triggered and uploaded.

Line Crossing

The direction from which the target goes across the line.

Quantity

Check **Quantity** and select the alarm rule from the drop-down box. Set **Threshold** or the range (**Min** and **Max**) according to the alarm rule. When the number of the target satisfies the setting alarm rule, the device will trigger the alarm.

Report Time Interval

It refers to the time interval for uploading the counting results when selecting **Region Target Number Counting**.



Note

Rule parameters vary according to different rules, please refer to the actual device.

6. Click **Save**.

Chapter 11 EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement. If you want to use the EPTZ function, make sure your device supports the **Third Stream**. Third stream and EPTZ should be both enabled simultaneously.



Note

The function is only supported by certain device models.

11.1 Patrol

Steps

1. Go to **Configuration** → **EPTZ**.
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Patrol** in **Application Mode**.
5. Click **Save**.

What to do next

For the detailed information about the patrol settings, see the PTZ operations on live view page.

11.2 Auto-Tracking

Steps

1. Go to **Configuration** → **EPTZ**.
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Auto-tracking** in **Application Mode**.
5. Click  to start drawing. Click on the live view video to specify the four vertexes of the detection area, and right click to complete drawing.
6. Set rules.

Detection Target

Human and vehicle are available. If the detection target is not selected, all the detected targets will be tracked, including the human and vehicle.



Note

Only certain camera models support this function.

Sensitivity

It stands for the percentage of the body part of an acceptable target that is tracked.

$\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that enters the pre-defined area. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the target can be tracked.

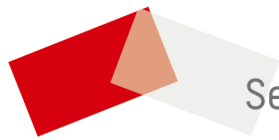
7. Click **Save**.

Appendix A. FAQ

Scan the following QR code to find the frequently asked questions of the device.

Note that some frequently asked questions only apply to certain models.





See Far, Go Further

DS-2CD3666G2T-IZS(Y)-M 6 MP AcuSense IR Varifocal Bullet Network Camera

AcuSense

Powered by

DarkFighter



Empowered by deep learning algorithms, Hikvision AcuSense technology brings human and vehicle targets classification alarms to front- and back-end devices. The system focuses on human and vehicle targets, vastly improving alarm efficiency and effectiveness.

Hikvision has been dedicated to develop products with security since established. Hikvision always follows security by design principle and has adopted many methods of security technologies into our product development lifecycle, including terminal security, data security, application security, network security, and privacy protection. In the meantime, the security technologies used by Hikvision are all in compliance with local applicable laws and safety regulations. These security measures could enhance product's cyber security protection capability and protect your devices as well as your data from malicious cyber attacks.

- Supports Hikvision Embedded Open Platform (HEOP) and importing third party applications
- Supports 1.5 Tops computing power, 40 MB system memory, 350 MB smart RAM, and 2 GB eMMC storage for sharing resources
- High quality imaging with 6 MP resolution
- Excellent low-light performance with powered-by-DarkFighter technology
- Clear imaging against strong back light due to 120 dB true WDR technology
- Efficient H.265+ compression technology
- False alarm reduction through human and vehicle target classification based on deep learning
- Audio and alarm interface available
- 3D DNR technology delivers clean and sharp images
- Motorized varifocal lens for easy installation
- Water and dust resistant (IP67) and vandal-resistant (IK10)

▪ Specification

Camera	
Image Sensor	1/2.4" Progressive Scan CMOS
Max. Resolution	3200 × 1800
Min. Illumination	Color: 0.003 Lux @ (F1.6, AGC ON),B/W: 0 Lux with IR
Shutter Time	1/3 s to 1/100,000 s
Day & Night	IR cut filter
Angle Adjustment	Pan: 0° to 355°,tilt: 0° to 90°,rotate: 0° to 360°
Lens	
Lens Type	Varifocal lens, motorized lens, 2.7 to 13.5 mm and 7 to 35 mm optional
Focal Length & FOV	2.7 to 13.5 mm: horizontal FOV 106° to 35.6°, vertical FOV 55.9° to 20°, diagonal FOV 127.4° to 40.8° 7 to 35 mm: horizontal FOV 34.4° to 12.5°, vertical FOV 19° to 7.1°, diagonal FOV 39.8° to 14.3°
Lens Mount	2.7 to 13.5 mm: Ø14; 7 to 35 mm: Integrated
Focus	Auto,Semi-auto,Manual
Iris Type	Auto-iris
Aperture	2.7 to 13.5 mm: F1.6; 7 to 35 mm: F1.6
DORI	
DORI	2.7 to 13.5 mm: D: 68 to 200 m, O: 27 to 79 m, R: 13 to 40 m, I: 6 to 20 m 7 to 35 mm: D: 218 to 580 m, O: 86 to 230 m, R: 43 to 116 m, I: 21 to 58 m
Illuminator	
Supplement Light Type	IR
Supplement Light Range	2.7 to 13.5 mm: up to 60 m; 7 to 35 mm: up to 80 m
Smart Supplement Light	Yes
IR Wavelength	850 nm
HEOP	
Open Resources	Memory: 40 MB, Smart RAM: 350 MB, eMMC: 2 GB
Computing Power	1.5 TOPS
Open Capability	HEOP 2.0 OpendevSDK
Deep Learning Structure	Caffe,PyTorch,TensorFlow,PaddlePaddle, ONNX
Programming Language	C,C++
Video	
Main Stream	50 Hz: 20 fps (3200 × 1800) 25 fps (2688 × 1520, 1920 × 1080, 1280 × 720) 60 Hz: 20 fps (3200 × 1800) 30 fps (2688 × 1520, 1920 × 1080, 1280 × 720)
Sub-Stream	50 Hz: 25 fps (1280 × 720, 640 × 480, 640 × 360) 60 Hz: 30 fps (1280 × 720, 640 × 480, 640 × 360)
Third Stream	50 Hz: 10 fps (1920 × 1080, 1280 × 720, 640 × 480, 640 × 360) 60 Hz: 10 fps (1920 × 1080, 1280 × 720, 640 × 480, 640 × 360)

Fourth Stream	50 Hz: 10 fps (1280 × 720, 640 × 480, 640 × 360) 60 Hz: 10 fps (1280 × 720, 640 × 480, 640 × 360)
Video Compression	Main stream: H.265/H.264/H.264+/H.265+, Sub-stream: H.265/H.264/MJPEG, Third stream: H.265/H.264, Fourth stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 16 Mbps
H.264 Type	Baseline Profile, Main Profile, High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR, VBR
Scalable Video Coding (SVC)	H.264 and H.265 encoding
Region of Interest (ROI)	5 fixed regions for main stream and sub-stream
Target Cropping	Yes
Audio	
Audio Compression	G.711/G.722.1/G.726/MP2L2/PCM/MP3/AAC-LC
Audio Bit Rate	64 Kbps (G.711ulaw/G.711alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 192 Kbps (MP2L2)/8 to 320 Kbps (MP3)/16 to 64 Kbps (AAC-LC)
Audio Sampling Rate	8 kHz/16 kHz/32 kHz/44.1 kHz/48 kHz
Environment Noise Filtering	Yes
Network	
Protocols	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, NTP, UPnP, SMTP, IGMP, 802.1X, QoS, IPv4, IPv6, UDP, Bonjour, SSL/TLS, PPPoE, SFTP, ARP, SNMP, WebSocket, WebSockets, SRTP
Simultaneous Live View	Up to 6 channels
API	ONVIF (Profile S, Profile G, Profile T), ISAPI, SDK, ISUP
User/Host	Up to 32 users 3 user levels: administrator, operator, and user
Security	Password protection, complicated password, secure boot, HTTPS encryption, 802.1X authentication (EAP-TLS, EAP-LEAP, EAP-MD5), watermark, brute force protection, IP address filter, firmware protection, basic and digest authentication for HTTP/HTTPS, WSSE and digest authentication for Open Network Video Interface, RTP/RTSP over HTTPS, end-to-end protection, control timeout settings, security audit log, TLS 1.1/1.2/1.3, host authentication (MAC address).
Network Storage	NAS (NFS, SMB/CIFS), Auto Network Replenishment (ANR), Together with high-end Hikvision memory card, memory card encryption and health detection are supported.
Client	iVMS-4200, Hik-Connect, Hik-Central
Web Browser	Plug-in required live view: IE 10, IE 11, Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Edge 89+, Local service: Chrome 57.0+, Firefox 52.0+, Edge 89+
Image	
Image Parameters Switch	Yes
Image Settings	Rotate mode, saturation, brightness, contrast, sharpness, gain, white balance, adjustable by client software or web browser
Day/Night Switch	Day, Night, Auto, Schedule
Wide Dynamic Range (WDR)	120 dB

Image Enhancement	BLC,HLC,3D DNR,Defog
SNR	≥ 52 dB
Privacy Mask	4 programmable polygon privacy masks
Interface	
Ethernet Interface	1 RJ45 10 M/100 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 512 GB
Audio	1 input (line in), two-core terminal block, max. input amplitude: 3.3 Vpp, input impedance: 4.7 KΩ, interface type: non-equilibrium, 1 output (line out), two-core terminal block, max. output amplitude: 3.3 Vpp, output impedance: 100 Ω, interface type: non-equilibrium
Alarm	2 inputs, 2 outputs (max. 24 VDC/24 VAC, 1 A)
Reset Key	Yes
Power Output	12 VDC, max. 100 mA
Event	
Basic Event	Motion detection (support alarm triggering by specified target types (human and vehicle)),video tampering alarm,exception
Smart Event	scene change detection,audio exception detection,defocus detection, unattended baggage detection,object removal detection
Linkage	Upload to FTP/NAS/memory card,notify surveillance center,send email,trigger alarm output,trigger recording,trigger capture,audible warning
Deep Learning Function	
Perimeter Protection	Line crossing, intrusion, region entrance, region exiting Support alarm triggering by specified target types (human and vehicle)
Face Capture	Yes
People Counting	Yes (Can be as People Gathering Detection)
General	
Power	12 VDC ± 25%, 1.08 A, max. 13 W,Ø5.5 mm coaxial power plug,reverse polarity protection, PoE: IEEE 802.3at, Class 4, max. 15 W
Material	Aluminum alloy body
Dimension	Ø105 mm × 332.8 mm (Ø4.1" × 13.1")
Package Dimension	385 mm × 190 mm × 180 mm (15.2" × 7.5" × 7.1")
Weight	Approx. 1475 g (2.9 lb.)
With Package Weight	Approx. 2276 g (4.8 lb.)
Storage Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
General Function	Heartbeat,anti-banding,mirror,flash log,password reset via email,pixel counter
Language	33 languages: English, Russian, Estonian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Danish, Swedish, Norwegian, Finnish, Croatian, Slovenian, Serbian, Turkish, Korean, Traditional Chinese, Thai, Vietnamese, Japanese, Latvian, Lithuanian, Portuguese (Brazil), Ukrainian

Approval	
EMC	FCC: 47 CFR Part 15, Subpart B, CE-EMC: EN 55032: 2015, EN 61000-3-2:2019, EN 61000-3-3: 2013+A1:2019, EN 50130-4: 2011 +A1: 2014, RCM: AS/NZS CISPR 32: 2015, IC: ICES-003: Issue 7, KC: KN32: 2015, KN35: 2015
Safety	UL: UL 62368-1, CB: IEC 62368-1: 2014+A11, CE-LVD: EN 62368-1: 2014/A11: 2017, BIS: IS 13252 (Part 1): 2010/IEC 60950-1: 2005, LOA: IEC/EN 60950-1
Environment	CE-RoHS: 2011/65/EU, WEEE: 2012/19/EU, Reach: Regulation (EC) No 1907/2006
Protection	IP67: IEC 60529-2013,IK10: IEC 62262:2002
Anti-Corrosion Protection	-Y: NEMA 4X (NEMA 250-2018)

▪ Typical Application

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

With -Y model: This model has MODERATE PROTECTION.

Without -Y model: This model has NO SPECIFIC PROTECTION.

Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ Available Model

DS-2CD3666G2T-IZS(2.7-13.5mm)(H)

DS-2CD3666G2T-IZS(7-35mm)(H)

DS-2CD3666G2T-IZS-M(2.7-13.5mm)(H)

DS-2CD3666G2T-IZS-M(7-35mm)(H)

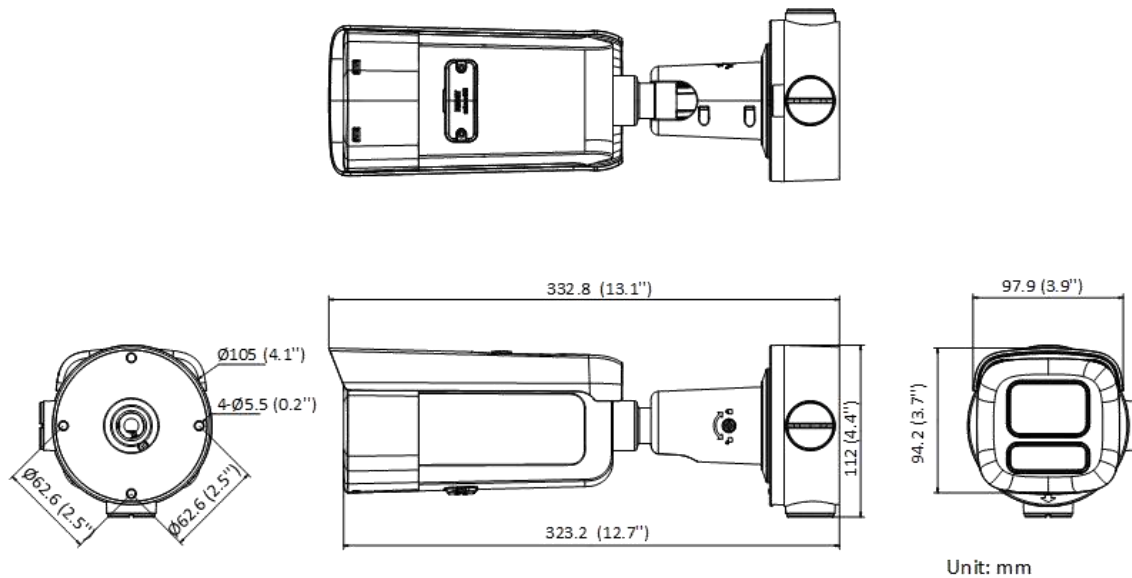
DS-2CD3666G2T-IZSY(2.7-13.5mm)(H)

DS-2CD3666G2T-IZSY(7-35mm)(H)

DS-2CD3666G2T-IZSY-M(2.7-13.5mm)(H)

DS-2CD3666G2T-IZSY-M(7-35mm)(H)

Dimension



Accessory

Included

DS-1260ZJ

Junction box



Optional

DS-1275ZJ-SUS Vertical pole mount	DS-1276ZJ-SUS Corner mount	DS-1275ZJ-S-SUS Vertical pole mount

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com



Follow us on social media to get the latest product and solution information.



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



Hikvision
Corporate Channel



hikvisionhq

HS-TF-L2

Introduction

Hikvision L2 Micro SD (TF) Card for surveillance, specially designed for video surveillance recording, with a read and write speed of Class 10 and above; using TLC storage medium, with strong compatibility and lower price, it can be widely used in light storage, backup storage and other recordings Scenarios with low intensity or relatively simple usage environment



Features

- **Cost-effective**

Compared with the same TLC material in the market, the price of farmland can fully meet the needs of light storage level with low video intensity and relatively simple usage scenarios.

- **Strong compatibility**

Better compatibility, optimized according to Hikvision storage system, compatible with covering more products, and used with Hikvision products, the effect is better

- **Adaptable**

Waterproof, shockproof, X-ray proof, high and low temperature resistant, can be widely adapted to various working environments

- **S.M.A.R.T. Mechanism**

Unique functions of life forewarning and health monitoring when used with Hikvision cameras. It can calculate the remaining available time based on the past records of use frequency and the number of bad blocks, and realize real-time warning to secure user data to the largest extent

- **Unique SecurityMechanism**

Unique function of read-write lock when used with Hikvision cameras, preventing irrelevant personnel from reading or writing even if they get the Micro SD (TF) card

Ordering Information

Capacity	Model
16 GB	HS-TF-L2(STD)/16G
32 GB	HS-TF-L2(STD)/32G
64 GB	HS-TF-L2(STD)/64G
128 GB	HS-TF-L2(STD)/128G
256 GB	HS-TF-L2(STD)/256G



Note

Please contact the local sales for detailed model information.

Specification

Model	HS-TF-L2				
Capacity	16 GB	32GB	64GB	128 GB	256 GB
Max. Read speed	95 MB/s	95 MB/s	95 MB/s	95 MB/s	95 MB/s
Max. Write speed	15 MB/s	25 MB/s	40 MB/s	50 MB/s	55 MB/s
NAND flash memory	TLC（Teiple-Level Cell）				
Specification	MicroSDHC		MicroSDXC		
Speed	Class10, U1,V10		Class10,U3,V30		
Dimensions	0.59" x 0.43" x 0.04"（14.99mm x 10.92mm x 1.02mm）				
Working Temperature	0°C to 70°C				
Storage Temperature	-25 °C to 85 °C				
Compatibility	Compatible with microSDHC、microSDXC、microSDHC UHS-I and microSDXC UHS-I host devices				
Warranty	2 years				

Note

Performance test is performed in specific testing environment. Any change of the computer system, operation system, hardware, software, or functions will influence the test result.

Revision History

Version	Description	Date
V1.0.0	HS-TF-L2	20220216

Data subject to change without notice.

© 2022 HANGZHOU HIKSTORAGE TECHNOLOGY CO.,LTD. All rights reserved.

Unless otherwise expressly stated herein, HIKSTORAGE does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the HIKSTORAGE website (<http://en.hikstorage.com/>).

DS-2CD3566G2-IS 6 MP Acusense IR Fixed Mini Dome Network Camera

AcuSense

Powered by

DarkFighter



Empowered by deep learning algorithms, Hikvision AcuSense technology brings human and vehicle targets classification alarms to front- and back-end devices. The system focuses on human and vehicle targets, vastly improving alarm efficiency and effectiveness.

Hikvision has been dedicated to develop products with security since established. Hikvision always follows security by design principle and has adopted many methods of security technologies into our product development lifecycle, including terminal security, data security, application security, network security, and privacy protection. In the meantime, the security technologies used by Hikvision are all in compliance with local applicable laws and safety regulations. These security measures could enhance product's cyber security protection capability and protect your devices as well as your data from malicious cyber attacks.

- Supports Hikvision Embedded Open Platform (HEOP) and importing third party applications
- Supports 1.5 Tops computing power, 40 MB system memory, 350 MB smart RAM, and 2 GB eMMC storage for sharing resources
- High quality imaging with 6 MP resolution
- Excellent low-light performance with powered-by-DarkFighter technology
- Clear imaging against strong backlight due to 120 dB WDR technology
- Efficient H.265+ compression technology
- Focus on human and vehicle targets classification based on deep learning
- Audio and alarm interface available
- Water and dust resistant (IP67) and vandal resistant (IK08)

▪ Specification

Camera	
Image Sensor	1/2.4" Progressive Scan CMOS
Max. Resolution	3200 × 1800
Min. Illumination	Color: 0.003 Lux @ (F1.6, AGC ON),B/W: 0 Lux with IR
Shutter Time	1/3 s to 1/100,000 s
Day & Night	IR cut filter
Angle Adjustment	Pan: -30° to 30°,tilt: 0° to 75°,rotate: 0° to 360°
Lens	
Lens Type	Fixed focal lens, 2.8 and 4 mm optional
Focal Length & FOV	2.8 mm, horizontal FOV 105°, vertical FOV 55°, diagonal FOV 127° 4 mm, horizontal FOV 78°, vertical FOV 38°, diagonal FOV 96°
Lens Mount	M12
Iris Type	Fixed
Aperture	F1.6
DORI	
DORI	2.8 mm: D: 76 m, O: 30 m, R: 15 m, I: 7 m 4 mm: D: 115 m, O: 45 m, R: 23 m, I: 11 m
Illuminator	
Supplement Light Type	IR
Supplement Light Range	Up to 30 m
Smart Supplement Light	Yes
IR Wavelength	850 nm
HEOP	
Open Resources	Memory: 40 MB, Smart RAM: 350 MB, eMMC: 2 GB
Computing Power	1.5 TOPS
Open Capability	HEOP 2.0 OpendevSDK
Deep Learning Structure	Caffe,PyTorch,TensorFlow,PaddlePaddle,ONNX
Programming Language	C,C++
Video	
Main Stream	50 Hz: 20 fps (3200 × 1800) 25 fps (2688 × 1520, 1920 × 1080, 1280 × 720) 60 Hz: 20 fps (3200 × 1800) 30 fps (2688 × 1520, 1920 × 1080, 1280 × 720)
Sub-Stream	50 Hz: 25 fps (1280 × 720, 640 × 480, 640 × 360) 60 Hz: 30 fps (1280 × 720, 640 × 480, 640 × 360)
Third Stream	50 Hz: 10 fps (1920 × 1080, 1280 × 720, 640 × 480, 640 × 360) 60 Hz: 10 fps (1920 × 1080, 1280 × 720, 640 × 480, 640 × 360)
Fourth Stream	50 Hz: 10 fps (1280 × 720, 640 × 480, 640 × 360) 60 Hz: 10 fps (1280 × 720, 640 × 480, 640 × 360)

Video Compression	Main stream: H.265/H.264/H.264+/H.265+, Sub-stream: H.265/H.264/MJPEG, Third stream: H.265/H.264, Fourth stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 16 Mbps
H.264 Type	Baseline Profile,Main Profile,High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR,VBR
Scalable Video Coding (SVC)	H.264 and H.265 encoding
Region of Interest (ROI)	5 fixed regions for main stream and sub-stream
Target Cropping	Yes
Audio	
Audio Compression	G.711/G.722.1/G.726/MP2L2/PCM/MP3/AAC-LC
Audio Bit Rate	64 Kbps (G.711ulaw/G.711alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 192 Kbps (MP2L2)/8 to 320 Kbps (MP3)/16 to 64 Kbps (AAC-LC)
Audio Sampling Rate	8 kHz/16 kHz/32 kHz/44.1 kHz/48 kHz
Environment Noise Filtering	Yes
Network	
Protocols	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, NTP, UPnP, SMTP, IGMP, 802.1X, QoS, IPv4, IPv6, UDP, Bonjour, SSL/TLS, PPPoE, SFTP, ARP, SNMP, WebSocket, WebSockets, SRTP
Simultaneous Live View	Up to 6 channels
API	ONVIF (Profile S, Profile G, Profile T),ISAPI,SDK,ISUP
User/Host	Up to 32 users 3 user levels: administrator, operator, and user
Security	Password protection, complicated password, HTTPS encryption, 802.1X authentication (EAP-TLS, EAP-LEAP, EAP-MD5), watermark, IP address filter, basic and digest authentication for HTTP/HTTPS, WSSE and digest authentication for Open Network Video Interface, RTP/RTSP over HTTPS, control timeout settings, security audit log, TLS 1.1/1.2/1.3, host authentication (MAC address)
Network Storage	NAS (NFS, SMB/CIFS),Auto Network Replenishment (ANR), Together with high-end Hikvision memory card, memory card encryption and health detection are supported.
Client	iVMS-4200,Hik-Connect,Hik-Central
Web Browser	Plug-in required live view: IE 10, IE 11, Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Edge 89+, Local service: Chrome 57.0+, Firefox 52.0+, Edge 89+
Image	
Image Parameters Switch	Yes
Image Settings	Rotate mode,saturation,brightness,contrast,sharpness,gain,white balance,adjustable by client software or web browser
Day/Night Switch	Day,Night,Auto,Schedule
Wide Dynamic Range (WDR)	120 dB
SNR	≥ 52 dB
Image Enhancement	BLC,HLC,3D DNR,Defog
Privacy Mask	4 programmable polygon privacy masks

Interface	
Ethernet Interface	1 RJ45 10 M/100 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 512 GB
Built-in Microphone	Yes, 1 built-in microphone
Audio	1 input (line in), two-core terminal block, max. input amplitude: 3.3 Vpp, input impedance: 4.7 K Ω , interface type: non-equilibrium, 1 output (line out), two-core terminal block, max. output amplitude: 3.3 Vpp, output impedance: 100 Ω , interface type: non-equilibrium
Alarm	1 input, 1 output (max. 12 VDC, 30 mA)
Reset Key	Yes
Power Output	12 VDC, max. 100 mA
Event	
Basic Event	Motion detection (support alarm triggering by specified target types (human and vehicle)), video tampering alarm, exception
Smart Event	scene change detection, audio exception detection, defocus detection, unattended baggage detection, object removal detection
Linkage	Upload to FTP/NAS/memory card, notify surveillance center, send email, trigger alarm output, trigger recording, trigger capture, audible warning
Deep Learning Function	
Perimeter Protection	Line crossing, intrusion, region entrance, region exiting Support alarm triggering by specified target types (human and vehicle)
Face Capture	Yes
People Counting	Yes
General	
Power	12 VDC $\pm$ 25%, 0.66 A, max. 8 W, $\varnothing$ 5.5 mm coaxial power plug, reverse polarity protection, PoE: IEEE 802.3af, Class 3, max. 9 W
Material	Base: aluminum, cover: plastic
Dimension	$\varnothing$ 110 mm $\times$ 57.4 mm ($\varnothing$ 4.3" $\times$ 2.3")
Package Dimension	134 mm $\times$ 134 mm $\times$ 108 mm (5.3" $\times$ 5.3" $\times$ 4.3")
Weight	Approx. 385 g (0.8 lb.)
With Package Weight	Approx. 620 g (1.4 lb.)
Storage Conditions	-30 $^{\circ}$ C to 60 $^{\circ}$ C (-22 $^{\circ}$ F to 140 $^{\circ}$ F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-30 $^{\circ}$ C to 60 $^{\circ}$ C (-22 $^{\circ}$ F to 140 $^{\circ}$ F). Humidity 95% or less (non-condensing)
Language	33 languages: English, Russian, Estonian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Danish, Swedish, Norwegian, Finnish, Croatian, Slovenian, Serbian, Turkish, Korean, Traditional Chinese, Thai, Vietnamese, Japanese, Latvian, Lithuanian, Portuguese (Brazil), Ukrainian
General Function	Heartbeat, anti-banding, mirror, flash log, password reset via email, pixel counter
Approval	
EMC	CE-EMC: EN 55032: 2015, EN 61000-3-2:2019, EN 61000-3-3: 2013+A1:2019, EN 50130-4: 2011 +A1: 2014, IC: ICES-003: Issue 7, KC: KN32: 2015, KN35: 2015

Safety	UL: UL 62368-1, CB: IEC 62368-1: 2014+A11, CE-LVD: EN 62368-1: 2014/A11: 2017, BIS: IS 13252 (Part 1): 2010/IEC 60950-1: 2005, LOA: IEC/EN 60950-1
Environment	CE-RoHS: 2011/65/EU, WEEE: 2012/19/EU, Reach: Regulation (EC) No 1907/2006
Protection	IP67: IEC 60529-2013,IK08: IEC 62262:2002

▪ Typical Application

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

This model has NO SPECIFIC PROTECTION.

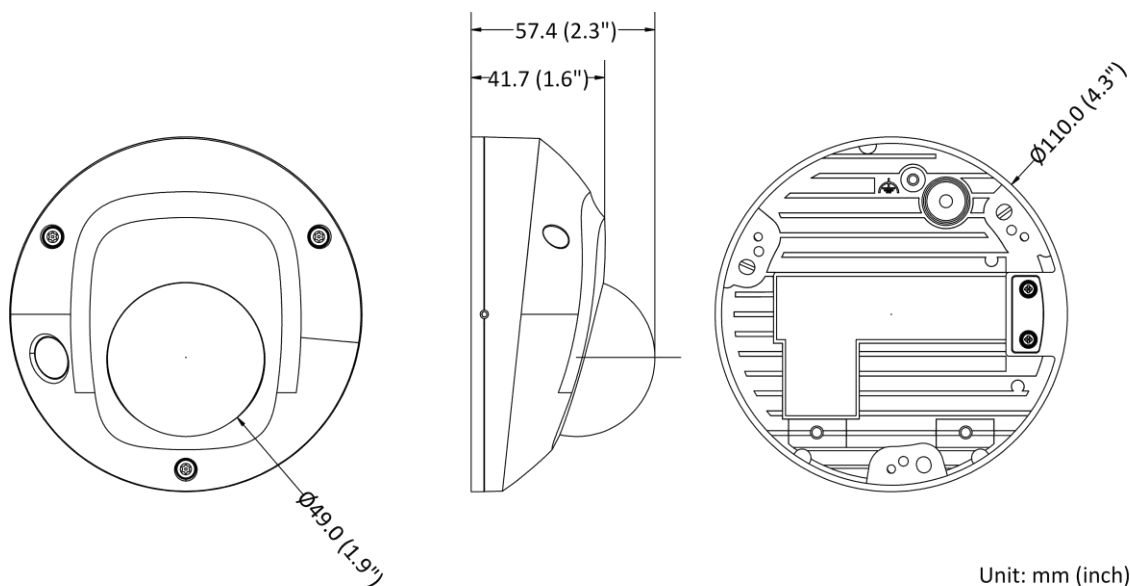
Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ Available Model

DS-2CD3566G2-IS(2.8mm)(H)

DS-2CD3566G2-IS(4mm)(H)

▪ Dimension



Unit: mm (inch)

▪ Accessory

▪ Optional

DS-1272ZJ-120 Wall mount	DS-1272ZJ-120B Wall mount	DS-1271ZJ-120 Pendant Mount	DS-1275ZJ-SUS Vertical pole mount	DS-1276ZJ-SUS Corner mount
				
DS-1280ZJ-DM46 Junction box	DS-2280ZJ-WA120 Junction box	DS-2210ZJ-WA-120 Pendant Mount	DS-2200ZJ-WA-120 Wall mount	DS-2200ZJ-WAJ-120 Wall mount
				

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com



Follow us on social media to get the latest product and solution information.



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



Hikvision
Corporate Channel



hikvisionhq



*Images are for illustrative purposes. Actual product appearance and specifications may vary.

DS-1280ZJ-DM46 *HOT*



Junction box

- Junction Box
- Aluminum Alloy
- Hikvision White

Sales Inquiry

Available models:

DS-1280ZJ-DM46



Specification

Parameters

Parameters

Description	Junction Box
Appearance	Hikvision White

DS-1280ZJ-DM46 *HOT*

Specification

Resources

Dimension Ø 120 mm x 37.2 mm (Ø 4.72" x 1.46")
250 g (0.55 lb.)

*Product performance is based on testing in a controlled environment. Your results may vary due to several external and environmental factors.

Resources

Technical documents

Quick Start Guide



About Us

Newsroom

Events

Quick Links

 [Contact Us](#)

✉ [Subscribe Newsletter](#)



in



© 2026 Hangzhou Hikvision Digital Technology Co., Ltd. All Rights Reserved.
Subscription

Privacy Policy.

Cookie Policy.

Cookies Preferences

Cancel

Subscription

GUARD TF Card

Introduction

HIKSEMI L2 Micro SD (TF) Card is specifically designed and ideal for video surveillance recording, boasting a read and write speed of Class 10 or higher. Utilizing TLC storage medium, it offers strong compatibility and adaptability. Widely applicable in scenarios such as light storage and backup storage, as well as other recording environments with low intensity or relatively simple usage requirements.



Features

- **Exceptional Compatibility**

Optimized for Hikvision storage systems, it is compatible with a wide range of products. When used with Hikvision products, the performance is even more outstanding.

- **Large Capacities**

Wide range of capacities from 32GB to 1TB for choice. Hold massive videos and information easily.

- **Strong Adaptability**

Waterproof, shockproof, X-ray proof, high and low temperature resistant, can be widely adapted to various working environments.

- **S.M.A.R.T. Mechanism**

Unique functions of life forewarning and health monitoring when used with Hikvision cameras. It can calculate the remaining available time based on the past records of use frequency and the number of bad blocks, and realize real-time warning to secure user data to the largest extent.

- **Unique Security Mechanism**

Unique function of read-write lock when used with Hikvision cameras, preventing irrelevant personnel from reading or writing even if they get the Micro SD (TF) card.

Ordering Information

Capacity	Model
32GB	HS-TF-L2 32G
64GB	HS-TF-L2 64G
128GB	HS-TF-L2 128G
256GB	HS-TF-L2 256G
512GB	HS-TF-L2 512G



Please contact the local sales for detailed model information.

Specification

Model	HS- TF-L2				
Capacity	32GB	64GB	128GB	256GB	512GB
Max. Read speed	95 MB/s				
Max. Write speed	20MB/s	30MB/s	40MB/s	50MB/s	60MB/s
File format	FAT32				
Specification	microSDHC, microSDXC				
Speed specifications	U1, U3				
NAND flash memory	TLC				
Dimensions	0.59" x 0.43" x 0.04" (14.99mm x 10.92mm x 1.02mm)				
Working Temperature	-0 °C to 70 °C (0 °F to 158 °F)				
Storage Temperature	-25°C to 85°C (-13 °F to 185 °F)				
Compatibility	Compatible with microSDHC, microSDXC, microSDHC UHS-I and SDXC UHS-I host devices				
Warranty	2 years				

Note

Performance test is performed in specific testing environment. Any change of the computer system, operation system, hardware, software, or functions will influence the test result.

Revision History

Version	Description	Date
V1.0.0	HS-TF-L2	20241106

Data subject to change without notice.

© 2024 HANGZHOU HIKSTORAGE TECHNOLOGY CO.,LTD. All rights reserved.

Unless otherwise expressly stated herein, HIKSTORAGE does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the HIKSTORAGE website ([http:// www.hiksemitech.com](http://www.hiksemitech.com)).



Network Camera

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Safety Instruction

Please scan the following QR code to obtain the "**Safety Instruction**" of the product, and read it carefully. These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.



Figure 1-1 Safety Instruction

Contents

Chapter 1 Overview	1
1.1 Configuration Process	1
1.2 Firmware Update	1
1.3 System Requirement	1
Chapter 2 Device Activation and Accessing	3
2.1 Activate the Device via SADP	3
2.2 Activate the Device via Browser	3
2.3 Login	4
2.3.1 Plug-in Installation	4
2.3.2 Admin Password Recovery	5
2.3.3 Illegal Login Lock	6
Chapter 3 Live View	7
3.1 Live View Parameters	7
3.1.1 Start and Stop Live View	7
3.1.2 Aspect Ratio	7
3.1.3 Live View Stream Type	7
3.1.4 Select the Third-Party Plug-in	7
3.1.5 Light	8
3.1.6 Count Pixel	8
3.1.7 Start Digital Zoom	8
3.1.8 Auxiliary Focus	8
3.1.9 Lens Initialization	9
3.1.10 Lens Parameters Adjustment	9
3.1.11 Conduct 3D Positioning	11
3.2 Set Transmission Parameters	11
Chapter 4 Video and Audio	13

4.1 Video Settings	13
4.1.1 Stream Type	13
4.1.2 Video Type	13
4.1.3 Resolution	13
4.1.4 Bitrate Type and Max. Bitrate	14
4.1.5 Video Quality	14
4.1.6 Frame Rate	14
4.1.7 Video Encoding	14
4.1.8 Smoothing	16
4.2 Audio Settings	16
4.2.1 Audio Encoding	17
4.2.2 Audio Input	17
4.2.3 Audio Output	17
4.2.4 Environmental Noise Filter	17
4.3 Two-way Audio	17
4.4 ROI	18
4.4.1 Set ROI	18
4.5 Set Target Cropping	19
4.6 Display Info. on Stream	19
4.7 Display Settings	19
4.7.1 Scene Mode	20
4.7.2 Image Parameters Switch	25
4.7.3 Video Standard	26
4.7.4 Local Video Output	26
4.8 OSD	26
4.9 Set Privacy Mask	27
4.10 Overlay Picture	27
Chapter 5 Video Recording and Picture Capture	28

5.1 Storage Settings	28
5.1.1 Memory Card	28
5.1.2 Set FTP	30
5.1.3 Set NAS	31
5.1.4 eMMC Protection	32
5.1.5 Set Cloud Storage	32
5.2 Video Recording	33
5.2.1 Record Automatically	33
5.2.2 Record Manually	35
5.2.3 Playback and Download Video	35
5.3 Capture Configuration	36
5.3.1 Capture Automatically	36
5.3.2 Capture Manually	36
5.3.3 View and Download Picture	37
Chapter 6 Event and Alarm	38
6.1 Set Motion Detection	38
6.1.1 Expert Mode	38
6.1.2 Normal Mode	39
6.2 Set Video Tampering Alarm	40
6.3 Set Alarm Input	41
6.4 Set Exception Alarm	42
6.5 Set Video Quality Diagnosis	42
6.6 Set Audio Exception Detection	43
6.7 Set Defocus Detection	44
6.8 Set Scene Change Detection	44
Chapter 7 Arming Schedule and Alarm Linkage	45
7.1 Set Arming Schedule	45
7.2 Linkage Method Settings	45

7.2.1 Trigger Alarm Output	46
7.2.2 FTP/NAS/Memory Card Uploading	47
7.2.3 Send Email	47
7.2.4 Notify Surveillance Center	48
7.2.5 Trigger Recording	48
7.2.6 Flashing Light	48
7.2.7 Audible Warning	49
7.2.8 Alarm Server	50
Chapter 8 Network Settings	51
8.1 TCP/IP	51
8.2 Access to Device via Domain Name	52
8.3 Access to Device via PPPoE Dial Up Connection	53
8.4 SNMP	53
8.5 Set IEEE 802.1X	54
8.6 Set QoS	54
8.7 HTTP(S)	55
8.8 Multicast	56
8.8.1 Multicast Discovery	56
8.9 RTSP	56
8.10 Set SRTP	57
8.11 Bonjour	57
8.12 WebSocket(s)	58
8.13 Port Mapping	58
8.13.1 Set Auto Port Mapping	58
8.13.2 Set Manual Port Mapping	58
8.13.3 Set Port Mapping on Router	59
8.14 RTCP	60
8.15 Wireless Dial	60

8.15.1 Set Wireless Dial	60
8.15.2 Wireless Expert Settings	61
8.16 WLAN AP (Access Point)	63
8.16.1 Set WLAN AP	63
8.16.2 Access to Device via AP	64
8.17 Traffic Shaping	65
8.18 Data Monitoring	65
8.19 Wi-Fi	65
8.19.1 Connect Device to Wi-Fi	66
8.20 Set ISUP	66
8.21 Access Camera via Hik-Connect	67
8.21.1 Enable Hik-Connect Service on Camera	67
8.21.2 Set Up Hik-Connect	68
8.21.3 Add Camera to Hik-Connect	69
8.22 Set Open Network Video Interface	70
8.23 Set SDK Service	70
Chapter 9 System and Security	71
9.1 System Settings	71
9.1.1 View Device Information	71
9.1.2 Time and Date	71
9.1.3 Set RS-232	72
9.1.4 Set RS-485	73
9.1.5 Set Live View Connection	73
9.1.6 Location Settings	73
9.1.7 External Device	74
9.1.8 View Open Source Software License	74
9.1.9 Wiegand	74
9.2 User and Account	74

9.2.1 Set User Account and Permission	74
9.2.2 Simultaneous Login	75
9.2.3 Online Users	75
9.3 Maintenance	75
9.3.1 Restart	75
9.3.2 Upgrade	75
9.3.3 Restore and Default	76
9.3.4 Import and Export Configuration File	76
9.3.5 Search and Manage Log	77
9.3.6 Search Security Audit Logs	77
9.3.7 SSH	77
9.3.8 Export Diagnose Information	78
9.3.9 Diagnosis	78
9.4 Security	80
9.4.1 Set IP Address Filter	80
9.4.2 Set MAC Address Filter	80
9.4.3 Control Timeout Settings	81
9.4.4 Certificate Management	81
9.4.5 TLS	84
Chapter 10 VCA Resource	85
10.1 Set Open Platform	85
10.2 General Settings	86
10.2.1 Set Camera Info	86
10.2.2 Metadata	86
10.2.3 AcuSearch	87
10.3 Smart Event	87
10.3.1 Set Intrusion Detection	88
10.3.2 Set Line Crossing Detection	89

10.3.3 Set Region Entrance Detection	91
10.3.4 Set Region Exiting Detection	92
10.3.5 Set Unattended Baggage Detection	94
10.3.6 Set Object Removal Detection	95
10.3.7 Set Loitering Detection	97
10.3.8 Set People Gathering Detection	98
10.3.9 Set Fast Moving Detection	99
10.3.10 Set Parking Detection	101
10.4 Face Capture	102
10.4.1 Set Face Capture	102
10.4.2 Overlay and Capture	103
10.4.3 Face Capture Algorithms Parameters	104
10.4.4 Set Shield Region	106
10.5 People Management	107
10.5.1 Regional People Counting	107
10.5.2 Overlay and Capture	113
10.5.3 Advanced Settings	113
10.6 People Counting	114
10.6.1 Set People Counting Rule	114
10.7 Road Traffic	116
10.7.1 Set Vehicle Detection	116
10.7.2 Set Mixed-Traffic Detection Rule	119
10.7.3 Overlay and Capture	121
10.7.4 Import or Export Blocklist & Allowlist	123
10.7.5 Advanced Parameters Configuration	124
10.8 AI Open Platform	124
10.8.1 Set AI Open Platform	124
10.8.2 Set Rules	125

Chapter 11 EPTZ 129

 11.1 Patrol 129

 11.2 Auto-Tracking 129

Appendix A. FAQ 131

Chapter 1 Overview

1.1 Configuration Process

This section briefly explains the software configuration process of the network camera. Please set up the device according to the actual situation.

General Configuration Process

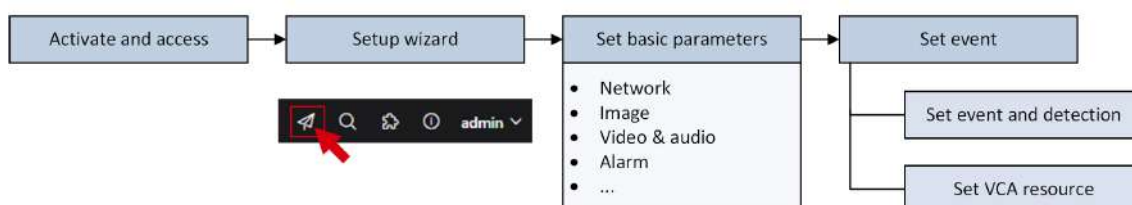


Figure 1-1 General Configuration Process

- **Activate and access device via web browser.** You should set a login password (for **admin** user) to activate the device when access the device via network. Open the web browser and enter the IP address. The default IP address of the device is 192.168.1.64.
- Follow the **Wizard** or click  on the web page to quickly set the device parameters.
- Set the basic parameters, including network, image, video and audio, alarm, etc.
- Set event and detection rules. You can set basic **event and detection** rules or **allocate VCA resources** for deep learning function.

1.2 Firmware Update

For better user experience, we recommend you to update your device to the latest firmware. Please get the latest firmware package from the official website or the local technical expert. For more information, please visit the official website: <https://www.hikvision.com/en/support/download/firmware/>.

For the upgrading settings, refer to **Upgrade**.

1.3 System Requirement

Your computer should meet the requirements for proper visiting and operating the product.

Operating System	Microsoft Windows XP SP1 and above version
CPU	2.0 GHz or higher
RAM	1G or higher
Display	1024×768 resolution or higher
Web Browser	For the details, see <u>Plug-in Installation</u>

Chapter 2 Device Activation and Accessing

To protect the security and privacy of the user account and data, you should set a login password to activate the device when access the device via network.



Note

Refer to the user manual of the software client for the detailed information about the client software activation.

2.1 Activate the Device via SADP

Search and activate the online devices via SADP software.

Before You Start

Access www.hikvision.com to get SADP software to install.

Steps

1. Connect the device to network using the network cable.
2. Run SADP software to search the online devices.
3. Check **Device Status** from the device list, and select **Inactive** device.
4. Create and input the new password in the password field, and confirm the password.



Caution

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.

5. Click **OK**.

Device Status changes into **Active**.

6. **Optional:** Change the network parameters of the device in **Modify Network Parameters**.

2.2 Activate the Device via Browser

You can access and activate the device via the browser.

Steps

1. Connect the device to the PC using the network cables.
2. Change the IP address of the PC and device to the same segment.



Note

The default IP address of the device is 192.168.1.64. You can set the IP address of the PC from 192.168.1.2 to 192.168.1.253 (except 192.168.1.64). For example, you can set the IP address of the PC to 192.168.1.100.

3. Input **192.168.1.64** in the browser.
4. Set device activation password.



Caution

We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: 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.

5. Click **OK**.
6. Input the activation password to log in to the device.
7. **Optional:** Go to **Configuration → Network → Network Settings → TCP/IP** to change the IP address of the device to the same segment of your network.

2.3 Login

Log in to the device via Web browser.

2.3.1 Plug-in Installation

Certain operating systems and web browsers may restrict the display and operation of the device function. You should install a plug-in or complete certain settings to ensure normal display and operation. For detailed restricted function, refer to the actual device.

Operating System	Web Browser	Operation
Windows	• Internet Explorer 10+ • Google Chrome 57 and earlier version • Mozilla Firefox 52 and earlier version	Follow pop-up prompts to complete plug-in installation.
	• Google Chrome 57+ • Mozilla Firefox 52+ • Edge 89+	Click  to download and install plug-in.
Mac OS	• Google Chrome 57+ • Mozilla Firefox 52+ • Mac Safari 16+	Plug-in installation is not required. Go to Configuration → Network → Network Service → WebSocket(s) to enable WebSocket or WebSockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.



Note

- The device only supports Windows and Mac OS system, and does not support Linux system.
 - To improve the user experience on certain devices, it's recommended to use a more advanced web browser for access. Please refer to the actual device or product specification.
 - Certain device models do not support Internet Explorer web browser.
-

2.3.2 Admin Password Recovery

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page after completing the account security settings.

You can reset the password by setting the security question or email.



Note

When you need to reset the password, make sure that the device and the PC are on the same network segment.

Security Question

You can set the account security during the activation. Or you can go to **Configuration → System → User Management**, click **Account Security Settings**, select the security question and input your answer.

You can click **Forget Password** and answer the security question to reset the admin password when access the device via browser.

Email

You can set the account security during the activation. Or you can go to **Configuration → System → User Management**, click **Account Security Settings**, input your email address to receive the verification code during the recovering operation process.

2.3.3 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.

Go to **Maintenance and Security → Security → Login Management**, and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

When your login attempts with the wrong password reach the set times, the device is locked.

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Live View

It introduces the live view parameters, function icons and transmission parameters settings.

3.1 Live View Parameters

The supported functions vary depending on the model.

3.1.1 Start and Stop Live View

Click **Live View**. Click  to start live view. Click  to stop live view.

3.1.2 Aspect Ratio

Aspect Ratio is the display ratio of the width to height of the image.

-  refers to 4:3 window size.
-  refers to 16:9 window size.
-  refers to original window size.
-  refers to self-adaptive window size.
-  refers to original ratio window size.

3.1.3 Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to **Stream Type**.

3.1.4 Select the Third-Party Plug-in

When the live view cannot display via certain browsers, you can change the plug-in for live view according to the browser.

Steps

1. Click **Live View**.
2. Click  to select the plug-in.
 - When you access the device via Internet Explorer, you can select Webcomponents or QuickTime.
 - When you access the device via the other browsers, you can select Webcomponents, QuickTime or MJPEG.

3.1.5 Light

Click  to turn on or turn off the illuminator.



Caution

For the device with laser:

- DO NOT stare at operating light source. May be harmful to the eyes.
 - If appropriate shielding or eye protection is not available, turn on the light only at a safe distance or in the area that is not directly exposed to the light.
 - When assembling, installing or maintaining the device, DO NOT turn on the light, or wear eye protection.
-

3.1.6 Count Pixel

It helps to get the height and width pixel of the selected region in the live view image.

Steps

1. Click  to enable the function.
2. Drag the mouse on the image to select a desired rectangle area.
The width pixel and height pixel are displayed on the bottom of the live view image.

3.1.7 Start Digital Zoom

It helps to see a detailed information of any region in the image.

Steps

1. Click  to enable the digital zoom.
2. In live view image, drag the mouse to select the desired region.
3. Click in the live view image to back to the original image.

3.1.8 Auxiliary Focus

It is used for motorized device. It can improve the image if the device cannot focus clearly.

For the device that supports ABF, adjust the lens angle, then focus and click ABF button on the device. The device can focus clearly.

Click  to focus automatically.

Note

- If the device cannot focus with auxiliary focus, you can use **Lens Initialization** , then use auxiliary focus again to make the image clear.
 - If auxiliary focus cannot help the device focus clearly, you can use manual focus.
-

3.1.9 Lens Initialization

Lens initialization is used on the device equipped with motorized lens. The function can reset lens when long time zoom or focus results in blurred image. This function varies according to different models.

Click  to operate lens initialization.

3.1.10 Lens Parameters Adjustment

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the device. In live view interface, you can click the direction control buttons to control the pan/tilt movement, and click the zoom/focus/iris buttons to realize lens control.

Note

- Supported PTZ functions may vary according to different camera models.
 - For the devices which support lens movements only, the direction buttons are invalid.
-

Direction Control



Click and hold the direction button to pan/tilt the device.

Zoom

- Click  , and the lens zooms in.
- Click  , and the lens zooms out.

Focus

- Click  , then the lens focuses near and the nearby object gets clear.
- Click  , then the lens focuses far and the distant object gets clear.

Iris

- When the image is too dark, click  to enlarge the iris.
- When the image is too bright, click  to stop down the iris.

PTZ Speed

- Slide  to adjust the speed of the pan/tilt movement.

PTZ Lock

PTZ lock means to disable the zoom, focus and PTZ rotation functions of the corresponding channel, so that to reduce the target missing caused by PTZ adjustment.



Note

The function is only supported by certain device models.

Click  to lock the PTZ operation, or click  to unlock it.

PTRZ Adjustment

PTRZ is an abbreviation for pan, tilt, rotate and zoom. It means the movement options of the device. In the interface, you can use the control buttons to adjust the movement of the device, such as device panning, tilting, rotating, and zooming.



Note

The function is only supported by certain device models.

Go to **Configuration → PTZ → PTRZ**.

Control Panel

	Click and hold the directional button to pan/tilt the device.
•  • 	Click and hold the button to adjust rotating position.

Auto Recovery

Click , the device will correct the rotating position automatically to make the live view image positive. Make sure the **Self-Test Status** is **Initialized**.



Note

- Go to **Configuration → PTZ → PTZ** to view the **Self-Test Status**.
- If you want to initialize PTZ and enable PTZ self-check manually, go to **Configuration → PTZ → PTZ** and click **Self-Test**, then the PTZ is initialized.

Refer to **Lens Parameters Adjustment** for more detailed settings of lens adjustment.

3.1.11 Conduct 3D Positioning

3D positioning is to relocate the selected area to the image center.

Steps

1. Click  to enable the function.
2. Select a target area in live image.
 - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
 - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
 - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
3. Click the button again to turn off the function.

3.2 Set Transmission Parameters

The live view image may be displayed abnormally according to the network conditions. In different network environments, you can adjust the transmission parameters to solve the problem.

Steps

1. Go to **Configuration → Local → Live View Parameters**.
2. Set the transmission parameters as required.

Protocol

TCP

TCP ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. It is suitable for the stable network environment.

UDP

UDP is suitable for the unstable network environment that does not demand high video fluency.

MULTICAST

MULTICAST is suitable for the situation that there are multiple clients. You should set the multicast address for them before selection.



Note

For detailed information about multicast, refer to ***Multicast***.

HTTP

HTTP is suitable for the situation that the third-party needs to get the stream from the device.

Playing Performance

Shortest Delay

The device takes the real-time video image as the priority over the video fluency.

Balanced

The device ensures both the real-time video image and the fluency.

Fluent

The device takes the video fluency as the priority over real-time. In poor network environment, the device cannot ensure video fluency even the fluency is enabled.

Custom

You can set the frame rate manually. In poor network environment, you can reduce the frame rate to get a fluent live view. But the rule information may not display.

3. Click **Save**.

Chapter 4 Video and Audio

This part introduces the configuration of video and audio related parameters.

4.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.

Go to setting page: **Configuration → Video/Audio → Video** .

4.1.1 Stream Type

For device supports more than one stream, you can specify parameters for each stream type.

Main Stream

The stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission.

Sub Stream

The stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

Other Streams

Streams other than the main stream and sub stream may also be offered for customized usage.

4.1.2 Video Type

Select the content (video and audio) that should be contained in the stream.

Video Stream

Only video content is contained in the stream.

Video&Audio

Video content and audio content are contained in the composite stream.

4.1.3 Resolution

Select video resolution according to actual needs. Higher resolution requires higher bandwidth and storage.

4.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but mosaic may occur on the image.

Variable Bitrate

It means that the device automatically adjust the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

4.1.5 Video Quality

When **Bitrate Type** is set as Variable, video quality is configurable. Select a video quality according to actual needs. Note that higher video quality requires higher bandwidth.

4.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).

A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

4.1.7 Video Encoding

It stands for the compression standard the device adopts for video encoding.



Note

Available compression standards vary according to device models.

H.264

H.264, also known as MPEG-4 Part 10, Advanced Video Coding, is a compression standard. Without compressing image quality, it increases compression ratio and reduces the size of video file than MJPEG or MPEG-4 Part 2.

H.264+

H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.264+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



Note

When H.264+ is enabled, **I Frame Interval** is not configurable.

H.265

H.265, also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2, is a compression standard. In comparison to H.264, it offers better video compression at the same resolution, frame rate and image quality.

H.265+

H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.265+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



Note

When H.265+ is enabled, **I Frame Interval** is not configurable.

I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.

In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

SVC

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.

The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.

SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able decode high quality video stream.

MPEG4

MPEG4, referring to MPEG-4 Part 2, is a video compression format developed by Moving Picture Experts Group (MPEG).

MJPEG

Motion JPEG (M-JPEG or MJPEG) is a video compression format in which intraframe coding technology is used. Images in a MJPEG format is compressed as individual JPEG images.

Profile

This function means that under the same bitrate, the more complex the profile is, the higher the quality of the image is, and the requirement for network bandwidth is also higher.

4.1.8 Smoothing

It refers to the smoothness of the stream. The higher value of the smoothing is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

4.2 Audio Settings

It is a function to set audio parameters such as audio encoding, environment noise filtering.

Go to the audio settings page: **Configuration → Video/Audio → Audio** .



Only certain camera models support the function.

4.2.1 Audio Encoding

Select the audio encoding compression of the audio.

4.2.2 Audio Input



- Connect the audio input device as required.
 - The audio input display varies with the device models.
-

LineIn	Set Audio Input to LineIn when the device connects to the audio input device with the high output power, such as MP3, synthesizer or active pickup.
MicIn	Set Audio Input to MicIn when the device connects to the audio input device with the low output power, such as microphone or passive pickup.

4.2.3 Audio Output



Connect the audio output device as required.

It is a switch of the device audio output. When it is disabled, all the device audio cannot output. The audio output display varies with the device modes.

4.2.4 Environmental Noise Filter

Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

4.3 Two-way Audio

It is used to realize the two-way audio function between the monitoring center and the target in the monitoring screen.

Before You Start

- Make sure the audio input device (pick-up or microphone) and audio output device (speaker) connected to the device is working properly. Refer to specifications of audio input and output devices for device connection.
- If the device has built-in microphone and speaker, two-way audio function can be enabled directly.

Steps

1. Click **Live View**.
2. Click  on the toolbar to enable two-way audio function of the camera.
3. Click , disable the two-way audio function.

4.4 ROI

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression. The technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

4.4.1 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video coding type. ROI is supported when the video coding type is H.264 or H.265.

Steps

1. Go to **Configuration → Video/Audio → ROI**.
2. Check **Enable**.
3. Select **Stream Type**.
4. Select **Region No.** and click  to draw ROI region on the live view.



Note

Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.

5. Input the **Area Name** and **ROI Level**.
6. Click **Save**.



Note

The higher the ROI level is, the clearer the image of the detected region is.

7. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

4.5 Set Target Cropping

You can crop the image, transmit and save only the images of the target area to save transmission bandwidth and storage.

Steps

1. Go to **Configuration → Video/Audio → Target Cropping** .
2. Check **Enable** and set **Third Stream** as the **Stream Type**.



Note

After enabling target cropping, the third stream resolution cannot be configured.

3. Select a **Cropping Resolution**.

A red frame appears in the live view.

4. Drag the frame to the target area.
5. Click **Save**.



Note

- Only certain models support target cropping and the function varies according to different camera models.
 - Some functions may be disabled after enabling target cropping.
-

4.6 Display Info. on Stream

The information of the objects (e.g. human, vehicle, etc.) is marked in the video stream. You can set rules on the connected rear-end device or client software to detect the events including line crossing, intrusion, etc.

Before You Start

This function is supported in smart events. Go to **VCA** , select **Smart Event** and click **Next** to enable **Smart Event**.

Steps

1. Go to **Configuration → Video/Audio → Display Info. on Stream** .
2. Check **Enable Dual-VCA**.
3. Click **Save**.

4.7 Display Settings

It offers the parameter settings to adjust image features.

Go to **Configuration → Image → Display Settings** .

Click **Default** to restore settings.

4.7.1 Scene Mode

There are several sets of image parameters predefined for different installation environments. Select a scene according to the actual installation environment to speed up the display settings.

Image Adjustment

By adjusting the **Brightness**, **Saturation**, **Contrast** and **Sharpness**, the image can be best displayed.

Exposure Settings

Exposure is controlled by the combination of iris, shutter, and photo sensibility. You can adjust image effect by setting exposure parameters.

In manual mode, you need to set **Exposure Time**, **Gain** and **Slow Shutter**.

Focus

It offers options to adjust the focus mode.

Focus Mode

Auto

The device focuses automatically as the scene changes. If you cannot get a well-focused image under auto mode, reduce light sources in the image and avoid flashing lights.

Semi-auto

The device focuses once after the PTZ and lens zooming. If the image is clear, the focus does not change when the scene changes.

Manual

You can adjust the focus manually on the live view page.

Day/Night Switch

Day/Night Switch function can provide color images and black/white images in day and night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The image is black/white or colorful and the supplement light will be enabled to ensure clear live view image at night.



Note

Only certain device models support the supplement light and colorful image.

Auto

The camera switches between the day mode and the night mode according to the light condition of environment.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.

Triggered by alarm input

You can set **Triggering Status** as **Day** or **Night**. For example, if the **Triggering Status** is **Night**, the mode turns into **Night** when the device receives alarm input signal.

Triggered by video

The camera switches between the day mode and the night mode according to the light condition of environment. This mode is applicable when the device supports road traffic and vehicle detection.



Note

- Day/Night Switch function varies according to models.
 - You can turn on the smart supplement light for better image effect. For supplement light settings, refer to ***Supplement Light Settings***.
-

Supplement Light Settings

You can set supplement light and refer to the actual device for relevant parameters.

Smart Supplement Light

Smart supplement light avoids over exposure when the supplement light is on.

Supplement Light Mode

When the device supports supplement light, you can select supplement light mode.

IR Supplement Light

IR light is enabled.

White Light

White light is enabled.

Mixed Light

Both IR light and white light are enabled.

Smart

When you select this mode after enabling certain smart events or motion detection, in the night state, the default supplement light mode is IR supplement light mode. When the alarm is triggered, the white light is enabled and the device captures the target. After the alarm ends, the supplement light mode will switch to IR supplement light mode.

Only device models with IR and white light or hybrid supplement light with IR and white light support this function.

Off

Supplement light is disabled.



Note

The supplement light mode may vary according to different device models.

Brightness Adjustment Mode

Auto

The brightness adjusts according to the actual environment automatically.

Manual

You can drag the slider or set value to adjust the brightness.

BLC

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set as **Custom**, you can draw a red rectangle on the live view image as the BLC area.

WDR

The WDR (Wide Dynamic Range) function helps the camera provide clear images in environment with strong illumination differences.

When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.



Note

When WDR is enabled, some other functions may be not supported. Refer to the actual interface for details.



Figure 4-1 WDR

HLC

When the bright area of the image is over-exposed and the dark area is under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright area and brighten the dark area, so as to achieve the light balance of the overall picture.

White Balance

White balance is the white rendition function of the camera. It is used to adjust the color temperature according to the environment.



Figure 4-2 White Balance

DNR

Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

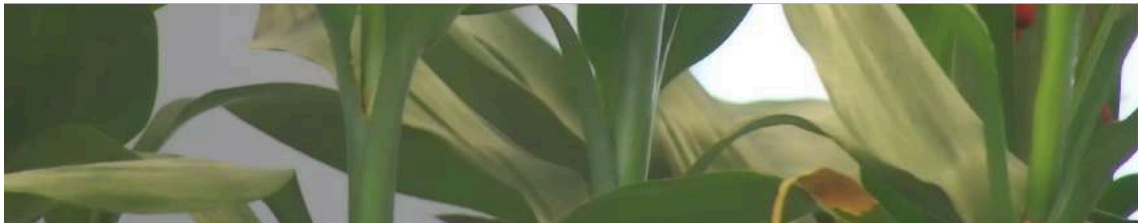
Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

Expert

Set the DNR level for both space DNR and time DNR to control the noise reduction degree. The higher level means stronger reduction degree.



DNR Off



DNR On

Figure 4-3 DNR

Defog

You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.



Defog Off



Defog On

Figure 4-4 Defog

EIS

Increase the stability of video image by using jitter compensation technology.

Gray Scale

You can choose the range of the **Gray Scale** as [0-255] or [16-235].

Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.



Note

The video recording will be shortly interrupted when the function is enabled.

Rotate

When this function is enabled, the live view will rotate 90° counterclockwise. For example, 1280 × 720 is rotated to 720 × 1280.

Enabling this function can change the effective range of monitoring in the vertical direction.



Note

This function is supported under certain settings.

Lens Distortion Correction

For device equipped with motorized lens, image may appear distorted to some extent. Enable this function to correct the distortion.



Note

- This function is only supported by certain device equipped with motorized lens.
 - The edge of image will be lost if this function is enabled.
-

4.7.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

Go to image parameters switch setting page: **Configuration** → **Image** → **Display Settings** → **Image Parameters Switch** , and set parameters as needed.

Set Scheduled-switch

Switch the image to the linked scene mode automatically in certain time periods.

Steps

1. Check **Scheduled-switch**.
2. Select and configure the corresponding time period and linked scene mode.



Note

For Linked Scene configuration, refer to ***Scene Mode***.

3. Click **Save**.

4.7.3 Video Standard

Video standard is an ability of a video card or video display device that defines the amount of colors that are shown and the resolution. The two most common video standard used are NTSC and PAL. In NTSC, 30 frames are transmitted each second. Each frame is made up of 525 individual scan lines. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines. Select video signal standard according to the video system in your country/region.

4.7.4 Local Video Output

If the device is equipped with video output interfaces, such as BNC, CVBS, HDMI, and SDI, you can preview the live image directly by connecting the device to a monitor screen.

Select the output mode as ON/OFF to control the output.

4.8 OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, color, and text overlay displayed on video stream.

Go to OSD setting page: **Configuration → Image → OSD Settings**. Set the corresponding parameters, and click **Save** to take effect.

Character Set

Select character set for displayed information. If Korean is required to be displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

Display

Set camera name, date, week, and their related display formats.

Format Settings

Set OSD parameters, such as **Display Mode**, **OSD Size**, **Font Color**, and **Alignment**.

Text Overlay

Set customized overlay text on image.

4.9 Set Privacy Mask

The function blocks certain areas in the live view to protect privacy. No matter how the device moves, the blocked scene will never be seen.

Steps

1. Go to **Configuration → Image → Privacy Mask**.
2. Check **Enable**.
3. Click . Drag the mouse in the live view to draw a closed area.
 - Drag the corners of the area** Adjust the size of the area.
 - Drag the area** Adjust the position of the area.
 - Click**  Clear all the areas you set.
4. Click **Add** to add a privacy mask and set **Region Name** and **Mask Type**.
5. Click **Save**.

4.10 Overlay Picture

Overlay a customized picture on live view.

Before You Start

The picture to overlay has to be in BMP format with 24-bit, and the maximum picture size is 128 × 128 pixel.

Steps

1. Go to **Configuration → Image → Picture Overlay**.
2. Check **Enable**.
3. Click **Upload** to select a picture and open it.

The picture with a red rectangle will appear in live view after successfully uploading.
4. Drag the red rectangle to adjust the picture position.
5. Click **Save**.

Chapter 5 Video Recording and Picture Capture

This part introduces the operations of capturing video clips and snapshots, playback, and downloading captured files.

5.1 Storage Settings

This part introduces the configuration of several common storage paths.

5.1.1 Memory Card

You can view the capacity, free space, status, type, and property of the memory card. Encryption of memory card is supported to ensure data security.

Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.

Steps

1. Go to **Configuration** → **Storage** → **Storage Management** → **HDD Management** .
2. Select the memory card.



Note

If an **Unlock** button appears, you need to unlock the memory card first. See [**Detect Memory Card Status**](#) for details.

-
3. Click **Format** to initialize the memory card.

When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.

4. **Optional:** Encrypt the memory card.

- 1) Click **Encrypted Format**.
- 2) Set the encryption password.
- 3) Click **OK**.

When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.



Note

Keep your encryption password properly. Encryption password cannot be found if forgotten.

-
5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
-

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

- Insert an encrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.
- You need to know the correct encryption password of the memory card.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management**.
2. Select the memory card.



Note

If an **Unlock** button appears, you need to unlock the memory card first. See [***Detect Memory Card Status***](#) for details.

3. Verify the encryption password.
 - 1) Click **Parity**.
 - 2) Enter the encryption password.
 - 3) Click **OK**.

When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.



Note

If the encryption password is forgotten and you still want to use this memory card, see [***Set New or Unencrypted Memory Card***](#) to format and set the memory card. All existing contents will be removed.

4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

The device detects the status of Hikvision memory card. You receive notifications when your memory card is detected abnormal.

Before You Start

The configuration page only appears when a Hikvision memory card is installed to the device.

Steps

1. Go to **Configuration → Storage → Storage Management → Memory Card Detection**.
2. Click **Status Detection** to check the **Remaining Lifespan** and **Health Status** of your memory card.

Remaining Lifespan

It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.

Health Status

It shows the condition of your memory card. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.



Note

It is recommended that you change the memory card when the health status is not "good".

-
3. Click **R/W Lock** to set the permission of reading and writing to the memory card.
 - Add a Lock
 - a. Select the **Lock Switch** as ON.
 - b. Enter the password.
 - c. Click **Save**
 - Unlock
 - If you use the memory card on the device that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of users.
 - If you use the memory card (with a lock) on a different device, you can go to **HDD Management** to unlock the memory card manually. Select the memory card, and click **Unlock**. Enter the correct password to unlock it.
 - Remove the Lock
 - a. Select the **Lock Switch** as OFF.
 - b. Enter the password in **Password Settings**.
 - c. Click **Save**.



Note

- Only admin user can set the **R/W Lock**.
- The memory card can only be read and written when it is unlocked.
- If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.

-
4. Set **Arming Schedule** and **Linkage Method**. See [Set Arming Schedule](#) and [Linkage Method Settings](#) for details.
 5. Click **Save**.

5.1.2 Set FTP

You can configure the FTP server to save images which are captured by events or a timed snapshot task.

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration → Event → Alarm Setting → FTP**.
2. Configure FTP settings.

Server Address and Port

The FTP server address and corresponding port.

User Name and Password

The FTP user should have the permission to upload pictures.

If the FTP server supports picture uploading by anonymous users, you can check **Anonymous** to hide your device information during uploading.

Directory Structure

The saving path of snapshots in the FTP server.

3. **Optional:** Check **Upload Picture** to enable uploading snapshots to the FTP server.

Picture Filing Interval

For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

Picture Name

Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.

4. **Optional:** Check **Enable Automatic Network Replenishment**.



Note

Upload to FTP/Memory Card/NAS in Linkage Method and **Enable Automatic Network Replenishment** should be both enabled simultaneously.

5. Click **Test** to verify the FTP server.
6. Click **Save**.

5.1.3 Set NAS

Take network server as network disk to store the record files, captured images, etc.

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration → Storage → Storage Management → Net HDD**.
2. Click **Add**.
3. Set **Mounting Type**.

Mounting Type

Select file system protocol according to the operation system.

Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.

4. Set the **Server Address** and **File Path** for the disk.

Server Address

The IP address of the network disk.

File Path

The saving path of network disk files.

5. Click **Test** to check whether the network disk is available.
6. Click **OK** to finish the steps to add a Net HDD.
7. **Optional:** Configure the Net HDD.

Edit Click  to edit the parameter setting.

Delete Delete the Net HDD.

- Click .
- Select the Net HDD, click **Delete**.

8. Click **Save**.

5.1.4 eMMC Protection

It is to automatically stop the use of eMMC as a storage media when its health status is poor.



Note

The eMMC protection is only supported by certain device models with an eMMC hardware.

Go to **Configuration → System → System Settings → System Service** for the settings.

eMMC, short for embedded multimedia card, is an embedded non-volatile memory system. It is able to store the captured images or videos of the device.

The device monitors the eMMC health status and turns off the eMMC when its status is poor. Otherwise, using a worn-out eMMC may lead to device boot failure.

5.1.5 Set Cloud Storage

It helps to upload the captured pictures and data to the cloud. The platform requests picture directly from the cloud for picture and analysis. The function is only supported by certain models.

Steps



Caution

If the cloud storage is enabled, the pictures are stored in the cloud video manager firstly.

1. Go to **Configuration → Storage → Storage Management → Cloud Storage** .

2. Check **Enable**.

3. Set basic parameters.

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. You are recommended to use the default port.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.
Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

4. Click **Test** to test the configured settings.

5. Click **Save**.

5.2 Video Recording

This part introduces the operations of manual and scheduled recording, playback, and downloading recorded files.

5.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

Select **Trigger Recording** in event settings for each record type except **Continuous**. See [**Event and Alarm**](#) for details.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule** .

2. Check **Enable**.

3. Select a record type.



Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

When motion detection is enabled and trigger recording is selected as linkage method, object movement is recorded.

Alarm

When alarm input is enabled and trigger recording is selected as linkage method, the video is recorded after receiving alarm signal from external alarm input device.

Motion | Alarm

Video is recorded when motion is detected or alarm signal is received from the external alarm input device.

Motion & Alarm

Video is recorded only when motion is detected and alarm signal is received from the external alarm input device.

Event

The video is recorded when configured event is detected.

4. Set schedule for the selected record type. Refer to **Set Arming Schedule** for the setting operation.
5. Set the advanced recording parameters.

Overwrite

Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos.

Pre-record

The time period you set to record before the scheduled time.

Post-record

The time period you set to stop recording after the scheduled time.

Stream Type

Select the stream type for recording.



Note

When you select the stream type with higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

Recording Expiration

The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they can not be recovered.

6. Click **Save**.

5.2.2 Record Manually

Steps

1. Go to **Configuration → Local**.
2. Set the **Video Size** and **Video Saving Path** for recorded video files.
3. Click **Save**.
4. Click  in the live view interface to start recording. Click  to stop recording.

What to do next

View the recorded video files.

Go to **Configuration → Local** and click **Open** behind **Video Saving Path** to open the saving path and view the files.

5.2.3 Playback and Download Video

You can search, playback, clip and download the videos stored in the local storage or network storage.

Steps

1. Go to **Playback → Video**.
2. Set search condition and click **Search**.
The matched video files showed on the timing bar.
3. Click  to play the video files.
 - Click  to play video files in full screen. Press **ESC** to exit full screen.
 - Click  to stop video playback for all channels.
4. **Optional:** Click  to clip video files. Click  again to stop clipping video files



Note

Go to **Configuration → Local → Clip Saving Path**, view and change the saving path of clipped video files.

-
5. **Optional:** Click  on the playback interface to download files.



Note

Go to **Configuration → Local → Downloaded File Saving Path**, view and change the saving path of downloaded video files.

5.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

5.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to **Event and Alarm** for event settings.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Picture Capture**.
2. Set capture schedule. Refer to **Set Arming Schedule** for configuring schedule time.

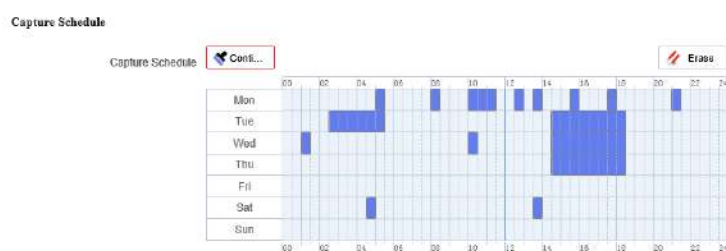


Figure 5-1 Set Capture Schedule

3. Set the capture type.

Scheduled

Capture a picture at the configured time interval.

Event-Triggered

Capture a picture when an event is triggered.

4. Set the **Format, Resolution, Quality, Interval, and Capture Number**.



Note

The resolution of the captured picture is the same as the resolution of the captured picture stream. You can select **Stream Type** in **Advanced**.

5. Click **Save**.

5.3.2 Capture Manually

Steps

1. Go to **Configuration → Local**.

2. Set the **Image Format** and saving path to for snapshots.

JPEG

The picture size of this format is comparatively small, which is better for network transmission.

BMP

The picture is compressed with good quality.

3. Click **Save**.
4. Click  near the live view or play back window to capture a picture manually.

5.3.3 View and Download Picture

You can search, view and download the pictures stored in the local storage or network storage.

Steps

1. Go to **Playback → Picture**.
2. Set search condition and click **Search**.
The matched pictures showed in the file list.
3. Download the pictures.
 - Select the pictures then click **Download** to download them.
 - Click **Download This Page** to download the pictures of this page.
 - Click **Download All** to download all the pictures.



Note

Go to **Configuration → Local → Playback Capture Saving Path**, view and change the saving path of captured pictures when playback.

Chapter 6 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm. Certain events may not be supported by certain device models.

6.1 Set Motion Detection

It helps to detect the moving objects in the detection region and trigger the linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Motion Detection**.
2. Check **Enable**.
3. **Optional:** Highlight to display the moving object in the image in green.
 - 1) Check **Enable Dynamic Analysis for Motion**.
 - 2) Go to **Configuration → Local**.
 - 3) Set **Rules** to **Enable**.
4. Select mode in **Configuration**, and set rule region and rule parameters.
 - For the information about normal mode, see **Normal Mode**.
 - For the information about expert mode, see **Expert Mode**.
5. Set the arming schedule and linkage methods. For the information about arming schedule settings, see **Set Arming Schedule**. For the information about linkage methods, see **Linkage Method Settings**.
6. Click **Save**.

6.1.1 Expert Mode

You can configure different motion detection parameters for day and night according to the actual needs.

Steps

1. Select **Expert Mode** in **Configuration**.
2. Set parameters of expert mode.

Scheduled Image Settings

OFF

Image switch is disabled.

Auto-Switch

The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

Scheduled-Switch

The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

Sensitivity

The higher the value of sensitivity is, the more sensitive the motion detection is. If scheduled image settings is enabled, the sensitivity of day and night can be set separately.

3. Select an **Area** and click . Click and drag the mouse on the live image and then release the mouse to finish drawing one area.



Figure 6-1 Set Rules

4. Click  to clear all the areas.
5. Click **Save**.
6. **Optional:** Repeat above steps to set multiple areas.

6.1.2 Normal Mode

You can set motion detection parameters according to the device default parameters.

Steps

1. Select **Normal Mode** in **Configuration**.
2. Set the **Sensitivity** of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to **0**, motion detection and dynamic analysis do not take effect.
3. Set **Detection Target**. Human and vehicle are available. If the detection target is not selected, all the detected targets will be reported, including the human and vehicle. This function allows alarm triggering by specified target types (human and vehicle).



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

4. Click  . Click and drag the mouse on the live image, and then right click the mouse to finish drawing one area.
5. **Optional:** Click  to clear all the areas.
6. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6.2 Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Video Tampering** .
2. Check **Enable**.
3. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
4. Click  and drag the mouse in the live view to draw the area.

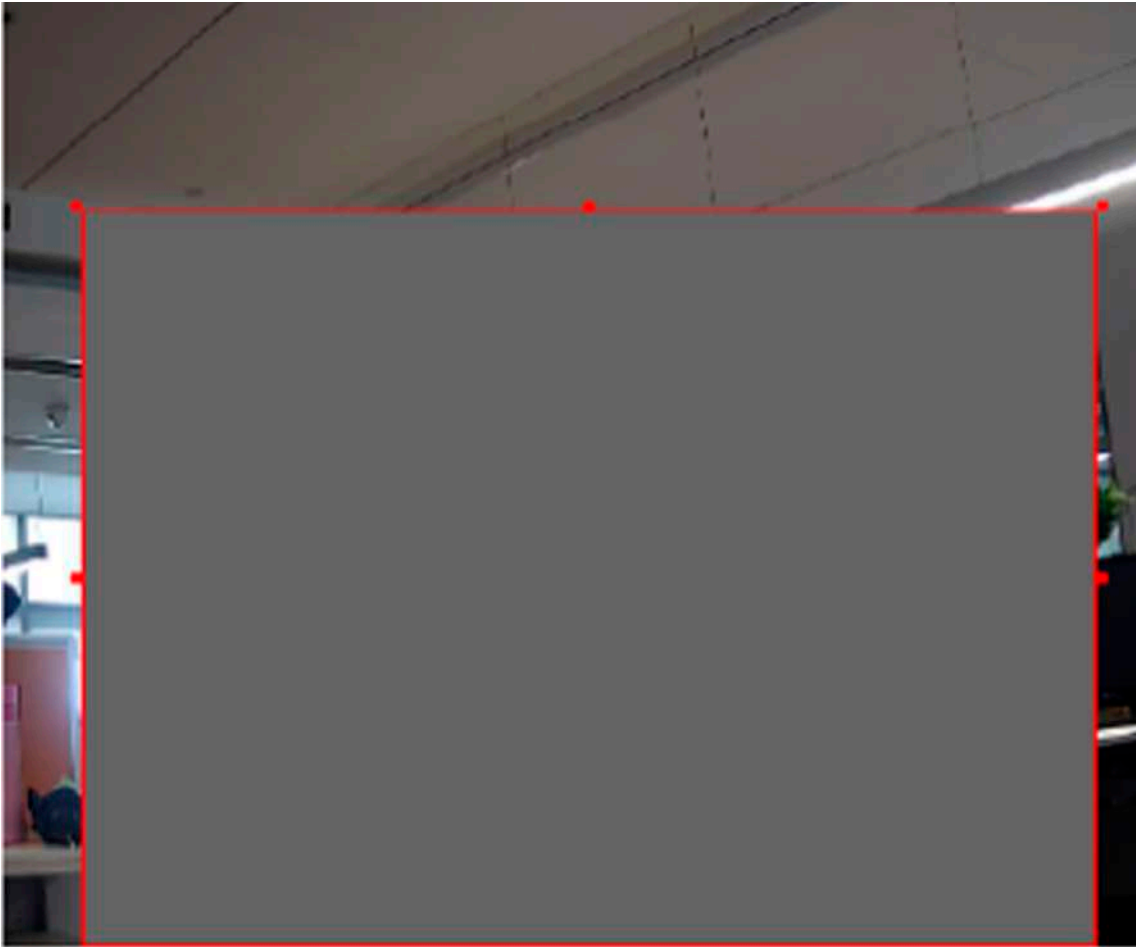


Figure 6-2 Set Video Tampering Area

5. **Optional:** Click  to delete all the drawn areas.
6. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
7. Click **Save**.

6.3 Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start



Note

This function is only supported by certain models.

Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Configuration → Event → Event and Detection → Alarm Input** .
2. Select an **Alarm Input NO.** and click  to set alarm input.
3. Select **Alarm Type** from the dropdown list. Edit the **Alarm Name**.
4. Check **Enable Alarm Input Handling**.
5. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
6. Click **Copy to...** to copy the settings to other alarm input channels.
7. Click **Save**.

6.4 Set Exception Alarm

Exception such as network disconnection can trigger the device to take corresponding action.

Steps

1. Go to **Configuration → Event → Event and Detection → Exception** .
2. Select **Exception Type**.

HDD Full

The HDD storage is full.

HDD Error

Error occurs in HDD.

Network Disconnected

The device is offline.

IP Address Conflicted

The IP address of current device is same as that of other device in the network.

Illegal Login

Incorrect user name or password is entered.

3. Refer to **Linkage Method Settings** for setting linkage method.
4. Click **Save**.

6.5 Set Video Quality Diagnosis

When the video quality of the device is abnormal and the alarm linkage is set, the alarm will be triggered automatically.

Steps

1. Go to **Configuration → Event → Event and Detection → Video Quality Diagnosis** .
2. Select **Diagnosis Type**.
3. Set the corresponding parameters.

Alarm Detection Interval

The time interval to detect the exception.

Sensitivity

The higher the value is, the more easily the exception will be detected, and the higher possibility of misinformation would be.

Alarm Delay Times

The device uploads the alarm when the alarm reaches the set number of times.

4. Check the selected diagnosis type, and the related type will be detected.
5. Set arming schedule. See **Set Arming Schedule** .
6. Set linkage method. See **Linkage Method Settings** .
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with models.

6.6 Set Audio Exception Detection

Audio exception detection function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

Steps

1. Go to **Configuration → Event → Event and Detection → Audio Exception Detection** .
2. Select one or several audio exception detection types.

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.



Note

- The lower the sensitivity is, the more significant the change should be to trigger the detection.
- The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage methods.
4. Click **Save**.



Note

The function is only supported by certain models. The actual function varies according to different models.

6.7 Set Defocus Detection

The blurred image caused by lens defocus can be detected. If it occurs, the device can take linkage actions.

Steps

1. Go to **Configuration → Event → Event and Detection → Defocus Detection** .
 2. Check **Enable**.
 3. Set **Sensitivity**. The higher the value is, the more easily the defocus image can trigger the alarm. You can adjust the value according to the actual environment.
 4. For the linkage method settings, refer to **Linkage Method Settings** .
 5. Click **Save**.
-



Note

The function is only supported by certain models. The actual display varies with models.

6.8 Set Scene Change Detection

Scene change detection function detects the change of the scene. Some certain actions can be taken when the alarm is triggered.

Steps

1. Go to **Configuration → Event → Event and Detection → Scene Change Detection** .
 2. Click **Enable**.
 3. Set the **Sensitivity**. The higher the value is, the more easily the change of scene can be detected. But the detection accuracy is reduced.
 4. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
 5. Click **Save**.
-



Note

The function is only supported by certain models. The actual display varies with models.

Chapter 7 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

7.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. **Optional:** Click **Arming Schedule and Linkage Method** in the related event interface.
2. Click **Edit** behind **Arming Schedule**.
3. Click **Draw**, and drag the time bar to draw desired valid time.



Note

- Each cell represents 30 minutes.
 - Move the mouse over the drawn time period to see specific time periods and fine-tune the start time and end time.
 - Up to 8 periods can be configured for one day.
4. Click **Erase**, and drag the time bar to clear selected valid time.
 5. Click **OK** to save the settings.



Figure 7-1 Set Arming Schedule

7.2 Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

7.2.1 Trigger Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps

1. Go to **Configuration → Event → Alarm Setting → Alarm Output** .
2. Set alarm output parameters.

Automatic Alarm For the information about the configuration, see [Automatic Alarm](#) .

Manual Alarm For the information about the configuration, see [Manual Alarm](#) .

Manual Alarm

You can trigger an alarm output manually.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click  to set alarm parameters.

Alarm Name

Custom a name for the alarm output.

2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Before You Start

Make sure the alarm output device is connected to the device.

Steps

1. Select the **Alarm Output No.** according to the alarm interface connected to the external alarm device. Click  to set alarm parameters.

Alarm Name

Custom a name for the alarm output.

Delay

It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see [Set Arming Schedule](#) .
3. **Optional:** Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

7.2.2 FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refer to [Set FTP](#) to set the FTP server.

Refer to [Set NAS](#) for NAS configuration.

Refer to [Set New or Unencrypted Memory Card](#) for memory card storage configuration.

7.2.3 Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refer to [Set Email](#) .

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated recipients if an alarm event is detected.

Before You Start

Set the DNS server before using the Email function. Go to **Configuration → Network → Network Settings → TCP/IP** for DNS settings.

Steps

1. Go to email settings page: **Configuration → Event → Alarm Setting → Email** .
2. Set email parameters.
 - 1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
 - 2) **Optional:** If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
 - 3) Set the **E-mail Encryption**.
 - When you select **TLS**, and disable **STARTTLS**, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
 - When you select **TLS** and check **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the **SMTP Port** should be set as 25.



If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.

- 4) **Optional:** If you want to receive notification with alarm pictures, check **Attached Picture**. The notification email has a certain number of attached alarm pictures about the event with configurable image capturing interval.



The number of alarm pictures may vary according to different device models and different events.

- 5) Input the recipient's information, including the recipient's name and address.
6) Click **Test** to see if the function is well configured.

3. Click **Save**.

7.2.4 Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

7.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event. For recording settings, refer to [**Video Recording and Picture Capture**](#).

7.2.6 Flashing Light

After enabling **Flashing Light** and setting the **Flashing Light Alarm Output**, the light flashes when an alarm event is detected.

Set Flashing Alarm Light Output

When events occur, the flashing light on the device can be triggered as an alarm.

Steps

1. Go to **Configuration → Event → Alarm Setting → Flashing Alarm Light Output**.
2. Set **Flashing Duration** and **Flashing Frequency**.

Flashing Duration

The time that the flashing lasts when one alarm happens.

Flashing Frequency

The rate at which the light flashes. High frequency, medium frequency, low frequency, and normally on are selectable.

3. Set the arming schedule. See [Set Arming Schedule](#) for details.

4. Click **Save**.



Note

Only certain device models support the function.

7.2.7 Audible Warning

After enabling **Audible Warning** and setting **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when an alarm happens.

For audible alarm output settings, refer to [Set Audible Alarm Output](#).



Note

The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Alarm Setting → Audible Alarm Output**.

2. Select **Sound Type** and set related parameters.

- Select **Prompt** and set the alarm times you need.
- Select **Warning** and its contents. Set the alarm times you need.
- Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Set → Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.

3. **Optional**: Click **Test** to play the selected audio file on the device.

4. Set arming schedule for audible alarm. See [Set Arming Schedule](#) for details.

5. Click **Save**.



Note

The function is only supported by certain device models.

7.2.8 Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTPS, or ISUP data transmission.

Set Alarm Server

Steps

1. Go to **Configuration → Event → Alarm Setting → Alarm Server** .
2. Enter **Destination IP or Host Name**, **URL**, and **Port**.
3. Select **Protocol**.



Note

HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

-
4. Click **Test** to check if the IP or host is available.
 5. Click **Save**.

Chapter 8 Network Settings

8.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration** → **Network** → **Network Settings** → **TCP/IP** for parameter settings.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.



Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.



Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address**, **IPv6 Subnet**, **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

Domain Name Settings

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.



Note

DHCP should be enabled for the dynamic domain name to take effect.

8.2 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name. The DDNS service of the device only supports HTTPS.

Before You Start

Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps

1. Refer to **TCP/IP** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Network Settings → DDNS**.
3. Check **Enable** and select **DDNS Type**.

DynDNS

Dynamic DNS server is used for domain name resolution.

NO-IP

NO-IP server is used for domain name resolution.

4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to **Port Mapping** for port mapping settings.
6. Access the device.

By Browsers

Enter the domain name in the browser address bar to access the device.

By Client Software Add domain name to the client software. Refer to the client manual for specific adding methods.

8.3 Access to Device via PPPoE Dial Up Connection

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps

1. Go to **Configuration → Network → Network Settings → PPPoE** .
2. Check **Enable**.
3. Set the PPPoE parameters.

Dynamic IP

After successful dial-up, the dynamic IP address of the WAN is displayed.

User Name

User name for dial-up network access.

Password

Password for dial-up network access.

Confirm

Input your dial-up password again.

4. Click **Save**.
5. Access the device.

By Browsers Enter the WAN dynamic IP address in the browser address bar to access the device.

By Client Software Add the WAN dynamic IP address to the client software. Refer to the client manual for details.



Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to **[Access to Device via Domain Name](#)** for detail information.

8.4 SNMP

You can set the SNMP (Simple Network Management Protocol) to get device information in network management.

Before You Start

Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to **Configuration → Network → Network Settings → SNMP**.
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.



Note

The SNMP version you select should be the same as that of the SNMP software.

And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

-
3. Configure the SNMP settings.
 4. Click **Save**.

8.5 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X.

Go to **Configuration → Network → Network Settings → 802.1X**, and enable the function.

Select protocol and version according to router information. User name and password of server are required.



Note

- If you set the **Protocol** to **EAP-TLS**, select the **Client Certificate** and **CA Certificate**.
 - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
-

8.6 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.



Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Network Settings → QoS**.
2. Set **Video/Audio DSCP**, **Event/Alarm DSCP** and **Management DSCP**.



Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.

3. Click **Save**.

8.7 HTTP(S)

HTTP is an application-layer protocol for transmitting hypermedia documents. HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Network Service → HTTP(S)**.
 2. Enter **HTTP Port**.
-



Note

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter `http://192.168.1.64:81` in the browser for login.

3. Check **Enable** in **HTTPS**.
-



Note

You can click **TLS Settings** to set the TLS version that the device supports. Refer to for details.

4. Enter **HTTPS Port**.
5. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
6. Select **Server Certificate**.
7. Set **Web Authentication**.

Authentication

Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

8. Click **Save**.

8.8 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Go to **Configuration → Network → Network Service → Multicast** for the multicast settings.

IP Address

It stands for the address of multicast host.

8.8.1 Multicast Discovery

Go to **Configuration → Network → Network Settings → TCP/IP** to enable this function.

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

8.9 RTSP

RTSP (Real Time Streaming Protocol) is an application-layer controlling protocol for streaming media.

Steps

1. Go to **Configuration → Network → Network Service → RTSP**.

2. Enter **Port**.

3. Set **Multicast** parameters.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

4. Set **RTSP Authentication**.

Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to

the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

5. Click **Save**.

8.10 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

Steps

1. Go to **Configuration → Network → Network Service → SRTP**.
2. Enter the **Port** number.
3. Set **Multicast** parameters.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

4. Select **Server Certificate**.
5. Select **Encrypted Algorithm**.
6. Click **Save**.



Note

- Only certain device models support this function.
 - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
-

8.11 Bonjour

It is an implementation of zero-configuration networking (zeroconf), a group of technologies that includes service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records.

Go to **Configuration → Network → Network Service → Bonjour** to enable the function, and click **Save**.

After enabling the function, the device spread and receive service information in local area network.

8.12 WebSocket(s)

WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

Go to **Configuration → Network → Network Service → WebSocket(s)** to set parameters, and click **Save**.

WebSocket

TCP-based full-duplex communication protocol port for plug-in free preview via HTTP protocol.

WebSockets

TCP-based full-duplex communication protocol port for plug-in free preview via HTTPS protocol.

8.13 Port Mapping

By setting port mapping, you can access devices through the specified port.

Steps

1. Go to **Configuration → Network → Network Service → NAT**.
2. Select the port mapping mode.

Auto Port Mapping Refer to [Set Auto Port Mapping](#) for detailed information.

Manual Port Mapping Refer to [Set Manual Port Mapping](#) for detailed information.

3. Click **Save**.

8.13.1 Set Auto Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.



Note

UPnP™ function on the router should be enabled at the same time.

8.13.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.

2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

8.13.3 Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding** → **Virtual Servers**, and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

108M Wireless Router
Model No.: TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- + Network
- + Wireless
- Advanced Settings ---
- + DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- + Security
 - Static Routing
 - Dynamic DNS
- Maintenance ---
- + System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☒
2	8000	192.168.10.23	ALL	☒
3	554	192.168.10.23	ALL	☒
4	8200	192.168.10.23	ALL	☒
5	81	192.168.10.24	ALL	☒
6	8001	192.168.10.24	ALL	☒
7	555	192.168.10.24	ALL	☒
8	8201	192.168.10.24	ALL	☒

Common Service Port: ID

Figure 8-1 Port Mapping on Router

Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

8.14 RTCP

The device relies on RTCP (Real-time Transport Control Protocol) to deliver packets sequentially to provide a reliable delivery mechanism and to provide services for flow control or congestion control.

Go to **Configuration → Network → Network Service → RTCP** and check **Enable** to enable the function.

8.15 Wireless Dial

Data of audio, video and image can be transferred via 3G/4G wireless network.

Note

The function is only supported by certain device models.

8.15.1 Set Wireless Dial

The built-in wireless module offers dial-up access to the Internet for the device.

Before You Start

Get a SIM card, and activate 3G/4G services. Insert the SIM card to the corresponding slot.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial**.
2. Check to enable the function.
3. Go to **Dial Parameters** to configure and save the parameters.
4. Click **Settings** behind **Dial Plan**. See [Set Arming Schedule](#) for detailed information.
5. View the **Dial Status**.

Click Refresh Refresh the dial status.

Click Disconnect Disconnect the 3G/4G wireless network.

When the **Dial Status** turns to **Connected**, it means a successful dial.

6. Access the device via the **IP Address** of the computer in the network.
 - Input the IP address in the browser to access the device.
 - Add the device in client application. Select **IP/Domain**, and input IP address and other parameters to access the device.

7. Optional: You can view 4G SIM card information and network carrier information.



Note

For certain device models working on **Performance Mode** or **Proactive Mode**, the wireless mode can be upgraded. If necessary, please upgrade the wireless mode under the guidance of a professional.

- 8. Optional:** Click **Re-Camp** to reconnect the device to wireless network manually. The device will maintain airplane mode for 10 seconds and then connects to network automatically.
- 9. Optional:** Check **Enable** to enable **Auto Re-Camp**, and then set the **Re-Camp Interval**. The device will reconnect to the wireless network at set **Re-Camp Interval** automatically.
-



Note

The function may vary according to different device models.

8.15.2 Wireless Expert Settings

Wireless expert settings provide more details of the 3G/4G wireless network to which the device connects and help the professionals troubleshoot potential network issues.

Cell Radio Frequency Parameters

Cell radio frequency parameters provides the current wireless network information to which the device is connected.

Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings** to view cell radio frequency parameters.

Network Info

It displays the current cellular network information. You can click **Refresh** to view the frequency information of different cells.

Radio Frequency Fluctuation

It records the fluctuation of the cellular network to which the device has connected during the past 7 days. Click **Export Report** and set and confirm the encryption password to export the fluctuation report.

Lock Band

You can lock a set of bands that get the device faster data rates to improve the network speed.

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings → Lock Band**.
2. Check **Enable**.

3. Click **Add** and enter the band.



Note

- The band you enter should be B + number or N + number. For example, you can enter B1 or N1.
- Up to five bands are supported.

4. **Optional:** Click  to delete the selected band. You can also click **Clear All** to clear the list.

Capture Baseband Packet

This function can capture the protocol interaction packet to help the professionals to locate the communication failures between 4G module and the base station.

Steps



Note

This function is reserved for the professionals and technical support staff.

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings**.
2. Click **Configuration** behind **Capture Baseband Packet** to enter the setting interface.
3. Check **Enable** to enable this function.
4. Set capture duration and the saving path. The saving path depends on the actual storage method of the device. You can click **Delete Captured Packet Under This Path** to delete the captured packet.
5. Click **Save**.
6. Click **Start Capturing Packet** to capture the baseband packet.
7. **Optional:** Click **Stop Capturing** to stop the capturing process.
8. After the capturing is completed, click **Export Captured Packet** to save the report.

Speed Test

Steps

1. Go to **Configuration → Network → Network Settings → Wireless Dial → Expert Settings**.
2. Click **Configuration** behind **Speed Test** to enter the setting interface.
3. Select the default server or enter the server address. You can follow the steps below to get the nearby server address.



Note

You can follow the steps below to get the nearby server address.

- a. Visit this website to get the nearby server address: <https://www.speedtest.net/speedtest-servers-static.php>.
- b. Select and copy the URL of the nearby speed test station and paste it in **Server Address**.

4. Click **Speed Test** to start the test.

You can view the speed details after the test is completed. You can also click **Export Speed Test Result**.

8.16 WLAN AP (Access Point)

The device can be used as a wireless access point with the WLAN AP function. You can connect your phone or PC to the device AP, so as to access to the device and configure the parameters via your phone or PC.



Note

The function is only supported by certain device models.

8.16.1 Set WLAN AP

Steps

1. Go to **Configuration → Network → Network Settings → WLAN AP**.
2. Select the WLAN AP mode.

On

The function is enabled.

Maintenance Mode

The WLAN AP function is automatically turned on for 5 minutes after the device is cold booted (by turning the switch on the device to **ON**), after which the WLAN AP function is turned off if the device's 4G communication is normal, and remains on if the device's 4G communication is abnormal.

Off

The function is disabled.

3. Set the related parameters.

SSID

For certain device models, the default SSID of the device is named as "Hik-Serial Number".

For certain device models, the default SSID of the device is named as "Default SSID" on the device label.

You can define it as needed.

Security Mode

WPA2-personal mode is supported.

Encryption Type

AES and **TKIP** are selectable.

Password

The password for wireless connection via the device AP. The default password is the nine-digit serial number of the camera. Please change the default password and set a strong password after logging in for the first time.



Caution

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 **Save**.



Note

The function may vary according to different device models.

What to do next

You can connect your mobile phone or PC to the AP.

8.16.2 Access to Device via AP

You can access to the device via the device AP when the device cannot connect to the network.

Steps

1. Go to **Configuration** → **Network** → **Network Settings** → **WLAN AP** to enable WLAN AP function.

For certain device models, the WLAN AP function is automatically turned on for 5 minutes after the device is cold booted (by turning the switch on the device to **ON**), after which the WLAN AP function is turned off if the device's 4G communication is normal, and remains on if the device's 4G communication is abnormal.

2. Search the device WLAN AP in the WLAN list of your phone or PC.

3. Enter the password and connect your mobile phone or PC to the AP.



Note

- The AP name is SSID ("Hik-Serial Number" by default). The password is serial number by default. The serial number can be obtained from **Configuration** → **System** → **System Settings** → **Basic Information**.
- For certain device models, the AP name is the "Default SSID" on the device label.

4. Enter the IP address in the browser.



Note

The default IP of the device AP is 192.168.8.1.

Result

The connected devices will be displayed in the **Connected Device** interface.

8.17 Traffic Shaping

Traffic shaping is used to shape and smooth video data packet before transmission.

It helps to improve latency and reduce packet loss caused by network congestion and ensure the video quality as well. Shaping level is configurable.

8.18 Data Monitoring

You can view and manage the SIM card data or wired network data used by the device. SIM card data is the data service provided by network carriers; wired network data is usually provided through a 4G router.

Steps

1. Go to **Configuration → Network → Network Settings → Data Monitoring**.
2. Check **Enable**.
3. Set the following parameters according to your data plan.

Plan Type

Daily, Monthly, or Annually can be selected.

Data Plan

Enter the amount of usable data and select the unit.

Pre-Alarm Threshold

When the used data reaches the set percentage of data plan, the device sends an alarm message, and shows notification on the OSD or pop-up window.

4. Select **Normal Linkage**.

If **Send Email** or **Notify Surveillance Center** is selected, the device sends an alarm message by Email or to surveillance center when the used data reaches the threshold.

5. Click **Save**.



Note

The function varies with different device models.

8.19 Wi-Fi

Connect the device to wireless network by setting Wi-Fi parameters.



Note

This function is only supported by certain device models.

8.19.1 Connect Device to Wi-Fi

Before You Start

Refer to the user manual of wireless router or AP to set SSID, key, and other parameters.

Steps

1. Go to TCP/IP settings page: **Configuration → Network → Network Settings → TCP/IP** .
2. Select **Wlan** to set the parameters. Refer to **TCP/IP** for detailed configuration.



Note

For stable use of Wi-Fi, it is not recommended to use DHCP.

3. Go to Wi-Fi settings page: **Configuration → Network → Network Service → Wi-Fi** .
4. Set and save the parameters.
 - 1) Check to enable Wi-Fi function.
 - 2) Click **Refresh** to view and select the available wireless router or AP, or click **+** to add it manually.
 - 3) Select or input a **SSID**, which should be the same as that of wireless router or AP.
The parameters of the network is automatically shown in **Wi-Fi**.
 - 4) Select the **Network Mode** as **Manage**.
 - 5) Select the **Security Mode** according to your needs, and the parameters should be the same as those of the wireless network connection you set on the router or AP.
 - 6) Click **Save**.

What to do next

Go to TCP/IP settings page: **Configuration → Network → Network Settings → TCP/IP** , and click **Wlan** to check the **IPv4 Address** and log in the device.

8.20 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Platform Access → ISUP** .
2. **Optional:** Select an access center.
3. Check **Enable**.
4. Select a protocol version and enter related parameters.
5. Click **Save**.

Register status turns to **Online** when the function is correctly set.

8.21 Access Camera via Hik-Connect

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.

Before You Start

Connect the camera to network with network cables.

Steps

1. Get and install Hik-Connect application by the following ways.
 - Visit <https://appstore.hikvision.com> to download the application according to your mobile phone system.
 - Visit the official site of our company. Then go to **Support** → **Tools** → **Hikvision App Store** .
 - Scan the QR code below to download the application.



Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit <https://appstore.hikvision.com/static/help/index.html> to refer to the troubleshooting.
- Visit <https://appstore.hikvision.com/> , and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

-
2. Start the application and register for a Hik-Connect user account.
 3. Log in after registration.
 4. In the app, tap "+" on the upper-right corner and then scan the QR code of the camera to add the camera. You can find the QR code on the camera or on the cover of the Quick Start Guide of the camera in the package.
 5. Follow the prompts to set the network connection and add the camera to your Hik-Connect account.

For detailed information, refer to the user manual of the Hik-Connect app.

8.21.1 Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

Before You Start

You need to activate the camera before enabling the service.

Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Platform Access → Hik-Connect .**
3. Check **Enable**.
4. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
5. Create a verification code or change the old verification code for the camera.



Note

The verification code is required when you add the camera to Hik-Connect service.

6. Save the settings.

Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.



Note

The verification code is required when you add the camera to Hik-Connect service.

5. Click and read "Terms of Service" and "Privacy Policy".
6. Confirm the settings.

8.21.2 Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
 - Visit <https://appstore.hikvision.com> to download the application according to your mobile phone system.
 - Visit the official site of our company. Then go to **Support → Tools → Hikvision App Store .**
 - Scan the QR code below to download the application.



Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit <https://appstore.hikvision.com/static/help/index.html> to refer to the troubleshooting.
- Visit <https://appstore.hikvision.com/>, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

-
2. Start the application and register for a Hik-Connect user account.
 3. Log in after registration.

8.21.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.



Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

-
5. Input the verification code of your camera.



Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

-
6. Tap **Connect to a Network** button in the popup interface.
 7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection

Input the Wi-Fi password that your mobile phone has connected to, and tap **Next** to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)

Wired Connection

Connect the camera to the router with a network cable and tap **Connected** in the result interface.



Note

The router should be the same one which your mobile phone has connected to.

8. Tap **Add** in the next interface to finish adding.

For detailed information, refer to the user manual of the Hik-Connect app.

8.22 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Platform Access → Open Network Video Interface**.
2. Check **Enable**.
3. Select an authentication mode.
 - If you select **Digest**, the device only supports digest authentication.
 - If you select **Digest&ws-username token**, the device supports digest authentication or ws-username token authentication.
4. Click **Add** to configure the Open Network Video Interface user.
5. Click **Save**.
6. **Optional**: Repeat the steps above to add more Open Network Video Interface users.
7. **Optional**: Manage the user.
 - Click  to delete the selected Open Network Video Interface user.
 - Click  to modify the selected Open Network Video Interface user.

8.23 Set SDK Service

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

Steps

1. Go to **Configuration → Network → Platform Access → SDK Service**.
2. Set **SDK Service** parameters.
 - 1) Check **Enable** to add the device to the client software with SDK protocol.
 - 2) Enter the **Port** number.
3. Set **Enhanced SDK Service** parameters.
 - 1) Check **Enable** to add the device to the client software with SDK over TLS protocol.
 - 2) **Optional**: Click **TLS Settings** to enable the TLS version that the device supports. Refer to [TLS](#) for details.
 - 3) Enter the **Port** number.
 - 4) Select a server certificate to make sure the data transmission security. You can click **Certificate Management** to add a certificate. Refer to [Certificate Management](#) for details.
4. Click **Save**.

Chapter 9 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

9.1 System Settings

9.1.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration → System → System Settings → Basic Information** to view the device information.

9.1.2 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

Synchronize Time Manually

Steps

1. Go to **Configuration → System → System Settings → Time Settings**.
2. Select **Time Zone**.
3. Select **Manual Time Sync.**
4. Choose one time synchronization method.
 - Select **Set Time**, and manually input or select date and time from the pop-up calendar.
 - Click **Sync. with computer time** to synchronize the time of the device with that of the local PC.
5. Click **Save**.

Set NTP Server

You can use NTP server when accurate and reliable time source is required.

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration → System → System Settings → Time Settings**.
2. Select **Time Zone**.

3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.



Note

Server Address is NTP server IP address.

5. Click **Test** to test server connection.
6. Click **Save**.

Synchronize Time by Satellite



Note

This function varies depending on different devices.

Steps

1. Enter **Configuration → System → System Settings → Time Settings**.
2. Select **Satellite Time Sync**.
3. Set **Interval**.
4. Click **Save**.

Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → Time Settings**.
2. Check **Enable**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

9.1.3 Set RS-232

RS-232 can be used to debug device or access peripheral device. RS-232 can realize communication between the device and computer or terminal when the communication distance is short.

Before You Start

Connect the device to computer or terminal with RS-232 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-232**.
2. Set RS-232 parameters to match the device with computer or terminal.
3. Click **Save**.

9.1.4 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

Before You Start

Connect the device and computer or terminal with RS-485 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-485**.
2. Set the RS-485 parameters.



Note

You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.

9.1.5 Set Live View Connection

It controls the remote live view connection amount.

Live view connection controls the maximum live view that can be streamed at the same time.

Enter **Configuration → System → System Settings → System Service** to set the upper limit of the remote connection number.

9.1.6 Location Settings

Location displays and uploads the current longitude and latitude of the device.

Auto Uploading

Check **Enable** and set **Location Upload Interval**.

The device will upload its location at the set interval. You can also click **Refresh** to upgrade the device location manually.

Manual Settings

Check **Enable** and set **Location Upload Interval**. Enter the longitude and latitude of the device and click **Save**.

The device will upload the set location at the set interval.



Note

This function may vary according to different device models.

9.1.7 External Device

For the device supporting external devices, including the supplement light, wiper on the housing, the LED light, and heater, you can control them via the Web browser when it is used with the housing. External devices vary with models.

9.1.8 View Open Source Software License

On the top-right corner, click  and select **Open Source Software Description** to download the license. You can view the license in the editor.

9.1.9 Wiegand



Note

This function is only supported by certain camera models.

Check **Enable** and select the protocol. The default protocol is SHA-1 26bit.

If enabled, the recognized license plate number will be output via the selected Wiegand protocol.

9.2 User and Account

9.2.1 Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.



Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

Steps

1. Go to **Configuration → System → User Management → User Management**.
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

Administrator

The administrator has the authority to all operations and can add users and operators and assign permission.

User

Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

Modify Select a user and click  to change the password and permission.

Delete Select a user and click  .



Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

9.2.2 Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management → Online Users** , click **General**, and set **Simultaneous Login**.

9.2.3 Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

9.3 Maintenance

9.3.1 Restart

You can restart the device via browser.

Go to **Maintenance and Security → Maintenance → Restart** , and click **Restart**.

9.3.2 Upgrade

Before You Start

You need to obtain the correct upgrade package.



Caution

DO NOT disconnect power during the process, and the device restarts automatically after upgrade.

Steps

1. Go to **Maintenance and Security → Maintenance → Upgrade**.
2. Choose one method to upgrade.

Firmware Locate the exact path of the upgrade file.

Firmware Directory Locate the directory which the upgrade file belongs to.

3. Click  to select the upgrade file.
4. Click **Upgrade**.

9.3.3 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps

1. Go to **Maintenance and Security → Maintenance → Backup and Restore**.
2. Click **Restore** or **Default** according to your needs.

Restore Reset device parameters, except user information, IP parameters and video format to the default settings.

Default Reset all the parameters to the factory default.



Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

9.3.4 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

Steps

1. Export configuration file.
 - 1) Go to **Maintenance and Security → Maintenance → Backup and Restore → Backup**.
 - 2) Click **Export** and input the encryption password to export the current configuration file.
 - 3) Set the saving path to save the configuration file in local computer.
2. Import configuration file.
 - 1) Access the device that needs to be configured via web browser.
 - 2) Go to **Maintenance and Security → Maintenance → Backup and Restore → Reset**.
 - 3) Click  to select the saved configuration file.
 - 4) Input the encryption password you have set when exporting the configuration file.

5) Click **Import**.

9.3.5 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Maintenance and Security → Maintenance → Log**.
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

The matched log files will be displayed on the log list.

4. **Optional:** Click **Export** to save the log files in your computer.

9.3.6 Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Steps



Note

This function is only supported by certain camera models.

1. Go to **Maintenance and Security → Maintenance → Security Audit Log**.
2. Select log types, **Start Time**, and **End Time**.
3. Click **Search**.

The log files that match the search conditions will be displayed on the Log List.

4. **Optional:** Click **Export** to save the log files to your computer.

9.3.7 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Maintenance and Security → Maintenance → Device Debugging**, and click **Settings** of **SSH**. You can edit the number of the port. Click **Save**.



Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

9.3.8 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Maintenance and Security → Maintenance → Device Debugging → Diagnose Information** . Click **Export**. In the pop-up window, check desired diagnose information and click **Export** to export corresponding diagnose information of the device.

9.3.9 Diagnosis

For the device that supports 4G network, diagnosis can help get the communication packet and the device power and network information for future maintenance and troubleshooting.

Capture Device Packet

This function is reserved for the professionals and is used to get the communication packet between the device and the external device for future problem diagnosis and debugging.

Steps



Note

This function is reserved for the professionals and technical support staff.

1. Go to **Maintenance and Security → Maintenance → Device Debugging** , and click **Settings** of **Capture Device Packet**.
2. Check **Enable** to enable this function.

Capture Device Packet

After the capture packet function is enabled, recording will stop automatically. Recording will recover after the capture packet function is disabled.

Enable

Capture Duration *

1

min

Save Captured Packet to

EMMC/2

Delete Captured Packet Under This Path

NIC Type

Wired Network

Wireless Dial/PPPoE

IP

0.0.0.0

Port No.

0

Auto Capture

After this function is enabled, the device packet will be captured when wakeup happens.

Packet Capturing Status

Save

Start Capturing Packet

Export Captured Packet

Figure 9-1 Capture Device Packet

- Set **Capture Duration** according to your need.
- Select the packet saving path.



Note

- The saving path option is subject to the actual storage method of the device.
- You can click **Delete Captured Packet Under This Path** to delete the saved packet file(s).

- Set NIC type, IP, and port.
- Optional:** You can select **Auto Capture** and the device packet will be captured when wakeup happens.
- Click **Save**.
- Click **Start Capturing Packet**.

9. After the capturing is completed, click **Export Captured Packet** to save the report.

Export Device Info

Go to **Maintenance and Security → Maintenance → Device Debugging → Export Device Info** , you can click **Export** to export device information, such as voltage, current, power, 4G data.

9.4 Security

You can improve system security by setting security parameters.

9.4.1 Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

Steps

1. Go to **Maintenance and Security → Security → IP Address Filter** .

2. Check **Enable**.

3. Select the type of IP address filter.

Blocklist IP addresses in the list cannot access the device.

Allowlist Only IP addresses in the list can access the device.

4. Edit the IP address filter list.

Add Add a new IP address or IP address range to the list.



Modify the selected IP address or IP address range in the list.



Delete the selected IP address or IP address range in the list.

5. Click **Save**.

9.4.2 Set MAC Address Filter

MAC address filter is a tool for access control. You can enable the MAC address filter to allow or forbid the visits from the certain MAC addresses.

Steps

1. Go to **Maintenance and Security → Security → MAC Address Filter** .

2. Check **Enable**.

3. Select the type of MAC address filter.

Blocklist MAC addresses in the list cannot access the device.

Allowlist Only MAC addresses in the list can access the device.

4. Edit the MAC address filter list.

Add Add a new MAC address to the list.



Modify the selected MAC address in the list.



Delete the selected MAC address in the list.

5. Click **Save**.

9.4.3 Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Maintenance and Security** → **Security** → **Login Management** → **Control Timeout Settings** to complete settings.

9.4.4 Certificate Management

It helps to manage the server/client certificates and CA certificate, and to send an alarm if the certificates are close to expiry date, or are expired/abnormal.



Note

The function is only supported by certain device models.

Server Certificate/Client Certificate



Note

The device has default self-signed server/client certificate installed. The certificate ID is **default**.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security** → **Security** → **Certificate Management**.
2. Click **Create Self-signed Certificate**.
3. Input certificate information.



Note

The input certificate ID cannot be the same as the existing ones.

4. Click **Save** to save and install the certificate.

The created certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain functions, the function name is shown in the column **Functions**.

5. Optional: Click **Property** to see the certificate details.

Install Self-signed Request Certificate

You can send the self-signed certificate to a trusted third-party for the signature, and install the certificate to the device.

Before You Start

Create a self-signed certificate first. See [**Create and Install Self-signed Certificate**](#) for instructions.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management**.
2. Select a self-signed certificate from the **Server/Client Certificate** list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **Save**.

The certificate request details are displayed in a pop-up window.

6. Copy the request content and save it as a request file.
7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
 - 1) Click **Import**.
 - 2) Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existed ones.

-
- 3) Click  to select the certificate file.
 - 4) Select **Self-signed Request Certificate**.
 - 5) Click **Save**.

The imported certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain function, the function name is shown in the column **Functions**.

9. Optional: Click **Property** see the certificate details.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management**.
2. Click **Import** in the **Server/Client Certificate** list.

3. Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existed ones.

4. Click to select the certificate file.

5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

Independent Key If your certificate has an independent key, select this option.
Browse to select the private key and input the private-key password.

PKCS#12 If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **Save**.

The imported certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain function, the function name is shown in the column **Functions**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security** → **Security** → **Certificate Management** .

2. Click **Import** in the **CA Certificate** list.

3. Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existing ones.

4. Click to select the certificate file.

5. Click **Save**.

The imported certificate is displayed in the **CA Certificate** list.

If the certificate is used by certain functions, the function name is shown in the **Functions** column.

Enable Certificate Expiration Alarm

Steps

1. Check **Enable Certificate Expiration Alarm**. If enabled, you will receive an email or the camera links to the surveillance center that the certificate will expire soon, or is expired or abnormal.
2. Set the **Remind Me Before Expiration (day)**, **Alarm Frequency (day)** and **Detection Time (hour)**.



Note

- If you set the reminding day before expiration to 1, then the camera will remind you the day before the expiration day. 1 to 30 days are available. Seven days is the default reminding days.
- If you set the reminding day before expiration to 1, and the detection time to 10:00, and the certificate will expire in 9:00 the next day, the camera will remind you in 10:00 the first day.

3. Click **Save**.

9.4.5 TLS

The Transport Layer Security (TLS) protocol aims primarily to provide privacy and data integrity between two or more communicating computer applications. TLS settings are effective for HTTP(S) and enhanced SDK service.

Go to **Maintenance and Security → Security → TLS** , and enable the desired TLS protocol. Click **Save**.



Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

Chapter 10 VCA Resource

VCA resource is a collection of smart functions supported by the device.

10.1 Set Open Platform

HEOP (Hikvision Embedded Open Platform) allows you to install the application for the third-party to develop and run its function and service. For the device supporting HEOP, you can follow the steps to import and run smart applications.

Steps

1. Go to **VCA** interface.



Note

Before installing the application, make sure that the application you want to install fits the following conditions.

- Each application has its own exclusive name.
- The FLASH memory space that the application takes up is less than the available FLASH memory space of the device.
- The memory and computing power of the application is less than that available memory and computing power of the device.

2. Click **Import Application** and browse your local path to select an application package and import.
3. Click **Import License** and browse your local path to select a license file and import.
4. **Optional:** Set application.

Click	Enable or disable the application.
Click	Delete the application.
Click	Export log.
Click	Browse a local path and import an application package to update the application.
Click	Clear memory fragmentation and free up more memory to enable more smart applications.
View details	Select an application and click on it to show the details on the page.

10.2 General Settings

Set the general parameters which are related to the smart applications.

Go to **VCA → Set Application → General Settings** to set the following parameters.

Camera Info.

For camera information settings, refer to **Set Camera Info** .

FTP

For FTP settings, refer to **Set FTP** .

Email

For Email settings, refer to **Set Email** .

Alarm Output

For alarm output settings, refer to **Automatic Alarm** .

Audible Alarm Output

For audible alarm output settings, refer to **Set Audible Alarm Output** .

Alarm Server

For alarm server settings, refer to **Alarm Server** .

Metadata

For metadata settings, refer to **Metadata** .

10.2.1 Set Camera Info

Customize specific information for the device. It may help identify a certain device when multiple devices are under management.

Go to **VCA → Set Application → General Settings → Camera Info** to set **Device No.** and **Camera Info**.

10.2.2 Metadata

Metadata is the raw data that the device collects before algorithm processing. It is often used for the third party integration.

Go to **VCA → Set Application → General Settings → metadata Settings** to enable metadata uploading of the desired function.



This function may vary according to different camera models.

Smart Event

The metadata of the smart event includes the target ID, target coordinate, time, etc.

Face Capture

The metadata of face capture includes the rule information, target ID, target coordinate, time information, etc. The camera detects the whole image by default. If the area is configured in the face capture settings, the camera detects the configured area.

10.2.3 AcuSearch

The device transmits the POS information of the target to network video recorder after detecting the target. It is to achieve accurate and quick search on the connected network video recorder.

Before You Start

- Make sure the connected network video recorder (NVR) supporting AcuSearch to do with the function.
- After the function is enabled, the ongoing smart application will be disabled while **Smart Event** or **Multi-Target-Type Detection** will be enabled.
- The function is only supported by certain models. The actual display varies with the models.

Steps

1. Enable the function for the device.
2. Set the function on the connected network video recorder.
 - 1) Enable AcuSearch function for the selected channel (refer to the configured camera device) on the network video recorder.
 - 2) Click the AcuSearch button on the playback page of the network video recorder.
 - 3) Click a target on a network video recorder to search for pictures that contain the target.
 - 4) Click a picture to play a video before and after that moment.



Refer to the *User Manual* of NVR for the actual settings on NVR.

10.3 Smart Event



- For certain device models, you need to enable the smart event function on **VCA** page first to show the function configuration page.
 - The function varies according to different models.
-

10.3.1 Set Intrusion Detection

It is used to detect objects entering and loitering in a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Intrusion Detection**.
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Threshold

Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missed.

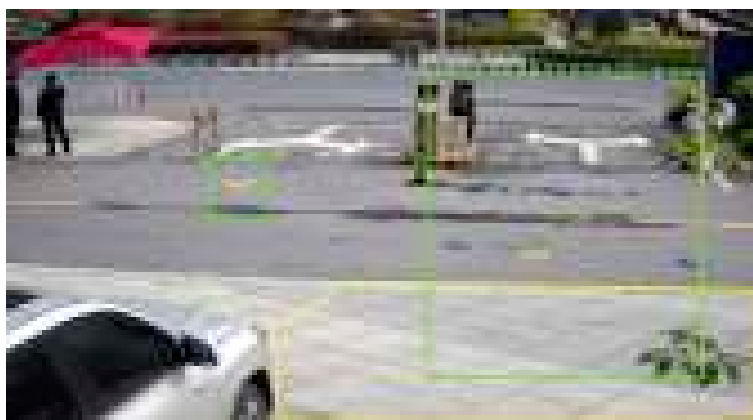


Figure 10-1 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.

10.3.2 Set Line Crossing Detection

It is used to detect objects crossing a predefined virtual line. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Line Crossing Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection line. Click  and a line with an arrow appears in the live view. Drag the line to the location on the live view as desired.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional:** Click  to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.

Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Direction

It stands for the direction from which the object goes across the line.

A<->B: The object going across the line from both directions 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.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the pre-defined line. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the pre-defined line. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

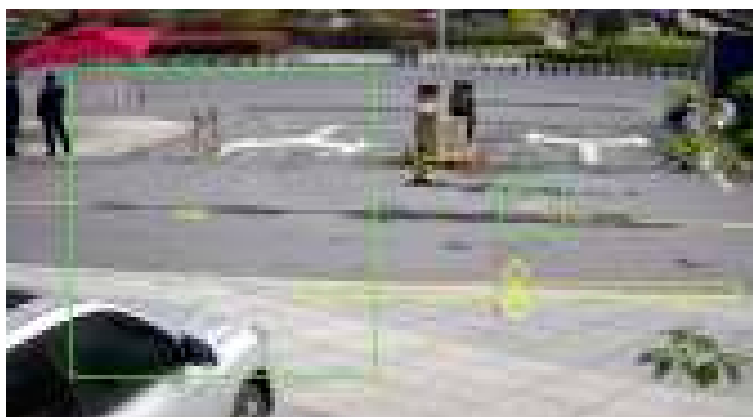


Figure 10-2 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.

10.3.3 Set Region Entrance Detection

It is used to detect objects entering a predefined virtual region from the outside place. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Region Entrance Detection**.
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. $S1$ stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

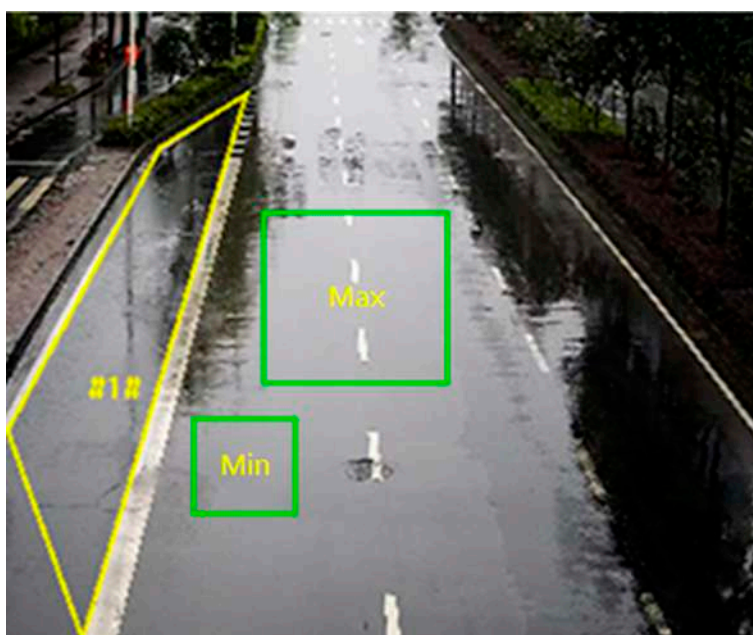


Figure 10-3 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.

10.3.4 Set Region Exiting Detection

It is used to detect objects exiting from a predefined virtual region. If it occurs, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Region Exiting Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.

3) **Optional:** Click  to delete all the setting areas.

4. Set parameters.

Detection Target

This function allows alarm triggering by specified selected target types. If the detection target is not selected, all the detected targets will be reported.



Note

This function is only available for certain device models under certain settings. Please refer to the actual settings.

Sensitivity

It stands for the percentage of the body part of an acceptable target that goes across the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Target Validity

If you set a higher validity, the required target features should be more obvious, and the alarm accuracy would be higher. The target with less obvious features would be missing.

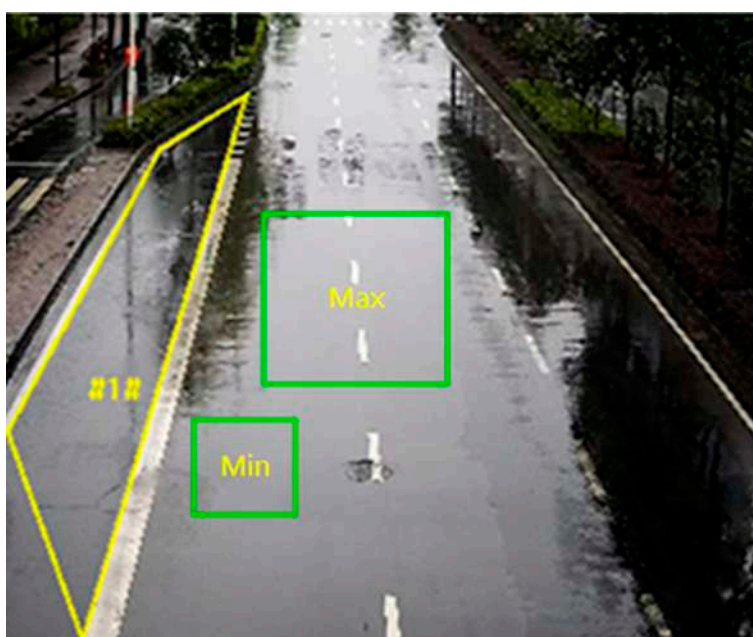


Figure 10-4 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.

10.3.5 Set Unattended Baggage Detection

It is used to detect the objects left over in the predefined region. Linkage methods can be triggered after the object is left and stays in the region for a set time period.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Unattended Baggage Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set parameters.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold

It stands for the time of the objects left in the region. Alarm is triggered after the object is left and stays in the region for the set time period.

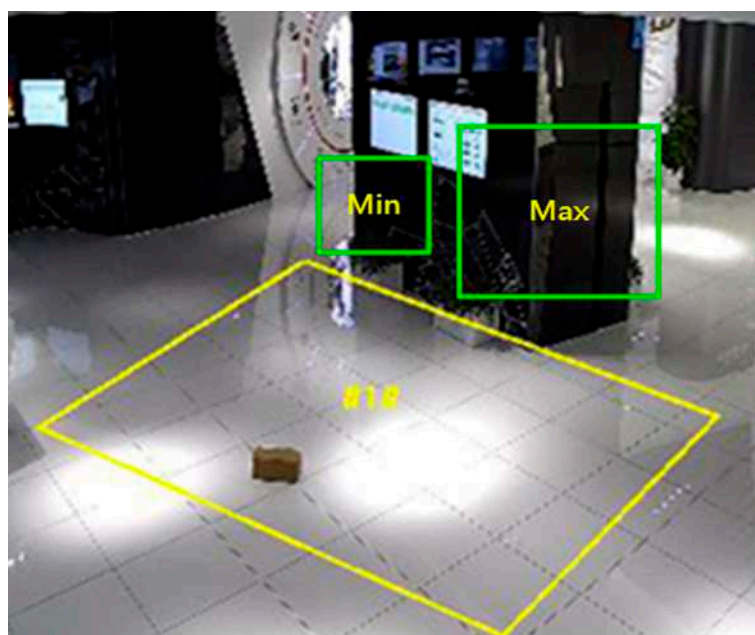


Figure 10-5 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to [**Set Arming Schedule**](#) . For the linkage method settings, refer to [**Linkage Method Settings**](#) .
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.6 Set Object Removal Detection

It detects whether the objects are removed from the predefined detection region, such as the exhibits on display. If it occurs, the device can take linkage actions and the staff can take measures to reduce property loss.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Object Removal Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.

2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.

3) **Optional:** Click  to delete all the setting areas.

4. Set parameters.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

Threshold

The threshold for 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.

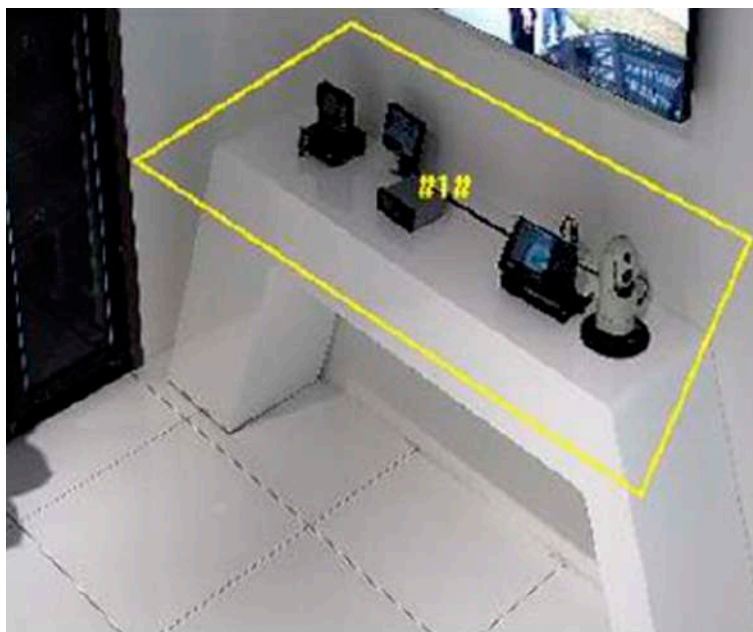


Figure 10-6 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.

6. For the arming schedule settings, see **Set Arming Schedule** . For the linkage method settings, see **Linkage Method Settings** .

7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.7 Set Loitering Detection

It detects whether there is any target loitering in a predefined area. If the time that the target loiters in the set region reaches the set threshold, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Loitering Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and  , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set rules.

Threshold

Threshold stands for the threshold for the time of the object loitering in the region. If the time that one object stays exceeds the threshold, the alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the predefined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the predefined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.

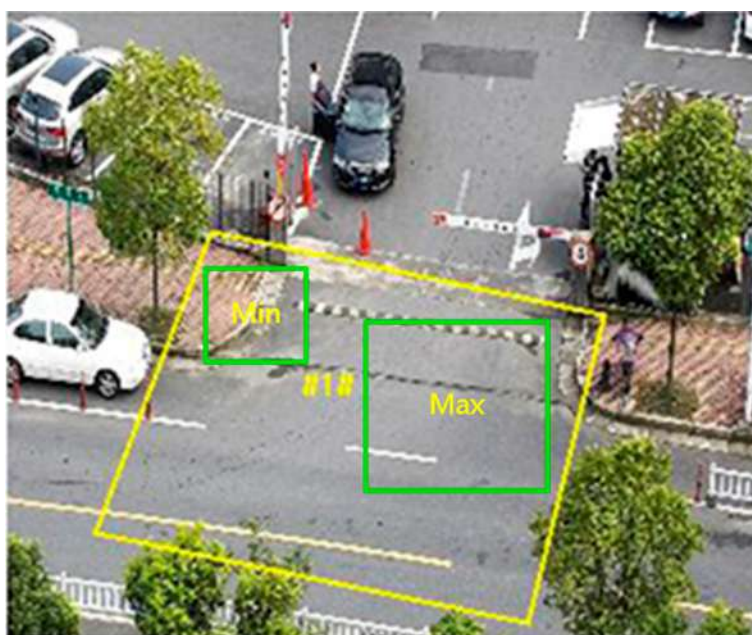


Figure 10-7 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.8 Set People Gathering Detection

It detects the people density in a predefined area. If the people density exceeds the set percentage, the device can take linkage actions.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → People Gathering Detection** .
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click  , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) **Optional:** Click  to delete all the setting areas.

4. Set rules.

Percentage

It stands for the percentage of people in the predefined area. When the people percentage in the live view exceeds the set value, the device will trigger an alarm.

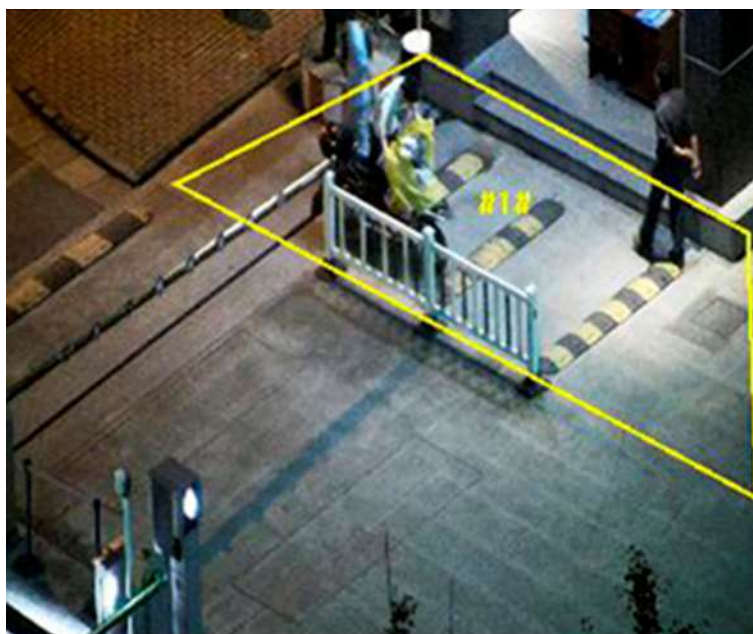


Figure 10-8 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings**
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.9 Set Fast Moving Detection

When there are targets moving at a high speed in a predefined area, the device will take linkage actions and trigger an alarm.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA** → **Set Application** → **Smart Event** → **Fast Moving Detection** .
2. Check **Enable**.

3. Click **Add** to add a rule and set a detection area.

- 1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
- 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and , then drag the mouse in the live view to draw the minimum and maximum target size.
- 3) **Optional:** Click  to delete all the setting areas.

4. Set Rules.

Sensitivity

Sensitivity stands for the percentage of the body part of an acceptable target that enters the pre-defined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that goes across the pre-defined region. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the alarm can be triggered.



Figure 10-9 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule**. For the linkage method settings, refer to **Linkage Method Settings**.
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.3.10 Set Parking Detection

It detects parking violation in a predefined area. When the parking time exceeds a set threshold, the device can take linkage actions. It is applicable in expressway and one-way street.

Before You Start

- Go to **VCA** and select the application. Select **Smart Event** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Smart Event**.

Steps

1. Go to **VCA → Set Application → Smart Event → Parking Detection**.
2. Check **Enable**.
3. Click **Add** to add a rule and set a detection area.
 - 1) Draw a detection area. Click , click on the live view to specify the vertexes and draw the boundaries of the detection area, and right click to complete drawing.
 - 2) Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection. Click  and , then drag the mouse in the live view to draw the minimum and maximum target size.
 - 3) **Optional**: Click  to delete all the setting areas.
4. Set rules.

Threshold

Threshold stands for the threshold for the parking time in the region. If the parking time exceeds the threshold, an alarm is triggered. The larger the value of the threshold is, the longer the alarm triggering time is.

Sensitivity

Sensitivity stands for the percentage of the part of an acceptable target that enters the pre-defined region. $\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target part that goes across the pre-defined region. ST stands for the complete target. The higher the value of sensitivity is, the more easily the alarm can be triggered.

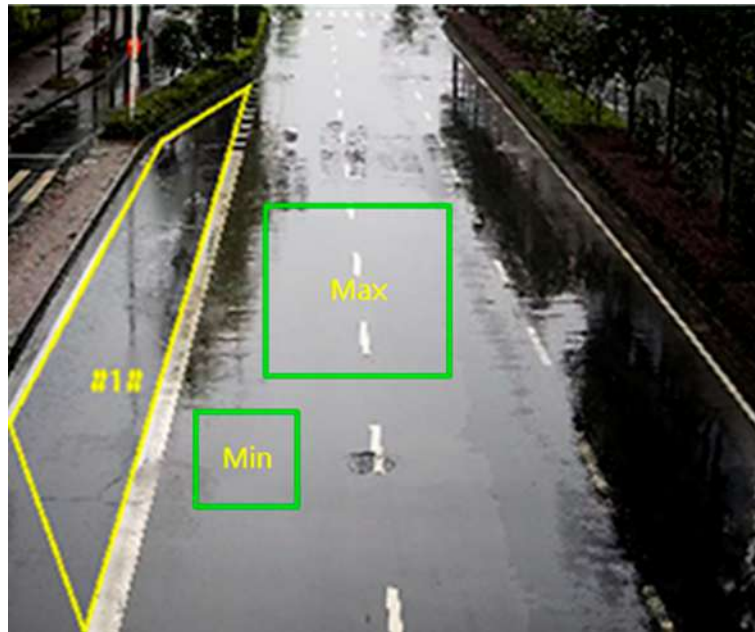


Figure 10-10 Set Rule

5. **Optional:** You can set the parameters of multiple areas by repeating the above steps.
6. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings**
7. Click **Save**.



Note

The function is only supported by certain models. The actual display varies with the models.

10.4 Face Capture

The device can capture the face that meets the rules in the configured rule area, and the captured picture will be uploaded.



Note

- For certain device models, you need to enable this function on **VCA** page first.
 - The function is only supported by certain device models.
-

10.4.1 Set Face Capture

The face that appears in the configured area can be captured.

Before You Start

- Go to **VCA** and select the application. Select **Face Capture** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **Face Capture**.

Steps

1. Go to **VCA → Set Application → Face Capture → Rule** .
2. Check **Enable** to enable the rule settings.
3. Click  to draw the detection area you want the face capture to take effect. Draw area by left-clicking end-points in the live view window, and right-clicking to finish the area drawing. It is recommended that the drawn area occupies 1/2 to 2/3 of the live view image.
4. Draw pupil distance.

Min. Pupil Distance

Click  to draw the minimum pupil distance. If the pupil distance of the face in the video image is smaller than the minimum pupil distance, the face will not be detected.

Max. Pupil Distance

Click  to draw the maximum pupil distance. If the pupil distance of the face in the video image is larger than the maximum pupil distance, the face will not be detected.

You can also input the value of distance in the text field.

5. **Optional:** For shield region settings, refer to [Set Shield Region](#) .
6. For the arming schedule settings, refer to [Set Arming Schedule](#) . For the linkage method settings, refer to [Linkage Method Settings](#) .
7. Click **Save**.
8. For overlay and capture settings, refer to [Overlay and Capture](#) . For advanced parameters settings, refer to [Face Capture Algorithms Parameters](#) .

Result

You can view and download captured pictures in **Playback → Picture** . Refer to [View and Download Picture](#) for details.

10.4.2 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Display VCA info. on Stream

Display smart information on stream, including the target and rules information.

Display Target info. on Alarm Picture

Overlay the alarm picture with target information.

Background Picture Settings

Comparing to target picture, background picture is the scene image which offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to the surveillance center, check **Background Upload**. For some devices, you can also check **Face Picture** to upload the captured face picture.

Target Picture Settings

Custom, Head Shot, Half-Body Shot and Full-Body Shot are selectable.



Note

If you select **Custom**, you can customize **width**, **head height** and **body height** as required.

You can check **Fixed Picture Height** to set the picture height.

Face Beautification

Check **Face Beautification** and adjust the beautification level as needed.



Note

Face Beautification slightly adjusts the captured face pictures and reduces facial noise.

Face Enhancement

Check **Face Enhancement** and the device is able to capture better and clearer face pictures when it is dark.

Text Overlay

You can check desired items and adjust their order to display on captured pictures.

See [Set Camera Info](#) to set **Device No.** and **Camera Info**.

10.4.3 Face Capture Algorithms Parameters

It is used to set and optimize the parameters of the algorithm library for face capture function.

Version

It stands for the current algorithm version.

Capture Parameters

Best Shot

The best shot after target leaves the detection area.

Capture Threshold

It stands for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area. The default value is 1.

Quick Shot

When the face picture grading value is higher than the quick shot threshold, the face picture will be captured and uploaded. Otherwise, the picture with the highest grading value that reaches the max. capture interval will be selected for upload.

Quick Shot Threshold

It stands for the quality of face to trigger quick shot.

Max. Capture Interval

It refers to the max. time occupation for one quick shot.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area.

Remove Duplicated Faces

This function can help filter out repeated captures of certain face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity value is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

The time from when each face picture is added to the duplicates removing library until when it is deleted.

Face Exposure

Check the checkbox to enable the face exposure.

Reference Brightness

The reference brightness of a face in the face exposure mode. If a face is detected, the camera adjusts the face brightness according to the value you set. The higher the value, the brighter the face is.

Min. Duration

The minimum duration of the camera exposures the face.



Note

If the face exposure is enabled, please make sure the WDR function is disabled, and the manual iris is selected.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture. If the detected face stays in the scene for a time shorter than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.



Note

The face filtering time (longer than 0 s) may increase the possibility of the actual capture times less than the set value above.

Facial Posture Filter

Facial posture filter can filter out face of certain postures. The figure on the right of the slider stands for the posture angle which is acceptable in the face capture action. Click ⓘ to display the diagram illustrating the face turning direction when setting up this filter.

Upload Feature

Feature stands for the feature information the algorithm can tell from face pictures. Check the function to upload the information.

Restore Parameters

Restore Defaults

Click **Restore** to restore all the settings in advanced configuration to the factory default.

10.4.4 Set Shield Region

The shield region allows you to set the specific region in which the set smart function rule is invalid.

Steps

1. Select **Shield Region**.
2. Click  to draw shield region. Repeat this step above to set more shield regions.
3. **Optional:** Select and click on the drawn region, then click  to delete the selected drawn region.
4. **Optional:** Click  to delete all drawn regions.
5. Click **Save**.

10.5 People Management

People management is used to detect and analyze people number and changes in a predefined region. It can be applied to the entrances and exits, supermarkets, etc.



Note

- For certain device models, you need to enable **People Management** on **VCA** page first.
 - The function is only supported by certain device models.
-

10.5.1 Regional People Counting

It counts people in a predefined area and detects people number changes and crowded situation. When the people number exception or waiting time exception occurs, the device can trigger an alarm.

Refer to **Set People Density** to set people density detection.

Refer to **Set People Exception Detection** to set people exception detection.

Refer to **Waiting Time Exception Detection** to set waiting time exception detection.

Set People Density

This function detects the level of people density in the set rule region.

Before You Start

- Go to **VCA → Select Application**, select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule**.
2. Click **Add** to add a rule and set its name.
3. Set a rule.

+ Add

Rule 1 ×

*Rule Name Rule 1

*Alarm Interval 5 sec

*First Alarm Delay 5 sec

Alarm Times Per Exception ☒

*Alarm Times 1

People Number OSD ☒

Figure 10-11 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Note

People density alarm does not support **Alarm Times Per Exception**, **Alarm Interval** and **First Alarm Delay** settings.

-
- Click  to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.

Note

- Up to 8 regions can be set at the same time.
 - Try not to overlap the regions.
-
- Check **People Density Alarm** to enable the function.

People Density Alarm

① People Density Alarm ☒

Upload Type

Scheduled Uploading ☒

Statistics Cycle

People Quantity Change Upload ☐

Congestion Level Upload ☐

Density Level

Level	Number of...	Custom Name
1		
2		
3		

Figure 10-12 People Density Alarm

Scheduled Uploading

The device uploads people density information within the set statistics cycle.

People Quantity Change Upload

The device uploads the people quantity change information if there is any change in the set rule region.

Congestion Level Upload

The device uploads the congestion information when there is any change of congestion level in the set rule region.

Density Level

Number of People

The range for each level by inputting the lower limit of the number of people in the set rule region.

Custom Name

The name of the level.



Note

- Set the **Number of People** before the **Custom Name**.
- Up to three levels can be configured. The density increases from level 1 to level 3.

6. Set arming schedule. See [Set Arming Schedule](#) .

7. Set linkage method. See [Linkage Method Settings](#) .

8. Click **Save**.

9. Optional: Set text overlay. For detailed settings, refer to [*Overlay and Capture*](#) .

10. Optional: View version and set filtering condition. For detailed settings, refer to [*Advanced Settings*](#) .

Set People Exception Detection

This function detects the number of people in the set rule region and an alarm is triggered when the situation meets the alarm-triggering condition.

Before You Start

- Go to **VCA → Select Application** , select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule** .
2. Click **Add** to add a rule and set its name.
3. Set a rule.

The screenshot shows the 'Set Rules' configuration interface. At the top, there is a dashed box with a '+ Add' button. Below it, a red box highlights 'Rule 1' with a close icon. The configuration fields are as follows:

- * Rule Name: Rule 1
- * Alarm Interval: 5 sec
- * First Alarm Delay: 5 sec
- Alarm Times Per Exception: ☒
- * Alarm Times: 1
- People Number OSD: ☒

Figure 10-13 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Alarm Times Per Exception

It refers to the alarm times after an alarm is triggered. If you do not check it and set the times, the device will keep sending alarms.

Alarm Interval

Within the set **Alarm Interval**, the same alarm will not be uploaded.

First Alarm Delay

When the first alarm is triggered, the alarm will be uploaded after a set time period.

- Click  to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.



Note

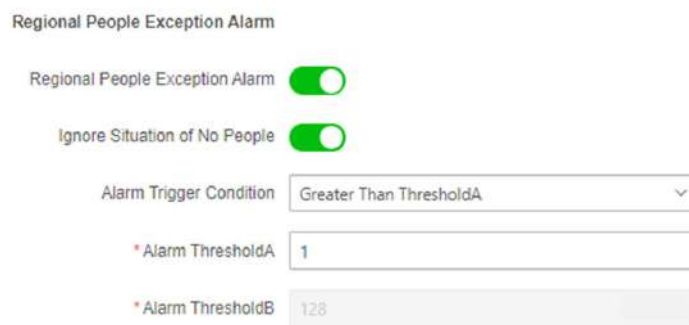
- Up to 8 regions can be set at the same time.
- Try not to overlap the regions.

- Check **Regional People Exception Alarm**, and set **Alarm Trigger Condition** and **Alarm Threshold**.



Note

- After enabling **Ignore Situation of No People**, the device will not trigger an alarm when there is no people in the region.
 - This function can filter the potential alarm condition under which the value is less than the set **Alarm Threshold** and no people in the region.
-



Regional People Exception Alarm

Regional People Exception Alarm ☒

Ignore Situation of No People ☒

Alarm Trigger Condition Greater Than ThresholdA

* Alarm ThresholdA

* Alarm ThresholdB

Figure 10-14 Regional People Exception Alarm

- Set arming schedule. See [Set Arming Schedule](#) .
- Set linkage method. See [Linkage Method Settings](#) .
- Click **Save**.
- Optional:** Set text overlay. For detailed settings, refer to [Overlay and Capture](#) .
- Optional:** View version and set filtering condition. For detailed settings, refer to [Advanced Settings](#) .

Waiting Time Exception Detection

This function detects the waiting time of the set rule region and an alarm is triggered when the waiting time meets the alarm-triggering condition.

Before You Start

- Go to **VCA → Select Application** , select **People Management** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Management**.

Steps

1. Go to **VCA → Set Application → People Management → Regional People Counting → Rule** .
2. Click **Add** to add a rule and set its name.
3. Set a rule.

+ Add

Rule 1 ×

*Rule Name Rule 1

*Alarm Interval 5 sec

*First Alarm Delay 5 sec

Alarm Times Per Exception ☒

*Alarm Times 1

People Number OSD ☒

Figure 10-15 Set Rules

People Number OSD

It displays the real-time people number in the live view window. You can drag the mouse to adjust the OSD window location.

Alarm Times Per Exception

It refers to the alarm times after an alarm is triggered. If you do not check it and set the times, the device will keep sending alarms.

Alarm Interval

Within the set **Alarm Interval**, the same alarm will not be uploaded.

First Alarm Delay

When the first alarm is triggered, the alarm will be uploaded after a set time period.



Note

Dwell time exception alarm supports **Alarm Times Per Exception**, **Alarm Interval** and **First Alarm Delay** settings only on the condition that the **Alarm Trigger Condition** is **Greater Than Threshold A**.

- Click  to draw a region in the live view window, left click the end-points in the live view window to define the boundary of the set rule region, and right click to finish drawing.



Note

- Up to 8 regions can be set at the same time.
- Try not to overlap the regions.

- Check **Dwell Time Exception Alarm**, and set **Alarm Trigger Condition** and **Alarm Threshold**.

Dwell Time Exception Alarm

 Dwell Time Exception Alarm ☒

Alarm Trigger Condition Greater Than ThresholdA 

* Alarm ThresholdA 300 sec

* Alarm ThresholdB 3600 sec

Figure 10-16 Dwell Time Exception Alarm

- Set arming schedule. See [Set Arming Schedule](#) .
- Set linkage method. See [Linkage Method Settings](#) .
- Click **Save**.
- Optional:** Set text overlay. For detailed settings, refer to [Overlay and Capture](#) .
- Optional:** View version and set filtering condition. For detailed settings, refer to [Advanced Settings](#) .

10.5.2 Overlay and Capture

Go to **VCA → People Management → Overlay & Capture** . Check the information you want to overlay on the captured pictures. You can also click   to adjust the order.

10.5.3 Advanced Settings

Set the advanced parameters for people management function and click **Save**.

Version

It stands for the current algorithm version.

Algorithm Mode

Select a mode according to the installation scene.

Filter

Target Size

It stands for the size of the target detection window. A target larger than this pixel can be counted as a real target. It can remove the false alarm of a certain fixed target.

Displacement

It stands for target displacement or the target width. A target will not be counted if its displacement is less than the set percentage.

Min. Waiting Duration

Waiting time shorter than the set value will be filtered.

Confidence

The higher the threshold is, the more difficult a target will be detected, but the higher the accuracy is.



Note

The filtering settings should be operated by the professionals. The filter settings can adjust the algorithm for detection to change the detection range, sensitivity, etc.

10.6 People Counting

People counting is used to calculate the number of people entering or exiting an area.



Note

- For certain device models, you need to enable **People Counting** on **VCA** page first.
 - The function is only supported by certain device models.
-

10.6.1 Set People Counting Rule

After setting the detection rules and algorithm parameters, the device calculates the number of people entering or exiting in the rule area, triggers linkage actions and uploads data automatically.

Before You Start

- Go to **VCA** and select the application. Select **People Counting** and click **Next** to enable the function.
- For the device supporting HEOP, go to **VCA** to import and enable **People Counting**.

Steps

1. Go to **VCA** → **Set Application** → **People Counting** → **Rule** .
2. Check **Enable** to enable the function.
3. Click **Add** to add a detection area.
4. Click  to draw the polygon detection area (count area). Left-click end-points in the live view window, and right-click to finish the drawing.
5. Click  to draw the detection line. The arrow shows entering direction, you can click  to change the direction.



Note

In order to improve the counting accuracy, please draw the detection area according to the following rules.

- The detection area needs to cover the people entering and exiting access.
- The detection line must be completely contained within the red detection area and perpendicular to the path of the person passing through.

6. **Optional:** Adjust the detection area and detection line.

Click  Clear the selected detection area or line.

Click  Clear all detection areas and lines.

7. **Optional:** Repeat the above steps to draw up to 3 detection areas and corresponding detection lines.

8. Set people counting parameters.

OSD Overlay Content

Select the counting data type to be displayed in the live view image from the drop-down list, and adjust the display position of people counting data in the live view image.



Note

OSD overlay only counts the number of the person on the current day. The data will be cleared automatically when the device restarts or at the daily reset time.

Daily Reset Time

The device clears the data in 00:00 each day by default. You can select a time point through the drop-down list. After selecting, the counting data will be automatically cleared at this time point every day.

You can click **Manual Reset** to manually trigger a data reset and clear the current people counting data.

9. Click **Save**.

10. Set arming schedule. See [***Set Arming Schedule***](#) .

11. Set linkage method. See [***Linkage Method Settings***](#) .

12. Click **Save**.

13. **Optional:** Set people counting data uploading parameters.

Click **Data Upload** to enter the interface. Click **Save** after finishing the settings.

Real-Time Data Uploading

Send the real-time data to the platform.

Upload Data Periodically

Set the **Data Statistics Cycle**, and the passenger flow counting data will be uploaded to the platform at intervals according to the **Data Statistics Cycle**.

14. **Optional:** Set people counting advanced parameters.

Click **Advanced** to enter the interface. Click **Save** after finishing the settings.

Version

It stands for the current algorithm version.

Clear Storage Data

Clear all people counting data stored in the device. This function must be used with caution.

Result

- If the target crosses the detection area along the entering direction and crosses the detection line, then it is counted as the entering number.
- If the target crosses the detection area along the exiting direction and crosses the detection line, then it is counted as the exiting number.

10.7 Road Traffic

Vehicle Detection and Mixed-Traffic Detection are available for the road traffic monitoring. The device captures the passing motor vehicles and non-motor vehicles and uploads the relevant information together with the captured pictures.



Note

- For certain device models, you need to select **Road Traffic** on **VCA** page first.
 - The function is only supported by certain device models.
-

10.7.1 Set Vehicle Detection

The vehicles that enter the set lane can be detected and the picture of the vehicle and its license plate can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

- Go to **VCA** and select the application. Select **Road Traffic** and click **Next** to enable the function.
- Make sure the device is installed properly.
- Make sure the image parameters are properly configured.
- Make sure the captured license plate picture is clear enough.

Steps

1. Go to **VCA → Set Application → Road Traffic → Rule** , and select **Vehicle Detection** as detection type.
2. Check **Enable**.
3. Select the operating mode.

Entrance/Exit

The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in the entrance/exit.

City Street

The license plate information of the detected vehicle will be uploaded when the vehicle passes the detection area and triggers the detection in the city street.

Alarm Input

It means the input alarm will trigger a license plate capture and recognition action.



Note

- When **Alarm Input** is selected, the alarm input A<-1 will automatically be assigned to trigger vehicle detection and its alarm type is always NO.
- If the A<-1 alarm input is used to trigger vehicle detection, it cannot be used for other basic events.
- When **Alarm Input** is selected and saved, previously configured linkage method for A<-1 will be canceled.

4. Select the total number of lanes.

5. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.

The blue detection line is the trigger line of the license plate, which is mainly used in the **Entrance/Exit** scene to improve the capture efficiency. It is recommended to put it in the lower middle of the screen to make sure that the full-size car with the plate can pass it.

6. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.



Note

Only 1 license plate can be captured at one time for each lane.

7. Select **Area** and **Country/Region**.

8. Set the detection mode.

Vehicle Priority

The device will detect the vehicle scale first, then catch the plate out to make the analysis. It will get the better accuracy but sometimes it will lose some results in the not-satisfied installation scenario.

License Plate & Vehicle

In license plate & vehicle mode, the device detects license plate and vehicle simultaneously and it uploads the alarm information and the captured pictures.



Note

It is recommended to select **Vehicle Priority** mode if there are no issues on installation and supplement light. After the issues of plate recognition are carried out, you can switch the mode to **License Plate & Vehicle** mode.

9. Check **Remove Duplicated License Plates** and set the **Time Interval**. The default time interval is 4 minutes.

10. Click **Save**.

11. Go to **Arming Schedule and Linkage Method**. You can set the arming schedule and linkage method independently for blocklist, allowlist and other list, and you should set them one by one.

Target Type **Blocklist** Allowlist Others

Arming Schedule

Arming Schedule **Edit**

Linkage Method

Direction ☒ All ☐ Forward ☐ Reverse

Notify Surveillance ... ☒

Upload to FTP/Mem... ☒

Trigger Alarm Output ☒ Select All

☒ A->1 ☒ A->2

Save

Figure 10-17 Arming Schedule and Linkage Method

- 1) Click to select the blocklist, allowlist and other list.
- 2) Set the arming schedule. Refer to **Set Arming Schedule** for details.
- 3) Set the linkage method. Check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

Direction

Only the vehicles moving as the selected direction can trigger the selected linkage methods.

All

All means that the vehicles in all moving directions will be considered. It is highly recommended to choose **All** if there is no special use.

Forward

Forward means that the vehicle moves toward the camera.

Reverse

Reverse means that the vehicle moves away from the camera.

Wiegand Linkage

The device can send reports to the third-party platform via the Wiegand protocol. Make sure the device supports Wiegand interface and the device is connected by Wiegand interface carefully.

Make sure the Wiegand is enabled and the protocol is properly configured in the system settings. Refer to **Wiegand** for details.

Enable **Wiegand Linkage** and select the wiegand interface connected to the external device.

The linkage will be triggered only when the detected vehicle driving direction is the same as the configured direction.

12. Go to **Road Traffic → Overlay & Capture** to set the image parameters and text overlay of the captured pictures. Refer to **Overlay and Capture** for details.
13. Import or export the license plate blocklist and allowlist. Refer to **Import or Export Blocklist & Allowlist** for details.

10.7.2 Set Mixed-Traffic Detection Rule

The motor vehicles and non-motor vehicles that enter the set lane can be detected, and the picture of targets can be captured and stored. Alarms will be triggered and captures can be uploaded.

Before You Start

- Go to **VCA** and select the application. Select **Road Traffic** and click **Next** to enable the function.
- Make sure the device is installed properly.
- Make sure the image parameters are properly configured.

Steps

1. Go to **VCA → Set Application → Road Traffic → Rule** , and select **Mixed-traffic Detection** as detection type.
2. Check **Enable**.
3. Select the total number of lanes.
4. Click and drag the lane line to set its position, or click and drag the line end to adjust the length and angle of the line.

The blue detection line is the trigger line of the license plate, which is mainly used in the **Entrance/Exit** scene to improve the capture efficiency. It is recommended to put it in the lower middle of the screen to make sure that the full-size car with the plate can pass it.

5. Adjust the zoom ratio of the camera so that the size of the vehicle in the image is close to that of the red frame. Only the position of red frame is adjustable.



Note

Only 1 license plate can be captured at one time for each lane.

-
6. Select **Area** and **Country/Region**.
 7. Check **Remove Duplicated License Plates** and set the **Time Interval**. The default time interval is 4 minutes.
 8. Click **Save**.

9. Go to **Arming Schedule and Linkage Method**. You can set the arming schedule and linkage method independently for blocklist, allowlist and other list, and you should set them one by one.

Target Type ☒ Blocklist ☐ Allowlist ☐ Others

Arming Schedule

Arming Schedule

Linkage Method

Direction ☒ All ☐ Forward ☐ Reverse

Notify Surveillance ... ☒

Upload to FTP/Mem... ☒

Trigger Alarm Output ☒ Select All

☒ A->1 ☒ A->2

Figure 10-18 Arming Schedule and Linkage Method

- 1) Click to select the blocklist, allowlist and other list.
- 2) Set the arming schedule. Refer to **Set Arming Schedule** for details.
- 3) Set the linkage method. Check the checkbox of corresponding linkage method for each rule, and click **Save** to save the settings.

Direction

Only the vehicles moving as the selected direction can trigger the selected linkage methods.

All

All means that the vehicles in all moving directions will be considered. It is highly recommended to choose **All** if there is no special use.

Forward

Forward means that the vehicle moves toward the camera.

Reverse

Reverse means that the vehicle moves away from the camera.

Wiegand Linkage

The device can send reports to the third-party platform via the Wiegand protocol.

Make sure the device supports Wiegand interface and the device is connected by Wiegand interface carefully.

Make sure the Wiegand is enabled and the protocol is properly configured in the system settings. Refer to **Wiegand** for details.

Enable **Wiegand Linkage** and select the wiegand interface connected to the external device.

The linkage will be triggered only when the detected vehicle driving direction is the same as the configured direction.

10. Go to **Road Traffic → Overlay & Capture** to set the image parameters and text overlay of the captured pictures. Refer to **Overlay and Capture** for details.
11. Import or export the license plate blocklist and allowlist. Refer to **Import or Export Blocklist & Allowlist** for details.

10.7.3 Overlay and Capture

You can set the image parameters of the captured images in vehicle detection and mixed-traffic detection.

Go to **VCA** and select **Road Traffic**.

Go to **VCA → Set Application → Road Traffic → Overlay & Capture** .



Note

The function varies according to different device models.

Picture Type ☒ License Plate/Target Close-up ☐ Vehicle ☒ Background

Picture Quality

Restriction Type ☒ Picture Quality ☐ Picture Size

Picture Quality 80

* Picture Size Kb

Picture Resolution

FTP Host

FTP Picture Name ☒ Default ☐ Custom

Picture Name

Text Overlay

Text Overlay ☒

Font Color

Background Color

Text Overlay

Text Overlay	To Be Selected	Selected
	☐ Type	☐ Type Sort

Figure 10-19 Overlay & Capture

Picture Quality

The larger the value is, the clearer the picture is, but larger storage space is also required.

Picture Size

The larger the value is, the larger the storage space is needed. And the level of network transmission requirement is also higher.

Picture Resolution

The captured background picture resolution.

Picture Capture Interval

The camera supports continuously trigger the alarm and upload captured picture each interval.

Check **Capture Interval** and set the interval.

FTP Picture Name

You can set the naming rule for captured pictures in vehicle detection and mixed-traffic detection in the FTP server.

Select **Default** to use the default rule.

Select **Custom**, select information for the picture name, and click   to adjust the order of picture name parameters. If **Capture Time** is not selected in custom mode, the captured picture triggered by the same vehicle later will replace the captured picture before due to the same picture name.



For more information about FTP settings, refer to ***Set FTP***.

Text Overlay

You can overlay camera, device or vehicle information on the captured image and click   to adjust the order of overlay texts.

Set the font color and background color by selecting the color box, and click the desired color in the pop-up palette or the drop-down box.

10.7.4 Import or Export Blocklist & Allowlist

You can import and export the blocklist and allowlist as desired, and check the list content in this interface.

Steps

1. Click **Import** to import the selected file.
2. Click  to open the PC local directory.
3. Find the blocklist & allowlist file and click to select it. Click **Open** to confirm.



- The file to import should corresponds with the file template that is required by the camera. You are recommended to export an empty blocklist & allowlist file from the camera as the template and fill in the content.
- The file should be in the .xls format and the cell format should be Text.

-
4. Click **Import** to import the selected file.
 5. Click **Export All** to export the license plate list.
 6. **Optional:** Click **Add** to add a license plate and set its related information one by one.
 7. **Optional:** Click  to select the filtering type. **All Types**, **Wiegand CardID**, **License Plate No.** and **Type** are selectable. As for **Type**, you can select **Keywords** to define the specific filtering type. Click **Search** to view the results.
 8. **Optional:** You can select a plate No. and click  to delete a plate from the blocklist or allowlist.
 9. **Optional:** You can select a plate No. and click  to edit the related information of the license plate from the blocklist or allowlist.

10.7.5 Advanced Parameters Configuration

Go to **VCA** and select the application. Enter the application configuration interface and click **Advanced** to set advanced parameters. Click **Save** after finishing the configuration.



Note

The function varies according to different device models.

Version

It stands for the current algorithm version.

Overlay Intelligent Information

Overlay the related intelligent information or POS information in the video.

10.8 AI Open Platform

AI Open Platform is to generate a model library based on the training material provided by the user, then load the model library into the device and allow user to configure tasks and rules. When a target in the scene is detected to trigger the rules, the device can take linkage actions, which can realize personalized smart applications.



Note

- The function is only supported by certain device models.
 - For certain device models, you need to enable **AI Open Platform** on **VCA** page first.
-

10.8.1 Set AI Open Platform

Steps

1. Go to **VCA → Set Application → AI Open Platform** .



Note

- Specific smart functions are supported for configuration via the AI Open Platform, such as hard hat detection, coal mine safety detection, etc.
 - After selecting a specific function, the device will load the model package of the corresponding function.
 - The function varies according to different device models, please refer to the actual device.
-
- For **Hard Hat Detection**, it detects targets in the set detection area who do not wear the hard hat and triggers an alarm.
 - For **Coal Mine Safety Detection**, you should go to **VCA → Set Application → Coal Mine Safety Management** and enable the function. In coal mine scenarios, it detects targets such as persons and mine cars in the detection area, detects if the belt deviates from the idlers, and if

the person not wears a hard hat. It triggers an alarm according to the set rules for coal mine safety detection.

2. **Optional:** Add a model into **Model Library**. Select the **Model Library** and related **Label File** from the local path, then set the **Model Name**. The model types are as follows.

Detection Model

Detects a specific target in the live view and provides the detection result and coordinate position of the target.

Classification Model

Classifies pictures or targets with attributes.

Mixed Model

Detects targets in the live view and classifies them.



Note

Max. Number of Model Packages refers to the maximum number of model packages that the device supports.

3. Select a model and enable it.

4. Select an **Analysis Mode**.

Live Video Analysis	The device analyzes the live video to realize target detection and result uploading.

Scheduled Capture Analysis	The device captures based on the set Auto-Switch Interval to analyze the captured picture and upload results.

5. **Optional:** Enable **Overlay Target Frame** and **Rule Overlay** according to your needs.

Overlay Target Frame	Overlay the alarm picture with target frame.

Rule Overlay	Overlay the alarm picture with rule information.

6. Set the arming schedule and linkage method. For the arming schedule settings, refer to **Set Arming Schedule** . For the linkage method settings, refer to **Linkage Method Settings** .

7. Set rules for the linked channel. Refer to **Set Rules** for details.

8. Click **Save**.

10.8.2 Set Rules

Set rules for the linked channel.

Before You Start

Make sure the related model in **VCA → AI Open Platform** is selected, and the task configuration is finished.

Steps

1. Click **Linked Channel** to select a channel in **Channel Management**.
2. Click  of the linked channel to set rules.

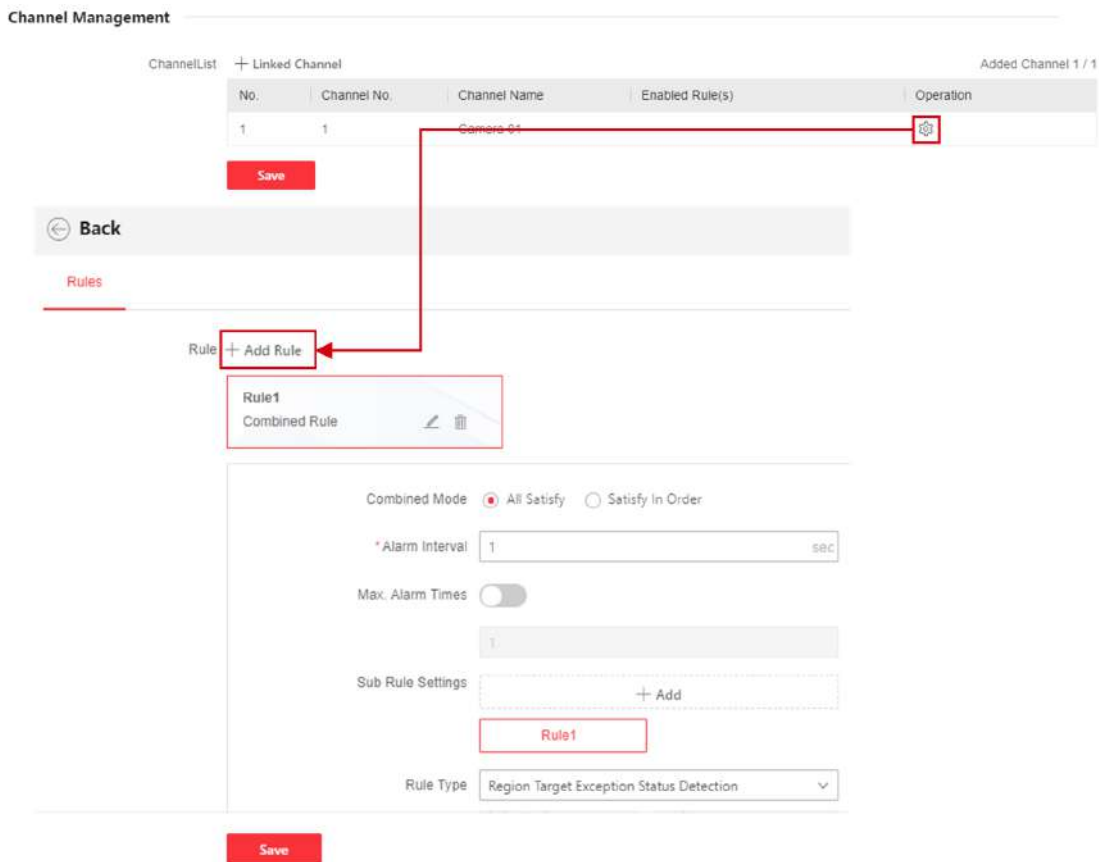


Figure 10-20 Set Rules

3. Click **Add Rule**. Select the rule and click  to rename the rule and select the rule type.

Region Target Exception Status Detection

Detects and counts the number of the target in the predefined virtual rule area, and compares it with the setting rule. When satisfying the triggering condition, it will trigger the alarm.

Line Crossing Target Detection

Detects if any targets crossing the predefined virtual rule line and triggers the alarm when detects.

Full Analysis Rule

Detects and analyzes all targets in the predefined virtual rule area.

Line Crossing Target Counting

Detects and counts the number of the target crossing the predefined virtual rule line.

Region Target Number Counting

Detects and counts the number of the target in the predefined virtual rule area.

Combined Rule

Supports **Region Target Exception Status Detection** and **Line Crossing Target Detection** in the predefined virtual rule area. You can set **Combined Mode** as **All Satisfy** or **Satisfy In Order** for the detection order.



Note

Rule types vary according to different model packages, please refer to the actual device.

4. Set the detection rule and draw rule area or line.
 - Draw a rule area: click  to draw a convex area in the live view window, left click the end-points in the live view window to define the boundary of the set rule area, and right click to finish drawing.
 - Draw a rule line: click  and a line with an arrow appears in the live video. Drag the line to the location in the live view window as desired.
5. Set rule parameters.

Object

The detection target type of the model.

Attribute

The detection target property of the model.

Duration

The duration of the status. The alarm will be triggered when the set time duration is reached.

Alarm Interval

During the set alarm interval, alarms of the same type only trigger one notification.

Sensitivity

The higher the value of sensitivity is, the easier the alarm can be triggered. If the sensitivity value is too large, the false alarm may be produced easier. Please set it according to the actual situation.

Max. Alarm Times

The maximum number of times an alarm can be triggered in the status that triggers the alarm.

Counting Interval

The time interval for counting.

Algorithm Validity

When the confidence threshold given by the algorithm is greater than or equal to the set validity, an alarm is triggered and uploaded.

Line Crossing

The direction from which the target goes across the line.

Quantity

Check **Quantity** and select the alarm rule from the drop-down box. Set **Threshold** or the range (**Min** and **Max**) according to the alarm rule. When the number of the target satisfies the setting alarm rule, the device will trigger the alarm.

Report Time Interval

It refers to the time interval for uploading the counting results when selecting **Region Target Number Counting**.



Note

Rule parameters vary according to different rules, please refer to the actual device.

6. Click **Save**.

Chapter 11 EPTZ

EPTZ (Electronic PTZ) is a high-resolution function that digitally zooms and pans into portions of the image, with no physical camera movement. If you want to use the EPTZ function, make sure your device supports the **Third Stream**. Third stream and EPTZ should be both enabled simultaneously.



Note

The function is only supported by certain device models.

11.1 Patrol

Steps

1. Go to **Configuration** → **EPTZ**.
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Patrol** in **Application Mode**.
5. Click **Save**.

What to do next

For the detailed information about the patrol settings, see the PTZ operations on live view page.

11.2 Auto-Tracking

Steps

1. Go to **Configuration** → **EPTZ**.
2. Check **Enable**.
3. The default **Stream Type** is **Third Stream** and cannot be configured.
4. Select **Auto-tracking** in **Application Mode**.
5. Click  to start drawing. Click on the live view video to specify the four vertexes of the detection area, and right click to complete drawing.
6. Set rules.

Detection Target

Human and vehicle are available. If the detection target is not selected, all the detected targets will be tracked, including the human and vehicle.



Note

Only certain camera models support this function.

Sensitivity

It stands for the percentage of the body part of an acceptable target that is tracked.

$\text{Sensitivity} = 100 - S1/ST \times 100$. S1 stands for the target body part that enters the pre-defined area. ST stands for the complete target body. The higher the value of sensitivity is, the more easily the target can be tracked.

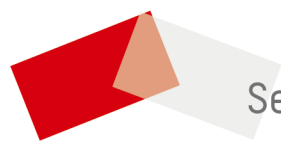
7. Click **Save**.

Appendix A. FAQ

Scan the following QR code to find the frequently asked questions of the device.

Note that some frequently asked questions only apply to certain models.





See Far, Go Further

DS-2CD2387G2P-LSU/SL 8 MP Panoramic Fixed Turret Network Camera

ColorVu



Hikvision ColorVu technology provides 24/7 vivid colorful images with F1.0 advanced lenses, high performance sensors and friendly lighting. F1.0 super-aperture collects more light to produce brighter images. Advanced sensor technology can vastly improve the utilization of available light.

- High quality imaging with 8 MP resolution
- One image that presents all the scenes covered by the camera
- 24/7 colorful imaging
- Efficient H.265+ compression technology
- Clear imaging against strong back light due to 130 dB WDR technology
- Focus on human and vehicle classification based on deep learning
- Active strobe light and audio alarm to warn intruders off
- Water and dust resistant (IP67)

▪ Specification

Camera	
Image Sensor	2 × 1/1.8" Progressive Scan CMOS
Max. Resolution	5120 × 1440
Min. Illumination	Color: 0.0005 Lux @ (F1.0, AGC ON), 0 Lux with light
Shutter Time	1/3 s to 1/100,000 s
Angle Adjustment	Pan: 0° to 30°, tilt: -75° to 75°
Lens	
Lens Type	Fixed focal lens, Dual lens: 4 mm
Focal Length & FOV	4 mm, horizontal FOV: 180°, vertical FOV: 44°
Lens Mount	M16
Iris Type	Fixed
Aperture	F1.0
Depth of Field	3.6 m to ∞
DORI	
DORI	4 mm, D: 77 m, O: 30 m, R: 15 m, I: 7 m
Illuminator	
Supplement Light Type	White Light
Supplement Light Range	Up to 30 m
Smart Supplement Light	Yes
Video	
Main Stream	When WDR is On: 50 Hz: 12.5 fps (5120 × 1440) 60 Hz: 15 fps (5120 × 1440) When WDR is Off: 50 Hz: 20 fps (5120 × 1440) 60 Hz: 20 fps (5120 × 1440)
Sub-Stream	When WDR is On: 50 Hz: 12.5 fps (1920 × 536, 960 × 272) 60 Hz: 15 fps (1920 × 536, 960 × 272) When WDR is Off: 50 Hz: 20 fps (1920 × 536, 960 × 272) 60 Hz: 20 fps (1920 × 536, 960 × 272)
Video Compression	Main stream: H.265+/H.265/H.264+/H.264, Sub-stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 16 Mbps
H.264 Type	Baseline Profile, Main Profile, High Profile
H.265 Type	Main Profile
Bit Rate Control	CBR, VBR
Scalable Video Coding (SVC)	H.264 and H.265 encoding
Region of Interest (ROI)	1 fixed region for main stream
Audio	
Audio Type	Mono sound
Audio Compression	G.711/G.722.1/G.726/MP2L2/PCM/MP3/AAC-LC

Audio Bit Rate	64 Kbps (G.711ulaw/G.711alaw)/16 Kbps (G.722.1)/16 Kbps (G.726)/32 to 192 Kbps (MP2L2)/8 to 320 Kbps (MP3)/16 to 64 Kbps (AAC-LC)
Audio Sampling Rate	8 kHz/16 kHz/32 kHz/44.1 kHz/48 kHz
Environment Noise Filtering	Yes
Network	
Protocols	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS, IPv4, IPv6, UDP, Bonjour, SSL/TLS, ISUP, ARP, WebSocket, WebSockets
Simultaneous Live View	Up to 6 channels
API	Open Network Video Interface (Profile S, Profile G, Profile T), ISAPI, SDK, ISUP
User/Host	Up to 32 users 3 user levels: administrator, operator, and user
Security	Password protection, complicated password, HTTPS encryption, 802.1X authentication (EAP-MD5), watermark, IP address filter, basic and digest authentication for HTTP/HTTPS, WSSE and digest authentication for Open Network Video Interface, RTP/RTSP over HTTPS, control timeout settings, security audit log, TLS 1.2, host authentication (MAC address)
Network Storage	NAS (NFS, SMB/CIFS), Auto Network Replenishment (ANR), NVR, Together with high-end Hikvision memory card, memory card encryption and health detection are supported.
Client	iVMS-4200, Hik-Connect, Hik-Central
Web Browser	Plug-in required live view: IE 10, IE 11 , Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Edge 89+, Local service: Chrome 57.0+, Firefox 52.0+, Edge 89+
Image	
Image Parameters Switch	Yes
Image Settings	saturation, brightness, contrast, sharpness, gain, white balance, adjustable by client software or web browser
Day/Night Switch	Day, Night, Auto, Schedule
Wide Dynamic Range (WDR)	130 dB
SNR	≥ 52 dB
Image Enhancement	BLC, HLC, 3D DNR
Privacy Mask	8 rectangular privacy masks
Interface	
Ethernet Interface	1 RJ45 10 M/100 M self-adaptive Ethernet port
On-Board Storage	Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 512 GB
Built-in Microphone	Yes
Built-in Speaker	Max. power consumption: 1.2 W, max. sound pressure: 10 cm: 95 dB
Audio	1 input (line in), terminal block, max. input amplitude: 3.3 Vpp, input impedance: 4.7 KΩ, interface type: non-equilibrium, 1 output (line out), terminal block, max. output amplitude: 3.3 Vpp, output impedance: 100 Ω, interface type: non-equilibrium
Alarm	1 input, 1 output (max. 24 VDC, 1 A)
Reset Key	Yes

Event	
Basic Event	Motion detection (support alarm triggering by specified target types (human and vehicle)), alarm input and output, flashing alarm light output, audible alarm output, exception
Smart Event	scene change detection
Linkage	Upload to FTP/NAS/memory card, notify surveillance center, send email, trigger alarm output, trigger recording, trigger capture, audible warning, white light flashing
Deep Learning Function	
Perimeter Protection	Line crossing, intrusion, region entrance, region exiting Support alarm triggering by specified target types (human and vehicle)
General	
Power	12 VDC $\pm$ 25%, 0.88 A, max. 10.5 W, $\varnothing$ 5.5 mm coaxial power plug, PoE: IEEE 802.3af, Class 3, 36 V to 57 V, 0.35 A to 0.22 A, max. 12.5 W
Material	Base: metal, cover: metal
Dimension	$\varnothing$ 155 mm $\times$ 155.3 mm ($\varnothing$ 6.1" $\times$ 6.1")
Package Dimension	230 mm $\times$ 230 mm $\times$ 230 mm (9" $\times$ 9" $\times$ 9")
Weight	Approx. 1110 g (2.4 lb.)
With Package Weight	Approx. 1900 g (4.2 lb.)
Storage Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Startup and Operating Conditions	-30 °C to 60 °C (-22 °F to 140 °F). Humidity 95% or less (non-condensing)
Language	33 languages: English, Russian, Estonian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Danish, Swedish, Norwegian, Finnish, Croatian, Slovenian, Serbian, Turkish, Korean, Traditional Chinese, Thai, Vietnamese, Japanese, Latvian, Lithuanian, Portuguese (Brazil), Ukrainian
General Function	Anti-banding, heartbeat, password reset via email, password protection, one-key reset
Flashing Light	Yes
Approval	
EMC	FCC: 47 CFR Part 15, Subpart B, CE-EMC: EN 55032: 2015, EN 61000-3-2:2019, EN 61000-3-3: 2013+A1:2019, EN 50130-4: 2011 +A1: 2014, RCM: AS/NZS CISPR 32: 2015, IC: ICES-003: Issue 7
Safety	UL: UL 62368-1, CB: IEC 62368-1: 2014+A11, CE-LVD: EN 62368-1: 2014/A11: 2017
Environment	CE-RoHS: 2011/65/EU, WEEE: 2012/19/EU, Reach: Regulation (EC) No 1907/2006
Protection	IP67: IEC 60529-2013

▪ Typical Application

Hikvision products are classified into three levels according to their anti-corrosion performance. Refer to the following description to choose for your using environment.

This model has NO SPECIFIC PROTECTION.

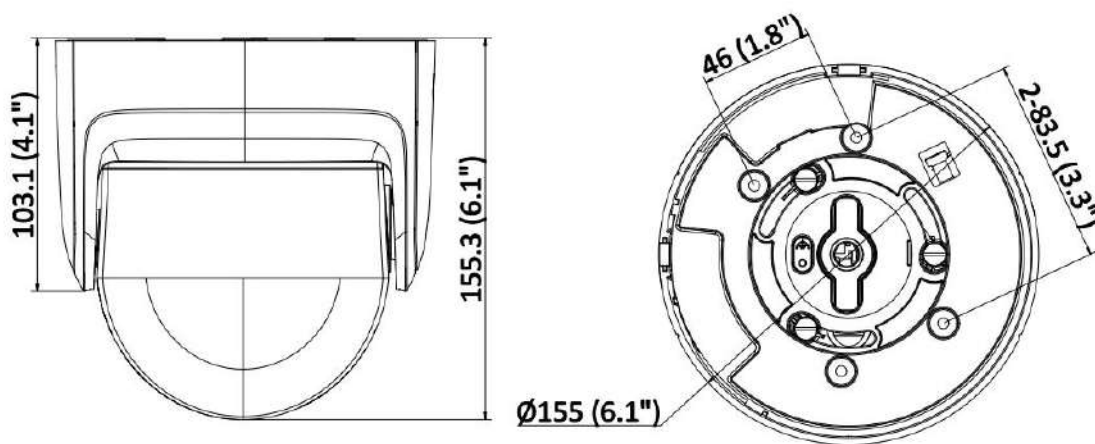
Level	Description
Top-level protection	Hikvision products at this level are equipped for use in areas where professional anti-corrosion protection is a must. Typical application scenarios include coastlines, docks, chemical plants, and more.
Moderate protection	Hikvision products at this level are equipped for use in areas with moderate anti-corrosion demands. Typical application scenarios include coastal areas about 2 kilometers (1.24 miles) away from coastlines, as well as areas affected by acid rain.
No specific protection	Hikvision products at this level are equipped for use in areas where no specific anti-corrosion protection is needed.

▪ Available Model

DS-2CD2387G2P-LSU/SL(4mm)(C)

DS-2CD2387G2P-LSU/SL(4mm)(C)/海康黑

▪ Dimension



Unit:mm (inch)

▪ Accessory

▪ Optional

DS-1473ZJ-155 Wall mount	DS-1471ZJ-155 Pendant Mount	DS-1473ZJ-155B Wall mount	DS-1471ZJ-155(Black) Pendant Mount	DS-1473ZJ-155(Black) Wall mount
				
DS-1473ZJ-155B(Black) Wall mount				
				

**Please choose accessories of the same color as the camera.*

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5998
www.hikvision.com



Follow us on social media to get the latest product and solution information.



GUARD TF Card

Introduction

HIKSEMI L2 Micro SD (TF) Card is specifically designed and ideal for video surveillance recording, boasting a read and write speed of Class 10 or higher. Utilizing TLC storage medium, it offers strong compatibility and adaptability. Widely applicable in scenarios such as light storage and backup storage, as well as other recording environments with low intensity or relatively simple usage requirements.



Features

- **Exceptional Compatibility**

Optimized for Hikvision storage systems, it is compatible with a wide range of products. When used with Hikvision products, the performance is even more outstanding.

- **Large Capacities**

Wide range of capacities from 32GB to 1TB for choice. Hold massive videos and information easily.

- **Strong Adaptability**

Waterproof, shockproof, X-ray proof, high and low temperature resistant, can be widely adapted to various working environments.

- **S.M.A.R.T. Mechanism**

Unique functions of life forewarning and health monitoring when used with Hikvision cameras. It can calculate the remaining available time based on the past records of use frequency and the number of bad blocks, and realize real-time warning to secure user data to the largest extent.

- **Unique Security Mechanism**

Unique function of read-write lock when used with Hikvision cameras, preventing irrelevant personnel from reading or writing even if they get the Micro SD (TF) card.

Ordering Information

Capacity	Model
32GB	HS-TF-L2 32G
64GB	HS-TF-L2 64G
128GB	HS-TF-L2 128G
256GB	HS-TF-L2 256G
512GB	HS-TF-L2 512G



Please contact the local sales for detailed model information.

Specification

Model	HS- TF-L2				
Capacity	32GB	64GB	128GB	256GB	512GB
Max. Read speed	95 MB/s				
Max. Write speed	20MB/s	30MB/s	40MB/s	50MB/s	60MB/s
File format	FAT32				
Specification	microSDHC, microSDXC				
Speed specifications	U1, U3				
NAND flash memory	TLC				
Dimensions	0.59" x 0.43" x 0.04" (14.99mm x 10.92mm x 1.02mm)				
Working Temperature	-0 °C to 70 °C (0 °F to 158 °F)				
Storage Temperature	-25°C to 85°C (-13 °F to 185 °F)				
Compatibility	Compatible with microSDHC, microSDXC, microSDHC UHS-I and SDXC UHS-I host devices				
Warranty	2 years				

Note

Performance test is performed in specific testing environment. Any change of the computer system, operation system, hardware, software, or functions will influence the test result.

Revision History

Version	Description	Date
V1.0.0	HS-TF-L2	20241106

Data subject to change without notice.

© 2024 HANGZHOU HIKSTORAGE TECHNOLOGY CO.,LTD. All rights reserved.

Unless otherwise expressly stated herein, HIKSTORAGE does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the HIKSTORAGE website ([http:// www.hiksemitech.com](http://www.hiksemitech.com)).

DS-1678ZJ

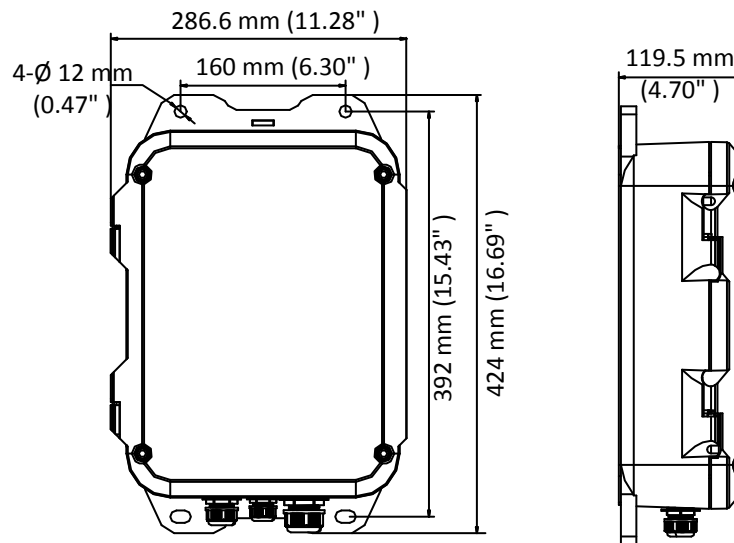
Terminal Box



Feature

- Aluminum alloy with surface spray treatment
- The terminal box facilitates the cable wiring

Dimension



Available Model

DS-1678ZJ

Parameter

Model	DS-1678ZJ
Parameters	Terminal Box
Appearance	Hikvision white
Material	Aluminum alloy
Dimension	424 mm × 286.6 mm × 119.5 mm (16.69" × 11.28" × 4.70")
Weight	6.2 kg (13.67 lb.)

Note

- The installation surface must be capable of supporting at least 8 times as much as the total weight of the camera, and the terminal box.
- The terminal box's maximum load capacity is 10 kg (22 lb.).

DS-1678ZJ

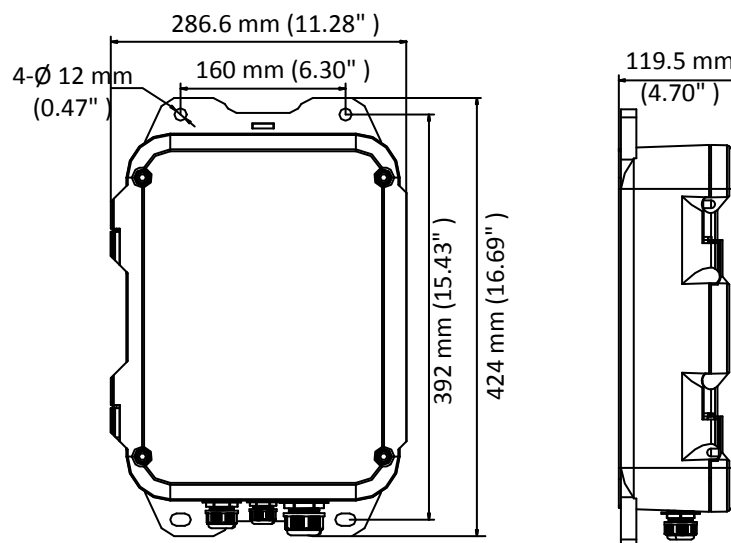
Terminal Box



Feature

- Aluminum alloy with surface spray treatment
- The terminal box facilitates the cable wiring

Dimension



Available Model

DS-1678ZJ

Parameter

Model	DS-1678ZJ
Parameters	Terminal Box
Appearance	Hikvision white
Material	Aluminum alloy
Dimension	424 mm × 286.6 mm × 119.5 mm(16.69" × 11.28" × 4.70")
Weight	6.2 kg (13.67 lb.)

Note

- The installation surface must be capable of supporting at least 8 times as much as the total weight of the camera, and the terminal box.
- The terminal box's maximum load capacity is 10 kg (22 lb.).



TandemVu PTZ Camera

User Manual

Initiatives on the Use of Video Products

Thank you for choosing Hikvision products.

Technology affects every aspect of our life. As a high-tech company, we are increasingly aware of the role technology plays in improving business efficiency and quality of life, but at the same time, the potential harm of its improper usage. For example, video products are capable of recording real, complete and clear images. This provides a high value in retrospect and preserving real-time facts. However, it may also result in the infringement of a third party's legitimate rights and interests if improper distribution, use and/or processing of video data takes place. With the philosophy of "Technology for the Good", Hikvision requests that every end user of video technology and video products shall comply with all the applicable laws and regulations, as well as ethical customs, aiming to jointly create a better community.

Please read the following initiatives carefully:

- Everyone has a reasonable expectation of privacy, and the installation of video products should not be in conflict with this reasonable expectation. Therefore, a warning notice shall be given in a reasonable and effective manner and clarify the monitoring range, when installing video products in public areas. For non-public areas, a third party's rights and interests shall be evaluated when installing video products, including but not limited to, installing video products only after obtaining the consent of the stakeholders, and not installing highly-invisible video products.
- The purpose of video products is to record real activities within a specific time and space and under specific conditions. Therefore, every user shall first reasonably define his/her own rights in such specific scope, in order to avoid infringing on a third party's portraits, privacy or other legitimate rights.
- During the use of video products, video image data derived from real scenes will continue to be generated, including a large amount of biological data (such as facial images), and the data could be further applied or reprocessed. Video products themselves could not distinguish good from bad regarding how to use the data based solely on the images captured by the video products. The result of data usage depends on the method and purpose of use of the data controllers. Therefore, data controllers shall not only comply with all the applicable laws and regulations and other normative requirements, but also respect international norms, social morality, good morals, common practices and other non-mandatory requirements, and respect individual privacy, portrait and other rights and interests.
- The rights, values and other demands of various stakeholders should always be considered when processing video data that is continuously generated by video products. In this regard, product security and data security are extremely crucial. Therefore, every end user and data controller, shall undertake all reasonable and necessary measures to ensure data security and avoid data leakage, improper disclosure and improper use, including but not limited to, setting up access

control, selecting a suitable network environment (the Internet or Intranet) where video products are connected, establishing and constantly optimizing network security.

- Video products have made great contributions to the improvement of social security around the world, and we believe that these products will also play an active role in more aspects of social life. Any abuse of video products in violation of human rights or leading to criminal activities are contrary to the original intent of technological innovation and product development. Therefore, each user shall establish an evaluation and tracking mechanism of their product application to ensure that every product is used in a proper and reasonable manner and with good faith.

Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Contents

Chapter 1 Overview	1
1.1 Product Introduction	1
1.2 Key Function	1
1.3 System Requirement	2
Chapter 2 Device Activation and Accessing	3
2.1 Activate Device	3
2.1.1 Activate Device via Web Browser	3
2.1.2 Activate via SADP	4
2.2 Access Device via Web Browser	5
2.2.1 Plug-in Installation	5
2.2.2 Admin Password Recovery	6
2.2.3 Illegal Login Lock	6
Chapter 3 Smart Function	8
3.1 Allocate VCA Resource	8
3.2 Set Camera Info	8
3.3 Capture Target with Feature	8
3.3.1 Set Detection Rule	8
3.3.2 Overlay and Capture	9
3.3.3 Advanced Parameters	10
3.4 Person Arming	11
3.4.1 Device Auto Person Arming	12
3.4.2 Manual Person Arming	14
3.4.3 Capture Settings	14
3.5 Intelligent Traffic Event (ITS)	17
3.5.1 Basic Settings	17
3.5.2 Common Settings	18

3.5.3 Enforcement	20
3.5.4 Traffic Event Detection	28
3.5.5 Vehicle Detection	31
3.5.6 Traffic Data Collection	34
3.5.7 ITS Linkage and Alarm	34
3.5.8 Vehicle Arming	36
3.5.9 Advanced Settings	38
3.6 People Density	39
3.7 Smart Display	42
Chapter 4 PTZ	43
4.1 PTZ Control	43
4.2 Set Preset	45
4.2.1 Special Presets	45
4.3 Set Patrol Scan	46
4.3.1 Set One-Touch Patrol	47
4.4 Set Pattern Scan	47
4.5 Set Limit	48
4.6 Set Initial Position	49
4.7 Set Scheduled Tasks	49
4.8 Operate Wiper	49
4.9 Set Park Action	50
4.9.1 Set One-Touch Park	50
4.10 Set Privacy Mask	51
4.11 Set Power Off Memory	52
4.12 Set PTZ Priority	52
4.13 Set Rapid Focus	52
4.14 Set Device Position	53
4.15 Panorama Tracking	54

4.15.1 Link Channels by Calibration	54
4.15.2 Set Tracking Parameters	55
4.16 GPS Calibration	56
4.16.1 Set GPS Calibration	56
4.16.2 Verify Calibration	57
Chapter 5 Live View	58
5.1 Live View Parameters	58
5.1.1 Start and Stop Live View	58
5.1.2 Aspect Ratio	58
5.1.3 Window Division	58
5.1.4 Live View Stream Type	59
5.1.5 Quick Set Live View	59
5.1.6 Select the Third-Party Plug-in	59
5.1.7 Start Digital Zoom	59
5.1.8 Conduct Regional Focus	60
5.1.9 Conduct Regional Exposure	60
5.1.10 Light	60
5.1.11 Lens Initialization	60
5.1.12 Track Manually	60
5.1.13 Conduct 3D Positioning	61
5.1.14 OSD Menu	61
5.1.15 Display Target Information on Live View	61
5.2 Set Transmission Parameters	61
Chapter 6 Video and Audio	63
6.1 Video Settings	63
6.1.1 Stream Type	63
6.1.2 Video Type	63
6.1.3 Resolution	64

6.1.4 Bitrate Type and Max. Bitrate	64
6.1.5 Video Quality	64
6.1.6 Frame Rate	64
6.1.7 Video Encoding	64
6.1.8 I-Frame Interval	66
6.2 Audio Settings	66
6.2.1 Audio Input	67
6.2.2 Audio Output	67
6.2.3 Environmental Noise Filter	67
6.3 Two-way Audio	67
6.4 ROI	68
6.4.1 Set ROI	68
6.5 Display Info. on Stream	68
6.6 Display Settings	69
6.6.1 Scene Mode	69
6.6.2 Image Parameters Switch	74
6.6.3 Mirror	75
6.6.4 Video Standard	75
6.7 OSD	75
Chapter 7 Video Recording and Picture Capture	76
7.1 Storage Settings	76
7.1.1 Memory Card	76
7.1.2 Set FTP	78
7.1.3 Set NAS	79
7.1.4 Set Cloud Storage	80
7.2 Video Recording	80
7.2.1 Record Automatically	81
7.2.2 Record Manually	82

7.2.3 Playback and Download Video	82
7.3 Capture Configuration	83
7.3.1 Capture Automatically	83
7.3.2 Capture Manually	83
7.3.3 View and Download Picture	84
Chapter 8 Event and Alarm	85
8.1 Basic Event	85
8.1.1 Set Motion Detection	85
8.1.2 Set Video Tampering Alarm	87
8.1.3 Set Exception Alarm	88
8.1.4 Set Alarm Input	89
8.2 Smart Event	89
8.2.1 Detect Audio Exception	89
8.2.2 Set Intrusion Detection	90
8.2.3 Set Line Crossing Detection	92
8.2.4 Set Region Entrance Detection	93
8.2.5 Set Region Exiting Detection	95
8.2.6 Set Tracking Parameters	97
Chapter 9 Arming Schedule and Alarm Linkage	98
9.1 Set Arming Schedule	98
9.2 Linkage Method Settings	98
9.2.1 Trigger Alarm Output	98
9.2.2 FTP/NAS/Memory Card Uploading	99
9.2.3 Send Email	100
9.2.4 Notify Surveillance Center	101
9.2.5 Trigger Recording	101
9.2.6 Flashing Light	101
9.2.7 Audible Warning	102

Chapter 10 Network Settings	103
10.1 TCP/IP	103
10.1.1 Multicast	104
10.1.2 Multicast Discovery	104
10.2 Port	105
10.3 Port Mapping	106
10.3.1 Set Auto Port Mapping	106
10.3.2 Set Manual Port Mapping	106
10.3.3 Set Port Mapping on Router	107
10.4 SNMP	108
10.5 Access to Device via Domain Name	108
10.6 Access to Device via PPPoE Dial Up Connection	109
10.7 Accessing via Mobile Client	109
10.7.1 Enable Hik-Connect Service on Camera	110
10.7.2 Set Up Hik-Connect	111
10.7.3 Add Camera to Hik-Connect	111
10.8 Set ISUP	112
10.9 Set Open Network Video Interface	112
10.10 Set Network Service	113
10.11 Set Alarm Server	114
10.12 TCP Acceleration	114
10.13 Traffic Shaping	114
10.14 Data Monitoring	114
10.15 Set SRTP	115
Chapter 11 System and Security	116
11.1 View Device Information	116
11.2 Restore and Default	116
11.3 Search and Manage Log	116

11.4 Import and Export Configuration File	117
11.5 Export Diagnose Information	117
11.6 Reboot	117
11.7 Upgrade	117
11.8 Undervoltage Alarm	118
11.9 View Open Source Software License	118
11.10 Set Live View Connection	118
11.11 Time and Date	118
11.11.1 Synchronize Time Manually	118
11.11.2 Set NTP Server	119
11.11.3 Set DST	119
11.12 Set RS-485	119
11.13 Security	120
11.13.1 Authentication	120
11.13.2 Set IP Address Filter	120
11.13.3 Set MAC Address Filter	121
11.13.4 Set HTTPS	121
11.13.5 Security Audit Log	122
11.13.6 Set QoS	123
11.13.7 Set IEEE 802.1X	123
11.13.8 Certificate Management	124
11.13.9 Control Timeout Settings	126
11.13.10 SSH	126
11.13.11 User and Account	127
Appendix A. FAQ	129

Chapter 1 Overview

1.1 Product Introduction

The network speed dome combines a panoramic channel and a PTZ channel to offer overall and detailed HD monitoring.

1.2 Key Function

The key functions of the device are as follows.

Audio and Visual Alarm

The device supports flashing light alarm and audio alarm to warn intruders off.

Linked Tracking and Capture

The panoramic channel and the PTZ channel work together to detect, locate and track targets in both overall pictures and adequate details.

Face Capture

The device detects, captures, grades, and filters moving faces, and outputs captured pictures.

Capture Target with Feature

The device captures faces and human bodies and extracts features of the target.

Person Arming

The device detects the armed face or human body in the monitoring scene. When the wanted targets are found, the device triggers alarms, and starts tracking and capturing the target. The realtime target location and other related information are uploaded during tracking if properly configured.

Vehicle Detection

The device detects vehicles in the detection area, recognizes license plates, captures and saves pictures, and uploads alarms.

Vehicle Arming

The device detects the armed vehicle (license plates) in the monitoring scene. When the wanted vehicles are found, the device triggers alarms, and starts tracking and capturing the target. The real-time target location and other related information are uploaded during tracking if properly configured.

Event Function

The device detects basic events and multiple smart events.

People Density

The device detects the level of people density in the detection areas.

PTZ Function

The device supports PTZ functions, such as presets, scans, patrol, and power-off memory.

1.3 System Requirement

Your computer should meet the requirements for visiting and operating the product.

Recommended Specifications	
Operating System	Microsoft Windows XP/ Windows 7/ Windows 8/ Windows 10 Mac OS 10.13 or later
CPU	Intel® Pentium® IV 3.0 GHz or higher
RAM	1 GB or higher
Display	1024 × 768 resolution or higher
Web Browser	Internet Explorer 10 and above version, Apple Safari 12 and above version, Mozilla Firefox 52 and above version, Google Chrome 57 and above version.

Chapter 2 Device Activation and Accessing

To protect the security and privacy of the user account and data, you should set a login password to activate the device when access the device via network.



Note

Refer to the user manual of the software client for the detailed information about the client software activation.

2.1 Activate Device

The device needs to be activated by setting a strong password before use. This part introduces activation using different client tools.

2.1.1 Activate Device via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or PC client to activate the device.

Before You Start

Make sure your device and your PC connect to the same LAN.

Steps

1. Change the IP address of your PC to the same subnet as the device.
The default IP address of the device is 192.168.1.64.
2. Open a web browser and input the default IP address.
3. Create and confirm the admin password.



Caution

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 complete activation and enter **Live View** page.
5. Modify IP address of the camera.
 - 1) Enter IP address modification page. **Configuration → Network → TCP/IP**
 - 2) Change IP address.
 - 3) Save the settings.

- 2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
- 3) Input the admin password and click **Modify** to activate your IP address modification.

2.2 Access Device via Web Browser

Before You Start

Check the system requirement to confirm that the operating computer and web browser meets the requirements. See **System Requirement** .

Steps

1. Open the web browser.
2. Input IP address of the device to enter the login interface.
3. Input user name and password.



Note

Illegal login lock is activated by default. If admin user performs seven failed password attempts (five attempts for user/operator), the IP address is blocked for 30 minutes.

If illegal login lock is not needed, go to **Configuration → System → Security → Security Service** to turn it off.

-
4. Click **Login**.
 5. Download and install appropriate plug-in for your web browser.
For IE based web browser, webcomponents and QuickTime™ are optional. For non-IE based web browser, webcomponents, QuickTime™, VLC and MJPEG are optional.

2.2.1 Plug-in Installation

Certain operation systems and web browser may restrict the display and operation of the device function. You should install plug-in or complete certain settings to ensure normal display and operation. For detailed restricted function, refer to the actual device.

Operating System	Web Browser	Operation
Windows	Internet Explorer 10+	Follow pop-up prompts to complete plug-in installation.
Windows 7 and above version	Google Chrome 57+ Mozilla Firefox 52+	Click  Download Plug-in to download and install plug-in.
Mac OS	Google Chrome 57+ Mozilla Firefox 52+ Mac Safari 12+	Plug-in installation is not required. Go to Configuration → Network → Advanced Settings

Operating System	Web Browser	Operation
		→ Network Service to enable WebSocket or Websockets for normal view. Display and operation of certain functions are restricted. For example, Playback and Picture are not available. For detailed restricted function, refer to the actual device.

Note

The device only supports Windows and Mac OS system and do not support Linux system.

2.2.2 Admin Password Recovery

If you forget the admin password, you can reset the password by clicking **Forget Password** on the login page after completing the account security settings.

You can reset the password by setting the security question or email.

Note

When you need to reset the password, make sure that the device and the PC are on the same network segment.

Security Question

You can set the account security during the activation. Or you can go to **Configuration → System → User Management**, click **Account Security Settings**, select the security question and input your answer.

You can click **Forget Password** and answer the security question to reset the admin password when access the device via browser.

Email

You can set the account security during the activation. Or you can go to **Configuration → System → User Management**, click **Account Security Settings**, input your email address to receive the verification code during the recovering operation process.

2.2.3 Illegal Login Lock

It helps to improve the security when accessing the device via Internet.

Go to **Configuration → System → Security → Security Service** , and enable **Enable Illegal Login Lock**. **Illegal Login Attempts** and **Locking Duration** are configurable.

Illegal Login Attempts

When your login attempts with the wrong password reach the set times, the device is locked.

Locking Duration

The device releases the lock after the setting duration.

Chapter 3 Smart Function

3.1 Allocate VCA Resource

VCA resource offers you options to enable certain VCA functions according to actual needs. It helps allocate more resources to the desired functions.

Steps

1. Go to **VCA → VCA Resource**.
2. Select desired VCA functions.
3. Save the settings.



Note

Certain VCA functions are mutually exclusive. When a certain function or functions are selected and saved, others will be hidden.

3.2 Set Camera Info

Customize specific information for the device. It may help identify a certain device when multiple devices are under management.

Go to **VCA → General VCA Resource** to set **Camera No.** and **Camera Info**.

3.3 Capture Target with Feature

It is to detect, capture and upload features of targets in multiple types, such as human face and human body.

3.3.1 Set Detection Rule

After the rules and algorithm parameters are set, the device captures targets of multiple types and triggers linkage actions automatically.

Steps

1. Go to **VCA → Face+Human → Rule**.
2. Check **Enable**.
3. Select a configuration mode.

Normal One detection scene is allowed to set. The device captures targets in the scene in the set arming schedule.
See for details.

Expert The device can patrol among the detection scenes and capture target images. Detection scenes and patrol schedule should be set in advance.
See for details.

4. Click **Save**.

What to do next

Go to **Picture** to search and view the captured pictures.

Go to **Smart Display** to see currently captured target pictures.

3.3.2 Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Display VCA Info. on Stream

Display smart information on stream, including the target and rules information.

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Target Picture Settings

You can set the face picture type by selecting **Custom**, **Head Shot**, **Half-Body Shot**, or **Full-Body Shot**. If you select **Custom**, you can define detailed picture width and height of a picture freely. If the captured pictures should have the same picture height, check **Fixed Value** and input desired picture height.

Face Beautification

Check **Face Beautification** and adjust the beautification level as needed.



Note

Face Beautification slightly adjusts skin tone and reduces facial noise.

Background Picture Settings

Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

Text Overlay

You can check desired items (Device No., Camera Info. and Capture Time) and adjust their order to display on captured pictures by  .

See **Set Camera Info** to set **Device No.** and **Camera Info.**

3.3.3 Advanced Parameters

It is used to set the parameters of the algorithm library for better detection performance.

HMS Version

It refers to the current algorithm version, which cannot be edited.

Restore Defaults

Click **Restore** to restore all the settings in advanced configuration to the factory default.

Capture Parameters

Best Shot

The device captures the target picture with the highest score after setting the parameters.

Capture Times

It refers to the capture times a face will be captured during its stay in the detection area.

Capture Threshold

It refers for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Remove Duplicated Faces

This function can filter out repeated captures of certain face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

Every face picture is kept in the duplicates removing library for the set update time.

Quick Shot

The device captures the target picture once the score of the captured face exceeds the **Quick Shot Threshold** during the **Max. Capture Interval**. Otherwise, the device selects and uploads the picture with the highest score during the **Max. Capture Interval**.

Quick Shot Threshold

It refers to the quality of face to trigger quick shot.

Max. Capture Interval

It describes the max. time occupation for one quick shot.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area. The device captures the target face according to the set times.

Face Exposure

Enable the function, and the device automatically adjusts exposure level when human faces appear in the scene.

Reference Brightness

It refers to the reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lowers the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.

Minimum Duration

The extra time the device keeps the face exposure level after the face disappears in the scene.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Data Upload

Check one or more desired target types for picture uploading.

3.4 Person Arming

When the device detects the armed face or human body in the monitoring scene, it triggers alarms, and tracks and captures the target. During the tracking, the target location and other related information are uploaded.



Note

- Select **Person Arming** on **VCA Resource** page to show the configuration page.
- Target location information can be uploaded only when you set the GPS Calibration properly. See **GPS Calibration** for instructions.
- This function is only supported by certain device models.

Device Auto Person Arming and **Manual Person Arming** are supported. The **Manual Person Arming** has a higher priority than the other, which means it can interrupt the ongoing auto person arming.

Manual Person Arming	The device tracks and captures the manually selected target and uploads the related data.
Device Auto Person Arming	The device tracks and captures targets automatically according to the setting rule.

3.4.1 Device Auto Person Arming

You need to set face picture libraries and auto person arming rules to realize device auto person arming.

Set Auto Person Arming Rule

Before You Start

The face picture library should be set in advance. See .

Steps

1. Go to **VCA → Set Application → Person Arming → Basic Settings** .

2. Check **Enable**.

3. Set the parameters for face picture comparison and arming.

1) Set the **Face Grading Threshold for Detection** and **Max. Detection Time of Face**.

Face Grading Threshold for Detection

Every face entering the monitoring scene is graded by the device according to the quality. When a face with its grading exceeds the set threshold, it triggers the comparison with the pictures in the selected face picture library.

Max. Detection Time of Face

If the grading of a target face does not reach the set **Face Grading Threshold for Detection** during the set time, the device stops grading the target face.

2) Select a desired library, and set as the **Face Picture Library**.

3) Set the arming schedule and linkage method for the selected library.



Note

The arming schedule and linkage method for different libraries are allowed to set independently.

4. Click **Save**.

Advanced Settings

In advanced parameters, you can set the tracking, capture and other parameters for the person arming.

Tuning Mode

The mode is only for the professional users.

Tracking Capture

Check to enable the device to capture the targets during the tracking.

Some capture parameters are allowed to adjust.

Face Capture Threshold

It refers for the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Human Body Capture Threshold

It refers for the quality of human body to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Tracking Parameters

Zooming Control

Two modes are available. Controlled by target frame or by tilt angle of the device.

By Tilt Angle

The device calculates the tracking zoom ratio automatically according to the tilt angle of the device.



Note

The attitude of the device affects the accuracy of this zooming control mode. For the model with a built-in gyroscope, try to calibrate the attitude if some zooming problems happen during tracking. See [***Set Device Position***](#) for instructions.

By Target Frame

The tracked target has a virtual frame around. The device calculates a suitable zoom ratio according to the frame and the set **Tracking Zoom Ratio**. Larger value means bigger zoom ratio.

Dwell Time after Failed Tracking

The time the device stays at the position where the target tracking fails.

Report Interval of Tracking Info

The alarming information upload interval during tracking.

Wait to Stop Tracking If Low Validity

The validity is an internal parameter that helps judge whether the device should keep tracking or not. This parameter is the waiting time level before the device stops tracking when the validity is low. Larger value means longer waiting time.

Wait to Lower Tracking Speed If Low Validity

The validity is an internal parameter that helps judge whether the PTZ channel should lower the tracking speed or not. This parameter is the waiting time level before the device lowers the tracking speed when the validity is low. Larger value means longer waiting time.

Tracking Duration

When you set the **Tracking Duration** as **0**, the device keeps tracking the target until it disappears.

When you set the **Tracking Duration** as a number other than 0, the device tracks a target for the set time. The tracking stops when the time is up or when the target disappears.

Display Tracking Target on Panorama

Check to display a frame around the target that is tracked by the PTZ channel.



Note

Go to **Configuration → Local → Live View Parameters**, and enable **Rules** before using this function.

3.4.2 Manual Person Arming

The device tracks and captures the manually selected target and uploads the related data.



Note

Manual face capture is prior to the manual person arming. When the manual face capture is in use, the manual person arming is temporarily unavailable.

Steps

1. Click **Live View**.
2. Click  to start manual person arming.
3. Click or frame a person as the target.

The device starts to track the target and upload related data.

4. Click  to stop manual person arming.

3.4.3 Capture Settings

Multi-target-type detection is used for capturing armed persons. You can set the capture rules and parameters according to your needs.

Set Detection Rule

After the rules and algorithm parameters are set, the device captures targets of multiple types and triggers linkage actions automatically.

Steps

1. Go to **VCA → Face+Human → Rule** .
2. Check **Enable**.
3. Select a configuration mode.

Normal One detection scene is allowed to set. The device captures targets in the scene in the set arming schedule.
See for details.

Expert The device can patrol among the detection scenes and capture target images. Detection scenes and patrol schedule should be set in advance.
See for details.

4. Click **Save**.

What to do next

Go to **Picture** to search and view the captured pictures.

Go to **Smart Display** to see currently captured target pictures.

Overlay and Capture

Choose to configure capture parameters and the information you want to display on stream and picture.

Display VCA Info. on Stream

Display smart information on stream, including the target and rules information.

Display Target Info. on Alarm Picture

Overlay the alarm picture with target information.

Target Picture Settings

You can set the face picture type by selecting **Custom**, **Head Shot**, **Half-Body Shot**, or **Full-Body Shot**. If you select **Custom**, you can define detailed picture width and height of a picture freely. If the captured pictures should have the same picture height, check **Fixed Value** and input desired picture height.

Face Beautification

Check **Face Beautification** and adjust the beautification level as needed.



Note

Face Beautification slightly adjusts skin tone and reduces facial noise.

Background Picture Settings

Comparing to target picture, background picture is the scene image offers extra environmental information. You can set the background picture quality and resolution. If the background image need to be uploaded to surveillance center, check **Background Upload**.

Text Overlay

You can check desired items (Device No., Camera Info. and Capture Time) and adjust their order to display on captured pictures by  .

See [Set Camera Info](#) to set **Device No.** and **Camera Info.**

Advanced Parameters

It is used to set the parameters of the algorithm library for better detection performance.

HMS Version

It refers to the current algorithm version, which cannot be edited.

Restore Defaults

Click **Restore** to restore all the settings in advanced configuration to the factory default.

Capture Parameters

Best Shot

The device captures the target picture with the highest score after setting the parameters.

Capture Times

It refers to the capture times a face will be captured during its stay in the detection area.

Capture Threshold

It refers to the quality of face to trigger capture and alarm. Higher value means better quality should be met to trigger capture and alarm.

Remove Duplicated Faces

This function can filter out repeated captures of certain face.

Similarity Threshold for Duplicates Removing

It is the similarity between the newly captured face and the picture in the duplicates removing library. When the similarity is higher than the value you set, the captured picture is regarded as a duplicated face and will be dropped.

Duplicates Removing Library Grading Threshold

It is the face grading threshold that triggers duplicates checking. When the face grading is higher than the set value, the captured face is compared with the face pictures that are already in the duplicates removing library.

Duplicates Removing Library Update Time

Every face picture is kept in the duplicates removing library for the set update time.

Quick Shot

The device captures the target picture once the score of the captured face exceeds the **Quick Shot Threshold** during the **Max. Capture Interval**. Otherwise, the device selects and uploads the picture with the highest score during the **Max. Capture Interval**.

Quick Shot Threshold

It refers to the quality of face to trigger quick shot.

Max. Capture Interval

It describes the max. time occupation for one quick shot.

Capture Times

It refers to the capture times a face will be captured during its stay in the configured area. The device captures the target face according to the set times.

Face Exposure

Enable the function, and the device automatically adjusts exposure level when human faces appear in the scene.

Reference Brightness

It refers to the reference brightness of a face in the face exposure mode. If a face in the actual scene is brighter than the set reference brightness, the device lowers the exposure level. If a face in the actual scene is darker than the set reference, the device increases the exposure level.

Minimum Duration

The extra time the device keeps the face exposure level after the face disappears in the scene.

Face Filtering Time

It means the time interval between the camera detecting a face and taking a capture action. If the detected face stays in the scene for less than the set filtering time, capture will not be triggered. For example, if the face filtering time is set as 5 seconds, the camera will capture the detected face when the face keeps staying in the scene for 5 seconds.

Data Upload

Check one or more desired target types for picture uploading.

3.5 Intelligent Traffic Event (ITS)

The device detects vehicles, traffic violations, and traffic accidents, captures evidence pictures, and collects traffic data. You can set the rules for detection, alarm messages, and data uploading.

3.5.1 Basic Settings

You can set the basic information, listening server, and ANR.

Go to **VCA → Intell Traffic Event → Common Settings → Basic Configuration** to complete the settings.

Basic Information

Select the **Country/Region**.

Listening Server

If the device uploads alarms in listening mode via our company's SDK, you should set the IP address and port for the listening server.

ANR

When the network is disconnected, data is temporarily saved on the memory card. When the network connection is resumed, the device automatically uploads the saved data to the arming host, in which case, the arming host IP address is required.



Note

A memory card should be installed in the device. Memory card settings should be completed. See ***Memory Card*** for instructions.

3.5.2 Common Settings

These are the commonly used settings for all types of ITS detections.

Set Lane Area

A lane area is where you want to set the detection rules. Mark the lane area according to the actual lanes in the view.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings** and click **Lane Area**.
2. Click **Add**.
Blue lane lines and a trigger line show on the live view.
3. Drag the lane lines to frame the actual lane on the image.



Note

- You can click **Full Screen** to enlarge the live view window. Press **ESC** on the keyboard to exit.
 - Lane lines cannot overlap.
-
4. Select the direction of the traffic and line type of the left and right lane lines according to the actual situation.
 5. Drag the trigger line to adjust its length and position.
The trigger line is where the device captures the vehicle pictures in some detections and where traffic data collection is triggered.
 6. **Optional:** Repeat the steps above to set multiple lane areas.

7. Click **Save**.

Set Polygon Area

A polygon area is where you want to set the detection rules. Draw the area according to the actual situation.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** and click **Polygon Area**.
2. Click **Add Area**.
3. Click to mark the corner points of the polygon area. Right click to complete drawing.



Note

- You can click to enlarge the live view window. Press **ESC** on the keyboard to exit.
- Polygon areas cannot overlap.
- Click on the area and you can drag the corner points to adjust the area.

4. Select the line type of the left and right side lines according to the actual situation.
5. **Optional:** Repeat the steps above to set multiple polygon areas.



Note

When there are multiple polygon areas, you can click on one area and click to delete it.

6. Click **Save**.
-

Set Detection Scene

A detection scene is an area you want to monitor. If one detection scene cannot cover all the intended monitoring areas, set multiple detection scenes.

Steps

1. Go to **VCA → Set Application → ITS (Intelligent Transportation System) → Close-up Rule Settings**.
2. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.
Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
3. Select a **Scene**.
4. Check **Enable** to enable the scene.
5. Click the PTZ control buttons to adjust the scene to where you want to monitor.
6. Enter a **Scene Name**.
7. Select the **Scene Direction** according to the traffic direction in the scene.
8. Click **Save**.

9. Optional: Repeat the steps above to set multiple detection scenes.

10. Optional: Select a **Scene** to turn the live view image to the scene.

Set ITS Arming Schedule

The device automatically detects among multiple scenes according to the arming schedule.

Before You Start

Set multiple detection scenes. See [Set Detection Scene](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Arming Schedule** .
2. Check **Enable**.
3. Draw a bar on the timeline to cover the arming hours.
4. **Optional:** Click on an arming period and adjust the arming hours.
 - Enter the start time and end time and click **Save** to fine-tune the arming period.
 - Click **Delete** to delete the arming period.
5. Click on an arming period, and click **Configuration**.
6. Set the **Patrol Sequence** and **Dwell Time** in each scene.

	Add a detection scene to the patrol sequence.
	Adjust the order of the scenes.
	Remove the detection scene from the patrol sequence.

7. Click  to copy the setting to another day.

8. Click **Save**.

9. Optional: Go to **VCA → Intell Traffic Event → Advanced Configuration → Advanced** to set **PTZ Camera Motion Parameters**.

Enforcement Park Time

Manual control of the device takes priority over automatic patrols. When manual control is over, the device waits for the set **Enforcement Park Time** before resuming automatic detection.

Scene Auto-switch

If only **Illegal Parking Detection** is enabled in a scene, the device automatically switches to the next scene when no evidence picture capturing is triggered for the set **Auto-switch Interval**.

3.5.3 Enforcement

Enforcement includes detection of traffic violations and evidence picture capturing.

Set Illegal Parking Detection

Illegal parking is the violation of parking rules, for example, parking in a restricted place. The device can automatically detect violations and capture evidence pictures or you can manually capture pictures on the live view image.

Set Auto Capture for Illegal Parking

Set the rules for the device to automatically detect illegal parking violations and capture evidence pictures.

Before You Start

Set detection scenes and detection areas. See [Set Detection Scene](#) and [Set Polygon Area](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings**.
2. Select **Enforcement**.
3. Click **Illegal Parking Detection** and check **Enable**.
4. Select **Arm Polygon**.

Illegal parking detection takes effect in the selected polygon areas.

5. Select the car types.

Only selected car types will trigger illegal parking alarms.

6. Check **Illegal Parking License Plate Recognition**.

When an illegal parking event is triggered, the device zooms in to recognize the license plate. If the **License Plate Thumbnail** in **Advanced** settings is enabled, a picture of the license plate is uploaded with the alarm message.

7. Set **Parking Tolerance**.

When the vehicle stays in the detection area longer than the parking tolerance, the device starts to take evidence pictures.

8. Set the evidence picture parameters.

1) Set **Amount of Pictures**.

2) Click **Illegal Parking Capture Settings**, select the **Picture Type** for each picture and set the **Capture Interval** between the pictures.



Note

- You can select **Picture Type** as **Custom** after you upload the custom picture in **VCA → Intell Traffic Event → Advanced Configuration → Picture**.
- To ensure clear license plate recognition, set at least one **Close View** picture.

-
9. Click **Advanced**.

No Alarm When Congestion Occurs in Detection Area

Check to enable this function and alarms will not be triggered when congestion occurs in the detection area.

Sensitivity

With higher sensitivity, the device is more sensitive to detect and recognize targets.

10. Click **Save**.

What to do next

Set the arming schedule, linkage and alarm. See [Set ITS Arming Schedule](#) and [ITS Linkage and Alarm](#) for details.

Set Manual Capture for Illegal Parking

Set the rules for manually selecting illegal parking vehicles and capturing evidence pictures.

Steps

1. Go to **VCA → Intell Traffic Event → Advanced Configuration → Manual Capture for Illegal Parking**.
2. Set the manual capture parameters.

Manual License Plate Recognition

When an illegal parking vehicle is manually selected on the live view image, the device zooms in to recognize the license plate. If the **License Plate Thumbnail** in **Advanced** settings is enabled, a picture of the license plate is uploaded with the alarm message.

Capture No Plate Vehicle

Check to enable this function. The device captures the evidence pictures even if the license plate of a vehicle is not recognized.

Plate Matching Ratio

The device compares the captured pictures of a vehicle and saves the pictures that have a higher matching ratio than the set **Plate Matching Ratio**. If the ratio is set to **0**, the device does not compare the pictures.

Amount of Pictures

Set the amount of pictures the device captures when a vehicle is manually selected.

Description

Select the **Picture Type** for each picture and set the **Capture Interval** between the pictures.

You can select **Picture Type** as **Custom** after you upload the custom picture in **VCA → Intell Traffic Event → Advanced Configuration → Picture**.

3. Click **Save**.
4. Go to **Live View** and click  on the toolbar.
5. Select an illegal parking vehicle on the live view image.
The device takes evidence pictures of the vehicle.
6. Click the icon again to end manual capture.

What to do next

Set the linkage and alarm. See [***ITS Linkage and Alarm***](#) for details.

Set Illegal Parking Evidence Capture Parameters

Go to **VCA → Intell Traffic Event → Advanced Configuration → Advanced** to set the parameters.

Illegal Parking LPR Area

Set the size of license plate recognition area that suits the actual situation to avoid mistakenly recognize the license plate of other vehicles around.

Illegal Parking LPR Double Check

The device double-checks the license plate to avoid mistakenly capturing of other vehicles.

Illegal Parking LPR Grading Threshold

If the confidence level of captured license plate or any character on the license plate is lower than the threshold, the plate will not be recognized. The alarm information may be filtered out if the threshold is too high.

Illegal Parking Plate Size Threshold

If the width of the captured license plate is lower than the set threshold, the plate will not be recognized. The lower the threshold is, the smaller plates will be filtered out. It is recommended to keep the default value.

Illegal Parking Target Lock

When the illegal parking target lock is enabled, the device focuses on the vehicle that triggers the evidence capture and ignores other vehicles. It is suitable for situations where strict enforcement is required, but it decreases the overall evidence capture efficiency.

Set Reverse Driving Detection

Reverse driving refers to driving against the direction of traffic. The device detects violations and captures evidence pictures.

Before You Start

Set detection scenes and detection areas. See [***Set Detection Scene***](#) and [***Set Lane Area***](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings**.
2. Select **Enforcement**.
3. Click **Reverse Driving Detection** and check **Enable**.
4. Select **Arm Lane**.



Note

The direction of the arm lane cannot be **Unknown**.

Reverse driving detection takes effect in the selected lane areas.

5. Set the **Amount of Pictures.**

The device takes evidence pictures of the set amount when a vehicle hits the trigger line in the detection area.

6. Set **Sensitivity.**

With higher sensitivity, the device is more sensitive to detect and recognize targets.

7. Click **Save.**

What to do next

Set the arming schedule, linkage and alarm. See [**Set ITS Arming Schedule**](#) and [**ITS Linkage and Alarm**](#) for details.

Set U-turning Detection

The device detects vehicles making a u-turn where it is not allowed and captures evidence pictures.

Before You Start

Set detection scenes and detection areas. See [**Set Detection Scene**](#) and [**Set Lane Area**](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings** .
2. Select **Enforcement**.
3. Click **U-turning Detection** and check **Enable**.
4. Select at least two lanes in **Arm Lane**.



Note

The direction of the arm lanes cannot be the same and the lane lines between the two lanes cannot be **Broken Line**. Otherwise, the u-turning event will not be triggered.

U-turning detection takes effect in the selected lane areas.

5. Set **Sensitivity.**

With higher sensitivity, the device is more sensitive to detect and recognize targets.

6. Click **Save.**

What to do next

Set the arming schedule, linkage and alarm. See [**Set ITS Arming Schedule**](#) and [**ITS Linkage and Alarm**](#) for details.

Set Over Lane Line Detection

The device detects vehicles driving over lane lines where it is not allowed and captures evidence pictures.

Before You Start

Set detection scenes and detection areas. See [Set Detection Scene](#) and [Set Lane Area](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings**.
2. Select **Enforcement**.
3. Click **Over Lane Line Detection** and check **Enable**.
4. Select **Arm Lane**.



Note

If the lane line is **Solid-Broken Line** or **Broken-Solid Line**, only driving from the solid side triggers the alarm.

Over lane line detection takes effect in the selected lane areas.

5. Set the **Amount of Pictures**.

The device takes evidence pictures of the set amount when a vehicle hits the trigger line in the detection area.

6. Set **Sensitivity**.

With higher sensitivity, the device is more sensitive to detect and recognize targets.

7. Click **Save**.

What to do next

Set the arming schedule, linkage and alarm. See [Set ITS Arming Schedule](#) and [ITS Linkage and Alarm](#) for details.

Set Illegal Lane Change Detection

The device detects vehicles changing lanes where it is not allowed and captures evidence pictures.

Before You Start

Set detection scenes and detection areas. See [Set Detection Scene](#), [Set Polygon Area](#) and [Set Lane Area](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings**.
2. Select **Enforcement**.
3. Click **Illegal Lane Change Detection** and check **Enable**.
4. Select **Arm Lane** or **Arm Polygon**.



Note

- If the line type is **Solid-Broken Line** or **Broken-Solid Line**, only driving from the solid side triggers the alarm.
 - If you choose **Arm Polygon**, set and select at least two polygon areas for the detection to take effect.
-

Illegal lane change detection takes effect in the selected lanes or areas.

5. Set Sensitivity.

With higher sensitivity, the device is more sensitive to detect and recognize targets.

6. Click Save.

What to do next

Set the arming schedule, linkage and alarm. See [Set ITS Arming Schedule](#) and [ITS Linkage and Alarm](#) for details.

Set Vehicle on Non-motor Vehicle Lane Detection

The device detects vehicles driving on non-motor vehicle lane and captures evidence pictures.

Before You Start

Set detection scenes and detection areas. See [Set Detection Scene](#) and [Set Lane Area](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings**.
2. Select **Enforcement**.
3. Click **Vehicle on Non-motor Vehicle Lane** and check **Enable**.
4. Select **Arm Lane**.

Vehicle on non-motor vehicle lane takes effect in the selected lane areas.

5. Set the Amount of Pictures.

The device takes evidence pictures of the set amount when a vehicle hits the trigger line in the detection area.

6. Set Duration.

When the vehicle stays in the detection area longer than the duration, an alarm is triggered.

7. Click Save.

What to do next

Set the arming schedule, linkage and alarm. See [Set ITS Arming Schedule](#) and [ITS Linkage and Alarm](#) for details.

Advanced Settings for Enforcement

Go to **VCA → Intell Traffic Event → Advanced Configuration → Advanced** to set the parameters.

Alarm Uploading

License Plate Thumbnail

When the license plate is recognized during enforcement, a license plate image is uploaded.

Upload Traffic Violation Data

Check to upload the alarm data when an enforcement event is triggered.

Upload Enforcement Data

Check to upload the alarm data when evidence capture of an enforcement is triggered.

Violation Filtering Parameters

Check to enable filtering mode.

Repeated Alarm Filtering Time

If a vehicle stays unmoved within the set filtering time, illegal parking alarm will not be triggered repeatedly.

Illegal Filtering Threshold

Within the set threshold time, the same vehicle will not trigger the same enforcement alarm repeatedly.

For example, when the illegal filtering threshold is set to **30** minutes, if a vehicle triggers reverse driving alarm, other reverse driving violations of the same vehicle within 30 minutes do not count. After 30 minutes, reverse driving of the vehicle will trigger a second alarm.

Capture No Plate Vehicle

Check to enable this function. The device captures the evidence pictures even if the license plate of a vehicle is not recognized.

Plate Matching Ratio

The device compares the captured pictures of a vehicle and saves the pictures that have a higher matching ratio than the set **Plate Matching Ratio**. If the ratio is set to **0**, the device does not compare the pictures.

Common Evidence Capture Parameters

Alarm Feature View

When **Alarm Feature View** is enabled, the last evidence picture of enforcement detections and the alarm picture of vehicle detection are set to be feature view pictures. A feature view picture is a close-up picture of a target vehicle. The function takes effect when **Track and Collect Evidence** is not enabled.

Feature View Size Level

The higher the feature view size level is, the larger the target vehicle is in feature view pictures.

Ratio Coefficient of Getting Evidence

The higher the ratio coefficient of getting evidence is, the more the picture is enlarged when the device is recognizing the license plate.

Track and Collect Evidence

When **Track and Collect Evidence** is enabled, the license plate recognition of reverse driving, over lane line, illegal lane change, u-turning, and vehicle on non-motor vehicle lane is completed during tracking. If it is not enabled, recognition is done when the license plate is large and close to the bottom of the image.

3.5.4 Traffic Event Detection

Traffic event detection includes detection of incidents happens on the road, for example, thrown objects and traffic congestion. The device captures pictures and uploads alarm data.

Set Fallen Object Detection

The device detects fallen objects on the road and captures pictures.

Before You Start

Set detection areas. See [Set Polygon Area](#) and [Set Lane Area](#) for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings**.
2. Click **Add Event** and select **Fallen Object Detection**.
3. Select **Arming Lane** or **Arming Polygon**.

Fallen object detection takes effect in the selected lanes or areas.

4. Set **Sensitivity**.

With higher sensitivity, the device is more sensitive to detect and recognize targets.

5. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See [Set Arming Schedule](#) and [ITS Linkage and Alarm](#) for details.

Set Pedestrian Detection

The device detects pedestrians and non-motor vehicles in the detection area and captures pictures.

Before You Start

Set detection areas. See [Set Polygon Area](#) and [Set Lane Area](#) for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings**.
2. Click **Add Event** and select **Pedestrian Detection**.
3. Select **Arming Lane** or **Arming Polygon**.

Pedestrian detection takes effect in the selected lanes or areas.

4. Set **Sensitivity**.

With higher sensitivity, the device is more sensitive to detect and recognize targets.

5. Set **Duration**.

When the target stays in the detection area longer than the duration (at night, three times the duration), an alarm is triggered.

6. Set **Filtering Time**.

Within the set filtering time, the same target will not trigger the alarm repeatedly.

7. Select the target types in **Detection Target**.

Only selected target types trigger linkage and alarm.

8. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See [**Set Arming Schedule**](#) and [**ITS Linkage and Alarm**](#) for details.

Set Congestion Detection

The device detects traffic congestion in the detection area and captures pictures.

Before You Start

Set detection areas. See [**Set Polygon Area**](#) and [**Set Lane Area**](#) for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** .

2. Click **Add Event** and select **Congestion Detection**.

3. Select **Arming Lane** or **Arming Polygon**.

Congestion detection takes effect in the selected lanes or areas.

4. Set **Sensitivity**.

With higher sensitivity, the device is more sensitive to detect and recognize targets.

5. Set **Duration**.

When the congestion in the detection area lasts longer than the duration, an alarm is triggered.

6. Set **Filtering Time**.

Within the set filtering time, the congestion in the same detection area will not trigger the alarm repeatedly.

7. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See [**Set Arming Schedule**](#) and [**ITS Linkage and Alarm**](#) for details.

Set Roadblock Detection

The device detects roadblocks in the detection area and captures pictures.

Before You Start

Set detection scenes and detection areas. See [**Set Detection Scene**](#) , [**Set Polygon Area**](#) and [**Set Lane Area**](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings** .
2. Select **Traffic Event Detection**.
3. Click **Roadblock Detection** and check **Enable**.
4. Select **Arm Lane** or **Arm Polygon**.
Roadblock detection takes effect in the selected lanes or areas.
5. Set **Sensitivity**.
With higher sensitivity, the device is more sensitive to detect and recognize targets.
6. Set **Duration**.
When the roadblock stays in the detection area longer than the duration, an alarm is triggered.
7. Set **Filtering Time**.
Within the set filtering time, the roadblocks in the same detection area will not trigger the alarm repeatedly.
8. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See [**Set ITS Arming Schedule**](#) and [**ITS Linkage and Alarm**](#) for details.

Set Construction Detection

The device detects ongoing construction in the detection area and captures pictures.

Before You Start

Set detection areas. See [**Set Polygon Area**](#) and [**Set Lane Area**](#) for details.

Steps

1. Go to **VCA → Set Application → Tunnel Event Detection → Panoramic Rule Settings** .
2. Click **Add Event** and select **Construction Detection**.
3. Select **Arming Lane** or **Arming Polygon**.
Construction detection takes effect in the selected lanes or areas.
4. Set **Sensitivity**.
With higher sensitivity, the device is more sensitive to detect and recognize targets.
5. Set **Duration**.
When the construction in the detection area lasts longer than the duration, an alarm is triggered.
6. Set **Filtering Time**.
Within the set filtering time, the construction in the same detection area will not trigger the alarm repeatedly.
7. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See [Set Arming Schedule](#) and [ITS Linkage and Alarm](#) for details.

Set Traffic Accident Detection

The device detects traffic accidents in the detection area and captures pictures.

Before You Start

Set detection scenes and detection areas. See [Set Detection Scene](#) and [Set Polygon Area](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings** .

2. Select **Traffic Event Detection**.

3. Click **Traffic Accident Detection** and check **Enable**.

4. Select **Arm Polygon**.

Traffic accident detection takes effect in the selected areas.

5. Set **Sensitivity**.

With higher sensitivity, the device is more sensitive to detect and recognize targets.

6. Set **Duration**.

When the traffic accident in the detection area lasts longer than the duration, an alarm is triggered.

7. Set **Filtering Time**.

Within the set filtering time, the traffic accidents in the same detection area will not trigger the alarm repeatedly.

8. Click **Save**.

What to do next

Set the arming schedule, linkage and alarm. See [Set ITS Arming Schedule](#) and [ITS Linkage and Alarm](#) for details.

3.5.5 Vehicle Detection

The device detects vehicles in the detection area, recognizes license plates, captures and saves pictures, and uploads alarms.

Before You Start

Set detection scenes and detection areas. See [Set Detection Scene](#) and [Set Lane Area](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings** .

2. Select **Vehicle Detection**.

3. Check **Enable**.

4. Select **Arm Lane**.

Vehicle detection takes effect in the selected lane areas.

5. Select the car types.

Only selected car types will trigger alarms.

6. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See [**Set ITS Arming Schedule**](#) and [**ITS Linkage and Alarm**](#) for details.

Set Detection Scene

A detection scene is an area you want to monitor. If one detection scene cannot cover all the intended monitoring areas, set multiple detection scenes.

Steps

1. Go to **VCA → Set Application → ITS (Intelligent Transportation System) → Close-up Rule Settings**.
2. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.
Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
3. Select a **Scene**.
4. Check **Enable** to enable the scene.
5. Click the PTZ control buttons to adjust the scene to where you want to monitor.
6. Enter a **Scene Name**.
7. Select the **Scene Direction** according to the traffic direction in the scene.
8. Click **Save**.
9. **Optional:** Repeat the steps above to set multiple detection scenes.
10. **Optional:** Select a **Scene** to turn the live view image to the scene.

Set Lane Area

A lane area is where you want to set the detection rules. Mark the lane area according to the actual lanes in the view.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings** and click **Lane Area**.
2. Click **Add**.
Blue lane lines and a trigger line show on the live view.
3. Drag the lane lines to frame the actual lane on the image.



Note

- You can click **Full Screen** to enlarge the live view window. Press **ESC** on the keyboard to exit.
- Lane lines cannot overlap.

4. Select the direction of the traffic and line type of the left and right lane lines according to the actual situation.
5. Drag the trigger line to adjust its length and position.
The trigger line is where the device captures the vehicle pictures in some detections and where traffic data collection is triggered.
6. **Optional:** Repeat the steps above to set multiple lane areas.
7. Click **Save**.

Set ITS Arming Schedule

The device automatically detects among multiple scenes according to the arming schedule.

Before You Start

Set multiple detection scenes. See [Set Detection Scene](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Arming Schedule**.
2. Check **Enable**.
3. Draw a bar on the timeline to cover the arming hours.
4. **Optional:** Click on an arming period and adjust the arming hours.
 - Enter the start time and end time and click **Save** to fine-tune the arming period.
 - Click **Delete** to delete the arming period.
5. Click on an arming period, and click **Configuration**.
6. Set the **Patrol Sequence** and **Dwell Time** in each scene.

	Add a detection scene to the patrol sequence.
	Adjust the order of the scenes.
	Remove the detection scene from the patrol sequence.

7. Click to copy the setting to another day.
8. Click **Save**.
9. **Optional:** Go to **VCA → Intell Traffic Event → Advanced Configuration → Advanced** to set **PTZ Camera Motion Parameters**.

Enforcement Park Time

Manual control of the device takes priority over automatic patrols. When manual control is over, the device waits for the set **Enforcement Park Time** before resuming automatic detection.

Scene Auto-switch

If only **Illegal Parking Detection** is enabled in a scene, the device automatically switches to the next scene when no evidence picture capturing is triggered for the set **Auto-switch Interval**.

3.5.6 Traffic Data Collection

The device collects and uploads traffic data including vehicle speed, traffic volume, headway time, headway distance, time occupancy of a lane, and space occupancy of a lane.

Before You Start

Set detection scenes and detection areas. See [**Set Detection Scene**](#) and [**Set Lane Area**](#) for details.

Steps

1. Go to **VCA → Intell Traffic Event → Common Settings → Speed Dome Rule Settings**.
2. Select **Traffic Data Collection**.
3. Check **Enable**.
4. Select **Arm Lane**.

Traffic data collection takes effect in the selected lane areas.

5. Set **Statistics Interval**.

Traffic volume in a lane is counted and uploaded by the statistics interval.

6. Click **Save**.

What to do next

Set the arming schedule and linkage and alarm. See [**Set ITS Arming Schedule**](#) and [**ITS Linkage and Alarm**](#) for details.

3.5.7 ITS Linkage and Alarm

When traffic events are detected, the device can perform linkage actions, for example, uploading captured pictures and sending alarm messages.



Note

Some linkage actions may not be supported by certain device models.

Upload Pictures

Set the parameters for the device to automatically upload captured pictures to FTP server or other platforms.

See [**Upload by FTP**](#) to upload captured pictures by FTP.

See [**Upload by SDK**](#) or [**Set ISUP**](#) to upload captured pictures to platforms.

Upload by FTP

Upload the data of enforcement, vehicle detection, and traffic data collection to an FTP server.

Before You Start

The FTP server is configured.

Steps

1. Go to **VCA → Intell Traffic Event → Advanced Configuration → FTP Host**
2. Check **Enable FTP**.
3. Select a **Character Encoding Mode**.
4. Enter the **IP Address**, **Port**, **User Name**, and **Password** of the FTP server.
5. Set the picture names and saving paths of detections.
6. Click **Save**.

Upload by SDK

Upload the alarm messages by SDK in listening and arming mode.

Go to **VCA → Intell Traffic Event → Common Settings → Basic Configuration** to set the parameters.

Listening Server

You can upload alarm messages and pictures to a listening server by SDK. Enter the **IP Address** and **Port** of the listening server and click **Save**.



Note

Make sure that the listening server is enabled with listening service and that the network connection with the device is normal.

ANR

You can upload alarm messages and pictures to an arming server by SDK. Enter the **Arming Host IP Address** and click **Save**. When the device loses connection with the arming server, the data is saved in the memory card of the device and will be uploaded again when the connection resumes.

Set Armed License Plates

You can specify the vehicles you want to arm by adding their license plates to the blocklist or allowlist.

Steps

1. Go to **VCA → Intell Traffic Event → Advanced Configuration → Blocklist & Allowlist**.
2. Click **Export** to export license plate list template.



Note

If a list of license plates exists, the existing list is exported.

3. Fill in the list.
4. Click **Browse** to import the list.
The list shows on the web page.
5. Select a mode according to your need.
 - Normal Mode** No vehicle is armed.
 - Allowlist Mode** Vehicles NOT on the list are armed.
 - Blocklist Mode** Only the vehicles on the list are armed.
6. Click **Save**.

Set Alarm Output Linkage

The device sends alarm signals to the connected alarm output devices when an alarm is triggered.

Before You Start

The device is connected to alarm output devices.

Steps

1. Go to **VCA → Intell Traffic Event → Advanced Configuration → Alarm Output Linkage**.
2. Select alarm output channels for each type of alarms.
3. Click **Save**.

What to do next

See [***Trigger Alarm Output***](#) for detailed alarm output settings.

3.5.8 Vehicle Arming

The device detects and tracks designated license plates, and uploads real-time target location and other related information.



Note

- Select **ITS (Intelligent Transportation System)** on **VCA Resource** page to show the configuration page.
- Target location information can be uploaded only when the GPS calibration is completed. See [***GPS Calibration***](#) for configuration instructions.
- This function is only supported by certain device models.

Manual vehicle arming and platform-controlled vehicle arming are supported, and manual vehicle arming has a higher priority.

Manual Vehicle Arming	The device tracks the target manually selected by user and uploads related information.
Platform-Controlled Vehicle Arming	The device receives orders from the platform and performs arming tasks.  Note To use platform-controlled vehicle arming, you need to build a platform with the SDK tool provided on our website.

Manual Vehicle Arming

Steps

1. Go to **Live View** .
2. Click  .
3. Frame or click on a vehicle in the live image.
The device starts to track the vehicle.
4. Click  to stop manual vehicle arming.

Platform-Controlled Vehicle Arming

The device receives arming tasks from the platform to detect and track target vehicles. You can view the arming tasks in arming status.

Set Arming Location

Steps

1. Go to **VCA → Intell Traffic Event → Vehicle Arming → Arming Scene** .

Note

The PTZ control is automatically locked to avoid interruption during configuration.

2. Adjust the live image to the target scene with PTZ control buttons.
3. Click **Add**.
The scene is added to the Arming Scene List.
4. Edit the scene name and moving direction of the vehicles.
5. Repeat the steps to add other scenes.
6. Click **Save**.

View Arming Task

Go to **VCA → Intell Traffic Event → Vehicle Arming → Arming Status** to view the arming tasks sent from the platform.

The device performs a single task at one time. If it receives multiple tasks, former tasks are interrupted and the device performs the latest task.

3.5.9 Advanced Settings

You can set the advanced settings according to your need to get better vehicle arming effect.

Advanced Parameters

Go to **Configuration → Vehicle Arming → Advanced Configuration → Advance Parameters** to set the following parameters.

License Plate Thumbnail

If the device recognizes a license plate, an additional thumbnail of the license plate is uploaded.

Tuning Mode

The tuning mode is for professional technicians. It is not recommended to other users as it may affect the live view image.

Capture No Plate Vehicle

When this function is enabled, the device captures and uploads vehicle pictures with or without license plate. If it is not enabled, only pictures of vehicles with license plate are uploaded.

Dwell Time after Failed Tracking

The time the device stays at the position where the target tracking fails.

Report Interval of Tracking Info

The alarming information upload interval during tracking.

Wait to Stop Tracking If Low Validity

The validity is an internal parameter that helps judge whether the device should keep tracking or not. This parameter is the waiting time level before the device stops tracking when the validity is low. Larger value means longer waiting time.

Wait to Lower Tracking Speed If Low Validity

The validity is an internal parameter that helps judge whether the PTZ channel should lower the tracking speed or not. This parameter is the waiting time level before the device lowers the tracking speed when the validity is low. Larger value means longer waiting time.

Self-adaptive Ratio Coefficient

It represents the ratio of vehicle size to live image size during tracking. The larger the coefficient is, the larger the vehicle is shown.

Uploading Picture Settings

Go to **VCA → Set Application → ITS (Intelligent Transportation System) → Advanced Settings → Picture** to set the parameters of alarm pictures.

Picture Quality

Pictures with higher resolution and better quality have more details and larger file size.

Enable OSD Overlay

The device OSD is overlaid on alarm pictures.

Display Target Info. on Alarm Picture

Check to display target information on alarm pictures.

License Plate Exposure

You can adjust the exposure parameters to make sure that the license plates are exposed properly during vehicle arming.

Steps

1. Go to **VCA → Set Application → ITS (Intelligent Transportation System) → Advanced Settings → License Plate Exposure**.
2. Select a channel.
3. Check **License Plate Exposure**.
4. Set exposure parameters.

Reference Brightness

Adjust the reference brightness to the value that the license plate is exposed properly.

Min. Duration

The minimum duration to maintain the exposure level for the license plates when they are detected.

Arming Schedule

Set the start time and end time when the license plate exposure settings are valid.

5. Click **Save**.

3.6 People Density

This function detects the level of people density in the detection areas.

Before You Start

People Density is supported by the panoramic channel. You need to select **People Density** for Camera 02 or Camera 03 on **VCA Resource** page first.

Steps

1. Enable the function in **Configuration → People Density → Rule**.
2. Set a detection area.
 - Click , and click on the live image to define the boundary of the detection area. Left click to finish drawing.
 - Click  to clear selected areas.
 - Click  to clear all the areas.



Note

Up to 8 areas can be set at the same time.

3. Select an area from the list and set the target size as **Large-size Target** or **Small-size Target**.
 - Click , and a frame of 40 × 40 pixels will be displayed in the live image. If the shoulder of the target is wider than the frame, you should select **Large-size Target**.
 - Click , and a frame of 20 × 20 pixels will be displayed in the live image. If the shoulder of the target is shorter than the frame, you should select **Small-size Target**.



Note

If the shoulder width is between the two modes, adjust installation position and device angle to meet the requirements.

4. Define the **Density Level** by the number of people in the detection area and the target pixel ratio.

Number of People	Set the range for each level by inputting the lower limit of the number of people in the detection area.
Target Pixel Ratio	Target pixel ratio refers to the ratio of the detection area occupied by people. Check Enable Target Pixel Ratio and input the lower limit of target pixel ratio for each level.



Note

- Up to three levels can be configured. The density increases from level 1 to level 3.
- The target pixel ratio is optional. When it is enabled, both the set number of people and the ratio should be met to reach the density level.

Example

Set the people number of **Level 1** as **10**, **Level 2** as **100**, and **Level 3** as **1000**. When the number of people in the detection area is less than 10, the alarm is not triggered. When the number of people is between 10 and 100, Level 1 alarm is triggered. When the number of people is between 100 and 1000, Level 2 alarm is triggered. When the number exceeds 1000, Level 3 alarm is triggered.

5. Click **Save**.

6. Set arming schedule. See ***Set Arming Schedule*** .

7. Set linkage method. See ***Linkage Method Settings*** .

8. Set data uploading parameters in **Data Upload**.

- 1) Check **Enable Data Uploading**, and the data of people density detection is uploaded to surveillance center.
- 2) **Optional**: Check **Enable Picture Uploading**, and the alarm is uploaded to surveillance center with pictures.
- 3) Set the **Uploading Mode**.

Scheduled Uploading

The detection data and pictures can be uploaded to surveillance center at certain time intervals. Select **Statistics Cycle** on your demand.

Instant Uploading

Once the level of people density changes, the detection data and pictures are uploaded to surveillance center immediately.

- 4) **Optional**: If required, set **HTTP Data Transmission**. Input IP address, URL, and port, and click **Test** to see if it succeeds.
- 5) Click **Save**.

9. Configure overlay information in **Advanced Configuration**.

Display Rule Info. on Stream

Check **Display Rule Info. on Stream** to overlay the rule information in live image.

Display Rule Info. on Alarm Picture

Check **Display Rule Info. on Alarm Picture** to overlay the rule information on alarm pictures.

Overlay Pseudo-Color Density

Check **Overlay Pseudo-Color Density** and the real-time density is marked with colors in live image.



Note

The pseudo-color density can only be displayed on devices with discrete graphics.

Flow Overlay

Select corresponding parameters to display people number, density level, or ratio in live image. You can edit the region name for the detection area.

10. Click **Save**.

11. Select the **Algorithm Mode** in **Parameters**.

- If the network condition is good, select **Low Latency**.
- If long distance transmission is required, select **Long Distance**.

12. Click **Save**.

What to do next

After configuration, you can monitor people density in live view image, and the overlay information will be displayed in live view.

Note

To display the overlaid information, make sure that **Display POS Information** in **Configuration → Local → Live View Parameters** has been enabled.

3.7 Smart Display

This function displays real time pictures captured by smart functions and analyzes the target in real time.

Note

To use this function, your web browser version should be above IE11.0.9600.17843.

Live View Parameter

Icon	Function
	Start or stop live view.
	For devices with multiple channels, you can choose a way to display the images.
	For devices with multiple channels, you can choose one or more channels for live view.
	Capture a picture.
	Start or stop recording.
	Adjust the volume of live view. Move the slider to right to turn up the volume and left to turn down the volume. Move to the left end to mute the live view.

Download Display Pictures

Click  and the device stores captured pictures to the browser cache. Hover the pointer over the icon to see the number of pictures in the cache. Click  again to download the pictures in a package.

Note

The browser cache has a limited size. The recommended number of pictures to download is no more than 200.

Layout

Click  and choose **Layout**. Check the display content you need to add it to the smart display page. When real-time analyze is selected, you can choose the contents you want to display.

Chapter 4 PTZ

PTZ is an abbreviation for pan, tilt, and zoom. It means the movement options of the camera.

4.1 PTZ Control

In live view interface, you can use the PTZ control buttons to control the device panning, tilting, and zooming.

PTZ Control Panel

	Click and hold the directional button to pan/tilt the device.  Note - You can set Keyboard Control Speed in Configuration → PTZ → Basic Settings. The speed of pan/tilt movement in live view is based on this speed level. - You can set Max. Tilt-angle in Configuration → PTZ → Basic Settings to limit tilt movement range.
	Click the button, then the device keeps panning.  Note You can set Auto Scan Speed in Configuration → PTZ → Basic Settings. The higher the value you set, the faster the device pans.
	Drag the slider to adjust the speed of pan/tilt movement.

 Note

You can set **Manual Control Speed** in **Configuration → PTZ → Basic Settings**.

Compatible	The control speed is same as Keyboard Control Speed .
Pedestrian	Choose Pedestrian when you monitor the pedestrians.
Non-motor Vehicle	Choose Non-motor Vehicle when you monitor the non-motor vehicles.
Motor Vehicle	Choose Motor Vehicle when you monitor the motor vehicles.
Auto	You are recommended to set it as Auto when the application scene of the speed dome is complicated.

To avoid blurred image resulted from fast zoom, you can check **Enable Proportional Pan** in **Configuration → PTZ → Basic Settings** . If you enable this function, the pan/tilt speed change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.

Zoom in/out

	Click the button, and the lens zooms in.
	Click the button, and the lens zooms out.

Note

- You can set **Zooming Speed** in **Configuration → PTZ → Basic Settings** . The higher the value is, the faster the zooming speed is.
- You can set **Zoom Limit** in **Configuration → Image → Display Settings → Other** to limit the maximum value of the total zoom (digital zoom and optical zoom).

Focus

	Click the button, then the lens focuses near and the object nearby gets clear.
	Click the button, then the lens focuses far and the object far away gets clear.

Iris

	When the image is too dark, click the button to enlarge the iris.
	When the image is too bright, click the button to stop down the iris.

4.2 Set Preset

A preset is a predefined image position. For the defined preset, you can call the preset No. to view the position.

Steps

1. Click  to show the setting panel, and click .
2. Use the PTZ control buttons to move the lens to the desired position.
3. Select a preset number from the preset list, and click  to finish the setting.



Note

Some presets are predefined with special command. You can only call them but not configure them.

4. Repeat the steps above to set multiple presets.



Click the button to call the preset.



Click the button to delete the preset.



Note

You can delete all presets in **Configuration → PTZ → Clear Config**. Click **Clear All Presets**, and click **Save**.

What to do next

Go to **Configuration → PTZ → Basic Settings** to set preset freezing and preset speed.

After enabling preset freezing, the live image switches directly from one preset to another, without showing the areas between these two scenes. It also guarantees the masked area will not be seen when the device is moving.

4.2.1 Special Presets

You can call the following presets with special demands to enable corresponding functions.

Preset No.	Function	Preset No.	Function
33	Auto flip	92	Set manual limits
34	Back to origin	93	Save manual limits
35	Call patrol 1	94	Remote reboot
36	Call patrol 2	95	Call OSD menu
37	Call patrol 3	96	Stop a scan
38	Call patrol 4	97	Start random scan
39	Day mode	98	Start frame scan
40	Night mode	99	Start auto scan
41	Call pattern 1	100	Start tilt scan
42	Call pattern 2	101	Start panorama scan
43	Call pattern 3	102	Call patrol 5
44	Call pattern 4	103	Call patrol 6
45	One-touch patrol	104	Call patrol 7
46	Day/Night Mode	105	Call patrol 8

4.3 Set Patrol Scan

Patrol scan is a function to automatically move among multiple presets.

Before You Start

Make sure that you have defined more than one presets. See [Set Preset](#) for detailed configuration.

Steps

1. Click  to show the setting panel, and click  to enter patrol setting interface.
2. Select a patrol number from the list and click .
3. Click  to add presets.

Preset

Select predefined preset.

Speed

Set the speed of moving from one preset to another.

Time

It is the duration staying on one patrol point.

-  Delete the presets in patrol.



Adjust the preset order.



Note

A patrol can be configured with 32 presets at most, and 2 presets at least.

4. Click **OK** to finish a patrol setting.
5. Repeat the steps above to configure multiple patrols.
6. Operate patrols.



Call the patrol.



Stop patrolling.



Delete the patrol.



Set the patrol.



Note

You can delete all patrols in **Configuration → PTZ → Clear Config** . Click **Clear All Patrols**, and click **Save**.

4.3.1 Set One-Touch Patrol

The device automatically adds presets to one patrol path and starts patrol scan.

Steps

1. Set two or more presets among preset No.1 to preset No.32. For setting presets, refer to **Set Preset** .

The device will automatically add presets to patrol path No.8.

2. Choose one of the following methods to enable the function.
 - Click  .
 - Call patrol path No.8.
 - Select and call preset No.45.

4.4 Set Pattern Scan

The device can move as the recorded pattern.

Steps

1. Click  to show the PTZ control panel, and click  .
2. Select one pattern scan path that needs to be set.
3. Click  to start recording pattern scan.
4. Click PTZ control buttons as demands.



Note

Recording stops when the space for pattern scan is 0%.

5. Click  to complete one pattern scan path settings.

6. Click  to call pattern scan.

-  Stop pattern scan.
-  Reset pattern scan path.
-  Delete the selected pattern scan.



Note

If you need to delete all the pattern scans, go to **Configuration → PTZ → Clear Config** , and check **Clear All Patterns**, and click **Save**.

4.5 Set Limit

The device can only move within the limited range.

Steps

1. Go to **Configuration → PTZ → Limit** .
2. Select **Limit Type**.

Manual Stops

It refers to the movement range limit when you control the device manually.

Scan Stops

It refers to the movement range limit when the device scans automatically.



Note

Scan limit is only supported by the device that has scan function.

3. Click **Set** and set limits according to the prompt on the live image.
4. **Optional:** Click **Clear** to clear the limit settings of the selected mode.
5. Click **Save**.
6. Check **Enable Limit**.



Note

If you need to cancel all the set patrol paths, go to **Configuration → PTZ → Clear Config** , select **Clear All PTZ Limited**, and click **Save**.

Result

The device can only move within the set region after saving the settings.

4.6 Set Initial Position

Initial position refers to the relative initial position of the device azimuth. You can set the initial position if you need to select one point in the scene as the base point.

Steps

1. Go to **Configuration → PTZ → Initial Position** .
2. Move the device to the needed position by manually controlling the PTZ control buttons.
3. Click **Set** to save the information of initial position.

Call The device moves to the set initial position.

Clear Clear the set initial position.

4.7 Set Scheduled Tasks

You can set the device to perform a certain task during a certain period.

Steps

1. Go to **Configuration → PTZ → Scheduled Tasks** .
2. Check **Enable Scheduled Task**.
3. Select the task type and set the period. For setting the period, refer to **Set Arming Schedule** .
4. Repeat step 3 to set more than one scheduled tasks.
5. Set **Park Time**. During the set task period, if you operate the device manually, the scheduled task will be suspended. When the manual operation is over, the device will continue to perform the scheduled task after the set park time.
6. Click **Save**.



If you want to clear all scheduled tasks, go to **Configuration → PTZ → Clear Config** , check **Clear All Scheduled Tasks**, and click **Save**.

4.8 Operate Wiper

For the device that has a wiper, you can control the wiper via web browser.



Wiper operation and settings vary on device models.

Steps

1. Go to **Configuration → PTZ → Wiper** .
2. Select a wiper mode.

One Time	The wiper wipes one time when you click  on live view page.
Cycle	The wiper works on schedule at set wiping interval. Click  on live view to start wiping. Duration The schedule in which the wiper is ready to work. Interval The interval between two successive wiping actions.
Auto	 Note Auto mode is only available for device that supports rain-sensing auto wiper. In auto mode, the wiper works when rain drops on the window.

4.9 Set Park Action

You can set the device to perform an action (for example, preset or patrol) or return to a position after a period of inactivity (park time).

Before You Start

Set the action type first. For example, if you want to select patrol as park action, you should set the patrol. See [Set Patrol Scan](#) for details.

Steps

1. Go to **Configuration → PTZ → Park Action**.
2. Check **Enable Park Action**.
3. Set **Park Time**: the inactive time before the device starts park action.
4. Select **Action Type** according to your needs.
5. Select an **Action Type ID**, if you select patrol or preset as action type.
When the action type is patrol, action type ID stands for patrol No. When the action type is preset, action type ID stands for preset No.
6. Click **Save**.

4.9.1 Set One-Touch Park

This function is used to start park instantly.

Steps

1. Refer to [Set Park Action](#) to set a park action.
2. Choose from the following methods to start one-touch park.
 - Click .

- Call Preset No. 32.

4.10 Set Privacy Mask

Privacy masks cover certain areas on the live image to protect personal privacy from being live viewed and recorded.

Steps

1. Go to **Configuration → PTZ → Privacy Mask**.
2. Select the PTZ channel.
 - 1) Check **Enable Privacy Masks**.
 - 2) Adjust the live image to the target scene via PTZ control buttons.
 - 3) Draw the area.

Draw Area	Click Draw Area and drag the mouse in live view image. You can drag the corners of the red rectangle to adjust the area.
Stop Drawing	Click Stop Drawing after drawing area.

- 4) Click **Add**.
It is listed in **Privacy Mask List**.
- 5) Edit **Name**, **Type**, and **Active Zoom Ratio** on your demand.

Active Zoom Ratio

When the actual zoom ratio is less than the set active zoom ratio, the set area can not be covered. When the actual zoom ratio is greater than the set active zoom ratio, the privacy mask is valid. The maximum value of active zoom ratio depends on the camera module.

- 6) Click **Save**.
- 7) Repeat the steps above to set other privacy masks.
3. Select panoramic channel.
 - 1) Check **Enable Privacy Masks**.
 - 2) Draw the area.

Draw Area	Click Draw Area and drag the mouse in live image. You can drag the corners of the red rectangle to adjust the area.
Stop Drawing	Click Stop Drawing after drawing area.

- 3) Click **Add**.
It will be listed in **Privacy Mask List**.
- 4) Edit **Name**, **Type** on your demand.
- 5) Click **Save**.
- 6) Repeat the steps above to set other privacy masks.

4.11 Set Power Off Memory

This function can resume the previous PTZ status of device after it restarting from a power-off.

Steps

1. Go to **Configuration → PTZ → Basic Settings** .
2. Select **Resume Time Point**. When the device stays at one position for the set resume time point or more, the position is saved as a memory point. The device returns to the last memory point when it restarts.
3. Click **Save**.

4.12 Set PTZ Priority

The function can set the PTZ priority of different signals.

Steps

1. Go to **Configuration → PTZ → Prioritize PTZ** .
2. Set the priority signal and delayed time.

Network

The network signal controls the device with priority.

RS-485

The RS-485 signal controls the device with priority.

Delay

It refers to the time interval of PTZ operation controlled by different signals. When the operation with high priority is finished, the low priority signal controls the device after the setting interval.

3. Click **Save**.

4.13 Set Rapid Focus

Rapid focus is a function to reduce time of focusing comparing with that of normal focusing. To use the function, calibration should be done first. Rapid focus may not be supported by certain device models.

Steps

1. Go to **Configuration → PTZ → Rapid Focus** .
2. Add scenes for calibration.
 - 1) Adjust the live image to a desired scene via PTZ control buttons, and click **Add**.
 - 2) Set the **Rate** and the **Calibration Point Amount** of the added scene.



Note

More calibration points may increase calibration accuracy, but more focusing time is required. The default amount is recommended.

3. Select the scene to display the calibration line.

A red line displays on live image.

4. Adjust the length and position of the line by dragging its two endpoints.
-



Note

The red line is recommended to stay in the center of the scene and to cover ground at the same time.

Double click the image to enter full screen mode.

5. Click **Start Calibration**.

Calibration status displays on the live image.

6. Repeat to add other scenes and complete the calibration.
7. Check **Enable Height Compensation** if the mounting height of the device is lower than 3 meters.
8. Check **Enable** after successful calibration.
9. Click **Save**.

4.14 Set Device Position

Before You Start

Go to **Configuration → PTZ → Basic Settings → PTZ OSD** to enable **PT Status** display. Use other direction indicating devices to find the North at the device location.

Steps

1. Go to **Configuration → PTZ → Position Settings**.
 2. Set compass.
 - 1) Adjust the tilt position of the device to 0 by controlling the up arrow and down arrow on the PTZ panel.
 - 2) Adjust the pan position to show the live view of the north direction by controlling the left arrow and right arrow on the PTZ panel.
 - 3) Click **Set as North**.
 3. Click **Gyroscope Attitude Calibration** to calibrate gyroscope.
-



Note

Only the device with built-in gyroscope supports this function.

4. Get the device location information in advance, and input the longitude and latitude of the device manually.
5. Set vandal-proof alarm.

The function enables the device to trigger alarms when its position changes because of shock or vandalism.

Sensitivity

The higher the value is, the easier the alarm will be triggered.

Upload Vandal-proof Alarm

The device uploads the alarm information when the alarm is triggered.

Vandal-proof Alarm Voice Warning

The device triggers the alarm with audible warning.

6. Click **Save**.

What to do next

If you lost direction when operating the device, you can click **Point to North** to call the north position that is saved in the device.

4.15 Panorama Tracking

This function links panoramic channel with PTZ channel through calibration. The PTZ channel tracks moving objects in panoramic channel and automatically adjusts its PTZ positions to keep the target in the center of PTZ view for more details.



Note

This function is only supported by certain device models.

4.15.1 Link Channels by Calibration

Calibrate the panoramic channel and the PTZ channel to establish the link.

Steps

1. Go to **Configuration → PTZ → Panorama Tracking**.

2. Click **Calibration**.

3. Calibrate the channels automatically.

1) Select the **Calibration Mode** as **Auto (Fast)**.

2) Adjust the PTZ positions of the two channels and make the centers of the two channels at approximately the same position.

3) Click **Start Calibration**.

The device starts calibration automatically.

4. **Optional:** If automatic calibration fails, you can use the manual calibration.

1) Select the **Calibration Mode** as **Manual**.

2) Select a calibration point in **Calibration Parameter** list.

A numbered green cross is displayed on the panoramic image. You can drag the green cross to adjust its position.

3) Click **Add** to save the cross position in the panoramic channel.

- 4) Adjust PTZ to place the green cross in the PTZ channel at the same position as the green cross in the panoramic channel. 1× zoom ratio is recommended.



Note

To quickly locate the desired point in the PTZ channel, you can click  and click the target position in the PTZ channel.

-
- 5) Click  to save the PTZ position of this calibration point.
 - 6) Repeat the steps above to set at least 4 calibration points.
 - 7) Click **Start Calibration**.
5. Click **Save** to finish calibration.

4.15.2 Set Tracking Parameters

The tracking parameters includes the initial tracking position, tracking zoom ratio, tracking duration, and advanced parameters.

Steps

1. Go to **Configuration → PTZ → Panorama Tracking → Calibration**.
2. Set the initial tracking position of the PTZ channel.

When the tracking task stops, the PTZ channel returns to the set initial position.

- 1) Adjust the PTZ channel to the desired scene as the initial position.
- 2) Click **Set Tracking Initial Position** to save the position.

3. Set the tracking zoom ratio.

Set a fixed zoom ratio

A fixed zoom ratio means the PTZ channel keeps the set zoom value throughout the tracking.

Adjust the **Self-adaptive Ratio Coefficient** to **0**.

Adjust the zoom to a desired level.

Click **Set Zoom Ratio** to save the zoom level.

Set auto zoom ratio control

The device determines the actual zoom ratio dynamically according to the detected target size and the set **Self-adaptive Ratio Coefficient**.

Larger **Self-adaptive Ratio Coefficient** means larger zoomed target during tracking.

4. Set the tracking duration.
 - When you set the **Tracking Duration** as **0**, the PTZ channel keeps tracking the target until it leaves the view of the panoramic channel.
 - When you set the **Tracking Duration** as a number other than 0, the PTZ channel tracks a target for the set time. The tracking stops when the time is up or when the target leaves the view of the panoramic channel.
5. Click **Save**.
6. Go to **Configuration → PTZ → Panorama Tracking → Advanced**.
7. **Optional:** Check to enable **Tracking Takeover**.

When the target leaves the view of the panoramic channel, the PTZ channel takes over the leading role of the task and keeps tracking.

8. Optional: Check to enable **Track in Turn**.

When multiple targets trigger events in the panoramic channel around the same time, the PTZ channel tracks the targets in turn. If this function is not enabled, the PTZ channel tracks a target until it leaves the view.

9. Click **Save**.

4.16 GPS Calibration

GPS calibration is used to map the geographical location to the camera scene so that the device can calculate the real-time geographic information of targets. This function is only supported under certain VCA resource options.

4.16.1 Set GPS Calibration

Before You Start

Choose at least 4 calibration points on the ground in the monitoring scene and measure the precise longitude and latitude of the points. The calibration points should scatter in a 2×2 or 3×3 array.

Steps

1. Go to **Configuration → PTZ → GPS Calibration → Calibration** .



Note

The PTZ control is automatically locked to avoid interruption during configuration.

2. Select the longitude and latitude type according to device location.

3. Set calibration points.

1) Adjust the pan, tilt, and zoom to find the scene with a calibration point.

2) Click  and click on the calibration point on the live image.

The selected point is zoomed in and placed in the center of the image.

3) Click  again.

A green cross shows on the point.

4) Click **Add** and input the precise longitude and latitude of the point.

5) Click  to save the pan, tilt, and zoom value of the point.

6) Click **Save**.

7) Repeat the steps to set other calibration points.

4.16.2 Verify Calibration

Before You Start

Choose verification points on the ground in the monitoring scene and measure the precise longitude and latitude of the points.

Steps

1. Go to **Configuration → PTZ → GPS Calibration → Calibration Verification**.



Note

The PTZ control is automatically locked to avoid interruption during configuration.

2. Set verification points.

- 1) Adjust the pan, tilt, and zoom to find the scene with a verification point.
- 2) Click  and click on the verification point on the live image.

The selected point is zoomed in and placed in the center of the image.

- 3) Click  again.

A red cross shows on the point.

- 4) Click **Add** and input the precise longitude and latitude of the point.

- 5) Click  to save the pan, tilt, and zoom value of the point.

- 6) Click **Save**.

- 7) Repeat the steps to set other verification points.

Numbered green and blue rectangles are displayed on the image. The blue rectangle marks the PTZ position of the verification point you set and the green rectangle marks the calculated PTZ position based on the longitude and latitude you input. If the two rectangles are close to each other, then the GPS calibration succeeds.

Chapter 5 Live View

It introduces the live view parameters, function icons and transmission parameters settings.

5.1 Live View Parameters

The supported functions vary depending on the model.



Note

For multichannel devices, select the desired channel first before live view settings.

5.1.1 Start and Stop Live View

On **Live View** page, click  to start all live view. Click  to stop all live view.

You can also start the live view of the channels one by one through clicking a divided window first and double-clicking a channel from the channel list on left.

5.1.2 Aspect Ratio

Aspect Ratio is the display ratio of the width to height of the image.

-  refers to 4:3 window size.
-  refers to 16:9 window size.
-  refers to original window size.
-  refers to self-adaptive window size.

5.1.3 Window Division

You can choose a layout for live view window.

-  displays live images in three rows.
-  displays two live images on the top and one live image on the bottom.
-  displays live images in two rows.
-  displays one live image.
-  displays live images in 2 × 2 layout.
-  displays live images in PIP (picture in picture) layout.

5.1.4 Live View Stream Type

Select the live view stream type according to your needs. For the detailed information about the stream type selection, refer to [**Stream Type**](#) .

5.1.5 Quick Set Live View

It offers the quick access to the display settings, OSD, and video/audio on live view page.

Steps

1.



Click  and click **General** to show quick setup page.

2. Set display settings, OSD, and video/audio.

- For parameter explanation and instructions of display settings, see [**Display Settings**](#) .
- For parameter explanation and instructions of OSD settings, see [**OSD**](#) .
- For parameter explanation and instructions of audio and video settings, see [**Video and Audio**](#) .

5.1.6 Select the Third-Party Plug-in

When the live view cannot display via certain browsers, you can change the plug-in for live view according to the browser.

Steps

1. Click **Live View**.

2. Click  to select the plug-in.

- When you access the device via Internet Explorer, you can select Webcomponents or QuickTime.
- When you access the device via the other browsers, you can select Webcomponents, QuickTime, VLC or MJPEG.

5.1.7 Start Digital Zoom

It helps to see a detailed information of any region in the image.

Steps

1. Click  to enable the digital zoom.

2. In live view image, drag the mouse to select the desired region.

3. Click in the live view image to back to the original image.

5.1.8 Conduct Regional Focus

You can enable the function to focus on certain area.

Steps

1. Click  to enable regional focus.
2. Drag the mouse on the live view to draw a rectangle as the desired focus area.
3. Click  to disable this function.

5.1.9 Conduct Regional Exposure

When the brightness of live view is not balanced, you can enable this function to optimize the exposure of the selected image region.

Steps

1. Click  to enable regional exposure.
2. Drag the mouse on the live view to draw a rectangle as the desired exposure area.
3. Click  to disable this function.

5.1.10 Light

Click  to turn on or turn off the illuminator.

5.1.11 Lens Initialization

Lens initialization is used on the device equipped with motorized lens. The function can reset lens when long time zoom or focus results in blurred image. This function varies according to different models.

Click  to operate lens initialization.

5.1.12 Track Manually

In live view, manually select a target for the device to track.

Steps

1. Click  on the toolbar of the live view page.
2. Click a moving object in the live image.

The camera tracks the target and keep it in the center of live view image.

5.1.13 Conduct 3D Positioning

3D positioning is to relocate the selected area to the image center.

Steps

1. Click  to enable the function.
2. Select a target area in live image.
 - Left click on a point on live image: the point is relocated to the center of the live image. With no zooming in or out effect.
 - Hold and drag the mouse to a lower right position to frame an area on the live: the framed area is zoomed in and relocated to the center of the live image.
 - Hold and drag the mouse to an upper left position to frame an area on the live: the framed area is zoomed out and relocated to the center of the live image.
3. Click the button again to turn off the function.

5.1.14 OSD Menu

When network access is unavailable, you can call the Preset No.95 to show OSD menu to start device configuration.

Click direction buttons or  and  to move up and down.

Click  to confirm your selection.

5.1.15 Display Target Information on Live View

Go to **Configuration → Local → Live View Parameters** for settings.



Note

Related smart function should be configured and enabled in advance.

Display POS Information

POS information refers to the target features, such as target ID, etc. Supported POS information types varies according to device models.

5.2 Set Transmission Parameters

The live view image may be displayed abnormally according to the network conditions. In different network environments, you can adjust the transmission parameters to solve the problem.

Steps

1. Go to **Configuration → Local**.
2. Set the transmission parameters as required.

Protocol

TCP

TCP ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected. It is suitable for the stable network environment.

UDP

UDP is suitable for the unstable network environment that does not demand high video fluency.

MULTICAST

MULTICAST is suitable for the situation that there are multiple clients. You should set the multicast address for them before selection.



Note

For detailed information about multicast, refer to ***Multicast*** .

HTTP

HTTP is suitable for the situation that the third-party needs to get the stream from the device.

Play Performance

Shortest Delay

The device takes the real-time video image as the priority over the video fluency.

Balanced

The device ensures both the real-time video image and the fluency.

Fluent

The device takes the video fluency as the priority over real-time. In poor network environment, the device cannot ensure video fluency even the fluency is enabled.

Custom

You can set the frame rate manually. In poor network environment, you can reduce the frame rate to get a fluent live view. But the rule information may not display.

Auto Start Live View

- **Yes** means the live view is started automatically. It requires a high performance monitoring device and a stable network environment.
- **No** means the live view should be started manually.

3. Click **OK**.

Chapter 6 Video and Audio

This part introduces the configuration of video and audio related parameters.

6.1 Video Settings

This part introduces the settings of video parameters, such as, stream type, video encoding, and resolution.

Go to setting page: **Configuration → Video/Audio → Video** .



Note

For device with multiple camera channels, select a channel before other settings.

6.1.1 Stream Type

For device supports more than one stream, you can specify parameters for each stream type.

Main Stream

The stream stands for the best stream performance the device supports. It usually offers the best resolution and frame rate the device can do. But high resolution and frame rate usually means larger storage space and higher bandwidth requirements in transmission.

Sub Stream

The stream usually offers comparatively low resolution options, which consumes less bandwidth and storage space.

Other Streams

Streams other than the main stream and sub stream may also be offered for customized usage.

6.1.2 Video Type

Select the content (video and audio) that should be contained in the stream.

Video

Only video content is contained in the stream.

Video & Audio

Video content and audio content are contained in the composite stream.

6.1.3 Resolution

Select video resolution according to actual needs. Higher resolution requires higher bandwidth and storage.

6.1.4 Bitrate Type and Max. Bitrate

Constant Bitrate

It means that the stream is compressed and transmitted at a comparatively fixed bitrate. The compression speed is fast, but mosaic may occur on the image.

Variable Bitrate

It means that the device automatically adjust the bitrate under the set **Max. Bitrate**. The compression speed is slower than that of the constant bitrate. But it guarantees the image quality of complex scenes.

6.1.5 Video Quality

When **Bitrate Type** is set as Variable, video quality is configurable. Select a video quality according to actual needs. Note that higher video quality requires higher bandwidth.

6.1.6 Frame Rate

The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps).

A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout. Note that higher frame rate requires higher bandwidth and larger storage space.

6.1.7 Video Encoding

It stands for the compression standard the device adopts for video encoding.



Note

Available compression standards vary according to device models.

H.264

H.264, also known as MPEG-4 Part 10, Advanced Video Coding, is a compression standard. Without compressing image quality, it increases compression ratio and reduces the size of video file than MJPEG or MPEG-4 Part 2.

H.264+

H.264+ is an improved compression coding technology based on H.264. By enabling H.264+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.264, H.264+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.264+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



Note

When H.264+ is enabled, **Video Quality, I Frame Interval, Profile** and **SVC** are not configurable.

H.265

H.265, also known as High Efficiency Video Coding (HEVC) and MPEG-H Part 2, is a compression standard. In comparison to H.264, it offers better video compression at the same resolution, frame rate and image quality.

H.265+

H.265+ is an improved compression coding technology based on H.265. By enabling H.265+, you can estimate the HDD consumption by its maximum average bitrate. Compared to H.265, H.265+ reduces storage by up to 50% with the same maximum bitrate in most scenes.

When H.265+ is enabled, **Max. Average Bitrate** is configurable. The device gives a recommended max. average bitrate by default. You can adjust the parameter to a higher value if the video quality is less satisfactory. Max. average bitrate should not be higher than max. bitrate.



Note

When H.265+ is enabled, **Video Quality, I Frame Interval, Profile** and **SVC** are not configurable.

Profile

This function means that under the same bitrate, the more complex the profile is, the higher the quality of the image is, and the requirement for network bandwidth is also higher.

SVC

Scalable Video Coding (SVC) is the name for the Annex G extension of the H.264 or H.265 video compression standard.

The objective of the SVC standardization has been to enable the encoding of a high-quality video bitstream that contains one or more subset bitstreams that can themselves be decoded with a complexity and reconstruction quality similar to that achieved using the existing H.264 or H.265 design with the same quantity of data as in the subset bitstream. The subset bitstream is derived by dropping packets from the larger bitstream.

SVC enables forward compatibility for older hardware: the same bitstream can be consumed by basic hardware which can only decode a low-resolution subset, while more advanced hardware will be able decode high quality video stream.

Smoothing

It refers to the smoothness of the stream. The higher value of the smoothing is, the better fluency of the stream will be, though, the video quality may not be so satisfactory. The lower value of the smoothing is, the higher quality of the stream will be, though it may appear not fluent.

MJPEG

Motion JPEG (M-JPEG or MJPEG) is a video compression format in which intraframe coding technology is used. Images in a MJPEG format is compressed as individual JPEG images.

6.1.8 I-Frame Interval

I-frame interval defines the number of frames between 2 I-frames.

In H.264 and H.265, an I-frame, or intra frame, is a self-contained frame that can be independently decoded without any reference to other images. An I-frame consumes more bits than other frames. Thus, video with more I-frames, in other words, smaller I-frame interval, generates more steady and reliable data bits while requiring more storage space.

6.2 Audio Settings

It is a function to set audio parameters such as audio encoding, environment noise filtering.

Go to the audio settings page: **Configuration → Video/Audio → Audio** .

6.2.1 Audio Input

External audio pick-up device is available for audio input, and audio encoding and input volume are configurable.

Audio Encoding

The device offers several compression standard. Select according to your need.

Audio Input

LineIn is supported for external audio pick-up device.

Input volume

Adjust the volume of the audio input.

6.2.2 Audio Output

The device outputs audio by the built-in speaker. You can adjust the output volume according to your need.

6.2.3 Environmental Noise Filter

Set it as OFF or ON. When the function is enabled, the noise in the environment can be filtered to some extent.

6.3 Two-way Audio

It is used to realize the two-way audio function between the monitoring center and the target in the monitoring screen.

Before You Start

- Make sure the audio input device (pick-up or microphone) and audio output device (speaker) connected to the device is working properly. Refer to specifications of audio input and output devices for device connection.
- If the device has built-in microphone and speaker, two-way audio function can be enabled directly.

Steps

1. Click **Live View**.
2. Click  on the toolbar to enable two-way audio function of the camera.
3. Click  , disable the two-way audio function.

6.4 ROI

ROI (Region of Interest) encoding helps to discriminate the ROI and background information in video compression. The technology assigns more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

6.4.1 Set ROI

ROI (Region of Interest) encoding helps to assign more encoding resource to the region of interest, thus to increase the quality of the ROI whereas the background information is less focused.

Before You Start

Please check the video coding type. ROI is supported when the video coding type is H.264 or H.265.

Steps

1. Go to **Configuration → Video/Audio → ROI**.
2. Check **Enable**.
3. Select the channel No. according to your need.
4. Select **Stream Type**.
5. Select **Region No.** in **Fixed Region** to draw ROI region.
 - 1) Click **Draw Area**.
 - 2) Click and drag the mouse on the view screen to draw the fixed region.
 - 3) Click **Stop Drawing**.



Note

Select the fixed region that needs to be adjusted and drag the mouse to adjust its position.

-
6. Input the **Region Name** and **ROI Level**.

7. Click **Save**.



Note

The higher the ROI level is, the clearer the image of the detected region is.

-
8. **Optional:** Select other region No. and repeat the above steps if you need to draw multiple fixed regions.

6.5 Display Info. on Stream

The information of the objects (e.g. human, vehicle, etc.) is marked in the video stream. You can set rules on the connected rear-end device or client software to detect the events including line crossing, intrusion, etc.

Steps

1. Go to the setting page: **Configuration → Video/Audio → Display Info. on Stream** .
2. Check **Enable Dual-VCA**.
3. Click **Save**.

6.6 Display Settings

It offers the parameter settings to adjust image features.

Go to **Configuration → Image → Display Settings** .

For device that supports multiple channels, display settings of each channel is required. The settings for different channels may be different. This part introduces all possible parameters among the channels.

Click **Default** to restore settings.

6.6.1 Scene Mode

There are several sets of image parameters predefined for different installation environments. Select a scene according to the actual installation environment to speed up the display settings.

Image Adjustment

By adjusting the **Brightness, Saturation, Contrast** and **Sharpness**, the image can be best displayed.

Exposure Settings

Exposure is controlled by the combination of iris, shutter, and gain. You can adjust image effect by setting exposure parameters.

Exposure Mode

Auto

The iris, shutter, and gain values are adjusted automatically.

You can limit the changing ranges of iris, shutter and gain by setting **Max. Iris Limit, Min. Iris Limit, Max. Shutter Limit, Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Iris Priority

The value of iris needs to be adjusted manually. The shutter and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the shutter and gain by setting **Max. Shutter Limit, Min. Shutter Limit** and **Limit Gain** for better exposure effect.

Shutter Priority

The value of shutter needs to be adjusted manually. The iris and gain values are adjusted automatically according to the brightness of the environment.

You can limit the changing ranges of the iris by setting **Max. Iris Limit**, **Min. Iris Limit** and **Limit Gain** for better exposure effect.

Manual

You need to set **Iris**, **Shutter**, and **Gain** manually.

Slow Shutter

The higher the slow shutter level is, the slower the shutter speed is. It ensures full exposure in underexposure condition.

Focus

It offers options to adjust the focus mode and the minimum focus distance.

Focus Mode

Auto

The device focuses automatically as the scene changes. If you cannot get a well-focused image under auto mode, reduce light sources in the image and avoid flashing lights.

Semi-auto

The device focuses once after the PTZ and lens zooming. If the image is clear, the focus does not change when the scene changes.

Manual

You can adjust the focus manually on the live view page.

Min. Focus Distance

When the distance between the scene and lens is shorter than the Min. Focus Distance, the lens does not focus.

Day/Night Switch

Day/Night Switch function can provide color images in the day mode and black/white images in the night mode. Switch mode is configurable.

Day

The image is always in color.

Night

The image is always black/white

Auto

The camera switches between the day mode and the night mode according to the illumination automatically.

Scheduled-Switch

Set the **Start Time** and the **End Time** to define the duration for day mode.



Note

Day/Night Switch function varies according to models.

Set Supplement Light

Steps

1. Go to **Configuration → Maintenance → System Service**.
2. Check **Enable Supplement Light**.
3. Click **Save**.
4. Go to **Configuration → Image → Display Settings → Day/Night Switch** to set supplement light parameters.

Smart Supplement Light

This feature uses smart image processing technology to reduce overexposure caused by supplement light.

IR Light Mode

When the mode is set to **Auto**, the supplement light is automatically turned in or off according to the image brightness.

Brightness Limit

Adjust the upper limit of supplement light power.

BLC

If you focus on an object against strong backlight, the object will be too dark to be seen clearly. BLC (backlight compensation) compensates light to the object in the front to make it clear. If BLC mode is set as **Custom**, you can draw a red rectangle on the live view image as the BLC area.

HLC

When the bright area of the image is over-exposed and the dark area is under-exposed, the HLC (High Light Compression) function can be enabled to weaken the bright area and brighten the dark area, so as to achieve the light balance of the overall picture.

WDR

The WDR (Wide Dynamic Range) function helps the camera provide clear images in environment with strong illumination differences.

When there are both very bright and very dark areas simultaneously in the field of view, you can enable the WDR function and set the level. WDR automatically balances the brightness level of the whole image and provides clear images with more details.

 Note

When WDR is enabled, some other functions may be not supported. Refer to the actual interface for details.



WDR Off

WDR On

Figure 6-1 WDR

DNR

Digital Noise Reduction is used to reduce the image noise and improve the image quality. **Normal** and **Expert** modes are selectable.

Normal

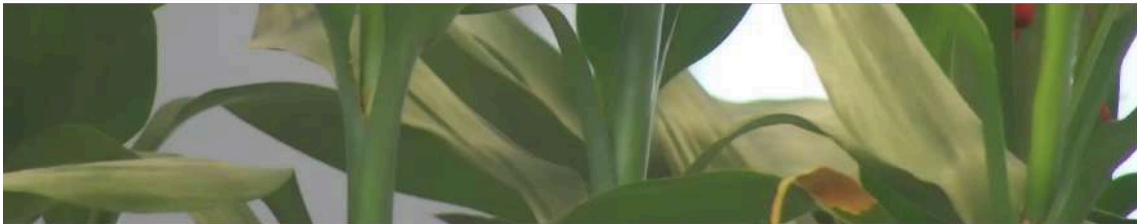
Set the DNR level to control the noise reduction degree. The higher level means stronger reduction degree.

Expert

Set the DNR level for both space DNR and time DNR to control the noise reduction degree. The higher level means stronger reduction degree.



DNR Off



DNR On

Figure 6-2 DNR

White Balance

White balance is the white rendition function of the camera. It is used to adjust the color temperature according to the environment.



Cold



Warm



Auto White Balance

Figure 6-3 White Balance

Defog

You can enable the defog function when the environment is foggy and the image is misty. It enhances the subtle details so that the image appears clearer.



Figure 6-4 Defog

EIS

Increase the stability of video image by using jitter compensation technology.

6.6.2 Image Parameters Switch

The device automatically switches image parameters in set time periods.

Go to image parameters switch setting page: **Configuration** → **Image** → **Image Parameters Switch** , and set parameters as needed.

Set Scheduled-switch

Switch the image to the linked scene mode automatically in certain time periods.

Steps

1. Check **Scheduled-switch**.
2. Select and configure the corresponding time period and linked scene mode.



Note

For Linked Scene configuration, refer to ***Scene Mode*** .

3. Click **Save**.

Set Link to Preset

You can set a preset to switch the image to a linked scene.

Steps

1. Check **Link to Preset**.
2. Select a preset.
3. Check and set a time period and a linked scene mode.
4. Click **Save**.

6.6.3 Mirror

When the live view image is the reverse of the actual scene, this function helps to display the image normally.

Select the mirror mode as needed.



Note

The video recording will be shortly interrupted when the function is enabled.

6.6.4 Video Standard

Video standard is an ability of a video card or video display device that defines the amount of colors that are shown and the resolution. The two most common video standard used are NTSC and PAL. In NTSC, 30 frames are transmitted each second. Each frame is made up of 525 individual scan lines. In PAL, 25 frames are transmitted each second. Each frame is made up of 625 individual scan lines. Select video signal standard according to the video system in your country/region.

6.7 OSD

You can customize OSD (On-screen Display) information such as device name, time/date, font, color, and text overlay displayed on video stream.

Go to OSD setting page: **Configuration → Image → OSD Settings** .

Select a channel.

Set the corresponding parameters, and click **Save** to take effect.

Character Set

Select character set for displayed information. If Korean is required to displayed on screen, select **EUC-KR**. Otherwise, select **GBK**.

Displayed Information

Set camera name, date, week, and their related display format.

Text Overlay

Set customized overlay text on image.

OSD Parameters

Set OSD parameters, such as **Display Mode**, **OSD Size**, **Font Color**, and **Alignment**.

Chapter 7 Video Recording and Picture Capture

This part introduces the operations of capturing video clips and snapshots, playback, and downloading captured files.

7.1 Storage Settings

This part introduces the configuration of several common storage paths.

7.1.1 Memory Card

You can view the capacity, free space, status, type, and property of the memory card. Encryption of memory card is supported to ensure data security.

Set New or Unencrypted Memory Card

Before You Start

Insert a new or unencrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.

Steps

1. Go to **Configuration** → **Storage** → **Storage Management** → **HDD Management** .
2. Select the memory card.



Note

If an **Unlock** button appears, you need to unlock the memory card first. See [**Detect Memory Card Status**](#) for details.

-
3. Click **Format** to initialize the memory card.

When the **Status** of memory card turns from **Uninitialized** to **Normal**, the memory card is ready for use.

4. **Optional:** Encrypt the memory card.

- 1) Click **Encrypted Format**.
- 2) Set the encryption password.
- 3) Click **OK**.

When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.



Note

Keep your encryption password properly. Encryption password cannot be found if forgotten.

-
5. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.

6. Click **Save**.

Set Encrypted Memory Card

Before You Start

- Insert an encrypted memory card to the device. For detailed installation, refer to *Quick Start Guide* of the device.
- You need to know the correct encryption password of the memory card.

Steps

1. Go to **Configuration → Storage → Storage Management → HDD Management**.
2. Select the memory card.



Note

If an **Unlock** button appears, you need to unlock the memory card first. See [***Detect Memory Card Status***](#) for details.

3. Verify the encryption password.
 - 1) Click **Parity**.
 - 2) Enter the encryption password.
 - 3) Click **OK**.

When the **Encryption Status** turns to **Encrypted**, the memory card is ready for use.



Note

If the encryption password is forgotten and you still want to use this memory card, see [***Set New or Unencrypted Memory Card***](#) to format and set the memory card. All existing contents will be removed.

4. **Optional:** Define the **Quota** of the memory card. Input the percentage for storing different contents according to your needs.
5. Click **Save**.

Detect Memory Card Status

The device detects the status of Hikvision memory card. You receive notifications when your memory card is detected abnormal.

Before You Start

The configuration page only appears when a Hikvision memory card is installed to the device.

Steps

1. Go to **Configuration → Storage → Storage Management → Memory Card Detection**.
2. Click **Status Detection** to check the **Remaining Lifespan** and **Health Status** of your memory card.

Remaining Lifespan

It shows the percentage of the remaining lifespan. The lifespan of a memory card may be influenced by factors such as its capacity and the bitrate. You need to change the memory card if the remaining lifespan is not enough.

Health Status

It shows the condition of your memory card. There are three status descriptions: good, bad, and damaged. You will receive a notification if the health status is anything other than good when the **Arming Schedule** and **Linkage Method** are set.



Note

It is recommended that you change the memory card when the health status is not "good".

3. Click **R/W Lock** to set the permission of reading and writing to the memory card.
 - Add a Lock
 - a. Select the **Lock Switch** as ON.
 - b. Enter the password.
 - c. Click **Save**
 - Unlock
 - If you use the memory card on the device that locks it, unlocking will be done automatically and no unlocking procedures are required on the part of users.
 - If you use the memory card (with a lock) on a different device, you can go to **HDD Management** to unlock the memory card manually. Select the memory card, and click **Unlock**. Enter the correct password to unlock it.
 - Remove the Lock
 - a. Select the **Lock Switch** as OFF.
 - b. Enter the password in **Password Settings**.
 - c. Click **Save**.
-



Note

- Only admin user can set the **R/W Lock**.
 - The memory card can only be read and written when it is unlocked.
 - If the device, which adds a lock to a memory card, is restored to the factory settings, you can go to **HDD Management** to unlock the memory card.
-

4. Set **Arming Schedule** and **Linkage Method**. See [Set Arming Schedule](#) and [Linkage Method Settings](#) for details.
5. Click **Save**.

7.1.2 Set FTP

You can configure the FTP server to save images which are captured by events or a timed snapshot task.

Before You Start

Get the FTP server address first.

Steps

1. Go to **Configuration → Network → Advanced Settings → FTP**.
2. Configure FTP settings.

Server Address and Port

The FTP server address and corresponding port.

User Name and Password

The FTP user should have the permission to upload pictures.

If the FTP server supports picture uploading by anonymous users, you can check **Anonymous** to hide your device information during uploading.

Directory Structure

The saving path of snapshots in the FTP server.

Picture Filing Interval

For better picture management, you can set the picture filing interval from 1 day to 30 days. Pictures captured in the same time interval will be saved in one folder named after the beginning date and ending date of the time interval.

Picture Name

Set the naming rule for captured pictures. You can choose **Default** in the drop-down list to use the default rule, that is, IP address_channel number_capture time_event type.jpg (e.g., 10.11.37.189_01_20150917094425492_FACE_DETECTION.jpg). Or you can customize it by adding a **Custom Prefix** to the default naming rule.

3. Click **Upload Picture** to enable uploading snapshots to the FTP server.
4. Click **Test** to verify the FTP server.
5. Click **Save**.

7.1.3 Set NAS

Take network server as network disk to store the record files, captured images, etc.

Before You Start

Get the IP address of the network disk first.

Steps

1. Go to NAS setting page: **Configuration → Storage → Storage Management → Net HDD**.
2. Click **HDD No.**. Enter the server address and file path for the disk.

Server Address

The IP address of the network disk.

File Path

The saving path of network disk files.

Mounting Type

Select file system protocol according to the operation system.

Enter user name and password of the net HDD to guarantee the security if **SMB/CIFS** is selected.

3. Click **Test** to check whether the network disk is available.
4. Click **Save**.

7.1.4 Set Cloud Storage

It helps to upload the captured pictures and data to the cloud. The platform requests picture directly from the cloud for picture and analysis. The function is only supported by certain models.

Steps



Caution

If cloud storage is enabled, the pictures are stored in the cloud video manager preferentially.

1. Go to **Configuration → Storage → Storage Management → Cloud Storage**.
2. Check **Enable Cloud Storage**.
3. Set basic parameters.

Protocol Version	The protocol version of the cloud video manager.
Server IP	The IP address of the cloud video manager. It supports IPv4 address.
Serve Port	The port of the cloud video manager. 6001 is the default port and you are not recommended to edit it.
AccessKey	The key to log in to the cloud video manager.
SecretKey	The key to encrypt the data stored in the cloud video manager.
User Name and Password	The user name and password of the cloud video manager.
Picture Storage Pool ID	The ID of the picture storage region in the cloud video manager. Make sure storage pool ID and the storage region ID are the same.

4. Click **Test** to test the configured settings.
5. Click **Save**.

7.2 Video Recording

This part introduces the operations of manual and scheduled recording, playback, and downloading recorded files.

7.2.1 Record Automatically

This function can record video automatically during configured time periods.

Before You Start

Select **Trigger Recording** in event settings for each record type except **Continuous**. See [Event and Alarm](#) for details.

Steps



Note

The function varies according to different models.

1. Go to **Configuration → Storage → Schedule Settings → Record Schedule**.
 2. Select channel No.
 3. Check **Enable**.
 4. Select a record type.
-



Note

The record type is vary according to different models.

Continuous

The video will be recorded continuously according to the schedule.

Motion

When motion detection is enabled and trigger recording is selected as linkage method, object movement is recorded.

Alarm

When alarm input is enabled and trigger recording is selected as linkage method, the video is recorded after receiving alarm signal from external alarm input device.

Motion | Alarm

Video is recorded when motion is detected or alarm signal is received from the external alarm input device.

Motion & Alarm

Video is recorded only when motion is detected and alarm signal is received from the external alarm input device.

Event

The video is recorded when configured event is detected.

5. Set schedule for the selected record type. Refer to [Set Arming Schedule](#) for the setting operation.
6. Click **Advanced** to set the advanced settings.

Overwrite

Enable **Overwrite** to overwrite the video records when the storage space is full. Otherwise the camera cannot record new videos.

Pre-record

The time period you set to record before the scheduled time.

Post-record

The time period you set to stop recording after the scheduled time.

Stream Type

Select the stream type for recording.



Note

When you select the stream type with higher bitrate, the actual time of the pre-record and post-record may be less than the set value.

Recording Expiration

The recordings are deleted when they exceed the expired time. The expired time is configurable. Note that once the recordings are deleted, they can not be recovered.

7. Click **Save**.

7.2.2 Record Manually

Steps

1. Go to **Configuration → Local**.
2. Set the **Record File Size** and saving path to for recorded files.
3. Click **Save**.
4. Click  in the live view interface to start recording. Click  to stop recording.

7.2.3 Playback and Download Video

You can search, playback and download the videos stored in the local storage or network storage.

Steps

1. Click **Playback**.
2. Select channel No.
3. Set search condition and click **Search**.
The matched video files showed on the timing bar.
4. Click  to play the video files.
 - Click  to clip video files.
 - Click  to play video files in full screen. Press **ESC** to exit full screen.



Note

Go to **Configuration → Local** , click **Save clips to** to change the saving path of clipped video files.

5. Click  on the playback interface to download files.
 - 1) Set search condition and click **Search**.
 - 2) Select the video files and then click **Download**.



Note

Go to **Configuration → Local** , click **Save downloaded files to** to change the saving path of downloaded video files.

7.3 Capture Configuration

The device can capture the pictures manually or automatically and save them in configured saving path. You can view and download the snapshots.

7.3.1 Capture Automatically

This function can capture pictures automatically during configured time periods.

Before You Start

If event-triggered capture is required, you should configure related linkage methods in event settings. Refer to **Event and Alarm** for event settings.

Steps

1. Go to **Configuration → Storage → Schedule Settings → Capture → Capture Parameters** .
2. Set the capture type.

Timing

Capture a picture at the configured time interval.

Event-Triggered

Capture a picture when an event is triggered.

3. Set the **Format, Resolution, Quality, Interval**, and **Capture Number**.
4. Refer to **Set Arming Schedule** for configuring schedule time.
5. Click **Save**.

7.3.2 Capture Manually

Steps

1. Go to **Configuration → Local** .
2. Set the **Image Format** and saving path to for snapshots.

JPEG

The picture size of this format is comparatively small, which is better for network transmission.

BMP

The picture is compressed with good quality.

3. Click **Save**.
4. Click  near the live view or play back window to capture a picture manually.

7.3.3 View and Download Picture

You can search, view and download the pictures stored in the local storage or network storage.

Steps

1. Click **Picture**.
2. Select channel No.
3. Set search condition and click **Search**.
The matched pictures showed in the file list.
4. Select the pictures then click **Download** to download them.



Note

Go to **Configuration → Local** , click **Save snapshots when playback** to change the saving path of pictures.

Chapter 8 Event and Alarm

This part introduces the configuration of events. The device takes certain response to triggered alarm.

8.1 Basic Event

8.1.1 Set Motion Detection

This function detects moving objects in the detection region and trigger linkage actions.

Steps

1. Go to **Configuration → Event → Basic Event → Motion Detection** .
2. Check **Enable Motion Detection**.
3. **Optional:** Check **Enable Motion Detection in PTZ Control**, and the device detects moving targets in PTZ movement.
4. **Optional:** Highlight moving objects in green.
 - 1) Check **Enable Dynamic Analysis for Motion**.
 - 2) Go to **Configuration → Local** to enable **Rules**.
5. Select **Configuration Mode**. Normal mode and expert mode are selectable.
 - For the information about normal mode, see [Normal Mode](#) .
 - For the information about expert mode, see [Expert Mode](#) .
6. Set the arming schedule. See [Set Arming Schedule](#) for details.
7. Set linkage methods. See [Linkage Method Settings](#) for details.
8. Click **Save**.

Normal Mode

You can set motion detection parameters according to the device default parameters.

Steps

1. Select normal mode in **Configuration**.
2. Set the sensitivity of normal mode. The higher the value of sensitivity is, the more sensitive the motion detection is. If the sensitivity is set to **0**, motion detection and dynamic analysis do not take effect.
3. Click **Draw Area**. Click and drag the mouse on the live video, then release the mouse to finish drawing one area.

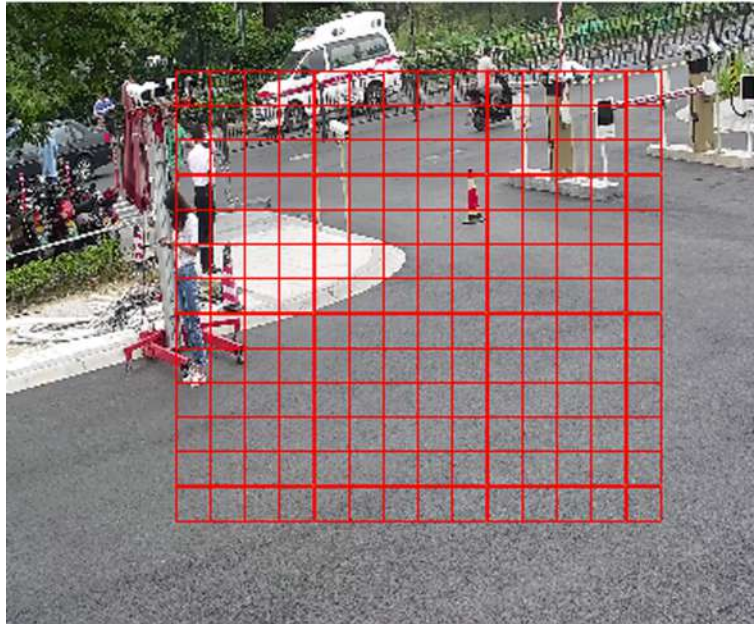


Figure 8-1 Set Rules

Stop Drawing Stop drawing one area.

Clear All Clear all the areas.

4. Optional: You can set the parameters of multiple areas by repeating the above steps.

Expert Mode

You can configure different motion detection parameters for day and night according to the actual needs.

Steps

1. Select **Expert Mode** in **Configuration**.
2. Set parameters of expert mode.

Scheduled Image Settings

OFF

Image switch is disabled.

Auto-Switch

The system switches day/night mode automatically according to environment. It displays colored image at day and black and white image at night.

Scheduled-Switch

The system switches day/night mode according to the schedule. It switches to day mode during the set periods and switches to night mode during the other periods.

Sensitivity

The higher the value of sensitivity is, the more sensitive the motion detection is. If scheduled image settings is enabled, the sensitivity of day and night can be set separately.

3. Select an **Area** and click **Draw Area**. Click and drag the mouse on the live image and then release the mouse to finish drawing one area.



Figure 8-2 Set Rules

Stop Drawing Finish drawing one area.

Clear All Delete all the areas.

4. Click **Save**.

5. **Optional:** Repeat above steps to set multiple areas.

8.1.2 Set Video Tampering Alarm

When the configured area is covered and cannot be monitored normally, the alarm is triggered and the device takes certain alarm response actions.

Steps

1. Go to **Configuration → Event → Basic Event → Video Tampering**.
2. Select the channel number.
3. Check **Enable**.
4. Set the **Sensitivity**. The higher the value is, the easier to detect the area covering.
5. Click **Draw Area** and drag the mouse in the live view to draw the area.

Stop Drawing Finish drawing.

Clear All

Delete all the drawn areas.

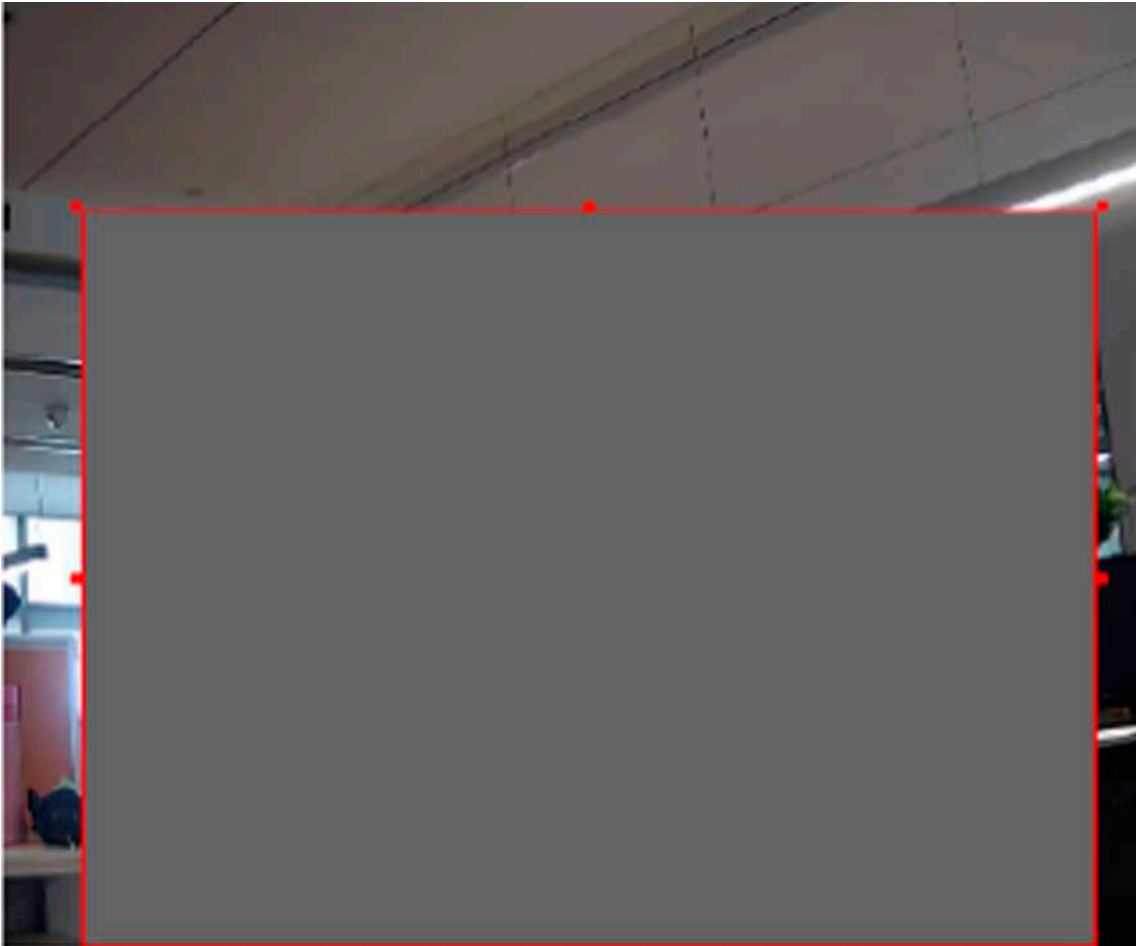


Figure 8-3 Set Video Tampering Area

6. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.
7. Click **Save**.

8.1.3 Set Exception Alarm

Exception such as network disconnection can trigger the device to take corresponding action.

Steps

1. Go to **Configuration → Event → Basic Event → Exception**.
2. Select **Exception Type**.

HDD Full	The HDD storage is full.
HDD Error	Error occurs in HDD.

Network Disconnected The device is offline.

IP Address Conflicted The IP address of current device is same as that of other device in the network.

Illegal Login Incorrect user name or password is entered.

3. Refer to **Linkage Method Settings** for setting linkage method.

4. Click **Save**.

8.1.4 Set Alarm Input

Alarm signal from the external device triggers the corresponding actions of the current device.

Before You Start

Make sure the external alarm device is connected. See *Quick Start Guide* for cable connection.

Steps

1. Go to **Configuration → Event → Basic Event → Alarm Input**.

2. Check **Enable Alarm Input Handling**.

3. Select **Alarm Input NO.** and **Alarm Type** from the dropdown list. Edit the **Alarm Name**.

4. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage method.

5. Click **Copy to...** to copy the settings to other alarm input channels.

6. Click **Save**.

8.2 Smart Event



Note

- For certain device models, you need to enable the smart event function on **VCA Resource** page first to show the function configuration page.
 - The function varies according to different models.
-

8.2.1 Detect Audio Exception

Audio exception detection function detects the abnormal sound in the scene, such as the sudden increase/decrease of the sound intensity, and some certain actions can be taken as response.

Steps

1. Go to **Configuration → Event → Smart Event → Audio Exception Detection**.

2. Select one or several audio exception detection types.

Audio Loss Detection

Detect sudden loss of audio track.

Sudden Increase of Sound Intensity Detection

Detect sudden increase of sound intensity. **Sensitivity** and **Sound Intensity Threshold** are configurable.



Note

- The lower the sensitivity is, the more significant the change should be to trigger the detection.
- The sound intensity threshold refers to the sound intensity reference for the detection. It is recommended to set as the average sound intensity in the environment. The louder the environment sound, the higher the value should be. You can adjust it according to the real environment.

Sudden Decrease of Sound Intensity Detection

Detect sudden decrease of sound intensity. **Sensitivity** is configurable.

3. Refer to **Set Arming Schedule** for setting scheduled time. Refer to **Linkage Method Settings** for setting linkage methods.

4. Click **Save**.



Note

The function varies according to different models.

8.2.2 Set Intrusion Detection

Intrusion detection detects the object movement of entering and loitering in a predefined area. When intrusion occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See **Allocate VCA Resource** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Intrusion Detection**.
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.
Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.
 - 1) Select a **Region No.**. Up to 4 regions can be set.
 - 2) Click **Detection Area**.
 - 3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.

- 6. Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
- 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
 - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
- 7.** Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value of sensitivity is, the more easily the target is detected.
Threshold	Threshold stands for the time of the target loitering in the region. If the time that she/he stays in the region exceeds the threshold, the alarm is triggered.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.



Figure 8-4 Draw Area

- 8.** Click **Save**.
- 9.** Repeat above steps to set other detection areas.
- 10.** Set arming schedule. See **Set Arming Schedule** .
- 11.** Set linkage method. See **Linkage Method Settings** .

8.2.3 Set Line Crossing Detection

Line crossing detection is used to detect the object movement of crossing a predefined line. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See **Allocate VCA Resource** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Line Crossing Detection**.
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.

Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.

4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection line.
 - 1) Select a **Line No.**. Up to 4 lines can be set in the scene.
 - 2) Click **Detection Area**.

A yellow line is displayed on live image.

- 3) Click on the line, and drag its end points to adjust the length and position.
- 4) Select the **Direction** for the detection line.

Direction

It stands for the direction from which the object goes across the line.

A<->B

The object going across the line from both directions can be detected and alarms are triggered.

A->B

Only the object crossing the configured line from side A to side B can be detected.

B->A

Only the object crossing the configured line from side B to side A can be detected.

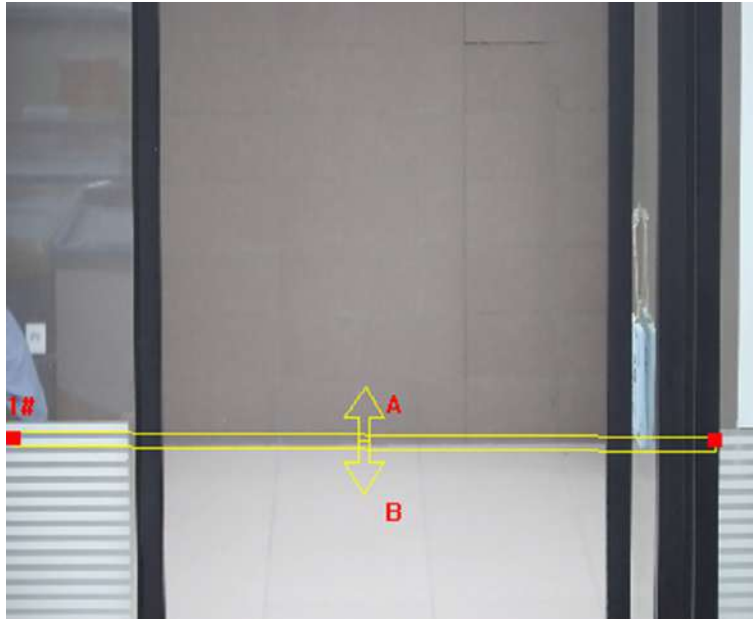


Figure 8-5 Draw Line

6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
 - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
 - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.
8. Click **Save**.
9. Repeat above steps to set other lines.
10. Set arming schedule. See **Set Arming Schedule** .
11. Set linkage method. See **Linkage Method Settings** .

8.2.4 Set Region Entrance Detection

Region entrance detection is used to detect the object movement of entering a predefined area. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See **Allocate VCA Resource** for instructions.

Steps

1. Go to **Open Platform → Smart Event → Region Entrance Detection**.
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.
Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.
 - 1) Select a **Region No.**. Up to 4 regions can be set.
 - 2) Click **Detection Area**.
 - 3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.
6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
 - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
 - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.



Figure 8-6 Draw Area

8. Click **Save**.
9. Repeat above steps to set other regions.
10. Set arming schedule. See [***Set Arming Schedule***](#) .
11. Set linkage method. See [***Linkage Method Settings***](#) .

8.2.5 Set Region Exiting Detection

Region exiting detection is used to detect the objects movement of exiting from a predefined area. When it occurs, the device takes linkage actions as response.

Before You Start

You need to enable **Smart Event** on the **VCA Resource** page to show the configuration page. See [***Allocate VCA Resource***](#) for instructions.

Steps

1. Go to **Open Platform → Smart Event → Region Exiting Detection** .
2. Check **Enable**.
3. **Optional:** Click **Lock** to lock PTZ control to prevent the interruption from other PTZ related action during configuration.
Normally, the PTZ control is automatically locked when you enter the configuration interface. You can manually resume the lock when the countdown is over.
4. Adjust the live image to the desired scene by using PTZ control buttons.
5. Draw detection area.
 - 1) Select a **Region No.**. Up to 4 regions can be set.

- 2) Click **Detection Area**.
- 3) Click on the live image to draw the boundaries of the detection area, and right click to complete drawing.
6. **Optional:** Set the minimum size and the maximum size for the target to improve detection accuracy. Only targets whose size are between the maximum size and the minimum size trigger the detection.
 - 1) Click **Max. Size**, and drag the mouse on live image. If you want to change the size, click the button and draw again.
 - 2) Click **Min. Size**, and drag the mouse on the live image. If you want to change the size, click the button and draw again.
7. Set detection parameters.

Sensitivity	It stands for the sensitivity of detecting an target. The higher the value is, the more easily the target is detected.
Detection Target	You can specify the object type, and the device only detects the selected type of objects.



Figure 8-7 Draw Area

8. Click **Save**.
9. Repeat above steps to set other regions.
10. Set arming schedule. See **Set Arming Schedule** .
11. Set linkage method. See **Linkage Method Settings** .

8.2.6 Set Tracking Parameters

Adjust the motion parameters of the device for better target tracking performance.

Steps

1. Go to **Open Platform → Smart Event → Advanced Parameters**.
2. **Optional:** Check **Tuning Mode**.



Tuning mode is to display the information that helps debugging the function. This mode is reserved for technical support.

3. Set the **Duration**.

The device stops tracking when it tracks a target uninterruptedly for the set duration.

4. Set the zooming control and other tracking parameters.

Zooming Control

Two modes are available. Controlled by target frame or by tilt angle of the device.

By Tilt Angle

The device calculates the tracking zoom ratio automatically according to the tilt angle of the device.



The attitude of the device affects the accuracy of this zooming control mode. For the model with a built-in gyroscope, try to calibrate the attitude if some zooming problems happen during tracking. See [***Set Device Position***](#) for instructions.

By Target Frame

The tracked target has a virtual frame around. The device calculates a suitable zoom ratio according to the frame and the set **Tracking Zoom Ratio**. Larger value means bigger zoom ratio.

Wait to Stop Tracking If Low Validity

The validity is an internal parameter that helps judge whether the device should keep tracking or not. This parameter is the waiting time level before the device stops tracking when the validity is low. Larger value means longer waiting time.

Wait to Lower Tracking Speed If Low Validity

The validity is an internal parameter that helps judge whether the PTZ channel should lower the tracking speed or not. This parameter is the waiting time level before the device lowers the tracking speed when the validity is low. Larger value means longer waiting time.

5. Click **Save**.

Chapter 9 Arming Schedule and Alarm Linkage

Arming schedule is a customized time period in which the device performs certain tasks. Alarm linkage is the response to the detected certain incident or target during the scheduled time.

9.1 Set Arming Schedule

Set the valid time of the device tasks.

Steps

1. Click **Arming Schedule**.
2. Drag the time bar to draw desired valid time.



Note

Up to 8 periods can be configured for one day.

3. Adjust the time period.
 - Click on the selected time period, and enter the desired value. Click **Save**.
 - Click on the selected time period. Drag the both ends to adjust the time period.
 - Click on the selected time period, and drag it on the time bar.
4. **Optional:** Click **Copy to...** to copy the same settings to other days.
5. Click **Save**.

9.2 Linkage Method Settings

You can enable the linkage functions when an event or alarm occurs.

9.2.1 Trigger Alarm Output

If the device has been connected to an alarm output device, and the alarm output No. has been configured, the device sends alarm information to the connected alarm output device when an alarm is triggered.

Steps

1. Go to **Configuration → Event → Basic Event → Alarm Output**.
2. Set alarm output parameters.

Automatic Alarm For the information about the configuration, see [***Automatic Alarm***](#).

Manual Alarm For the information about the configuration, see [***Manual Alarm***](#).

3. Click **Save**.

Automatic Alarm

Set the automatic alarm parameters, then the device triggers an alarm output automatically in the set arming schedule.

Steps

1. Set automatic alarm parameters.

Alarm Output No.

Select the alarm output No. according to the alarm interface connected to the external alarm device.

Alarm Name

Custom a name for the alarm output.

Delay

It refers to the time duration that the alarm output remains after an alarm occurs.

2. Set the alarming schedule. For the information about the settings, see [**Set Arming Schedule**](#).
3. Click **Copy to...** to copy the parameters to other alarm output channels.
4. Click **Save**.

Manual Alarm

You can trigger an alarm output manually.

Steps

1. Set the manual alarm parameters.

Alarm Output No.

Select the alarm output No. according to the alarm interface connected to the external alarm device.

Alarm Name

Custom a name for the alarm output.

Delay

Select **Manual**.

2. Click **Manual Alarm** to enable manual alarm output.
3. **Optional:** Click **Clear Alarm** to disable manual alarm output.

9.2.2 FTP/NAS/Memory Card Uploading

If you have enabled and configured the FTP/NAS/memory card uploading, the device sends the alarm information to the FTP server, network attached storage and memory card when an alarm is triggered.

Refer to **Set FTP** to set the FTP server.

Refer to **Set NAS** for NAS configuration.

Refer to **Set New or Unencrypted Memory Card** for memory card storage configuration.

9.2.3 Send Email

Check **Send Email**, and the device sends an email to the designated addresses with alarm information when an alarm event is detected.

For email settings, refer to **Set Email**.

Set Email

When the email is configured and **Send Email** is enabled as a linkage method, the device sends an email notification to all designated receivers if an alarm event is detected.

Before You Start

Set the DNS server before using the Email function. Go to **Configuration → Network → Basic Settings → TCP/IP** for DNS settings.

Steps

1. Go to email settings page: **Configuration → Network → Advanced Settings → Email**.
 2. Set email parameters.
 - 1) Input the sender's email information, including the **Sender's Address**, **SMTP Server**, and **SMTP Port**.
 - 2) **Optional**: If your email server requires authentication, check **Authentication** and input your user name and password to log in to the server.
 - 3) Set the **E-mail Encryption**.
 - When you select **TLS**, and disable **STARTTLS**, emails are sent after encrypted by TLS. The SMTP port should be set as 465.
 - When you select **TLS** and **Enable STARTTLS**, emails are sent after encrypted by STARTTLS, and the SMTP port should be set as 25.
-
-  **Note**

If you want to use STARTTLS, make sure that the protocol is supported by your email server. If you check the **Enable STARTTLS** while the protocol is not supported by your email sever, your email is sent with no encryption.
-
- 4) **Optional**: If you want to receive notification with alarm pictures, check **Attached Image**. The notification email has 3 attached alarm pictures about the event with configurable image capturing interval.
 - 5) Input the receiver's information, including the receiver's name and address.
 - 6) Click **Test** to see if the function is well configured.
3. Click **Save**.

9.2.4 Notify Surveillance Center

Check **Notify Surveillance Center**, the alarm information is uploaded to the surveillance center when an alarm event is detected.

9.2.5 Trigger Recording

Check **Trigger Recording**, and the device records the video about the detected alarm event. For device with more than one camera channels, you can set one or more channels to take recordings if needed.

For recording settings, refer to [Video Recording and Picture Capture](#)

9.2.6 Flashing Light

After enabling **Flashing Light** and setting the **Flashing Light Alarm Output**, the light flashes when an alarm event is detected.

Set Flashing Alarm Light Output

When events occur, the flashing light on the device can be triggered as an alarm.

Steps

1. Go to **Configuration → Event → Basic Event → Flashing Alarm Light Output**.
2. Set **Flashing Duration**, **Flashing Frequency** and **Brightness**.

Flashing Duration

The time that the flashing lasts when one alarm happens.

Flashing Frequency

The rate at which the light flashes. High frequency, medium frequency, low frequency, and normally on are selectable.

Brightness

The brightness of the light.

3. Set the arming schedule. See [Set Arming Schedule](#) for details.
4. Click **Save**.



Note

Only certain device models support the function.

9.2.7 Audible Warning

After enabling **Audible Warning** and setting **Audible Alarm Output**, the built-in speaker of the device or connected external speaker plays warning sounds when an alarm happens.

For audible alarm output settings, refer to **Set Audible Alarm Output**.



Note

The function is only supported by certain camera models.

Set Audible Alarm Output

When the device detects targets in the detection area, audible alarm can be triggered as a warning.

Steps

1. Go to **Configuration → Event → Basic Event → Audible Alarm Output**.
2. Select **Sound Type** and set related parameters.
 - Select **Prompt** and set the alarm times you need.
 - Select **Warning** and its contents. Set the alarm times you need.
 - Select **Custom Audio**. You can select a custom audio file from the drop-down list. If no file is available, you can click **Add** to upload an audio file that meets the requirement. Up to three audio files can be uploaded.
3. **Optional:** Click **Test** to play the selected audio file on the device.
4. Set arming schedule for audible alarm. See **Set Arming Schedule** for details.
5. Click **Save**.



Note

The function is only supported by certain device models.

Chapter 10 Network Settings

10.1 TCP/IP

TCP/IP settings must be properly configured before you operate the device over network. IPv4 and IPv6 are both supported. Both versions can be configured simultaneously without conflicting to each other.

Go to **Configuration → Network → Basic Settings → TCP/IP** for parameter settings.

NIC Type

Select a NIC (Network Interface Card) type according to your network condition.

IPv4

Two IPv4 modes are available.

DHCP

The device automatically gets the IPv4 parameters from the network if you check **DHCP**. The device IP address is changed after enabling the function. You can use SADP to get the device IP address.



Note

The network that the device is connected to should support DHCP (Dynamic Host Configuration Protocol).

Manual

You can set the device IPv4 parameters manually. Input **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway**, and click **Test** to see if the IP address is available.

IPv6

Three IPv6 modes are available.

Route Advertisement

The IPv6 address is generated by combining the route advertisement and the device Mac address.



Note

Route advertisement mode requires the support from the router that the device is connected to.

DHCP

The IPv6 address is assigned by the server, router, or gateway.

Manual

Input **IPv6 Address**, **IPv6 Subnet**, **IPv6 Default Gateway**. Consult the network administrator for required information.

MTU

It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.

The valid value range of MTU is 1280 to 1500.

DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Server** and **Alternate DNS server** properly if needed.

Dynamic Domain Name

Check **Enable Dynamic Domain Name** and input **Register Domain Name**. The device is registered under the register domain name for easier management within the local area network.



Note

DHCP should be enabled for the dynamic domain name to take effect.

10.1.1 Multicast

Multicast is group communication where data transmission is addressed to a group of destination devices simultaneously.

Go to **Configuration → Network → Basic Settings → Multicast** for the multicast settings.

IP Address

It stands for the address of multicast host.

Stream Type

The stream type as the multicast source.

Video Port

The video port of the selected stream.

Audio Port

The audio port of the selected stream.

10.1.2 Multicast Discovery

Check the **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.

10.2 Port

The device port can be modified when the device cannot access the network due to port conflicts.



Caution

Do not modify the default port parameters at will, otherwise the device may be inaccessible.

Go to **Configuration → Network → Basic Settings → Port** for port settings.

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

HTTPS Port

It refers to the port through which the browser accesses the device with certificate. Certificate verification is required to ensure the secure access.

RTSP Port

It refers to the port of real-time streaming protocol.

SRTP Port

It refers to the port of secure real-time transport protocol.

Server Port

It refers to the port through which the client adds the device.

Enhanced SDK Service Port

It refers to the port through which the client adds the device. Certificate verification is required to ensure the secure access.

WebSocket Port

TCP-based full-duplex communication protocol port for plug-in free preview.

WebSockets Port

TCP-based full-duplex communication protocol port for plug-in free preview. Certificate verification is required to ensure the secure access.



Note

- Enhanced SDK Service Port, WebSocket Port, and WebSockets Port are only supported by certain models.
 - For device models that support that function, go to **Configuration → Network → Advanced Settings → Network Service** to enable it.
-

10.3 Port Mapping

By setting port mapping, you can access devices through the specified port.

Before You Start

When the ports in the device are the same as those of other devices in the network, refer to **Port** to modify the device ports.

Steps

1. Go to **Configuration → Network → Basic Settings → NAT**.
2. Select the port mapping mode.

Auto Port Mapping Refer to **Set Auto Port Mapping** for detailed information.

Manual Port Mapping Refer to **Set Manual Port Mapping** for detailed information.

3. Click **Save**.

10.3.1 Set Auto Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the camera, or you can use the default name.
2. Select the port mapping mode to **Auto**.
3. Click **Save**.



Note

UPnP™ function on the router should be enabled at the same time.

10.3.2 Set Manual Port Mapping

Steps

1. Check **Enable UPnP™**, and choose a friendly name for the device, or you can use the default name.
2. Select the port mapping mode to **Manual**, and set the external port to be the same as the internal port.
3. Click **Save**.

What to do next

Go to the router port mapping settings interface and set the port number and IP address to be the same as those on the device. For more information, refer to the router user manual.

10.3.3 Set Port Mapping on Router

The following settings are for a certain router. The settings vary depending on different models of routers.

Steps

1. Select the **WAN Connection Type**.
2. Set the **IP Address**, **Subnet Mask** and other network parameters of the router.
3. Go to **Forwarding → Virtual Servers**, and input the **Port Number** and **IP Address**.
4. Click **Save**.

Example

When the cameras are connected to the same router, you can configure the ports of a camera as 80, 8000, and 554 with IP address 192.168.1.23, and the ports of another camera as 81, 8001, 555, 8201 with IP 192.168.1.24.

The screenshot shows the configuration interface of a 108M Wireless Router (Model No.: TL-WR641G / TL-WR642G). The left sidebar contains a navigation menu with options: Status, Quick Setup, Basic Settings, Network, Wireless, Advanced Settings, DHCP, Forwarding (selected), Virtual Servers (selected), Port Triggering, DMZ, UPnP, Security, Static Routing, Dynamic DNS, Maintenance, and System Tools. The main content area is titled "Virtual Servers" and displays a table with 5 columns: ID, Service Port, IP Address, Protocol, and Enable. The table contains 8 rows of data. Below the table, there is a "Common Service Port" section with a dropdown menu set to "DNS(53)", a "Copy to" button, and an "ID" dropdown set to "1". At the bottom, there are four buttons: "Previous", "Next", "Clear All", and "Save".

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☒
2	8000	192.168.10.23	ALL	☒
3	554	192.168.10.23	ALL	☒
4	8200	192.168.10.23	ALL	☒
5	81	192.168.10.24	ALL	☒
6	8001	192.168.10.24	ALL	☒
7	555	192.168.10.24	ALL	☒
8	8201	192.168.10.24	ALL	☒

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Figure 10-1 Port Mapping on Router



Note

The port of the network camera cannot conflict with other ports. For example, some web management port of the router is 80. Change the camera port if it is the same as the management port.

10.4 SNMP

You can set the SNMP network management protocol to get the alarm event and exception messages in network transmission.

Before You Start

Before setting the SNMP, you should download the SNMP software and manage to receive the device information via SNMP port.

Steps

1. Go to the settings page: **Configuration → Network → Advanced Settings → SNMP**.
2. Check **Enable SNMPv1**, **Enable SNMP v2c** or **Enable SNMPv3**.



Note

The SNMP version you select should be the same as that of the SNMP software.

And you also need to use the different version according to the security level required. SNMP v1 is not secure and SNMP v2 requires password for access. And SNMP v3 provides encryption and if you use the third version, HTTPS protocol must be enabled.

-
3. Configure the SNMP settings.
 4. Click **Save**.

10.5 Access to Device via Domain Name

You can use the Dynamic DNS (DDNS) for network access. The dynamic IP address of the device can be mapped to a domain name resolution server to realize the network access via domain name.

Before You Start

Registration on the DDNS server is required before configuring the DDNS settings of the device.

Steps

1. Refer to **TCP/IP** to set DNS parameters.
2. Go to the DDNS settings page: **Configuration → Network → Basic Settings → DDNS**.
3. Check **Enable DDNS** and select **DDNS type**.

DynDNS

Dynamic DNS server is used for domain name resolution.

NO-IP

NO-IP server is used for domain name resolution.

4. Input the domain name information, and click **Save**.
5. Check the device ports and complete port mapping. Refer to **Port** to check the device port, and refer to **Port Mapping** for port mapping settings.
6. Access the device.

By Browsers

Enter the domain name in the browser address bar to access the device.

By Client Software Add domain name to the client software. Refer to the client manual for specific adding methods.

10.6 Access to Device via PPPoE Dial Up Connection

This device supports the PPPoE auto dial-up function. The device gets a public IP address by ADSL dial-up after the device is connected to a modem. You need to configure the PPPoE parameters of the device.

Steps

1. Go to **Configuration → Network → Basic Settings → PPPoE** .
2. Check **Enable PPPoE**.
3. Set the PPPoE parameters.

Dynamic IP

After successful dial-up, the dynamic IP address of the WAN is displayed.

User Name

User name for dial-up network access.

Password

Password for dial-up network access.

Confirm

Input your dial-up password again.

4. Click **Save**.
5. Access the device.

By Browsers Enter the WAN dynamic IP address in the browser address bar to access the device.

By Client Software Add the WAN dynamic IP address to the client software. Refer to the client manual for details.



Note

The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the camera. To solve the inconvenience of the dynamic IP, you need to get a domain name from the DDNS provider (e.g. DynDns.com). Refer to **[Access to Device via Domain Name](#)** for detail information.

10.7 Accessing via Mobile Client

Hik-Connect is an application for mobile devices. Using the App, you can view live image, receive alarm notification and so on.



Hik-Connect service should be supported by the camera.

10.7.1 Enable Hik-Connect Service on Camera

Hik-Connect service should be enabled on your camera before using the service.

You can enable the service through SADP software or Web browser.

Enable Hik-Connect Service via Web Browser

Follow the following steps to enable Hik-Connect Service via Web Browser.

Before You Start

You need to activate the camera before enabling the service.

Steps

1. Access the camera via web browser.
2. Enter platform access configuration interface. **Configuration → Network → Advanced Settings → Platform Access**
3. Select Hik-Connect as the **Platform Access Mode**.
4. Check **Enable**.
5. Click and read "Terms of Service" and "Privacy Policy" in pop-up window.
6. Create a verification code or change the old verification code for the camera.



The verification code is required when you add the camera to Hik-Connect service.

7. Save the settings.

Enable Hik-Connect Service via SADP Software

This part introduce how to enable Hik-Connect service via SADP software of an activated camera.

Steps

1. Run SADP software.
2. Select a camera and enter **Modify Network Parameters** page.
3. Check **Enable Hik-Connect**.
4. Create a verification code or change the old verification code.



The verification code is required when you add the camera to Hik-Connect service.

5. Click and read "Terms of Service" and "Privacy Policy".

6. Confirm the settings.

10.7.2 Set Up Hik-Connect

Steps

1. Get and install Hik-Connect application by the following ways.
 - Visit <https://appstore.hikvision.com> to download the application according to your mobile phone system.
 - Visit the official site of our company. Then go to **Support** → **Tools** → **Hikvision App Store**.
 - Scan the QR code below to download the application.



Note

If errors like "Unknown app" occur during the installation, solve the problem in two ways.

- Visit <https://appstore.hikvision.com/static/help/index.html> to refer to the troubleshooting.
- Visit <https://appstore.hikvision.com/>, and click **Installation Help** at the upper right corner of the interface to refer to the troubleshooting.

-
2. Start the application and register for a Hik-Connect user account.
 3. Log in after registration.

10.7.3 Add Camera to Hik-Connect

Steps

1. Connect your mobile device to a Wi-Fi.
2. Log into the Hik-Connect app.
3. In the home page, tap "+" on the upper-right corner to add a camera.
4. Scan the QR code on camera body or on the *Quick Start Guide* cover.



Note

If the QR code is missing or too blur to be recognized, you can also add the camera by inputting the camera's serial number.

-
5. Input the verification code of your camera.



Note

- The required verification code is the code you create or change when you enable Hik-Connect service on the camera.
- If you forget the verification code, you can check the current verification code on **Platform Access** configuration page via web browser.

-
6. Tap **Connect to a Network** button in the popup interface.
 7. Choose **Wired Connection** or **Wireless Connection** according to your camera function.

Wireless Connection	Input the Wi-Fi password that your mobile phone has connected to, and tap Next to start the Wi-Fi connection process. (Locate the camera within 3 meters from the router when setting up the Wi-Fi.)
Wired Connection	Connect the camera to the router with a network cable and tap Connected in the result interface.



Note

The router should be the same one which your mobile phone has connected to.

8. Tap **Add** in the next interface to finish adding.

For detailed information, refer to the user manual of the Hik-Connect app.

10.8 Set ISUP

When the device is registered on ISUP platform (formerly called Ehome), you can visit and manage the device, transmit data, and forward alarm information over public network.

Steps

1. Go to **Configuration → Network → Advanced Settings → Platform Access**.
2. Select **ISUP** as the platform access mode.
3. Select **Enable**.
4. Select a protocol version and input related parameters.
5. Click **Save**.

Register status turns to **Online** when the function is correctly set.

10.9 Set Open Network Video Interface

If you need to access the device through Open Network Video Interface protocol, you can configure the user settings to enhance the network security.

Steps

1. Go to **Configuration → Network → Advanced Settings → Integration Protocol**.
2. Check **Enable Open Network Video Interface**.
3. Click **Add** to configure the Open Network Video Interface user.
 - Delete** Delete the selected Open Network Video Interface user.
 - Modify** Modify the selected Open Network Video Interface user.
4. Click **Save**.
5. **Optional:** Repeat the steps above to add more Open Network Video Interface users.

10.10 Set Network Service

You can control the ON/OFF status of certain protocol as desired.

Steps



Note

This function varies according to different models.

1. Go to **Configuration → Network → Advanced Settings → Network Service**.
2. Set network service.

WebSocket & WebSockets

WebSocket or WebSockets protocol should be enabled if you use Google Chrome 57 and its above version or Mozilla Firefox 52 and its above version to visit the device. Otherwise, live view, image capture, digital zoom, etc. cannot be used.

If the device uses HTTP, enable WebSocket.

If the device uses HTTPS, enable WebSockets.

When you use WebSockets, select the **Server Certificate**.



Note

Complete certificate management before selecting server certificate. Refer to **Certificate Management** for detailed information.

SDK Service & Enhanced SDK Service

Check **Enable SDK Service** to add the device to the client software with SDK protocol.

Check **Enable Enhanced SDK Service** to add the device to the client software with SDK over TLS protocol.

When you use Enhanced SDK Service, select the **Server Certificate**.



Note

- Complete certificate management before selecting server certificate. Refer to **Certificate Management** for detailed information.
 - When set up connection between the device and the client software, it is recommended to use Enhanced SDK Service and set the communication in Arming Mode to encrypt the data transmission. See the user manual of the client software for the arming mode settings.
-

TLS (Transport Layer Security)

The device offers TLS1.1, TLS1.2 and TLS1.3. Enable one or more protocol versions according to your need.

Bonjour

Uncheck to disable the protocol.

3. Click **Save**.

10.11 Set Alarm Server

The device can send alarms to destination IP address or host name through HTTP, HTTPS, or ISUP protocol. The destination IP address or host name should support HTTP, HTTP, or ISUP data transmission.

Steps

1. Go to **Configuration → Network → Advanced Settings → Alarm Server** .
2. Enter **Destination IP or Host Name, URL, and Port**.
3. Select **Protocol**.



Note

HTTP, HTTPS, and ISUP are selectable. It is recommended to use HTTPS, as it encrypts the data transmission during communication.

-
4. Click **Test** to check if the IP or host is available.
 5. Click **Save**.

10.12 TCP Acceleration

TCP acceleration is used to improve latency and reduce packet loss caused by network congestion in poor network condition, and guarantee the fluency of live view.

10.13 Traffic Shaping

Traffic shaping is used to shape and smooth video data packet before transmission.

It helps to improve latency and reduce packet loss caused by network congestion and ensure the video quality as well. Shaping level is configurable.

10.14 Data Monitoring

You can view and manage the SIM card data or wired network data used by the device. SIM card data is the data service provided by network carriers; wired network data is usually provided through a 4G router.

Steps

1. Go to **Configuration → Network → Network Settings → Data Monitoring** .
2. Check **Enable**.
3. Set the following parameters according to your data plan.

Plan Type

Daily, Monthly, or Annually can be selected.

Data Plan

Enter the amount of usable data and select the unit.

Pre-Alarm Threshold

When the used data reaches the set percentage of data plan, the device sends an alarm message, and shows notification on the OSD or pop-up window.

4. Select **Normal Linkage**.

If **Send Email** or **Notify Surveillance Center** is selected, the device sends an alarm message by Email or to surveillance center when the used data reaches the threshold.

5. Click **Save**.



Note

The function varies with different device models.

10.15 Set SRTP

The Secure Real-time Transport Protocol (SRTP) is a Real-time Transport Protocol (RTP) internet protocol, intended to provide encryption, message authentication and integrity, and replay attack protection to the RTP data in both unicast and multicast applications.

Steps

1. Go to **Configuration → Network → Advanced Settings → SRTP**.
2. Select **Server Certificate**.
3. Select **Encrypted Algorithm**.
4. Click **Save**.



Note

- Only certain device models support this function.
 - If the function is abnormal, check if the selected certificate is abnormal in certificate management.
-

Chapter 11 System and Security

It introduces system maintenance, system settings and security management, and explains how to configure relevant parameters.

11.1 View Device Information

You can view device information, such as Device No., Model, Serial No. and Firmware Version.

Enter **Configuration → System → System Settings → Basic Information** to view the device information.

11.2 Restore and Default

Restore and Default helps restore the device parameters to the default settings.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance**.
2. Click **Restore** or **Default** according to your needs.

Restore Reset device parameters, except user information, IP parameters and video format to the default settings.

Default Reset all the parameters to the factory default.



Note

Be careful when using this function. After resetting to the factory default, all the parameters are reset to the default settings.

11.3 Search and Manage Log

Log helps locate and troubleshoot problems.

Steps

1. Go to **Configuration → System → Maintenance → Log**.
2. Set search conditions **Major Type**, **Minor Type**, **Start Time**, and **End Time**.
3. Click **Search**.

The matched log files will be displayed on the log list.

4. **Optional:** Click **Export** to save the log files in your computer.

11.4 Import and Export Configuration File

It helps speed up batch configuration on other devices with the same parameters.

Steps

1. Export configuration file.
 - 1) Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
 - 2) Click **Device Parameters** and input the encryption password to export the current configuration file.
 - 3) Set the saving path to save the configuration file in local computer.
2. Import configuration file.
 - 1) Access the device that needs to be configured via web browser.
 - 2) Click **Browse** to select the saved configuration file.
 - 3) Input the encryption password you have set when exporting the configuration file.
 - 4) Click **Import**.

11.5 Export Diagnose Information

Diagnose information includes running log, system information, hardware information.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** . Check desired diagnose information and click **Diagnose Information** to export corresponding diagnose information of the device.

11.6 Reboot

You can reboot the device via browser.

Go to **Configuration → System → Maintenance → Upgrade & Maintenance** , and click **Reboot**.

11.7 Upgrade

Before You Start

You need to obtain the correct upgrade package.



Caution

DO NOT disconnect power during the process, and the device reboots automatically after upgrade.

Steps

1. Go to **Configuration → System → Maintenance → Upgrade & Maintenance** .
2. Choose one method to upgrade.

Firmware

Locate the exact path of the upgrade file.

Firmware Directory Locate the directory which the upgrade file belongs to.

3. Click **Browse** to select the upgrade file.

4. Click **Upgrade**.

11.8 Undervoltage Alarm

It is used to monitor the device voltage and warns you when the voltage is alarmingly low.

When the device voltage is too low, a sign ⚡ appears in live view image. Then, you are recommended to optimize the power supply, so as to avoid device abnormal.

The function is on by default.

11.9 View Open Source Software License

Go to **Configuration → System → System Settings → About Device** , and click **View Licenses**.

11.10 Set Live View Connection

It controls the remote live view connection amount.

Live view connection controls the maximum live view that can be streamed at the same time.

Enter **Configuration → System → Maintenance → System Service** to set the upper limit of the remote connection number.

11.11 Time and Date

You can configure time and date of the device by configuring time zone, time synchronization and Daylight Saving Time (DST).

11.11.1 Synchronize Time Manually

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .

2. Select **Time Zone**.

3. Click **Manual Time Sync..**

4. Choose one time synchronization method.

- Select **Set Time**, and manually input or select date and time from the pop-up calendar.
- Check **Sync. with computer time** to synchronize the time of the device with that of the local PC.

5. Click **Save**.

11.11.2 Set NTP Server

You can use NTP server when accurate and reliable time source is required.

Before You Start

Set up a NTP server or obtain NTP server information.

Steps

1. Go to **Configuration → System → System Settings → Time Settings** .
2. Select **Time Zone**.
3. Click **NTP**.
4. Set **Server Address**, **NTP Port** and **Interval**.



Note

Server Address is NTP server IP address.

5. Click **Test** to test server connection.
6. Click **Save**.

11.11.3 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **Configuration → System → System Settings → DST** .
2. Check **Enable DST**.
3. Select **Start Time**, **End Time** and **DST Bias**.
4. Click **Save**.

11.12 Set RS-485

RS-485 is used to connect the device to external device. You can use RS-485 to transmit the data between the device and the computer or terminal when the communication distance is too long.

Before You Start

Connect the device and computer or terminal with RS-485 cable.

Steps

1. Go to **Configuration → System → System Settings → RS-485** .
2. Set the RS-485 parameters.



Note

You should keep the parameters of the device and the computer or terminal all the same.

3. Click **Save**.

11.13 Security

You can improve system security by setting security parameters.

11.13.1 Authentication

You can improve network access security by setting RTSP and WEB authentication.

Go to **Configuration → System → Security → Authentication** to choose authentication protocol and method according to your needs.

RTSP Authentication

Digest and digest/basic are supported, which means authentication information is needed when RTSP request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

RTSP Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in RTSP authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.

WEB Authentication

Digest and digest/basic are supported, which means authentication information is needed when WEB request is sent to the device. If you select **digest/basic**, it means the device supports digest or basic authentication. If you select **digest**, the device only supports digest authentication.

WEB Digest Algorithm

MD5, SHA256 and MD5/SHA256 encrypted algorithm in WEB authentication. If you enable the digest algorithm except for MD5, the third-party platform might not be able to log in to the device or enable live view because of compatibility. The encrypted algorithm with high strength is recommended.



Note

Refer to the specific content of protocol to view authentication requirements.

11.13.2 Set IP Address Filter

IP address filter is a tool for access control. You can enable the IP address filter to allow or forbid the visits from the certain IP addresses.

IP address refers to IPv4.

Steps

1. Go to **Configuration → System → Security → IP Address Filter** .
2. Check **Enable IP Address Filter**.
3. Select the type of IP address filter.

Forbidden IP addresses in the list cannot access the device.

Allowed Only IP addresses in the list can access the device.

4. Edit the IP address filter list.

Add Add a new IP address or IP address range to the list.

Modify Modify the selected IP address or IP address range in the list.

Delete Delete the selected IP address or IP address range in the list.

5. Click **Save**.

11.13.3 Set MAC Address Filter

MAC address filter is a tool for access control. You can enable the MAC address filter to allow or forbid the visits from the certain MAC addresses.

Steps

1. Go to **Configuration → System → Security → MAC Address Filter** .
2. Check **Enable MAC Address Filter**.
3. Select the type of MAC address filter.

Forbidden MAC addresses in the list cannot access the device.

Allowed Only MAC addresses in the list can access the device.

4. Edit the MAC address filter list.

Add Add a new MAC address to the list.

Modify Modify the selected MAC address in the list.

Delete Delete the selected MAC address in the list.

5. Click **Save**.

11.13.4 Set HTTPS

HTTPS is a network protocol that enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **Configuration → Network → Advanced Settings → HTTPS** .
2. Check **Enable**.
3. **Optional:** Check **HTTPS Browsing** to access the device only via HTTPS protocol.
4. Select a server certificate.



Note

- Complete certificate management before selecting server certificate. Refer to **Certificate Management** for detailed information.
- If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.

5. Click **Save**.

11.13.5 Security Audit Log

The security audit logs refer to the security operation logs. You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Security audit logs can be saved on device internal storage. The log will be saved every half hour after device booting. Due to limited storage space, you can also save the logs on a log server.

Search Security Audit Logs

You can search and analyze the security log files of the device so as to find out the illegal intrusion and troubleshoot the security events.

Steps



Note

This function is only supported by certain camera models.

-
1. Go to **Configuration → System → Maintenance → Security Audit Log**.
 2. Select log types, **Start Time**, and **End Time**.
 3. Click **Search**.

The log files that match the search conditions will be displayed on the Log List.

4. **Optional:** Click **Export** to save the log files to your computer.

Set Log Server

The log server should support syslog (RFC 3164) over TLS.

Before You Start

- Install client and CA certificates before configuration. Refer to **Certificate Management** for detailed information.
- Select certificates according to the requirement of the log server. If two-way authentication is required, select the CA certificate and the client certificate. If one-way authentication is required, select the CA certificate only.

Steps

1. Check **Enable Log Upload Server**.
2. **Optional**: Check **Enable Encrypted Transmission** if you want the log data to be encrypted.
3. Input **Log Server IP** and **Log Server Port**.
4. **Optional**: Select client certificate.
5. Select CA certificate to the device.
6. Click **Test** to test the settings.
7. Click **Save**.

11.13.6 Set QoS

QoS (Quality of Service) can help improve the network delay and network congestion by setting the priority of data sending.



Note

QoS needs support from network device such as router and switch.

Steps

1. Go to **Configuration → Network → Advanced Configuration → QoS**.
2. Set **Video/Audio DSCP**, **Alarm DSCP** and **Management DSCP**.



Note

Network can identify the priority of data transmission. The bigger the DSCP value is, the higher the priority is. You need to set the same value in router while configuration.

3. Click **Save**.

11.13.7 Set IEEE 802.1X

You can authenticate user permission of the connected device by setting IEEE 802.1X.

Go to **Configuration → Network → Advanced Settings → 802.1X**, and enable the function.

Select protocol and version according to router information. User name and password of server are required.



Note

- If you set the **Protocol** to **EAP-TLS**, select the **Client Certificate** and **CA Certificate**.
 - If the function is abnormal, check if the selected certificate is abnormal in **Certificate Management**.
-

11.13.8 Certificate Management

It manages the server/client certificates and CA certificate of the device.

Server Certificate/Client Certificate



Note

The device has default self-signed server/client certificate installed. The certificate ID is **default**.

Create and Install Self-signed Certificate

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Create Self-signed Certificate**.
3. Input certificate information.



Note

The input certificate ID cannot be the same as the existing ones.

4. Click **OK** to save and install the certificate.

The created certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain functions, the function name is shown in the column **Functions**.

5. **Optional**: Click **Certificate Property** to see the certificate details.

Install Self-signed Request Certificate

You can send the self-signed certificate to a trusted third-party for the signature, and install the certificate to the device.

Before You Start

Create a self-signed certificate first. See [Create and Install Self-signed Certificate](#) for instructions.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Select a self-signed certificate from the Server/Client Certificate list.
3. Click **Create Certificate Request**.
4. Input request information.
5. Click **OK**.

The certificate request details are displayed in a pop-up window.

6. Copy the request content and save it as a request file.

7. Send the file to a trusted-third party for signature.
8. After receiving the certificated sent back from the third-party, install it to the device.
 - 1) Click **Import**.
 - 2) Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existed ones.

- 3) Click **Browse** to select the certificate file.
- 4) Select **Self-signed Request Certificate**.
- 5) Click **OK**.

The imported certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain function, the function name is shown in the column **Functions**.

9. **Optional:** Click **Certificate Property** see the certificate details.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Configuration → System → Security → Certificate Management** .
2. Click **Import**.
3. Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existed ones.

4. Click **Browse** to select the certificate file.
5. Select **Certificate and Key** and select a **Key Type** according to your certificate.

Independent Key If your certificate has a independent key, select this option.

Browse to select the private key and input the private-key password.

PKCS#12 If your certificate has the key in the same certificate file, select this option and input the password.

6. Click **OK**.

The imported certificate is displayed in the **Server/Client Certificate** list.

If the certificate is used by certain function, the function name is shown in the column **Functions**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Configuration → System → Security → Certificate Management**.
2. Input **Certificate ID**.



Note

The input certificate ID cannot be the same as the existing ones.

3. Click **Browse** to select the certificate file.
4. Click **OK**.

The imported certificate is displayed in the **CA Certificate** list.

If the certificate is used by certain functions, the function name is shown in the **Functions** column.

11.13.9 Control Timeout Settings

If this function is enabled, you will be logged out when you make no operation (not including viewing live image) to the device via web browser within the set timeout period.

Go to **Configuration → System → Security → Advanced Security** to complete settings.

11.13.10 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services over an unsecured network.

Go to **Configuration → System → Security → Security Service**, and check **Enable SSH**.

The SSH function is disabled by default.



Caution

Use the function with caution. The security risk of device internal information leakage exists when the function is enabled.

11.13.11 User and Account

Set User Account and Permission

The administrator can add, modify, or delete other accounts, and grant different permission to different user levels.



Caution

To increase security of using the device on the network, please change the password of your account regularly. Changing the password every 3 months is recommended. If the device is used in high-risk environment, it is recommended that the password should be changed every month or week.

Steps

1. Go to **Configuration → System → User Management → User Management**.
2. Click **Add**. Enter **User Name**, select **Level**, and enter **Password**. Assign remote permission to users based on needs.

Administrator

The administrator has the authority to all operations and can add users and operators and assign permission.

User

Users can be assigned permission of viewing live video, setting PTZ parameters, and changing their own passwords, but no permission for other operations.

Operator

Operators can be assigned all permission except for operations on the administrator and creating accounts.

Modify Select a user and click **Modify** to change the password and permission.

Delete Select a user and click **Delete**.



Note

The administrator can add up to 31 user accounts.

3. Click **OK**.

Simultaneous Login

The administrator can set the maximum number of users logging into the system through web browser simultaneously.

Go to **Configuration → System → User Management**, click **General** and set **Simultaneous Login**.

Online Users

The information of users logging into the device is shown.

Go to **Configuration → System → User Management → Online Users** to view the list of online users.

Appendix A. FAQ

Scan the following QR code to find the frequently asked questions of the device.

Note that some frequently asked questions only apply to certain models.





See Far, Go Further

DS-2SF8C425MXG1-ELWY/26 4 MP 25 × Speed Dome



Hikvision has been dedicated to develop products with security since established. Hikvision always follows security by design principle and has adopted many methods of security technologies into our product development lifecycle, including terminal security, data security, application security, network security, and privacy protection. In the meantime, the security technologies used by Hikvision are all in compliance with local applicable laws and safety regulations. These security measures could enhance product's cyber security defense capability and protect your devices as well as your data from malicious cyber attacks.

- Captures a large area and great details at the same time
- High quality imaging with 6 MP resolution for bullet channel
- 24/7 colorful imaging and excellent low-light performance with DarkFighter 2.0 technology
- Panoramic channel tilt adjustable from 12° to 24°
- Secures an expansive area with 25 × optical zoom and 16 × digital zoom
- Expansive night view with up to 30 m white light distance and 300 m IR distance
- Supports deep learning functions
- Water and dust resistant (IP67) and vandal resistant (IK10) excluding glass window
- Audio visual alarm: The white flashing light and audible warning can be triggered by certain events

▪ Specification

Camera	
Image Sensor	[Bullet channel] 1/2.5" Progressive Scan CMOS, [PTZ channel] 1/1.8" Progressive Scan CMOS
Min. Illumination	[Bullet channel] Color: 0.0005 Lux @ (F1.0, AGC ON), B/W: 0.0001 Lux @ (F1.0, AGC ON), 0 Lux with light, [PTZ channel] Color: 0.0005 Lux @ (F1.5, AGC ON), B/W: 0.0001 Lux @ (F1.5, AGC ON), 0 lux with IR
Shutter Speed	1 s to 1/30000 s
Slow Shutter	Yes
Day & Night	[Panoramic channel] Day,Night,Schedule,Auto, [PTZ channel] Day,Night,Schedule,Auto
Zoom	[PTZ channel] 25 × optical, 16 × digital
Max. Resolution	[Panoramic channel] 3680 × 1656, [PTZ channel] 2688 × 1520
Lens	
FOV	[Panoramic channel] horizontal field of view: 190° ± 5°, vertical field of view: 80° ± 5°, [PTZ channel] horizontal field of view: 58.5° to 3.1°, vertical field of view: 34° to 1.7°, diagonal field of view: 65.8° to 3.5°
Focus	Auto,semi-auto>manual
Zoom Speed	[Panoramic channel] No, [PTZ channel] approx. 5.6 s
Focal Length	[Panoramic channel] 2.8 mm, [PTZ channel] 6 to 150 mm
Aperture	[Panoramic channel] F1.0, [PTZ channel] F1.6
Illuminator	
Supplement Light Range	[Panoramic channel] white light: up to 30 m, [PTZ channel] IR: up to 300 m
Smart Supplement Light	Yes
PTZ	
Movement Range (Pan)	360° endless
Movement Range (Tilt)	[Panoramic channel] 12° to 24°, [PTZ channel] -20° to 90°
Pan Speed	[PTZ channel] pan speed: configurable from 0.1° to 160°/s, preset speed: 240°/s
Tilt Speed	[PTZ channel] tilt speed: configurable from 0.1° to 120°/s, preset speed 200°/s,[Panoramic channel] tilt speed configurable
Proportional Pan	[Panoramic channel] No, [PTZ channel] Yes
Presets	300
Patrol Scan	8 patrols, up to 32 presets for each patrol
Pattern Scan	4 pattern scans, record time over 10 minutes for each scan
Power-off Memory	Yes
Park Action	Preset,pattern scan,patrol scan,auto scan,tilt scan,random scan,framescan,panorama scan
3D Positioning	Yes
PTZ Status Display	Yes
Preset Freezing	Yes
Scheduled Task	Preset,pattern scan,patrol scan,auto scan,tilt scan,random scan,framescan,panorama scan,dome reboot,dome adjust,aux output

Video	
Main Stream	[Panoramic channel] 50 Hz: 25 fps (3680 × 1656 , 3632 × 1632), 60 Hz: 30 fps (3680 × 1656 , 3632 × 1632) [PTZ channel] 50 Hz: 50 fps (2688 × 1520, 2560 × 1440), 100 fps (1920 × 1080, 1280 × 960, 1280 × 720), 60 Hz: 60 fps (2688 × 1520, 2560 × 1440), 120 fps (1920 × 1080, 1280 × 960, 1280 × 720) *High frame rate is supported under monitoring mode only.
Sub-Stream	[PTZ channel] 50 Hz: 25 fps (704 × 576, 640 × 480, 352 × 288), 60 Hz: 30 fps (704 × 480, 640 × 480, 352 × 240), [Panoramic channel] 50 Hz: 25 fps (1200 × 536 , 960 × 432), 60 Hz: 30 fps (1200 × 536, 960 × 432)
Third Stream	[PTZ channel] 50 Hz: 25 fps (1920 × 1080, 1280 × 960, 1280 × 720, 704 × 576, 640 × 480, 352 × 288), 60 Hz: 30 fps (1920 × 1080, 1280 × 960, 1280 × 720, 704 × 480, 640 × 480, 352 × 240), [Panoramic channel] No
Video Compression	Main stream: H.265+/H.265/H.264+/H.264, Sub-stream: H.265/H.264/MJPEG, Third stream: H.265/H.264/MJPEG
Video Bit Rate	32 Kbps to 16 Mbps
H.264 Type	Baseline profile, Main profile, High profile
H.265 Type	Main profile
Scalable Video Coding (SVC)	H.264 and H.265 encoding
Region of Interest (ROI)	8 fixed regions for each stream
Audio	
Audio Compression	G.711, G.722.1, G.726, MP2L2, PCM, AAC-LC, MP3
Audio Bit Rate	32 to 192 Kbps (MP2L2), 16 to 64 Kbps (AAC-LC), 64 Kbps (G.711), 16 Kbps (G.726), 16 Kbps (G.722.1), 8-48 Kbps (PCM)
Audio Sampling Rate	8 kHz, 16 kHz, 32 kHz, 48 kHz
Environment Noise Filtering	Yes
Network	
API	ONVIF (Profile S, Profile G, Profile T, Profile M), ISUP, ISAPI, SDK, OTAP
Security	Password protection, complicated password, HTTPS encryption, IP address filter, 802.1X authentication (EAP-TLS, EAP-LEAP, EAP-MD5), watermark, host authentication (MAC address), TPM 2.0 (FIPS 140-2 level 2)
Network Storage	NAS (NFS, SMB/CIFS), auto network replenishment (ANR)
Protocols	IPv4/IPv6, HTTP, HTTPS, 802.1X, QoS, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTCP, RTP, TCP/IP, UDP, IGMP, ICMP, DHCP, PPPoE, Bonjour, FTP
Simultaneous Live View	Up to 20 channels
User/Host	Up to 32 users. 3 user levels: administrator, operator, and user
Client	iVMS-4200, HikCentral Pro, Hik-Connect
Web Browser	Plug-in required live view: IE8+ Plug-in free live view: Chrome 57.0+, Firefox 52.0+, Safari 11+ Local service: Chrome 41.0+, Firefox 30.0+
Image	
Wide Dynamic Range (WDR)	[Bullet channel] 120 dB, [PTZ channel] 150 dB
Day/Night Switch	Day, night, auto, schedule

Privacy Mask	[Panoramic channel] 8 programmable polygon privacy masks, [PTZ channel] 24 programmable polygon privacy masks; mask color or mosaic configurable
Image Enhancement	HLC, 3D DNR
Defog	Digital defog
Image Stabilization	EIS (Built-in gyroscope to improve EIS performance)
Regional Exposure	Yes
Regional Focus	[Panoramic channel] No, [PTZ channel] Yes
Image Settings	Saturation, brightness, contrast, sharpness, gain, and white balance adjustable by client software or web browser
Image Parameters Switch	Yes
SNR	≥ 52 dB
Supplement Detection	
Satellite Positioning	No
Gyroscope	Yes
Compass	No
Interface	
On-board Storage	Built-in memory card slot, support microSD/microSDHC/microSDXC card, up to 1 TB .
Built-in Speaker	1 built-in speaker
Ethernet Interface	1 RJ45 100M self-adaptive Ethernet port
Alarm	7 input(s), 2 output(s)
Audio	1 input (line in), max. input amplitude: 2-2.4 vpp, input impedance: 1 KΩ ± 10%, 1 output (line out), line level, output impedance: 600 Ω
RS-485	1 RS-485 (Half duplex, HIKVISION, Pelco-P, Pelco-D, self-adaptive)
Reset	Yes
Event	
Basic Event	[PTZ channel & panoramic channel] alarm input and output, exception, [PTZ channel] video tampering alarm
Smart Event	Line crossing detection, intrusion detection, region entrance detection, region exiting detection, unattended baggage detection, object removal detection, loitering detection, people gathering detection, fast moving detection, parking detection
Linkage	[Panoramic channel] Upload to FTP/NAS/memory card, notify surveillance center, send email, trigger alarm output, trigger recording, audible warning, white light flashing, [PTZ channel] Upload to FTP/NAS/memory card, notify surveillance center, send email, trigger alarm output, trigger recording, and PTZ actions (such as preset, patrol scan, pattern scan)
Smart Linkage	Manual tracking, tracking takeover, linked tracking capture
Deep Learning Function	
Face Capture	Detects up to 30 faces simultaneously, Uploads face with background and closed-up face pictures
Face Comparison	Up to 10 face libraries. 30000 faces for each library. 150000 faces in total, Recognizes face identity via face modeling, grading and comparing to those in face library, Supports face library encryption

Road Traffic and Vehicle Detection	Smart Function: Support license plate recognition of vehicles and motorcycles (only in checkpoint scenario) Support vehicle attribute detection, including vehicle type, color, brand, driving direction, etc. Support vehicle and non-vehicle counting Blocklist and allowlist: up to 10,000 records LPR Countries/Regions: 4 areas (Europe, Middle East, Asia-Pacific, Africa) and more than 124 countries/regions Accuracy (Under recommended installation and lighting conditions): License plate recognition rate $\geq 98\%$ Capture rate $\geq 99\%$ Driving direction accuracy rate $\geq 98\%$ Vehicle Capture Speed: Front installation in checkpoint scenario: up to 120 km/h Side installation: up to 80 km/h Capture Mode: License Plate and Vehicle Mode, Vehicle Priority Mode
Multi-Target-Type Detection	Supports simultaneous detection and capture of human body, face and vehicle, Gets 7 face features, 14 human body features and 8 vehicle features
Perimeter Protection	Line crossing detection, region entrance detection, intrusion detection, region exiting detection
Linkage and Tracking	
Smart Tracking	Manual tracking, auto-tracking 3.0
Object Tracking	Support person arming. When the device detects the armed face or human body in the monitoring scene, it triggers alarms, and tracks and captures the target. During the tracking, the target location and other related information are uploaded. Support vehicle arming. When the device detects the armed vehicles in the monitoring scene, it triggers alarms, and tracks and captures the target. During the tracking, the target location and other related information are uploaded.
General	
General Function	mirror, password protection
Power	36V, 2.5 A, PoE(802.3 bt), 42.5 to 57 V, 1.76 A
Operating Condition	-40 °C to 70 °C (-40 °F to 158 °F). Humidity 95% or less (non-condensing), For speaker: -30 °C to 55 °C (-22 °F to 131 °F)
Wiper	Yes
Demist	Yes
Material	ADC12
Dimension	Ø290 mm × 453.2 mm (Ø11.42" × 17.84")
Weight	Approx. 10.5 kg (23.15 lb.)
Language	33 languages: English, Russian, Estonian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Danish, Swedish, Norwegian, Finnish, Croatian, Slovenian, Serbian, Turkish, Korean, Traditional Chinese, Thai, Vietnamese, Japanese, Latvian, Lithuanian, Portuguese (Brazil), Ukrainian
Approval	
EMC	CE-EMC (EN 55032: 2015, EN 61000-3-2: 2019, EN 61000-3-3: 2013 + A1: 2019, EN 50130-4: 2011 + A1: 2014), RCM (AS/NZS CISPR 32: 2015), IC (ICES-003: Issue 7)
Safety	CB (IEC 62368-1: 2014 + A11), CE-LVD (EN 62368-1: 2014/A11: 2017)

Environment	CE-RoHS (2011/65/EU),WEEE (2012/19/EU),Reach (Regulation (EC) No 1907/2006)
Protection	IP67 (IEC 60529-2013),TVS 6000 V lightning protection, surge protection and voltage transient protection,IK10 (IEC 62262:2002, excluding glass window)
Anti-Corrosion Protection	NEMA 4X (NEMA 250-2018)

▪ DORI

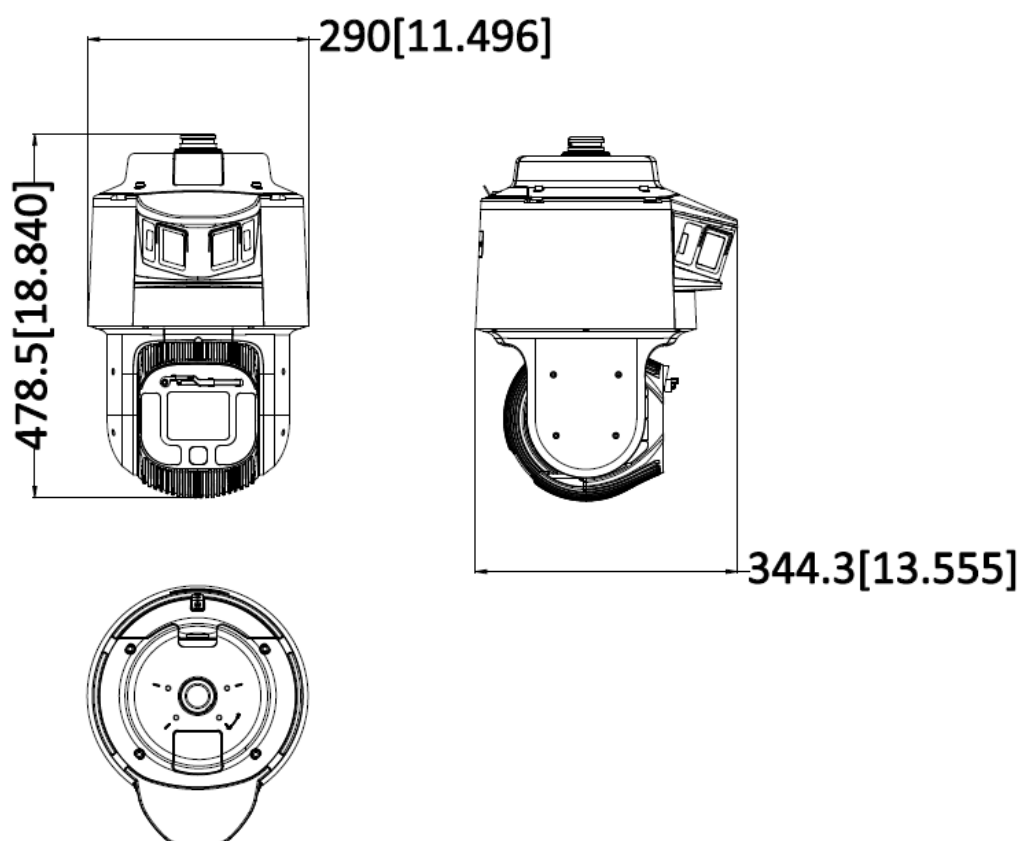
The DORI (detect, observe, recognize, identify) distance gives the general idea of the camera ability to distinguish persons or objects within its field of view. It is calculated based on the camera sensor specification and the criteria given by EN 62676-4: 2015.

DORI	Detect	Observe	Recognize	Identify
Definition	25 px/m	63 px/m	125 px/m	250 px/m
[Bullet channel] Distance	77.0m	30.5m	15.4m	7.7m
[PTZ channel] Distance (Tele)	2965.5m	1176.8m	593.1m	296.6m

▪ Available Model

DS-2SF8C425MXG1-ELWY/26(F0)

▪ Dimension



Unit: mm [inch]

SCALE	1:1

▪ **Accessory**

▪ **Optional**

DS-2115ZJ-PSAC	DS-4614ZJ-PAAC	DS-4604ZJ-PAAC	DS-1684ZJ-P-Y
			

See Far, Go Further



www.hikvision.com
support@hikvision.com





*Images are for illustrative purposes. Actual product appearance and specifications may vary.

DS-1603ZJ-Pole-P



Vertical pole mount

- Vertical Pole Mount
- Aluminum Alloy, Steel, and Stainless Steel
- Platinum Gray

Sales Inquiry

Available models:

DS-1603ZJ-Pole-P



Specification

Resources

Specification

Parameters

Parameters

2450 g (5.4 lb.)

Appearance

Platinum Gray

Material	Aluminum Alloy, Steel, and Stainless Steel
Dimension	410.6 mm × 194 mm × 126.1 mm (16.17" × 7.64" × 4.96")
Description	Vertical Pole Mount

*Product performance is based on testing in a controlled environment. Your results may vary due to several external and environmental factors.

Resources

Technical documents

Quick Start Guide



About Us

Newsroom

Partner

Quick Links

 [Contact Us](#)

✉ [Subscribe Newsletter](#)



© 2026 Hangzhou Hikvision Digital Technology Co., Ltd. All Rights Reserved. [Privacy Policy](#) [Cookie Policy](#) [Cookies Preferences](#) [General Terms of Use](#)

HS-TF-L2

Introduction

Hikvision L2 Micro SD (TF) Card for surveillance, specially designed for video surveillance recording, with a read and write speed of Class 10 and above; using TLC storage medium, with strong compatibility and lower price, it can be widely used in light storage, backup storage and other recordings Scenarios with low intensity or relatively simple usage environment



Features

- **Cost-effective**

Compared with the same TLC material in the market, the price of farmland can fully meet the needs of light storage level with low video intensity and relatively simple usage scenarios.

- **Strong compatibility**

Better compatibility, optimized according to Hikvision storage system, compatible with covering more products, and used with Hikvision products, the effect is better

- **Adaptable**

Waterproof, shockproof, X-ray proof, high and low temperature resistant, can be widely adapted to various working environments

- **S.M.A.R.T. Mechanism**

Unique functions of life forewarning and health monitoring when used with Hikvision cameras. It can calculate the remaining available time based on the past records of use frequency and the number of bad blocks, and realize real-time warning to secure user data to the largest extent

- **Unique Security Mechanism**

Unique function of read-write lock when used with Hikvision cameras, preventing irrelevant personnel from reading or writing even if they get the Micro SD (TF) card

Ordering Information

Capacity	Model
16 GB	HS-TF-L2(STD)/16G
32 GB	HS-TF-L2(STD)/32G
64 GB	HS-TF-L2(STD)/64G
128 GB	HS-TF-L2(STD)/128G
256 GB	HS-TF-L2(STD)/256G



Note

Please contact the local sales for detailed model information.

Specification

Model	HS-TF-L2				
Capacity	16 GB	32GB	64GB	128 GB	256 GB
Max. Read speed	95 MB/s	95 MB/s	95 MB/s	95 MB/s	95 MB/s
Max. Write speed	15 MB/s	25 MB/s	40 MB/s	50 MB/s	55 MB/s
NAND flash memory	TLC（Teiple-Level Cell）				
Specification	MicroSDHC		MicroSDXC		
Speed	Class10, U1,V10		Class10,U3,V30		
Dimensions	0.59" x 0.43" x 0.04"（14.99mm x 10.92mm x 1.02mm）				
Working Temperature	0°C to 70°C				
Storage Temperature	-25 °C to 85 °C				
Compatibility	Compatible with microSDHC、microSDXC、microSDHC UHS-I and microSDXC UHS-I host devices				
Warranty	2 years				

Note

Performance test is performed in specific testing environment. Any change of the computer system, operation system, hardware, software, or functions will influence the test result.

Revision History

Version	Description	Date
V1.0.0	HS-TF-L2	20220216

Data subject to change without notice.

© 2022 HANGZHOU HIKSTORAGE TECHNOLOGY CO.,LTD. All rights reserved.

Unless otherwise expressly stated herein, HIKSTORAGE does not make any warranties, guarantees or representations, express or implied, regarding to the Manual, any information contained herein.

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the HIKSTORAGE website (<http://en.hikstorage.com/>).



Network Video Recorder

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Conditions

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

- This device may not cause harmful interference.
- 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 2014/30/EU, LVD Directive 2014/35/EU, 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 see: <http://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 see: <http://www.recyclethis.info> .

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Table 1-1 Applicable Model

Series	Model
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P

Series	Model
	DS-7716NI-M4/16P
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-7700NXI-M4/VPro	DS-7716NXI-M4/VPro
	DS-7732NXI-M4/VPro
DS-7700NXI-M4/16P/VPro	DS-7716NXI-M4/16P/VPro
	DS-7732NXI-M4/16P/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro

Series	Model
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-I2/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-I2/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-I4/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-I8/S	DS-8616NXI-I8/S
	DS-8632NXI-I8/S
	DS-8664NXI-I8/S
DS-8600NXI-I8/24P/S	DS-8632NXI-I8/24P/S
DS-9600NXI-I8/S	DS-9616NXI-I8/S

Series	Model
	DS-9632NXI-I8/S
	DS-9664NXI-I8/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X
DS-9600NXI-S16	DS-9632NXI-S16
	DS-9664NXI-S16

Series	Model
	DS-9664NXI-S16(LCD)
DS-96000NXI-S16	DS-96128NXI-S16
	DS-96128NXI-S16(LCD)
	DS-96256NXI-S16
DS-9600NXI-S16R	DS-9632NXI-S16R
	DS-9664NXI-S16R
DS-96000NXI-S16R	DS-96128NXI-S16R
	DS-96128NXI-S16R(LCD)
	DS-96256NXI-S16R
	DS-96256NXI-S16R(LCD)
DS-96000NXI-S24R	DS-96128NXI-S24R
	DS-96128NXI-S24R(LCD)
	DS-96256NXI-S24R
	DS-96256NXI-S24R(LCD)
DS-96000NXI-S36R	DS-96128NXI-S36R
	DS-96256NXI-S36R
DS-9600NXI-S8	DS-9616NXI-S8
	DS-9632NXI-S8
	DS-9664NXI-S8
DS-96000NXI-S8	DS-96128NXI-S8
DS-9600NXI-S8R	DS-9632NXI-S8R
	DS-9664NXI-S8R
DS-96000NXI-S8R	DS-96128NXI-S8R

Safety Instruction

- 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.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the device and shall be easily accessible.
- For the device with the sign ⚡ indicating hazardous live, the external wiring connected to the terminals requires installation by an instructed person.
- Never place the device in an unstable location. The device may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC62368.
- High touch current! Connect to earth before connecting to the power supply.
- 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.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Do not ingest battery. Chemical Burn Hazard!
- This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- Use only power supplies same with the original model, or LPS power supplies with the same voltage and electric current.

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
-  identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- If the device has been powered off or placed for a long time, its coin/button cell battery may run out power.
- When the coin/button cell battery runs out power, the system time would be incorrect, please contact the after-sales service to replace the battery.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.
- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- Do not touch the bare components (such as the metal contacts of the inlets) and wait for at least 5 minutes, since electricity may still exist after the device is powered off.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only. The current for the connected device shall be not more than 0.1 A.
- The serial port of the device is used for debugging only.
- If the power output port of the device does not comply with Limited Power Source, the connected device powered by this port shall be equipped with a fire enclosure.
- If a power adapter is provided in the device package, use the provided adapter only.

- For the device with sticker  or  , pay attention to the following cautions: CAUTION: Hot parts! Do not touch. Burned fingers when handling the parts. Wait one-half hour after switching off before handling the parts.
- If the device needs to be installed on the wall or ceiling,
 1. Install the device according to the instructions in this manual.
 2. To prevent injury, this device must be securely attached to the installation surface in accordance with the installation instructions.
- Under high working temperature (40 °C (104 °F) to 55 °C (131 °F)), the power of some power adapters may decrease.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device.
- If the device needs to be wired by yourself, select the corresponding wire to supply power according to the electric parameters labeled on the device. Strip off wire with a standard wire stripper at corresponding position. To avoid serious consequences, the length of stripped wire shall be appropriate, and conductors shall not be exposed.
- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

Content Convention

In order to simplify description, please read the following conventions.

- Recorder or device mainly refers to video recorder.
- IP device mainly refers to network camera (IP camera), IP dome (speed dome), DVS (Digital Video Server), or NVS (Network Video Server).
- Channel mainly refers to the video channel in video recorder.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Indicator and Interface Description

Front Panel Indicator Description

The indicators at the front panel indicates different working status of your device.

Table 1-1 Common Indicator Description

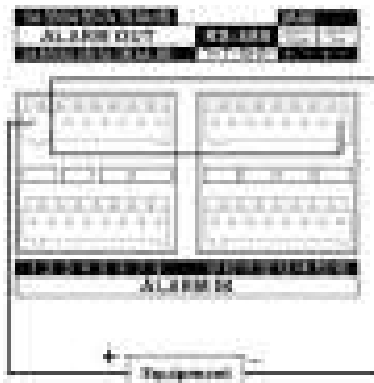
Indicator	Description
	The indicator turns on when device is powered up.
	The indicator flashes when data is being read from or written to HDD.
	The indicator flashes when network connection is functioning properly.

Interface Description

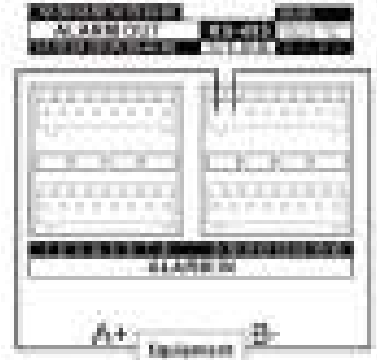
The panel interfaces vary with different models. Refer to the following table for common interface description.

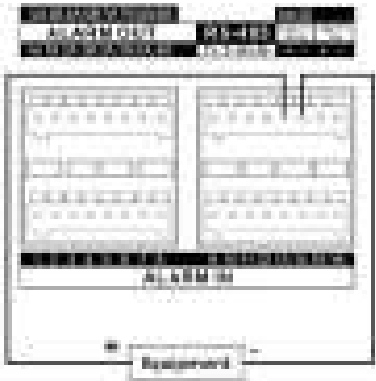
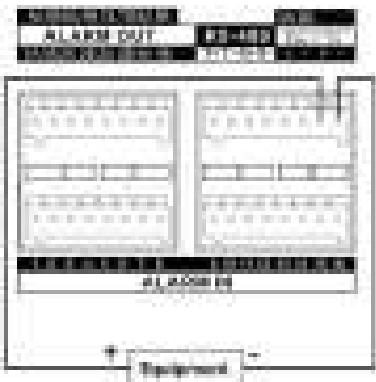
Table 1-2 Common Indicator Description

Item	Description
VIDEO IN	BNC interface for Turbo HD and analog video input.
VIDEO OUT	BNC connector for video output.
AUDIO IN	RCA connector for audio input.
AUDIO OUT	RCA connector for audio output.
LINE IN	RCA connector for two-way audio input.
USB	Universal Serial Bus (USB) interface for additional device.
VGA	DB15 connector for local video output and menu display.
HDMI	HDMI interface for video output.
RS-485	RS-485 serial interface for pan/tilt unit, speed dome, etc.
RS-232	RS-232 interface for parameter configuration, or transparent channel.
LAN	RJ-45 self-adaptive Ethernet interface.
eSATA	Storage and expansion interface for record or backup.
GND	Ground.

Item	Description
Power Switch	Switch for turning on/off the device.
Power Supply	100 to 240 VAC, 48 VDC, or 12 VDC power supply.
USIM Card	UIM/SIM card slot.
	SMA antenna interface.
ALARM IN	The alarm input receives alarm input signal. The equipment positive terminal (+) should connect to a number, and the equipment negative terminal (-) should connect to “-” or “G”. Use the following diagram as a connection example for alarm input. 
ALARM OUT	The alarm output sends out alarm signal. When an equipment uses DC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should both connect to the corresponding number with “B”, and then connect to “-” or “G”. Use the following diagram as an alarm output connection example for DC equipment. 

Item	Description
	When an equipment uses AC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should connect to the corresponding number with “B”. Use the following diagram as an alarm output connection example for AC equipment. Note For the reason that the AC load voltage could be high, please use an external relay for safety. Use the following diagram for reference.
KB	KB represents keyboard. Connect “D+” and “D-” to “T+” and “T-” respectively. Use the following diagram for reference.

Item	Description
	
RS-485	RS-485 is an electrical specification of a two-wire, half-duplex, multipoint serial connection. Connect “T+” and “T-” to “A+” and “B-” respectively. Use the following diagram for reference. 
Ctrl 12V/ $\frac{12V}{0.5A}$	Controllable 12 VDC and 0.5/1 A power output for external alarm device. The power will be turned on when the corresponding alarm output is triggered. Use the following diagram for reference.

Item	Description
	 The diagram shows a terminal block with three main sections. The top section is labeled 'ALARM OUT' and 'RS-485'. The middle section is labeled 'ALARM IN'. The bottom section is labeled 'Equipment'. Wires are connected to the terminals, and a ground symbol is shown at the bottom.
DC 12V/ $\frac{12V}{1A}$	It provides 12 VDC and 1 A power output. Use the following diagram for reference.  This diagram is identical to the one in the previous row, showing the terminal block connections for Alarm Out, RS-485, Alarm In, and Equipment, with a ground symbol at the bottom.

HDD Installation

If your device does not support HDD hot swapping, disconnect the power from the device before installing a hard disk drive (HDD). A factory recommended HDD should be used for this installation.

Scan the QR code below to view HDD installation videos.



Figure 1-1 HDD Installation

Bracket Installation

Bracket installation is applicable when it requires to remove the device cover, and install HDD on the internal bracket.

Steps

1. Unfasten screws on the back, and push the cover backwards to remove the cover.

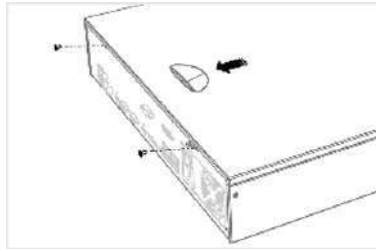


Figure 1-2 Remove Cover

2. Fix the HDD on the bracket with screws.



Note

Please uninstall the upper layer bracket first before installing HDD on the lower layer bracket.

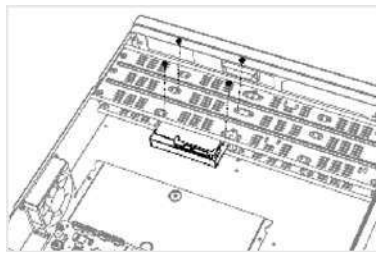


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

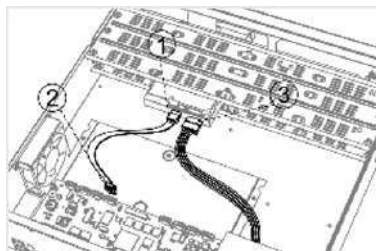


Figure 1-4 Connect Cable



Note

You can repeat the steps above to install other HDDs.

4. Reinstall the device cover and fasten screws.

Front Panel Plug-Pull Installation

Front panel plug-pull installation is applicable when you need to open the device front panel with key and install the HDD.

Steps

1. Fix mounting ears to HDD with screws.

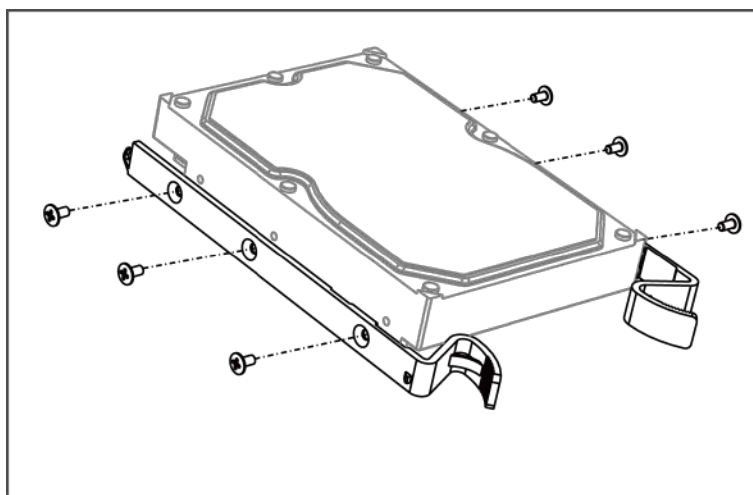


Figure 1-5 Fix Mounting Ears to HDD

2. Unlock the front panel with the attached key, and press the buttons on both sides of the front panel to open it.

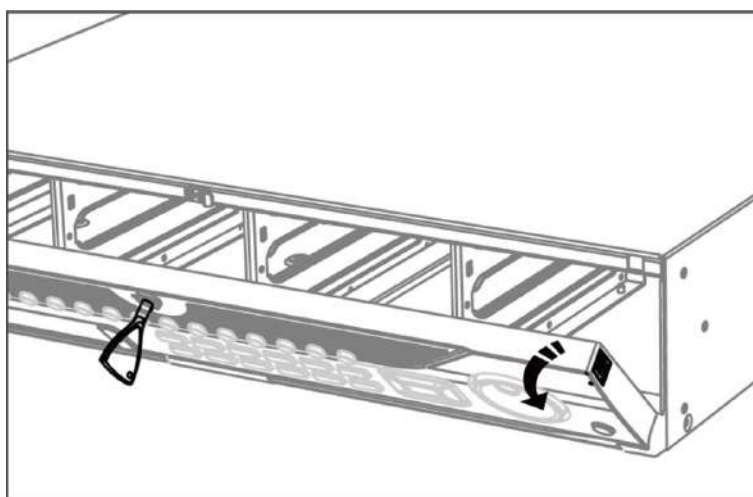


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

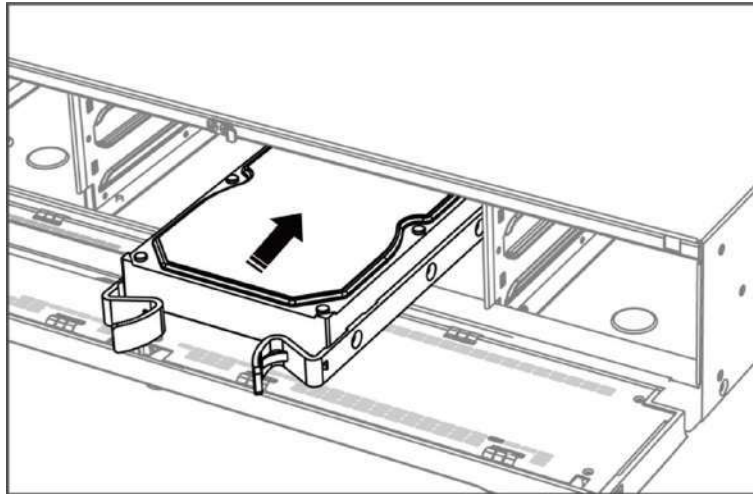


Figure 1-7 Insert HDD

4. **Optional:** Repeat the steps above to install other HDDs.
5. Close the front panel and lock it with key.

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

1. Unlock the front panel with panel key.
2. Pull the front panel out of the device and make it a little above the left handle.



Note

The angle between the front panel and the device must be within 10°.

3. Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
4. Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

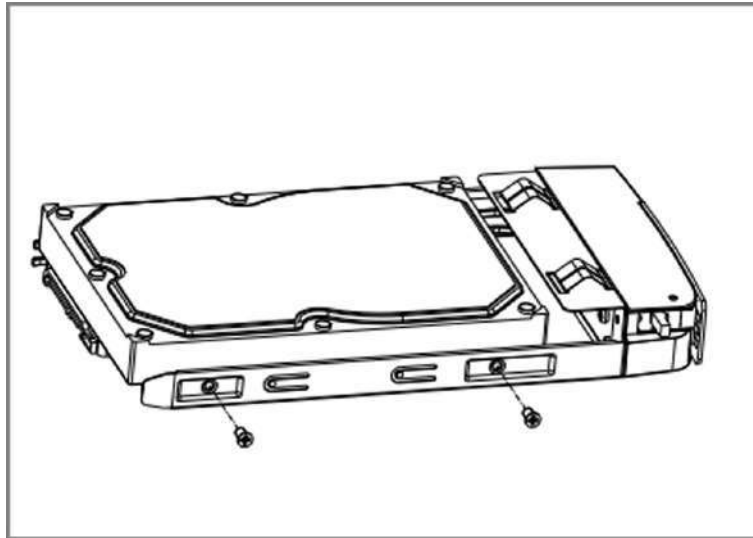


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

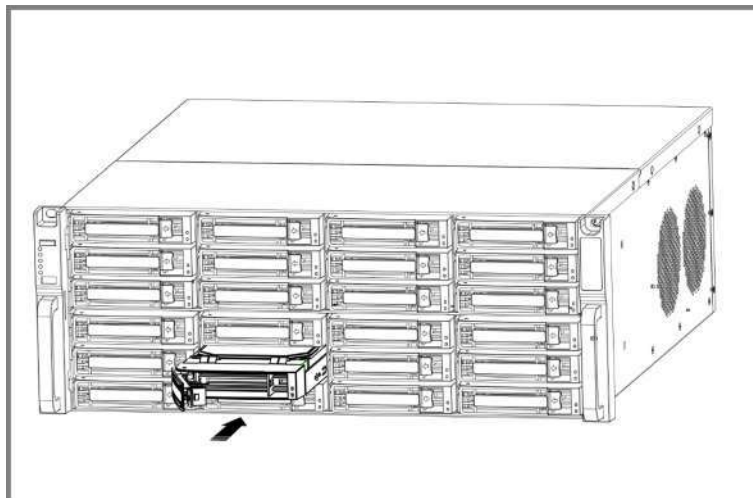


Figure 1-9 Push HDD Case into Slot

6. Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
7. Close the front panel, and lock it with the panel key.

Fix-on-Bottom Installation

Fix-on-bottom installation is applicable when you need to install and fix the HDD on the device bottom.

Steps

1. Remove the cover from device by unfastening the screws on panels.

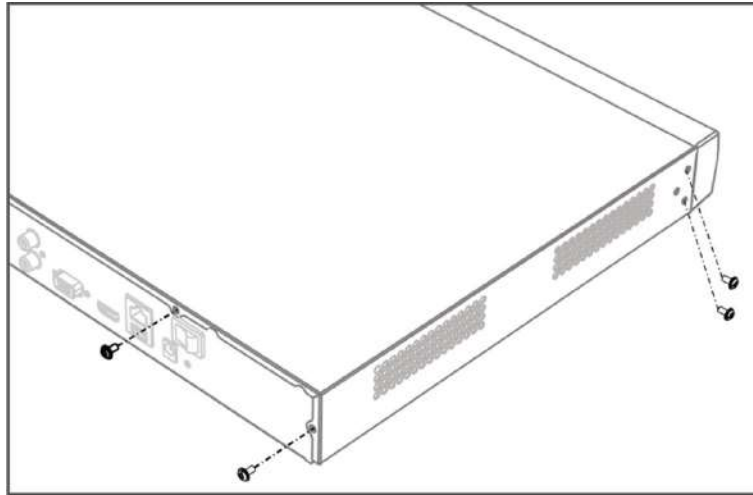


Figure 1-10 Remove Cover

2. Connect the data cable and power cable.
 - 1) Connect one end of data cable to the device motherboard.
 - 2) Connect the other end of data cable to HDD.
 - 3) Connect one end of power cable to HDD.
 - 4) Connect the other end of power cable to the device motherboard.

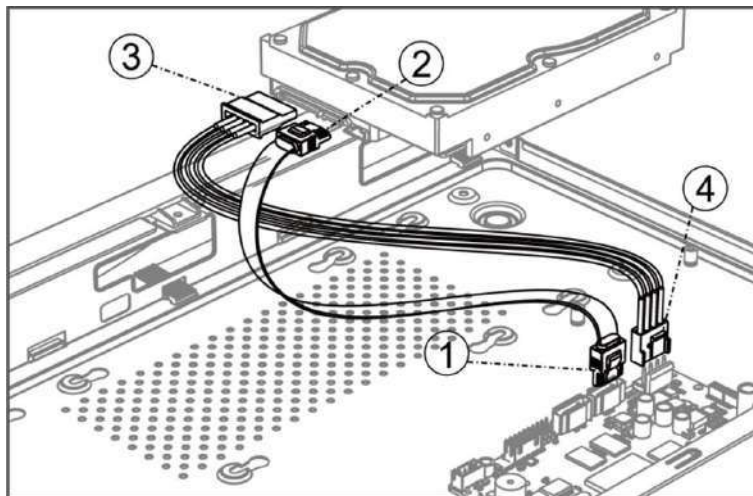


Figure 1-11 Connect Cables

3. Set the device up, match HDD screw threads with the reserved holes on the device bottom, and fix HDD with screws.

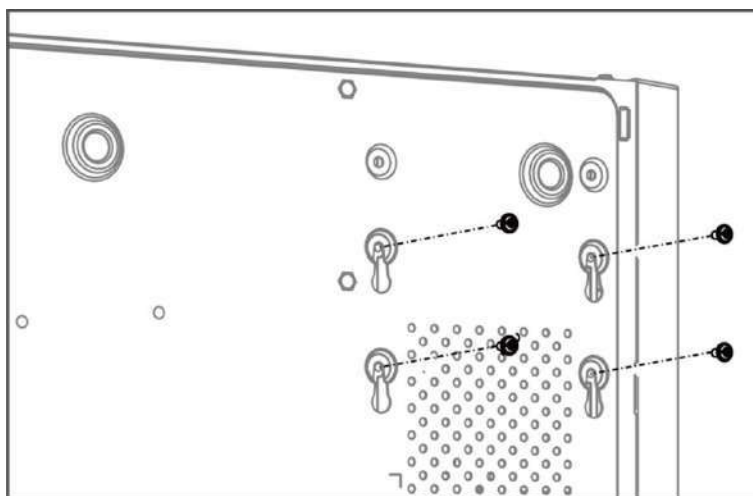


Figure 1-12 Fix HDD to Device Bottom

- 4. Optional:** Repeat the steps above to install other HDDs.
- 5.** Reinstall the device cover and fasten screws.

Coin/Button Cell Battery Replacement

The coin/button cell battery should be replaced when the device has been powered off or placed for a long time, and the system time is incorrect.

Before You Start

Power off your device.

Steps

1. Remove the device chassis cover.
2. Find the coin/button cell battery on motherboard.
3. Use tweezers to push the metal latch at the middle from its inside, and the battery would automatically pop up.

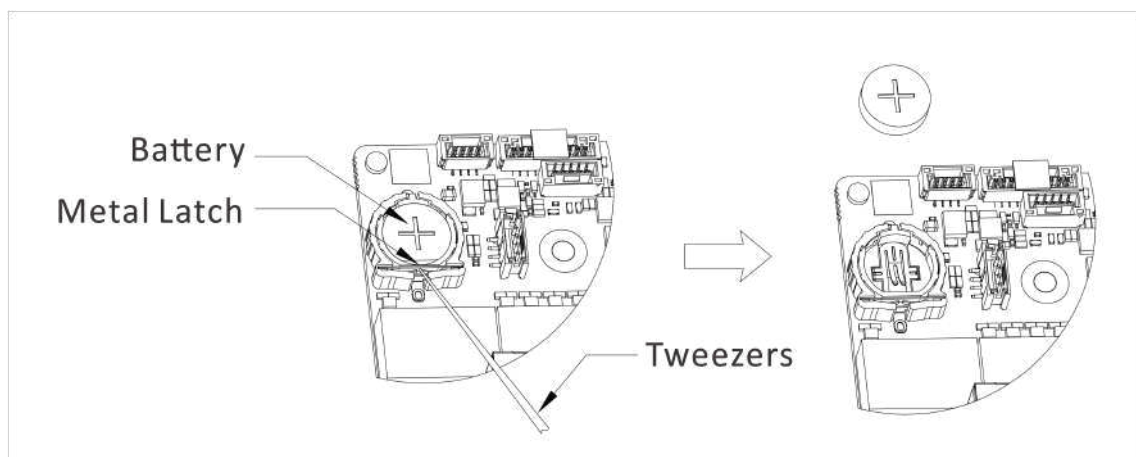


Figure 1-1 Remove Battery

4. Take out the old battery and press a new battery with the same model in to the battery slot.

Note

The battery positive terminal (+ identifies the positive terminal) should be placed upward.

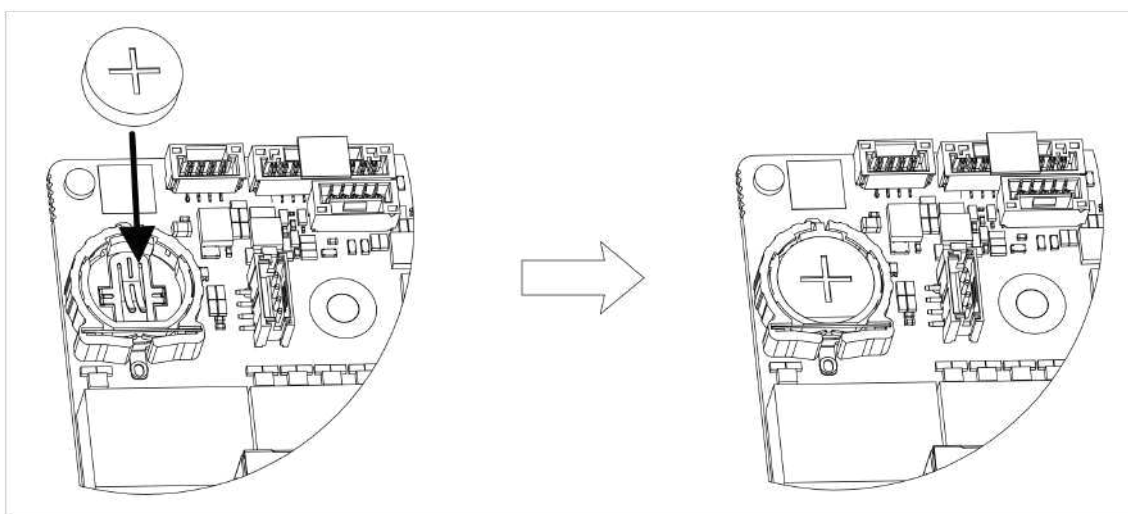


Figure 1-2 Replace Battery

5. Reinstall the device chassis cover.

What to do next

If the system time is incorrect, please go to configure the time.

Contents

Chapter 1 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	9
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP	11
4.2.3 Configure ISUP	12
4.2.4 Configure SDK Service	13
4.2.5 Enable ISAPI	14
4.2.6 Configure ONVIF	14
4.2.7 Configure Log Server	15
4.3 Network Service Settings	16
4.3.1 Configure HTTP(S)	16
4.3.2 Configure RTSP	17
4.3.3 Configure WebSocket(s)	18
4.3.4 Configure Port Mapping (NAT)	18
4.3.5 Configure IoT	20
Chapter 5 User Management	21
Chapter 6 Device Access	22
6.1 Access Video Device	22

6.1.1 Add Automatically Searched Online Network Camera	22
6.1.2 Add Network Camera Manually	22
6.1.3 Add Network Camera through PoE	24
6.1.4 Add Solar-Powered Camera through OTAP Protocol	24
6.1.5 Add Network Camera via Custom Protocol	25
6.1.6 Add Network Camera through Camera Configuration File	26
6.2 Add Access Control Device	26
6.3 Add Audio Device	26
6.4 Add POS Device	27
6.5 Channel Management	28
Chapter 7 Device Grouping	29
Chapter 8 Video or Audio Device Settings	30
8.1 Enable H.265 Stream Access	30
8.2 Configure Display Settings	30
8.3 Configure Video Parameters	31
8.4 Configure Privacy Mask	31
8.5 Configure Audio Parameter	32
8.6 Configure OTAP Service	33
8.7 Batch Configuration	33
8.8 Configure PoE (Power over Ethernet) Interface	34
Chapter 9 Storage Management	36
9.1 Manage HDD	36
9.2 RAID Configuration	36
9.2.1 Create Disk Array	37
9.2.2 Rebuild Array	39
9.2.3 Delete Array	39
9.2.4 View Firmware Info	39
9.3 Configure Storage Mode	40

9.4 Configure Other Storage Parameters	40
9.5 Manage USB Flash Drive	41
Chapter 10 Schedule Configuration	42
10.1 Configure Schedule Template	42
10.2 Configure Recording Schedule	44
10.3 Configure Picture Capture Schedule	46
10.4 Configure Audio Recording	48
Chapter 11 Live View	49
11.1 Configure Live View Layout	49
11.2 GUI Introduction	49
11.3 PTZ Control	51
Chapter 12 Playback	52
12.1 GUI Introduction	52
12.2 Normal Playback	54
12.3 Event Playback	54
12.4 Slice Playback	55
12.5 Sub-Period Playback	55
Chapter 13 Event Center	57
13.1 Event Settings	57
13.1.1 Basic/Generic Event	57
13.1.2 Perimeter Protection	59
13.1.3 Abnormal Behavior Event	70
13.1.4 Target Event	72
13.1.5 Thermal Camera Detection	74
13.1.6 Alarm Input Event	76
13.1.7 Audio Analysis Event	78
13.2 Linkage Configuration	79
13.3 Disarming Configuration	81

13.4 Batch Configuration	82
13.5 Event Search	82
13.6 View Alarms	83
Chapter 14 Search and Backup	84
Chapter 15 AcuSearch	86
Chapter 16 Smart Settings	88
16.1 Algorithm Management	88
16.2 Engine Status	88
16.3 Task Plan Management	88
16.4 List library Management	88
16.4.1 Add a List Library	89
16.4.2 Upload Face Pictures to the Library	89
Chapter 17 Application Center	91
17.1 Human and Vehicle Detection	91
17.2 Person Check-In	91
17.2.1 Add Check-In Task	92
17.2.2 Search Check-In Records	93
17.3 Statistic Report	93
Chapter 18 System Parameter Settings	95
Chapter 19 Hot Spare Device Backup	97
19.1 Set Working Device	97
19.2 Set Hot Spare Device	97
Chapter 20 Configure Exception Event	99
Chapter 21 View System Info	101
Chapter 22 System Maintenance	102
22.1 Schedule Reboot	102
22.2 Upgrade Device	102
22.3 Backup and Restore	102

22.4 Log Info	103
22.5 Configure Log Server	103
22.6 Maintenance Tools	103
Chapter 23 Security Management	105
23.1 Address Filter	105
23.2 Stream Encryption	105
23.3 Select TLS Version	105
Chapter 24 Appendix	106
24.1 List of Applicable Power Adapter	106
24.2 Glossary	107
24.3 Frequently Asked Questions	108
24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?	108
24.3.2 Why is the video recorder notifying risky password after a network camera is added?	109
24.3.3 Why is the video recorder notifying the stream type is not supported?	109
24.3.4 How to confirm the video recorder is using H.265 to record video?	109
24.3.5 Why is the video recorder notifying IP conflict?	109
24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?	110
24.3.7 Why is the device not able to control PTZ camera via coaxitron?	110
24.3.8 Why does the PTZ seem unresponsive via RS-485?	110
24.3.9 Why is the video sound quality not good?	110
24.4 Notification for Corrosive Gas	111

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

Steps

1. Power on your device.
2. Select a system language.
3. Enter the admin password twice.



Caution

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

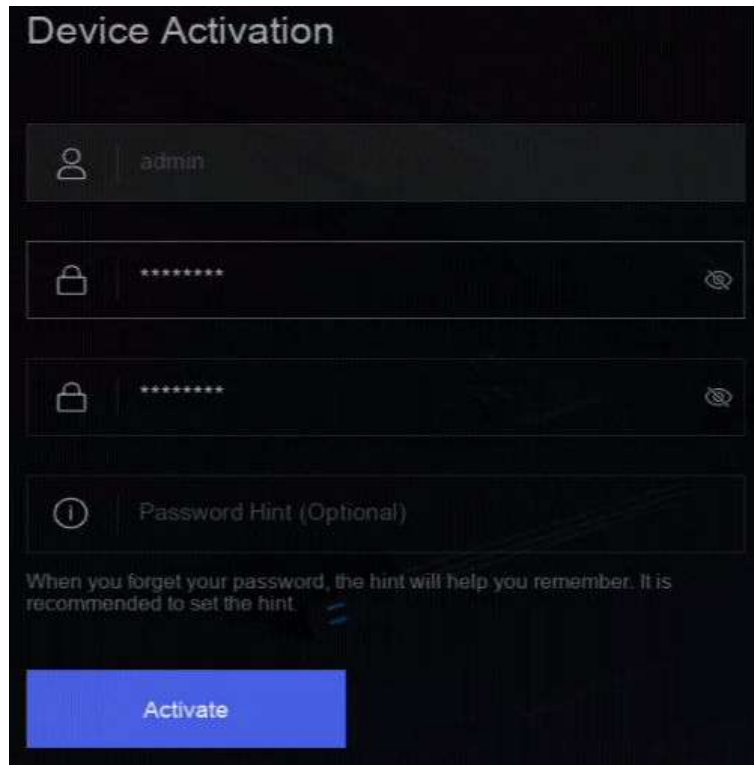


Figure 1-1 Activate via Local Menu

4. **Optional:** Enter a password hint. It will help you remember your password when you forget.
5. Click **Activate**.



Note

After the device is activated, you should properly keep the password.

-
6. **Optional:** Draw an unlock pattern.
 7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

1. Power on your device.
2. Right click to display the shortcut menu.
3. Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

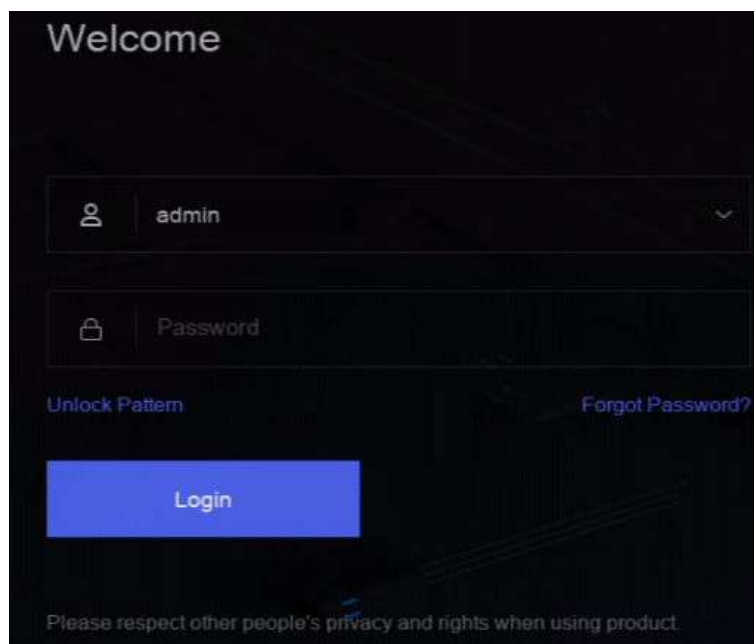


Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.

Note

- Unlock pattern is only available for admin user.
 - If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.
-

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

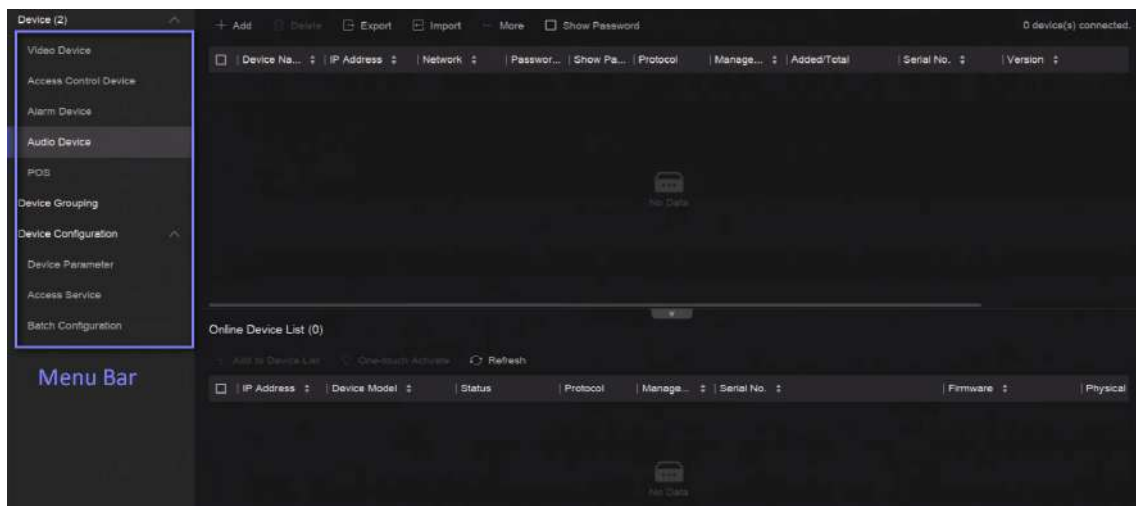


Figure 3-2 Menu Bar Example

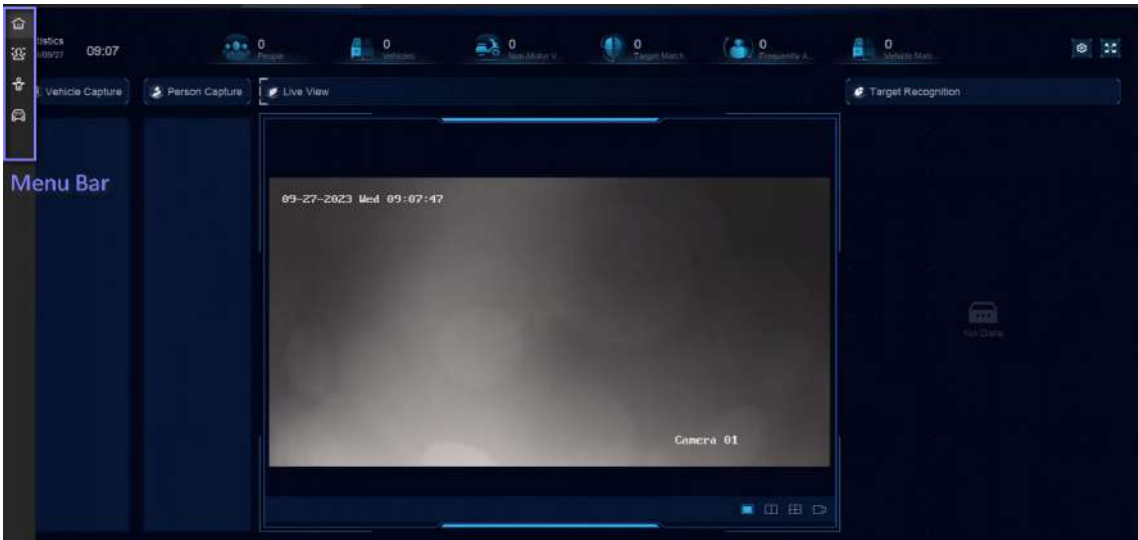


Figure 3-3 Human and Vehicle Detection Example of Application Center

Table 3-1 Interface Introduction

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab. Icon introduction : •  : Main menu. •  : Event center. Event alarms can be searched and viewed. •  : The download progress of each download task can be viewed here. •  : Shut down, log out, or reboot your device.
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.  Note For applications in Application Center, you can click  , or right click to display the menu bar.

Chapter 4 Network Settings

Network parameters, platform access settings, and network services are configurable.

4.1 Network Parameter Settings

You shall configure network parameters before using functions that require network access.

4.1.1 Configure TCP/IP

TCP/IP must be properly configured before you operate video recorder over network or access network devices.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **TCP/IP** .

Figure 4-1 TCP/IP Settings

2. Set **Working Mode** and **Select NIC**.

Multi-address

The parameters of the two NIC cards can be configured independently. You can select **LAN1** or **LAN2** in the NIC type field for parameter settings. You can select one NIC card as default route. And then the system is connecting with the extranet and the data will be forwarded through the default route.

Net-fault Tolerance

The two NIC cards use the same IP address, and you can set **Main NIC** to **LAN1** or **LAN2**. By this way, in case of one NIC card failure, the video recorder will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.



Note

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

If the DHCP server is available, you can enable **DHCP** to automatically obtain an IP address and other network settings from that server.

MTU

The maximum transmission unit (MTU) is the size of the largest network layer protocol data unit that can be communicated in a single network transaction.

Auto Obtain DNS Server

If **DHCP** is enabled. You can check **Auto Obtain DNS Server** to obtain **Preferred DNS Server** and **Alternate DNS Server**.

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click **Save**.

4.1.2 Configure DDNS

Dynamic domain name server (DDNS) maps dynamic user IP addresses to a fixed domain name server.

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **DDNS** .

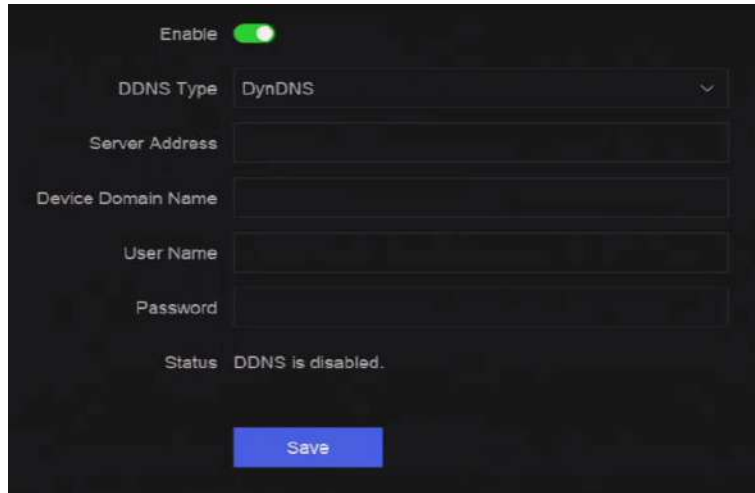


Figure 4-2 DDNS

2. Turn on **Enable**.
3. Select a DDNS type.
4. Set parameters, including service address, domain name, etc.
5. Click **Save**.

4.1.3 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly. Contact your Internet service provider for details about PPPoE service.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **PPPoE** .

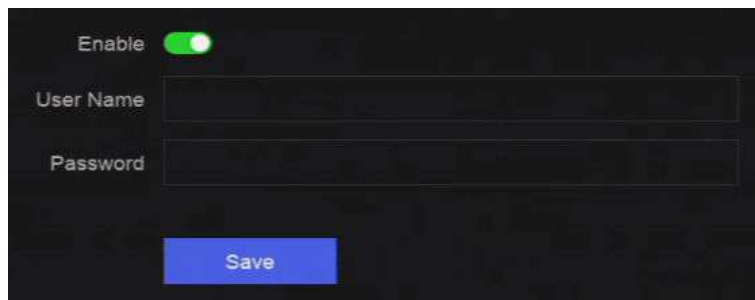


Figure 4-3 PPPoE

2. Turn on **Enable**.
3. Enter user name and password.
4. Click **Save**.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

1. Go to **System → System Settings → Network → Network → Other**.
2. Set **Multicast** parameters.



Note

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the CMS software, the multicast address must be the same as that of the device.

-
3. Click **Save**.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

Hik-Connect provides mobile phone application and platform service to access and manage your video recorder, which enables you to get a convenient remote access to the video security system.

Steps

1. Go to **System → System Settings → Network → Hik-Connect**.

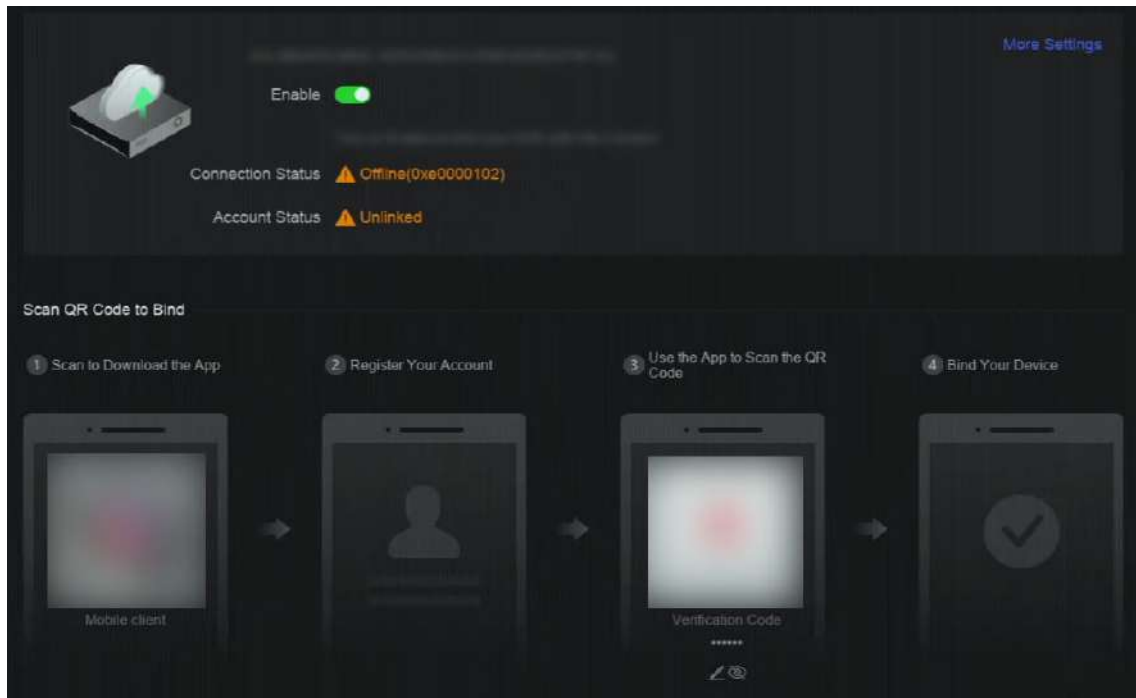


Figure 4-4 Hik-Connect

2. Turn on **Enable**, and the service terms will pop up.
3. Accept the service terms.
4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.
 - Download the app from <https://appstore.hikvision.com> .



Figure 4-5 Download Hik-Connect

5. Register an account at the app.
6. **Optional:** Click **More Settings** to enable **Stream Encryption**, **Platform Time Sync**, and **Adaptive Bitrate Streaming**, or edit **Server IP Address**.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

7. Click  to set verification code.
8. Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.



Note

If the device is already bound with an account, you can click **Unbind** to unbind with the current account.

Result

- If your device is connected with Hik-Connect, **Connection Status** will be **Online**.
- If your device is bound with a Hik-Connect account, **Account Status** will be **Linked**.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

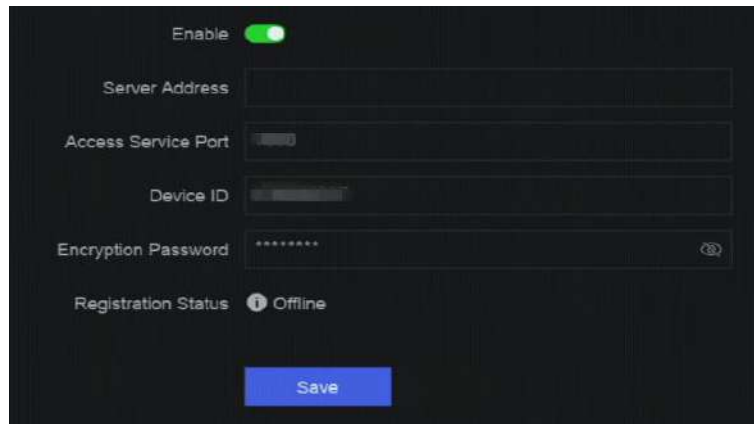
OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

1. Go to **System** → **System Settings** → **Network** → **Platform Access** → **OTAP** .



Enable ☒

Server Address

Access Service Port

Device ID

Encryption Password

Registration Status Offline

Save

Figure 4-6 OTAP

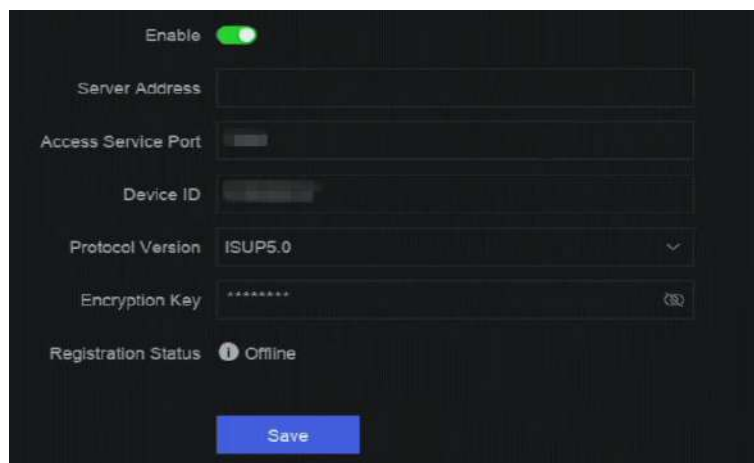
2. Turn on **OTAP**.
3. Set the parameters.
4. Click **Save**.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the third-party platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to **System → CX → System Settings → Network → Platform Access → ISUP**.



Enable ☒

Server Address

Access Service Port

Device ID

Protocol Version ISUP5.0

Encryption Key

Registration Status Offline

Save

Figure 4-7 ISUP

2. Turn on **Enable**.



Note

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click **Save**.

You can see the registration status (online or offline) after the device is restarted.

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to **System → System Settings → Network → Platform Access → SDK**.

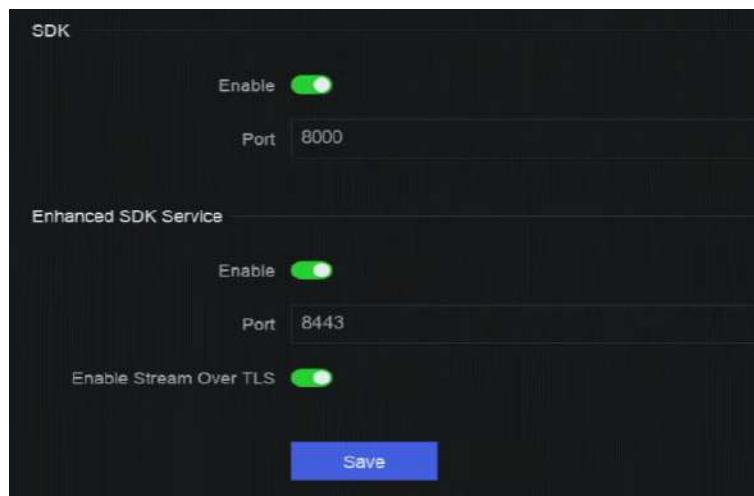


Figure 4-8 SDK Service

2. Configure **SDK** and **Enhanced SDK Service** according to your requirement.



Note

The port for **Enhanced SDK Service** is 8443 by default.

3. **Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
4. Click **Save**.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to **System → System Settings → Network → Platform Access → ISAPI** to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to **System → CX → System Settings → Network → Platform Access → ONVIF**.

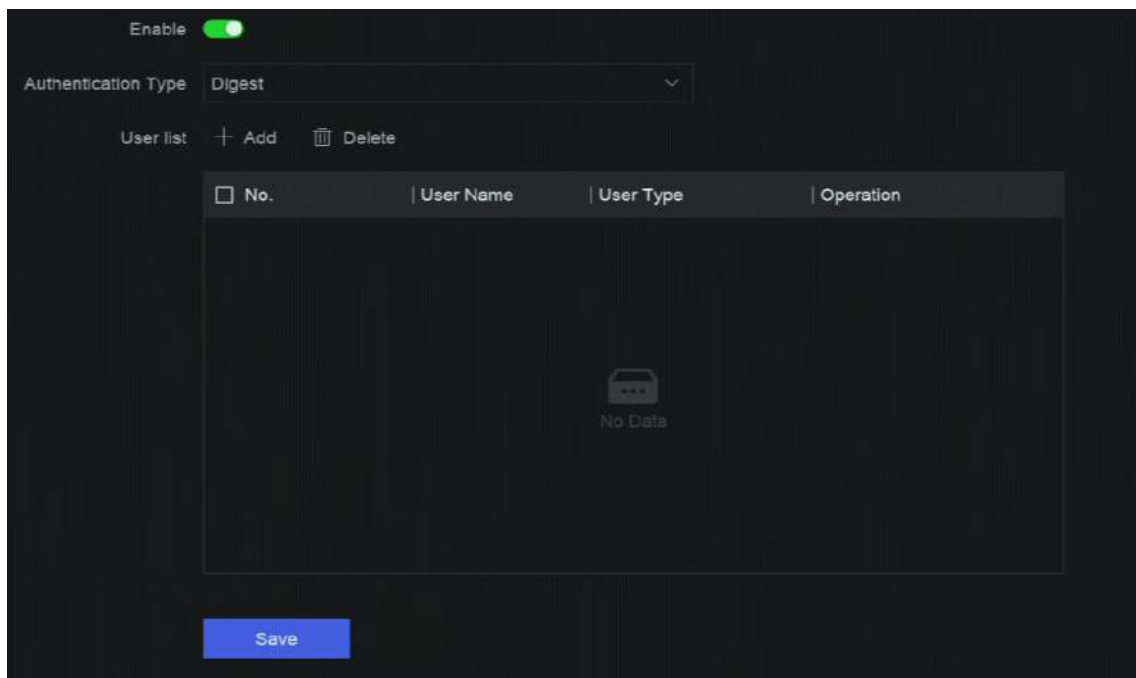


Figure 4-9 ONVIF

2. Turn on **Enable**.
3. Select an authentication type.
4. Click **Add** to add a user.
5. Set the user name and password.



Caution

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: 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

6. Click **Save**.
-

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to **System → System Settings → Network → Platform Access → Log Server**.

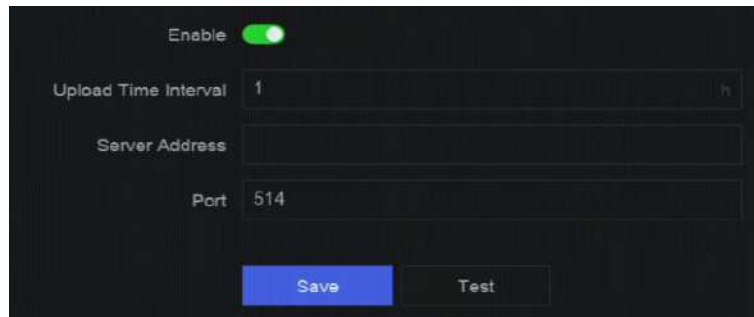


Figure 4-10 Log Server

2. Turn on **Enable**.
3. Set **Upload Time Interval**, **Server IP Address**, and **Port**.
4. **Optional**: Click **Test** to check if parameters are valid.
5. Click **Save**.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **HTTP(S)**.

The screenshot shows a configuration page for Network Video Recorder with three main sections: HTTP, HTTPS, and HTTP/HTTPS Authentication. The HTTP section has an 'Enable' toggle (green) and a 'Port' field (80). The HTTPS section has an 'Enable' toggle (green), a note 'Ensure the client TLS version is enabled.' with a link to 'TLS Settings', a 'Port' field (443), and an 'Enable HTTPS Browsing' toggle (grey). The HTTP/HTTPS Authentication section has a dropdown for 'Authentication Type' (Digest) and a dropdown for 'Digest Algorithm' (MD5). A note states 'Authentication type and digest algorithm are valid for both HTTP and HTTPS.' and a 'Save' button is at the bottom.

Section	Setting	Value
HTTP	Enable	On
	Port	80
HTTPS	Enable	On
	Port	443
	Enable HTTPS Browsing	Off
	Authentication Type	Digest
HTTP/HTTPS Authentication	Digest Algorithm	MD5

Figure 4-11 HTTP(S)

2. **Optional:** Turn on HTTP or HTTPS.
3. View or edit **Port** of HTTP or HTTPS.
4. Set **HTTP/HTTPS Authentication**.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click **Save**.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

1. Go to **System → System Settings → Network → Network Service → RTSP**.



Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

Two authentication types are selectable, if you select **Digest**, only the request with digest authentication can access the video stream by RTSP via the IP address. For security reasons, it is recommended to select **Digest** as the authentication type.

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click **Save**.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **WebSocket(s)** .
2. Turn on **Enable**.
3. Set **Port**.
4. Click **Save**.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ (Universal Plug and Play), and manual mapping. UPnP™ can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

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.

Steps

1. Go to **System → System Settings → Network → Network Service → NAT**.

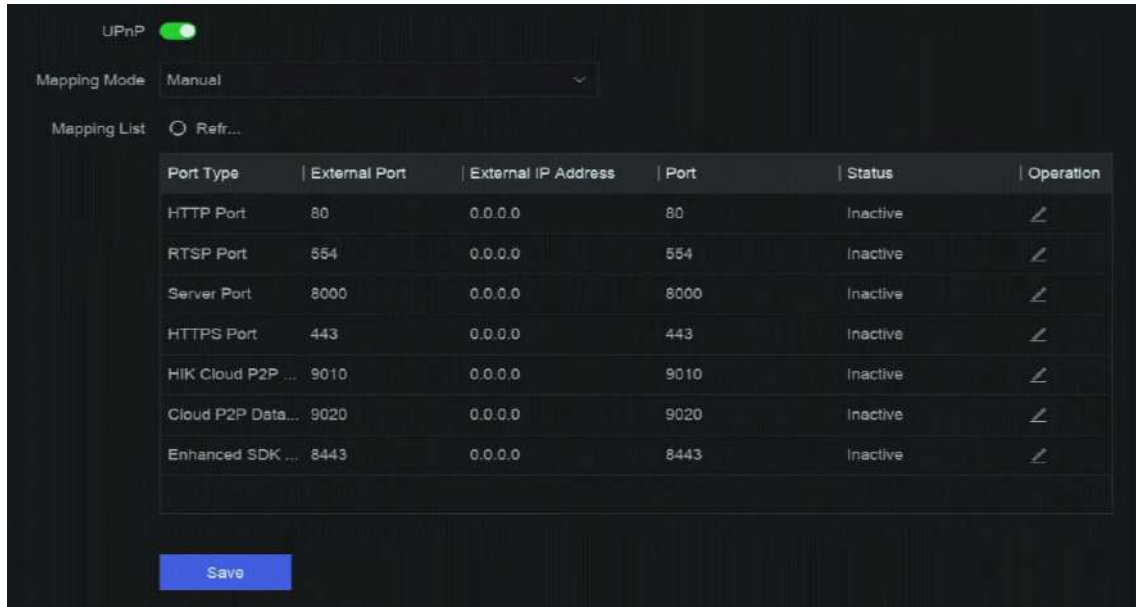


Figure 4-13 Port Mapping (NAT)

2. Turn on **Enable**.
3. Set **Mapping Mode**.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If **Mapping Mode** is selected as **Manual**, click  to edit corresponding ports.



Note

- The value of the RTSP port number 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.
- **External Port** indicates the internal port number for port mapping in the router.

5. Click **Save**.

What to do next

Enter the virtual server settings page of router, then fill in the blank of internal/external source port with the internal/external port value, and other required contents.

4.3.5 Configure IoT

You can configure the network port through which the NVR will receive alarms from a security control panel.

Go to **System → System Settings → Network → Network Service → IoT** to enable the function and configure the port number.



Note

The port number you configured here should be the same as the alarm sending port on the security control panel.

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to **System → System Settings → User Management** .

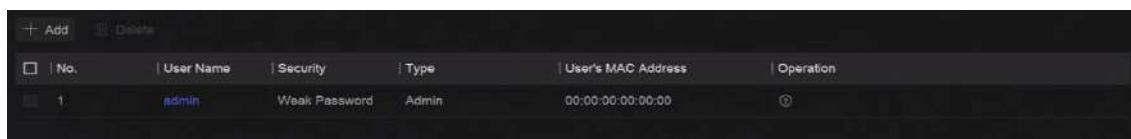


Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description
	Set account security.
Add	Add a new guest or operator user.
	Delete the selected user.

Note

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to **System → Device Access → Device → Video Device → Online Device List**.
2. Select the device(s) from the list.

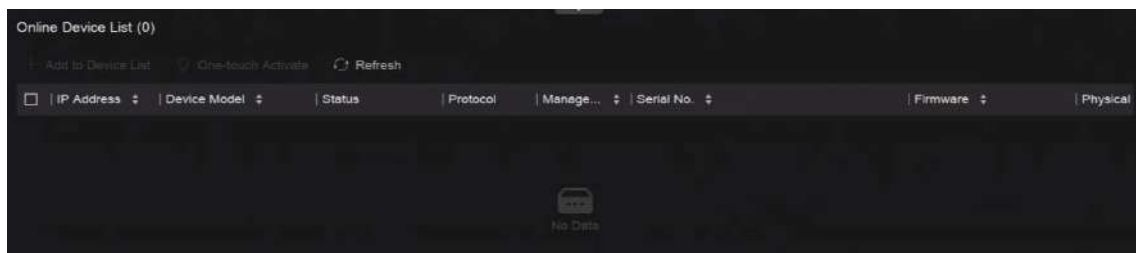


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click **Add to Device List**.



Note

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with that of your video recorder.
- Ensure the network connection is valid and correct.
- Ensure the network camera is activated.

Steps

1. Go to **System → Device Access → Device → Video Device**.

Figure 6-2 Add Network Camera Manually

2. Click **Add**.
3. Enter network camera parameters.

Use Channel Default Password

If it is enabled, the video recorder will add the camera by the set channel default password.

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

4. **Optional:** Click **Continue to Add** to add other network cameras.
5. Click **Add**.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to **Configure PoE (Power over Ethernet) Interface** for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

1. Go to **System → Device Access → Device Configuration → Access Service → OTAP Service**.
2. Turn on **Enable**.
3. Set **OTAP Server Port** and **Encryption Key**.
4. **Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
5. Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



Note

The solar-powered camera OTAP protocol parameters shall be the same as the device.

6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from **Online Device List**, and click **Quick Add**.
7. Click **Add** in **System → Device Access → Device → Video Device**, select **Protocol** as **OTAP**, and click **Add**.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to **Configure Recording Schedule**.

6.1.5 Add Network Camera via Custom Protocol

For network cameras that are not using standard protocols, you can configure custom protocols to add them. The system provides 8 custom protocols.

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

1. Go to **System → Device Access → Device → Video Device**.
2. Click **More → Custom Protocol Management**, or **Add → Protocol Management**.

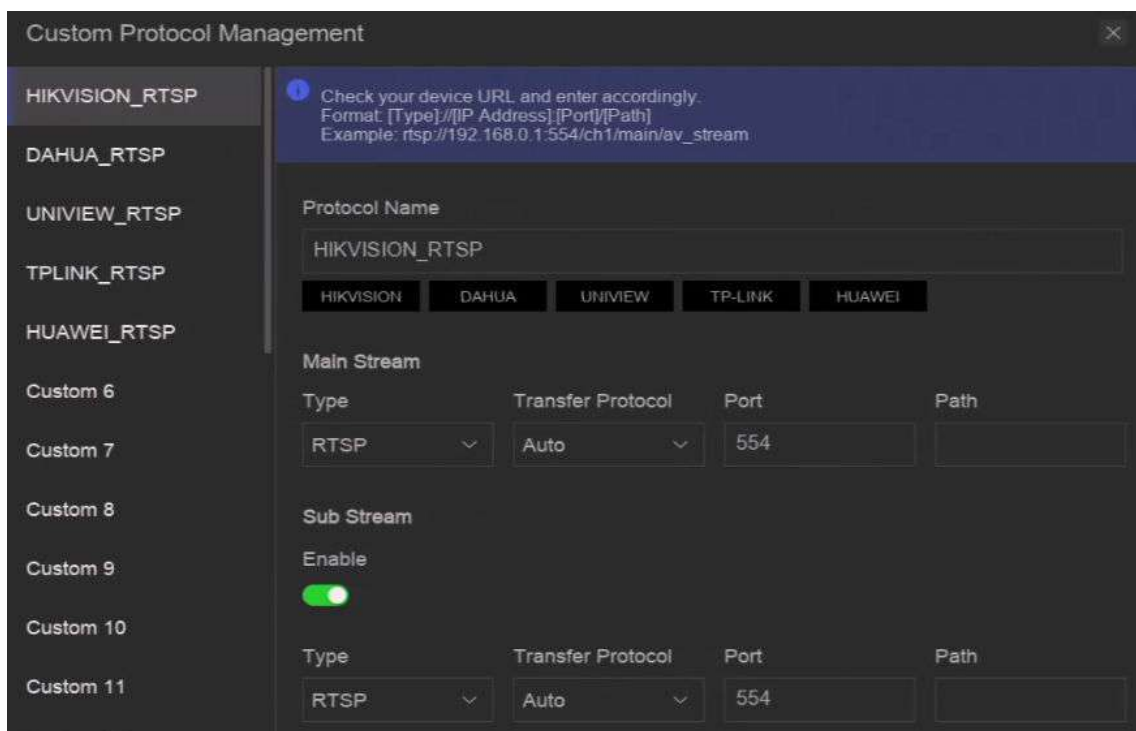


Figure 6-3 Add Network Camera via Customized Protocol

3. Select a protocol type at the left side.
4. Set protocol parameters.

Type

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

Transfer Protocol

3 types are selectable, including **Auto**, **UDP**, and **RTP Over RTSP**.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and sub-stream. The general format is *[Type]://[IP Address]:[Port]/[Resource Path]*, for example, *rtsp://192.168.0.1:554/ch1/main/av_stream*.



Note

- **Protocol Name** and **Path** can be automatically generated if you click a brand name below **Protocol Name**.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.

-
5. Click **OK**.
 6. Click **Add** in **System** → **Device Access** → **Device** → **Video Device** to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

1. Go to **System** → **Device Access** → **Device** → **Video Device**.
2. Click **Import** to import the configuration file in USB flash drive.
3. Set the folder path.
4. Click **Confirm**.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with [Access Video Device](#).

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with **Access Video Device** . If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

1. Go to **System → Device Access → Device → POS** .
2. Click **Add** to add a POS device.

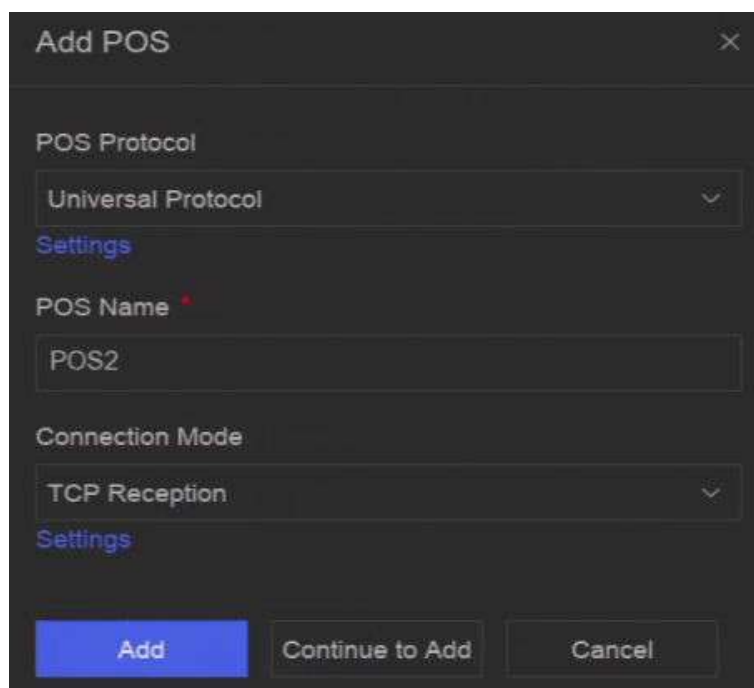


Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported.

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click **Add.**



Note

After a POS device is add, you can click  in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System → Device Access → Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to **System** → **Device Access** → **Device Grouping**.

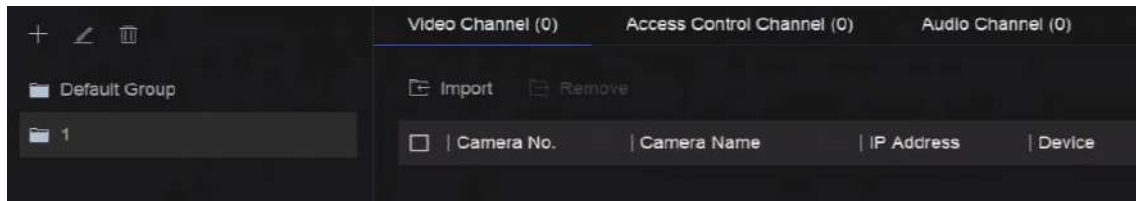


Figure 7-1 Device Grouping

2. Click  to add a group.

Note

After a group is added, you can click  /  to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.
-

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

1. Go to **System → Device Access → Device → Video Device**.
2. Click **More → Auto Switch to H.265**.
3. Enable this function.
4. Click **Save**.

8.2 Configure Display Settings

Configure the OSD (On-Screen Display), image settings, exposure settings, day/night switch settings, etc.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Display Settings**. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

Customize the image parameters including the brightness, contrast, and saturation for the live view and recording effect.

Exposure Time

Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.

Day/Night Switch

The camera can be set to day, night, or auto switch mode according to the surrounding illumination conditions.

Backlight

Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you should set the WDR value.

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Video Parameters**. Select a camera, and configure parameters as your desire.

Main Stream

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your video quality and image size. Comparing with the sub-stream, the main stream provides a higher quality video with higher resolution and frame rate.

Sub-Stream

Sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

It refers to the number of frames captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask**.

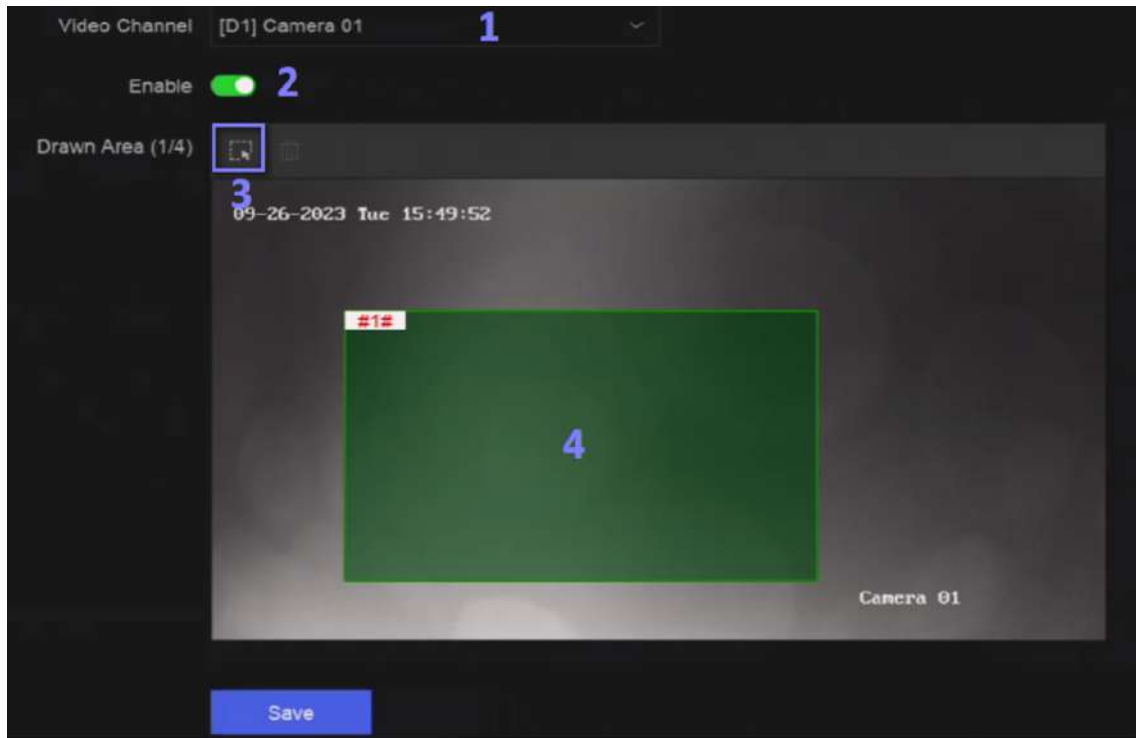


Figure 8-1 Privacy Mask

2. Select a camera.
3. Turn on **Enable**.
4. Draw mask areas on the preview window. The areas will be marked with different frame colors.



Note

Up to 4 privacy mask areas can be configured and the size of each area can be adjusted.

5. Click **Save**.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System → Device Access → Device Configuration → Device Parameter → Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

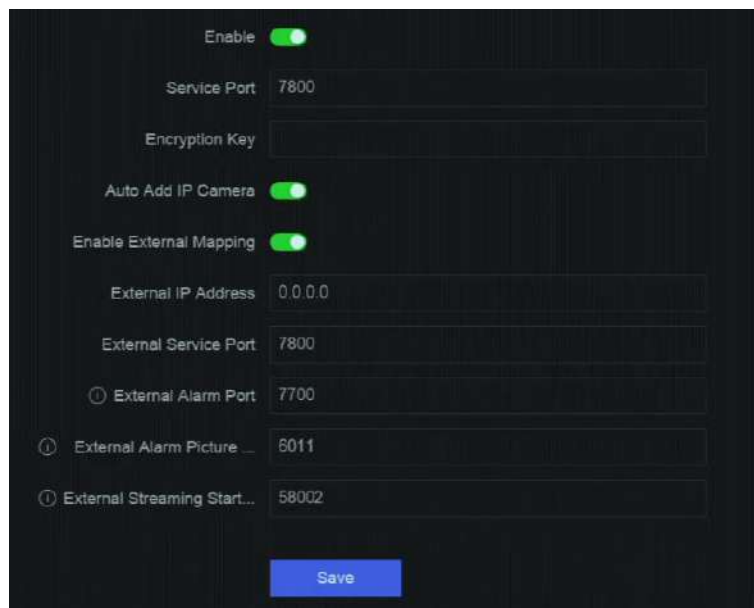
OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to **System → Device Access → Device Configuration → Access Service → OTAP Service**.



The screenshot shows the OTAP Service configuration page. At the top, there is an 'Enable' toggle switch which is turned on. Below it are several configuration fields: 'Service Port' (7800), 'Encryption Key' (empty), 'Auto Add IP Camera' (toggle on), 'Enable External Mapping' (toggle on), 'External IP Address' (0.0.0.0), 'External Service Port' (7800), 'External Alarm Port' (7700), 'External Alarm Picture' (8011), and 'External Streaming Start...' (58002). A blue 'Save' button is located at the bottom right of the form.

Figure 8-2 Configure OTAP Service

2. Turn on **Enable**.
3. Set the parameters.
4. Click **Save**.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

1. Go to **System → Device Access → Device Configuration → Batch Configuration**.

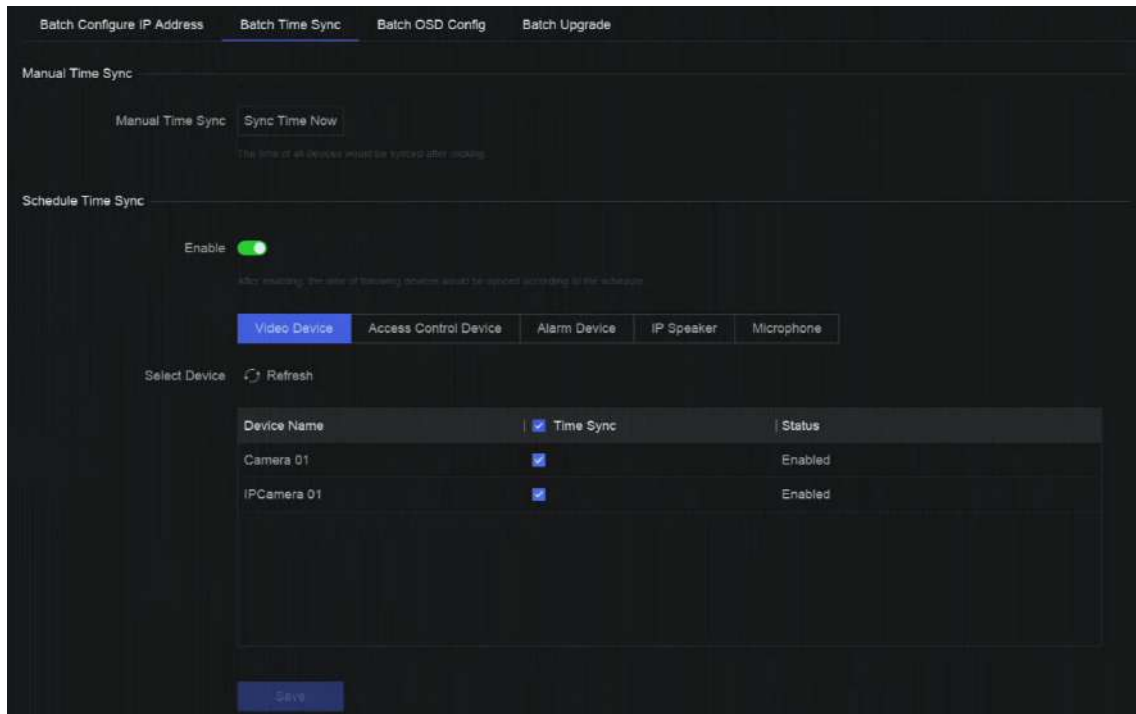


Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule.

3. For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

1. Go to **System → Device Access → Device Configuration → PoE**.
2. Enable **Plug-and-Play** function of PoE interfaces according to your requirement.

3. Select the device type as **IP Speaker** or **Camera**.

4. If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.



Note

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click **Save**.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

A newly installed hard disk drive (HDD) must be initialized before using. You can format HDD, repair database, and view HDD status through HDD management interface.

Before You Start

Ensure the HDD is properly installed to your device.

Steps

1. Go to **System → Storage Management → Storage HDD → Storage HDD**.



HDD No.	Free Space (GB)	Capacity (GB)	Status	Type	Property	Operation
1	166	466	Sleeping	Local	R/W	[Icon]
3	3685	3726	Sleeping	Local	R/W	[Icon]
5	3685	3726	Sleeping	Local	R/W	[Icon]

Figure 9-1 Manage HDD

2. **Optional:** Perform the following operations as your desire.

Add Network HDD Add a NAS or IP SAN.

Format Format the selected HDD.

Repair Database Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Note

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out the drive, or shut down the device during the process.



Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed

across the drives in one of several ways called "RAID levels", based the redundancy and performance required.



Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

Table 9-1 HDD Requirement for Each RAID Type

RAID Type	Required Number of HDDs
RAID0	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8



Note

- The function is only available for certain models.
 - When array exception event occurs, the corresponding linkage actions can be configured in **System → System Settings → Exception** .
-

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- **Storage Mode** is set to **Quota** in **System → Storage Management → Storage Mode** .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Enable Array Mode**, or enable **Array Mode**.

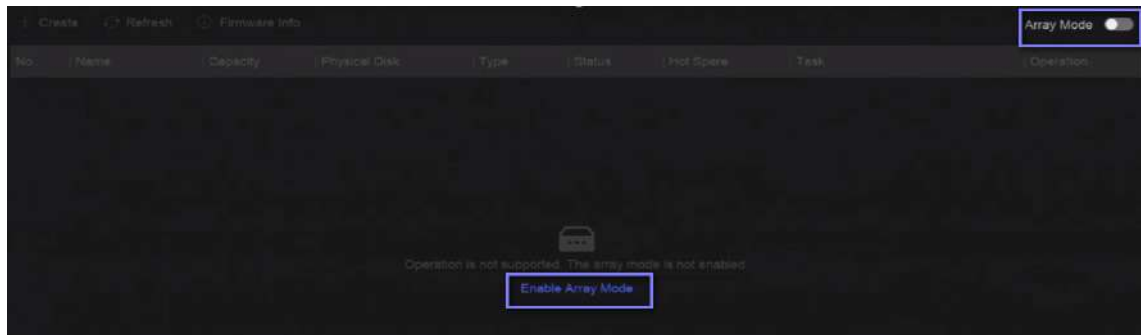


Figure 9-2 Enable RAID

- Wait for the device to restart.
- Go to **System → Storage Management → Storage HDD → Array Management** again.

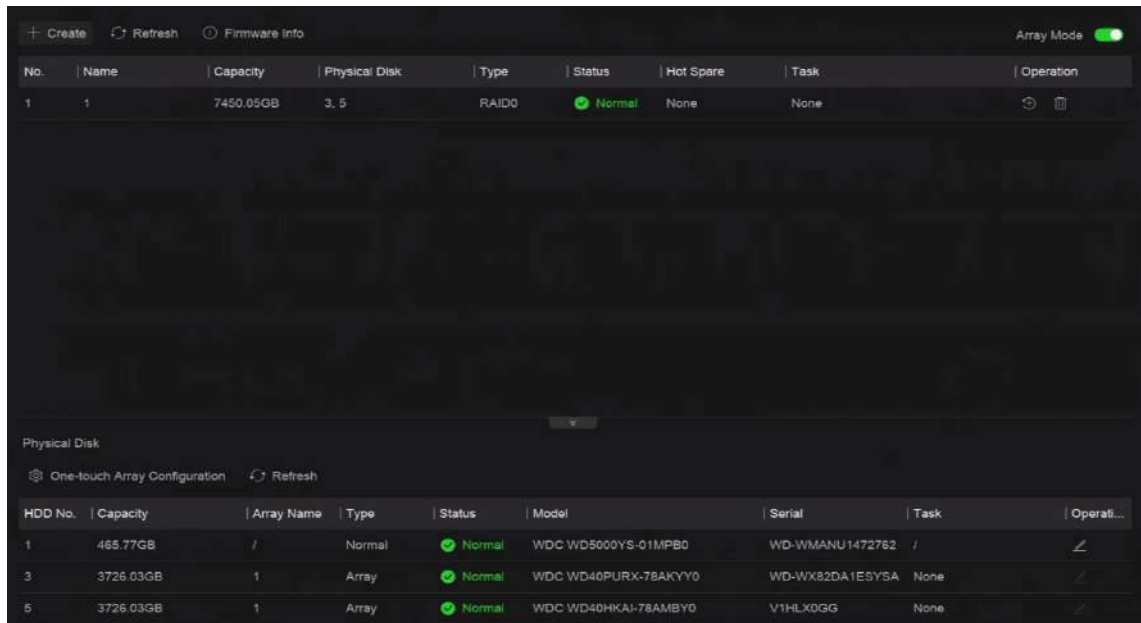


Figure 9-3 Array Management

- Create an array.

Creation Method

Description

One-touch Array Configuration

Click **One-touch Array Configuration**.



Note

By default, the array type created by one-touch configuration is RAID 5.

Manual Creation

Click **Create** to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

9.2.2 Rebuild Array

The array status includes **Functional**, **Degraded**, and **Offline**. To ensure the high security and reliability of the data stored in an array, take immediate and proper maintenance of the arrays according its status.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management**.
2. Rebuild an array.

Table 9-2 Rebuilding Method

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click  in Operation column under Physical Disk to set a hot spare disk. When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.  Note After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array. Go to System → Storage Management → Storage HDD → Array Management, and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to **System → Storage Management → Storage HDD** to click  to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Firmware Info**.
3. **Optional**: Set **Back Ground Task Speed**.

9.3 Configure Storage Mode

Steps

1. Go to **System → Storage Management → Storage Mode** .

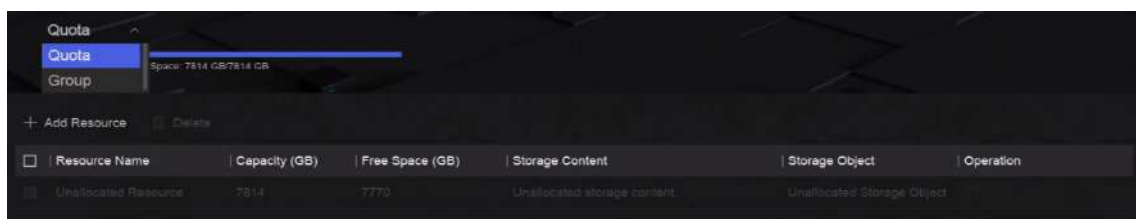


Figure 9-4 Storage Mode

2. Select **Quota** or **Group**.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

3. Set corresponding parameters.
 - **Quota**: Allocate space for storage objects.
 - **Group**: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to **System → Storage Management → Advanced Settings** .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.  Note - You can click  during live view or playback to add a tag. - For searching tag videos, go to  → Backup → By Tag.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon  displayed at the upper-right corner.

Chapter 10 Schedule Configuration

The device will follow the schedule to store files to the disk.

10.1 Configure Schedule Template

After a schedule template is configured, you can use the template as the recording schedule.

Steps

1. Go to **System → System Settings → Template Configuration → Holiday Schedule** .
2. Click **Add**.

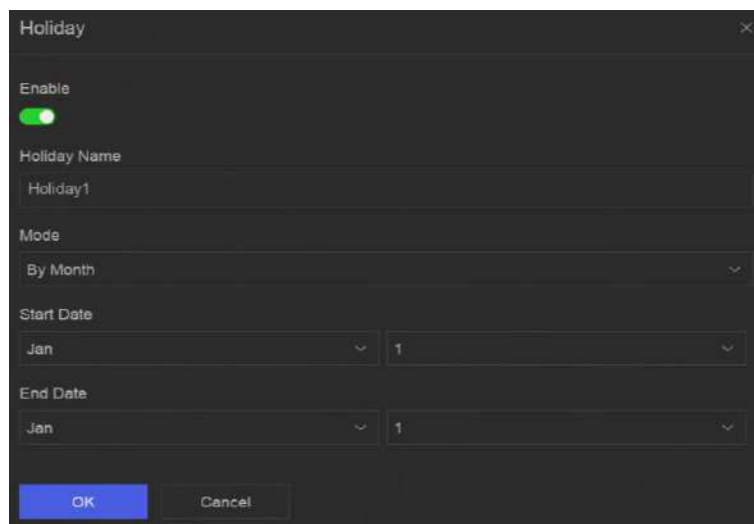


Figure 10-1 Add Holiday

3. Turn on **Enable**.
4. Configure the holiday.



Note

After holidays are configured, you will be able to set the holiday schedule independently. Holiday schedule has higher priority than normal schedule (from Mon to Sun).

-
5. Set **Storage Schedule**.
 - 1) Click **Storage Schedule**.
 - 2) Select a template name.

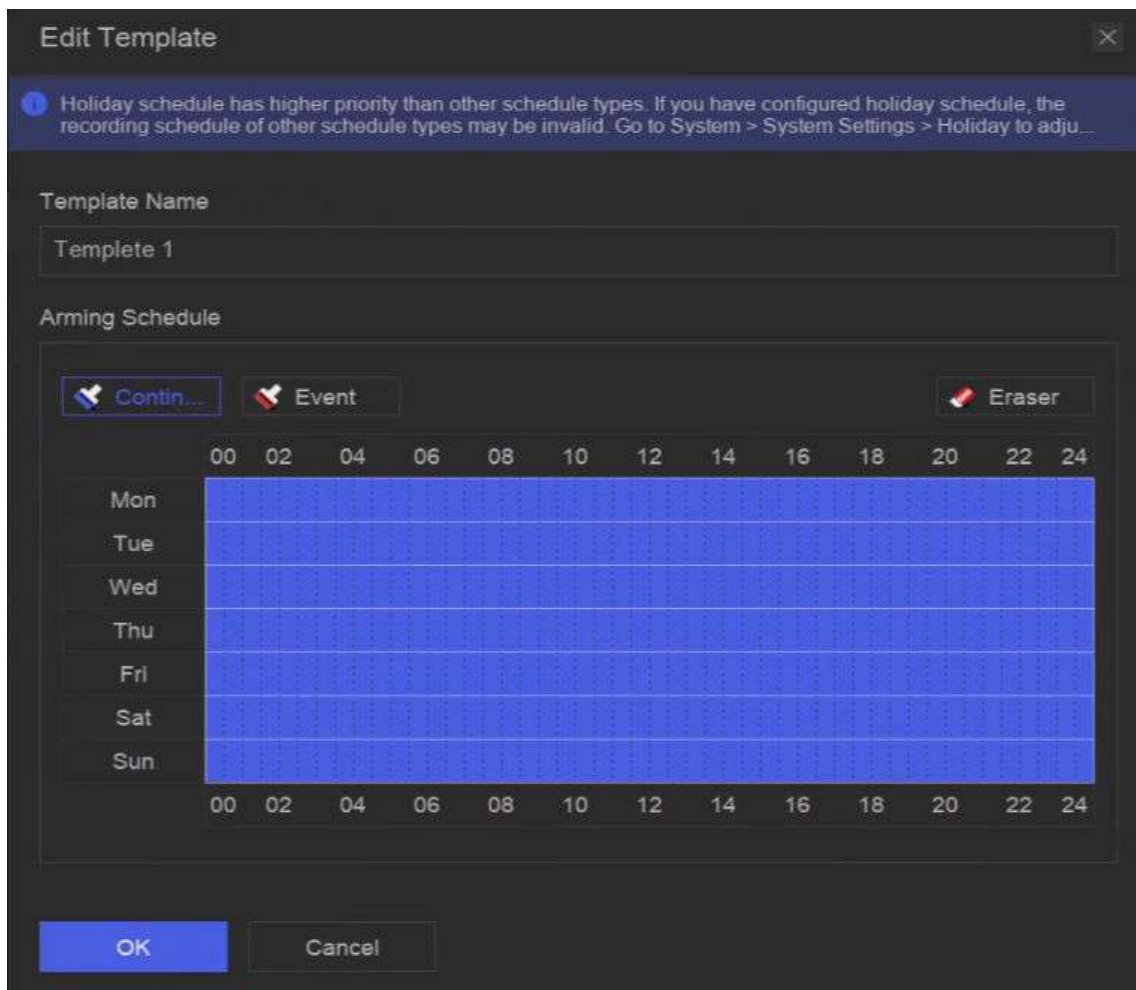


Figure 10-2 Edit Template

- 3) Select a recording type. For example, **Event**.
- 4) Drag the cursor on time bar to draw the schedule.



Note

- After moving the cursor on time bar, you can also click **00:00-24:00**  to set specified time schedule.
- You can click **Eraser** to clear schedule.



Note

You can also click **Configure Template** to configure template in **System → Storage Management → Storage Schedule → Video Recording / Picture Capture / Audio Recording**.

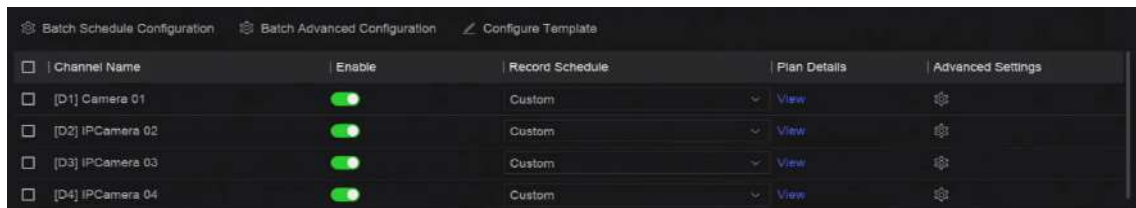
6. Click **OK**.

10.2 Configure Recording Schedule

The camera would automatically start/stop recording according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Video Recording** .



Channel Name	Enable	Record Schedule	Plan Details	Advanced Settings
[D1] Camera 01	☒	Custom	View	Settings
[D2] IPCamera 02	☒	Custom	View	Settings
[D3] IPCamera 03	☒	Custom	View	Settings
[D4] IPCamera 04	☒	Custom	View	Settings

Figure 10-3 Video Recording Configuration

2. Turn on **Enable** for a camera.
3. Select a schedule type.



Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

4. Click **View** to view the schedule.



Figure 10-4 View Schedule

5. **Optional:** Click  under **Advanced Settings** to set other advanced parameters.

Table 10-1 Advanced Parameter Description

Parameter	Description
Record Audio	Enable or disable audio recording.  Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.

Parameter	Description
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

- Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
- Click **Save**.

10.3 Configure Picture Capture Schedule

The device would automatically capture live pictures according to the schedule.

Steps

- Go to **System → Storage Management → Storage Schedule → Picture Capture**.

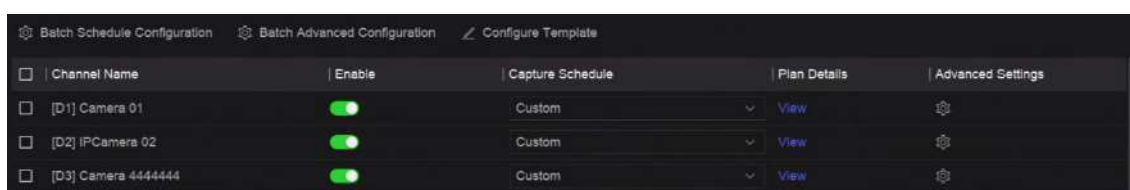


Figure 10-5 Picture Capture Configuration

- Turn on **Enable** for a camera.
- Select a schedule type.



Note

If you set **Capture Schedule** as **Custom**, you can drag the cursor on time bar to set customized picture capture schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

- Click **View** to view the schedule.



Figure 10-6 View Schedule

5. Click under **Advanced Settings** to set advanced picture parameters.

Table 10-2 Advanced Parameter Description

Parameter	Description
Capture Delay	The duration for picture capture.
Resolution	Set the resolution of the picture to capture.
Picture Quality	Set the picture quality to low, medium or high. High picture quality requires more storage space.
Interval	The time interval of capturing each live picture.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

10.4 Configure Audio Recording

The device would automatically record audios according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Audio Recording**.
2. Turn on **Enable** for a channel.
3. Select a schedule type.



Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

-
4. Click **View** to view the schedule.
 5. **Optional:** Click under **Advanced Settings** to set other advanced parameters.

Table 10-3 Advanced Parameter Description

Parameter	Description
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the channel records 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 recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

Chapter 11 Live View

11.1 Configure Live View Layout

Live view displays the video image of each camera in real time.

Steps

1. Go to **Live View**.
2. Click  at the lower-right corner.
3. Select a window division type, or click **Custom** to customize a new type as your desire.
4. Move the cursor on **Default View** in **View**.
5. Click  at the right side of **View**.
6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
7. Click .

11.2 GUI Introduction

You can view live image, play live audio, capture pictures, perform instant playback, etc.

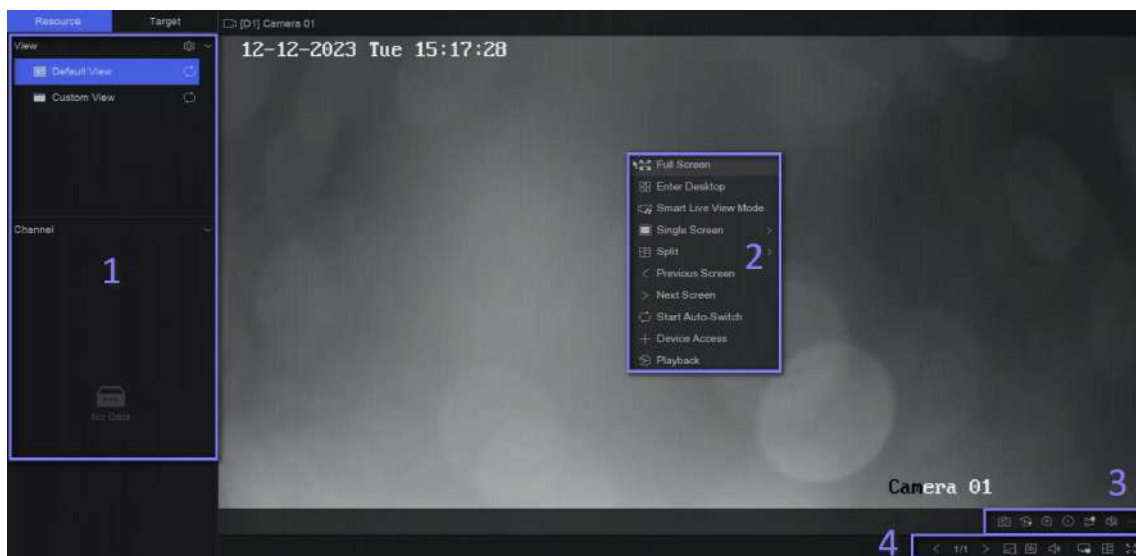


Figure 11-1 Live View (Type 1)

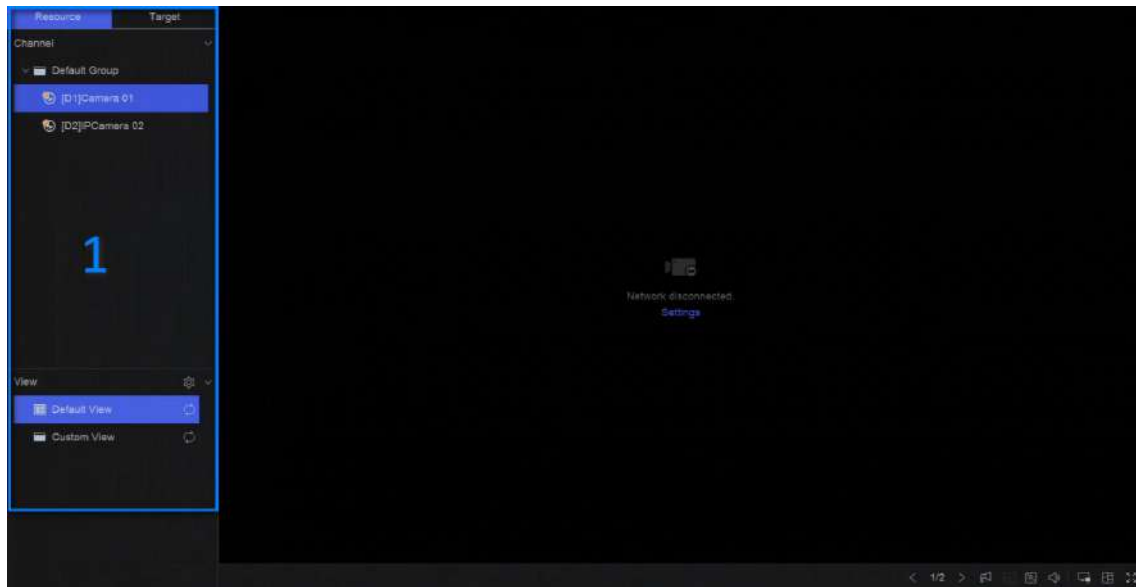


Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window. If you click Target , you can view live target detection results in the list, and click  to configure the corresponding settings.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	Channel tool bar. - Click  to add a tag go the channel. After adding, you can go to  → Backup → By Tag to search videos by tag. - You can select  → Show VCA Info to display rule frames.
4	Live view tool bar. Functions like Voice Broadcast , Display VCA Info and Switch Output can be performed here.

Note

- You can scroll up/down your mouse to turn to previous/next screen.
- If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Table 11-2 PTZ Operation

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click  .
		Call a preset: Click  .
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click  .
		3. Add presets for the patrol. 4. Click OK . Call a patrol: Click  .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	Set a pattern: 1. Click  .
		2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click  .

Note

If the PTZ panel cannot be used, please click  to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



Figure 12-1 Playback

Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	Channel tool bar. - Click  to add a tag to the channel. After adding, you can go to  → Backup → By Tag to search videos by tag. - Click  to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to  → Backup → By Tag to search videos by lock.

No.	Description
	- Select  → Dual-VCA to search videos that can trigger the corresponding event rule. Refer to the event configuration steps for details of each event type.  Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Scream to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. - You can select  → Show VCA Info to display rule frames.
5	Playback timeline. - Position the cursor on the timeline, drag the timeline to position to a certain time. - Period marked with blue bar contains video. Red bar indicates the video in the period is event video. - Scroll up/down to zoom out/in timeline.
6	Playback tool bar. - Click  to set normal video and smart video (the video that contains smart data) playback strategy. - Click  (Smart Search), then follow the pop-up tips to draw event rule and search videos that can trigger the corresponding event rule. The operations are similar with Dual-VCA function. - Click  to perform AcuSearch function. Refer to AcuSearch for details. - Click  /  to show videos that contain human/vehicle.  Note In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types.

12.2 Normal Playback

Play back videos for a channel. For certain devices, synchronous playback may be allowed for several channels.

Steps

1. Go to **Playback** → .
2. Select channel(s) in the list at the left side.



Group playback: Select a group in the list, and channels in the group can be played back.

3. Select a date in the calendar.



The blue triangle at the calendar date corner indicates there are available videos.

4. **Optional:** Play back videos that contain human or vehicle targets.
 -  : Videos that contain human would be marked in red.
 -  : Videos that contain vehicle would be marked in red.

12.3 Event Playback

When you select the event playback mode, the system will analyze and mark videos that contain the motion detection, line crossing detection, or intrusion detection information

Before You Start

- Ensure the camera has enabled **Dual-VCA**. You can enable it via the camera web browser interface in **Configuration** → **Video/Audio** → **Display Info. on Stream** .
- Ensure your video recorder has enabled **Save Camera VCA Data** in **Storage management** → **Advanced Settings** .

Steps

1. Select **Playback** → .
2. Select a date in the calendar.



The blue triangle at the calendar date corner indicates there are available videos.

3. Click  → **Dual-VCA** at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
4. Click **Search**.

Videos meet the detection rule requirement will be marked in red.
5. Click  to set normal video and smart video (the video that contains smart data) playback strategy.



Note

If **Dual-VCA** is not used, red segments in progress bar means the smart videos are generated by the original event.

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

1. Go to **Playback** →
2. Select a camera from the camera list.
3. Select a date on the calendar.
4. Click **Search**.
The retrieved video will be divided into one-hour slices for playback.
5. **Optional:** Select an one-hour slice and click to divide it into one-minute slices for playback.

12.5 Sub-Period Playback

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

Steps

1. Go to **Playback** →
2. Select a camera.
3. Set the start time and end time.
4. Click **Search**.

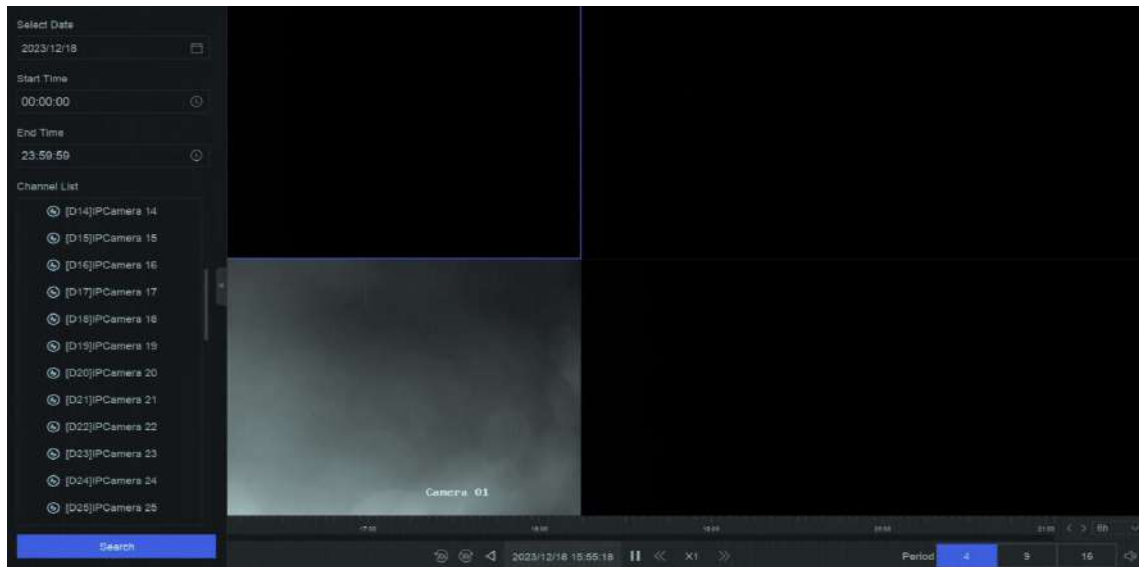


Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.



Note

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.

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Basic Event / Generic Event** .
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Configuration	
Motion Detection	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. • AI by NVR: The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects. • AI by Camera: The motion detection event will be analyzed by camera. • Detection Target: Human and Vehicle are selectable, apart from false alarms, only the	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.

Event Name	Event Description	Rule Configuration	
		selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-2 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.2 Perimeter Protection

Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

Configure Line Crossing Detection

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Steps



Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center →  → Event Configuration → Perimeter Protection**.

2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Line Crossing**.
6. Turn on **Enable**.

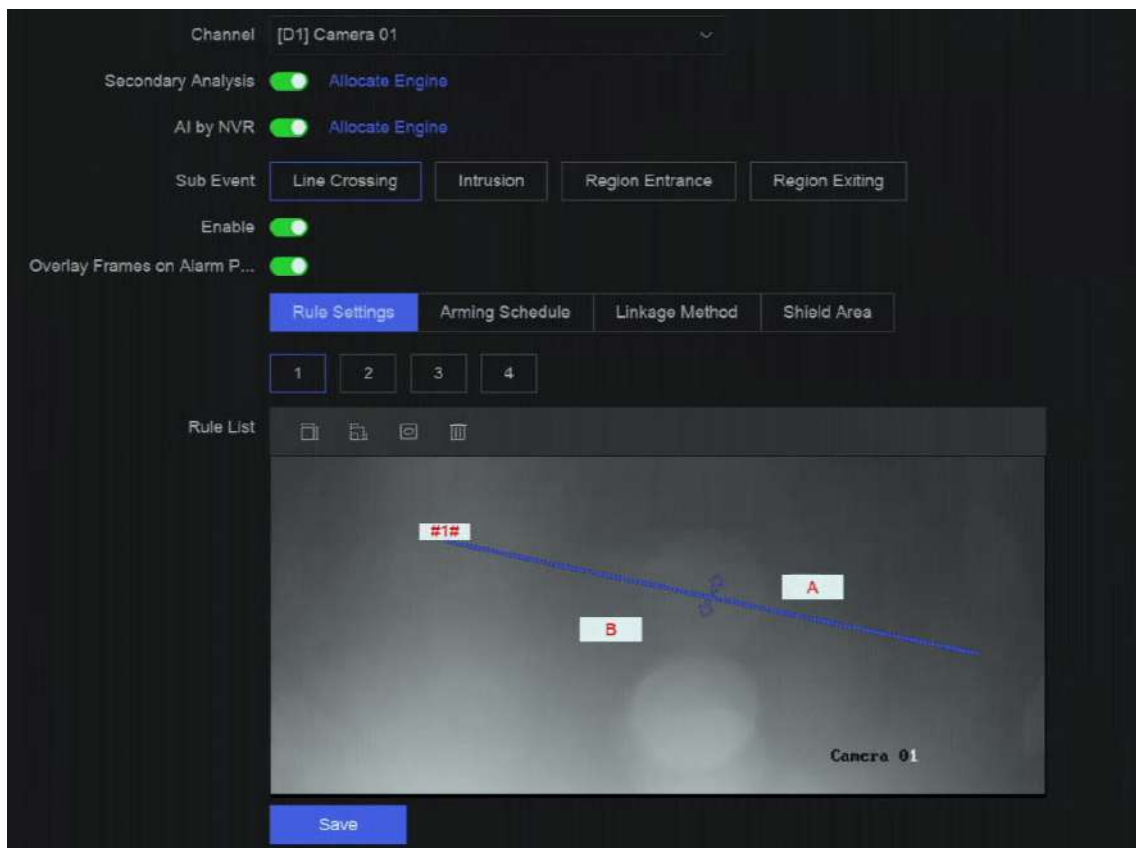


Figure 13-1 Line Crossing Detection

7. Click **Rule Settings** to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set **Direction**, **Sensitivity**, and **Detection Target**.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions 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.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click  /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-3 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Intrusion Detection

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

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Intrusion**.

6. Turn on **Enable**.

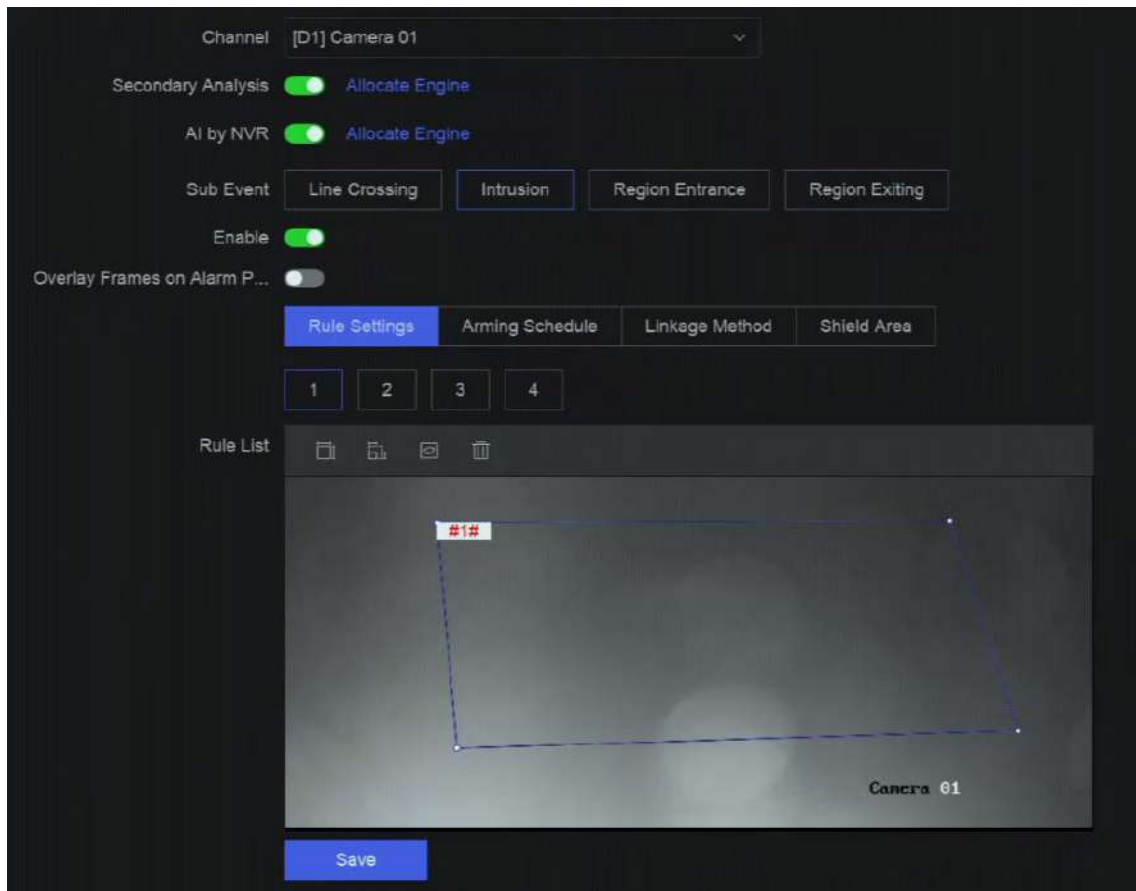


Figure 13-2 Intrusion Detection

7. Click **Rule Settings** to detection rules.

1) Select a rule number. For example, select **1**.

2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.

3) Set **Time Threshold**, **Sensitivity**, and **Detection Target**.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Click  /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.

5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-4 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Steps



Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.



Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Region Entrance**.
6. Turn on **Enable**.

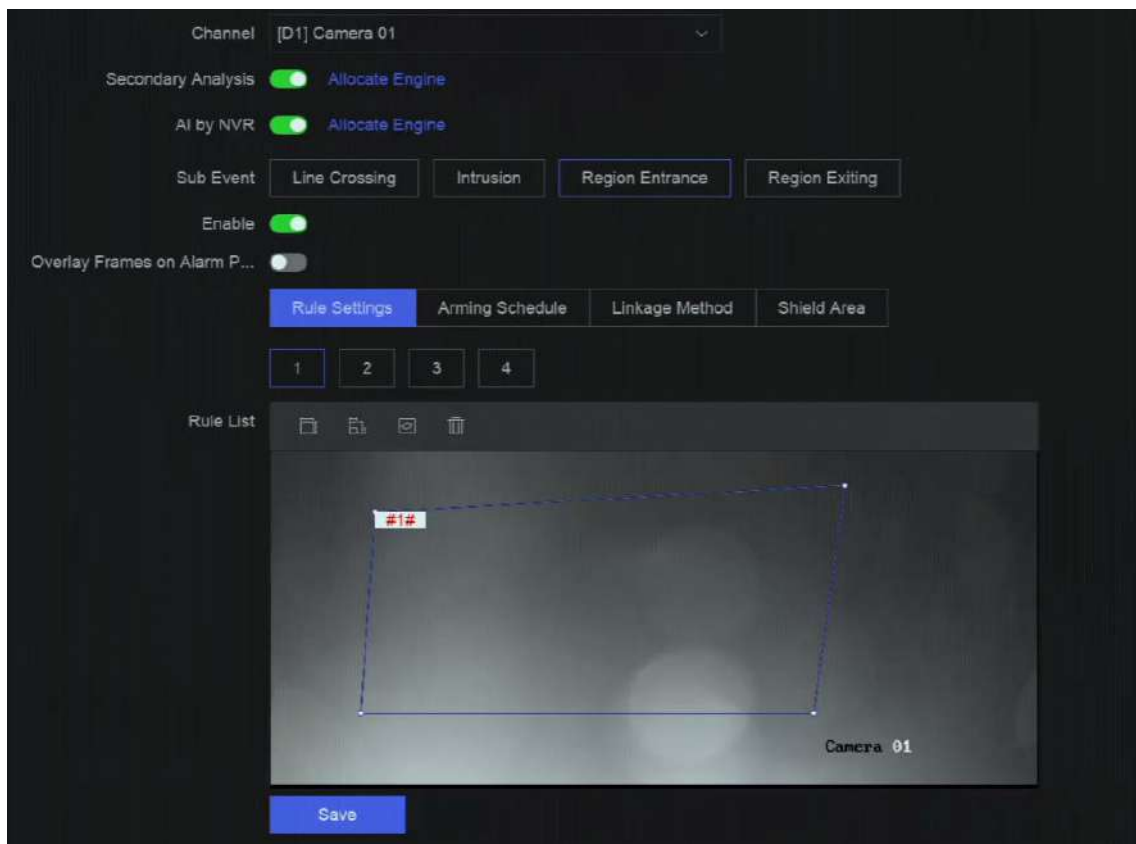


Figure 13-3 Region Entrance Detection

7. Click **Rule Settings to detection rules.**

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set **Sensitivity** and **Detection Target**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule to select an arming schedule type.**



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

9. Click **Linkage Method to set linkage methods.**

Table 13-5 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.

3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.



Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Region Exiting**.

6. Turn on **Enable**.

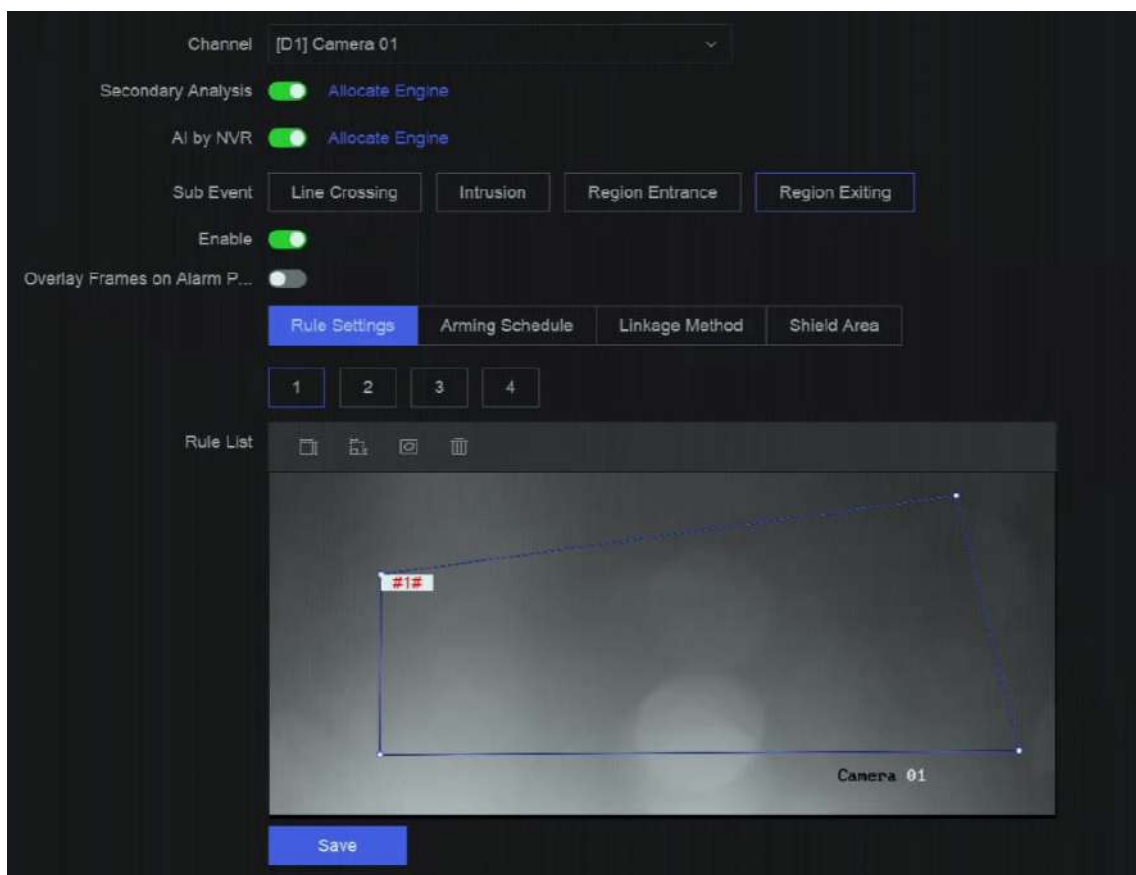


Figure 13-4 Region Exiting Detection

7. Click **Rule Settings** to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set **Sensitivity** and **Detection Target**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

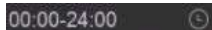
Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional**: Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-6 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System →

Linkage Method	Description
	Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Abnormal Behavior Event** .
2. Select a camera
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10]. Sensitivity Similarity of the background image to the object. The higher the value is, more
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions	

Event Name	Event Description	Rule Configuration
	can be taken when the alarm is triggered.	easily the detection alarm will be triggered.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	d. Optional: Repeat the above steps to set another one.
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage . Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **Event Center → Event Configuration → Smart Settings → Algorithm Configuration → Algorithm Management**.

Steps

1. Go to **Event Center →  → Event Configuration → Target Event**.
2. Select a camera.
3. Select an event.
4. Turn on **Enable**.
5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can be triggered when a human face is detected.	-
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	- Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). - Supports configuring prompts for failed and succeeded comparisons.
Stranger Detection	Faces not in the list library appearing in the video will be identified as strangers.	- Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). - Supports configuring the prompt for detecting strangers.
Multi-Target-Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Thermal Event** .
2. Select a camera.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature Detection	An alarm would be triggered when the temperature exceeds the threshold value.
Perimeter Protection	Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-11 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System →

Linkage Method	Description
	Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Alarm Input Event** .
2. Select an alarm input name.

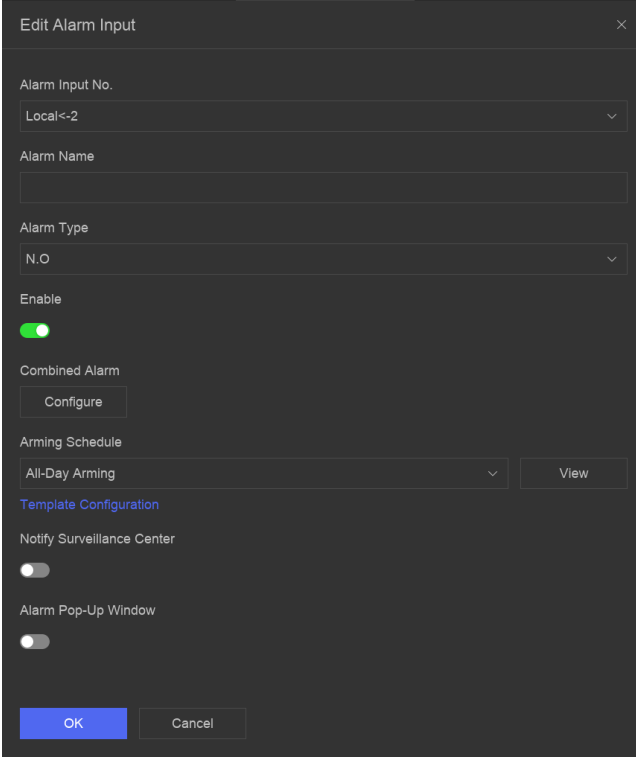


Figure 13-5 Configure Alarm Input

Note

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

3. Edit **Alarm Name**.
4. Set **Alarm Type**.
N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

5. Turn on **Enable**.

6. **Optional**: If you select **Local<-1** in Step 2, select the processing method.

- Select **Process Alarm Input**, and then you can set the corresponding arming schedule, linkage methods, etc.



Note

The operations below are all available when you select this processing method.

- Select **Quick Disarming**, and then linkage methods of all events will be disabled.

7. Click **Configure** to configure combined alarm.

- 1) Select a channel.
- 2) Select combined alarm events such as motion detection and video tampering detection.
- 3) Click **OK**.

The combined alarm will be triggered when it receives alarms from both alarm input and events.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-12 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Click **Save**.

13.1.7 Audio Analysis Event

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Audio Analysis**.
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-13 Audio Analysis Event

Event Name	Event Description	Rule Configuration
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	Sudden Increase of Sound Intensity Detection Detects a steep sound increase in the scene. Sudden Decrease of Sound Intensity Detection Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered. Sound Intensity Threshold It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

- Click **Linkage Method** to set linkage methods.

Table 13-14 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

- Click **Save**.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- Go to **Event Center** → → **Event Configuration** → **Linkage Configuration** or **System** → **Event Configuration** → → **Event Configuration** → **Linkage Configuration**.
- Click **Email** to configure email parameters.

Table 13-15 Email Linkage

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click **Audio Management** to manage audio files for alarm linkage.



Note

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.



Note

- This linkage action is only available for few event types.
- The uploaded audio file should be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.

5. Click **Alarm Output** to set alarm output parameters.



Note

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, **Local->1** means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

- If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.



Note

This linkage action is only available for few event types.

- Click **Security Control Panel** to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

- Go to **Event Center** → → **Event Configuration** → **Linkage Configuration** or **System** → **Event Configuration** → → **Event Configuration** → **Linkage Configuration**.

Batch Schedule Configuration		Disarming Template Configuration			
☐ Channel Name	☐ Allow Disarming ⓘ	Disarming Status	Disarming Method	Disarming Template	Details
☐ [D1] Camera 01	☒	Disabled	Quick Disarming	Mute Disarming	
☐ [D2] IPCamera 02	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D3] IPCamera 03	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D4] IPCamera 04	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D5] IPCamera 05	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D6] IPCamera 06	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D7] IPCamera 07	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D8] IPCamera 08	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D9] IPCamera 09	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D10] IPCamera 10	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D11] IPCamera 11	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D12] IPCamera 12	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D13] IPCamera 13	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D14] IPCamera 14	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D15] IPCamera 15	☐	Disabled	Quick Disarming	Mute Disarming	

Figure 13-6 Disarming Configuration

- Select channel(s) that are allowed for disarming.
- Click **Batch Schedule Configuration**.
- Turn on **Enable**.
- Select **Disarming Template**. Only two types are available



Note

Currently, only two template types are available and each template parameters cannot configured.

6. Click **OK**.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center** → → **Event Configuration** → **Batch Configuration** or **System** → **Event Configuration** → → **Event Configuration** → **Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

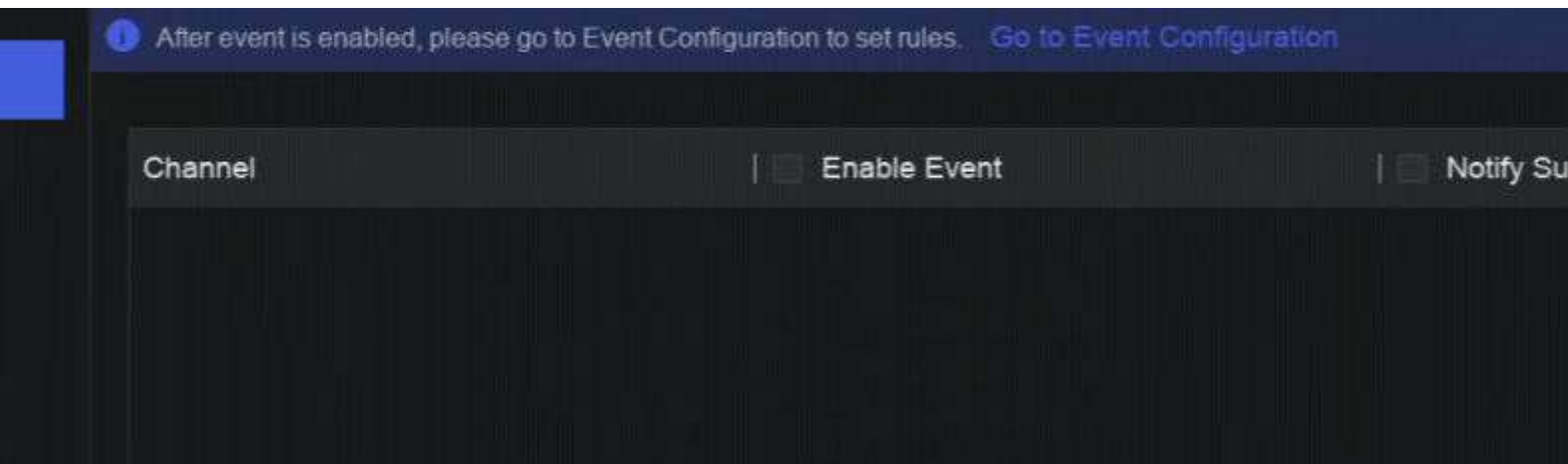


Figure 13-7 Batch Configuration

13.5 Event Search

You can search event files like videos and pictures according to the searching condition.

Steps

1. Go to **Event Center** → .

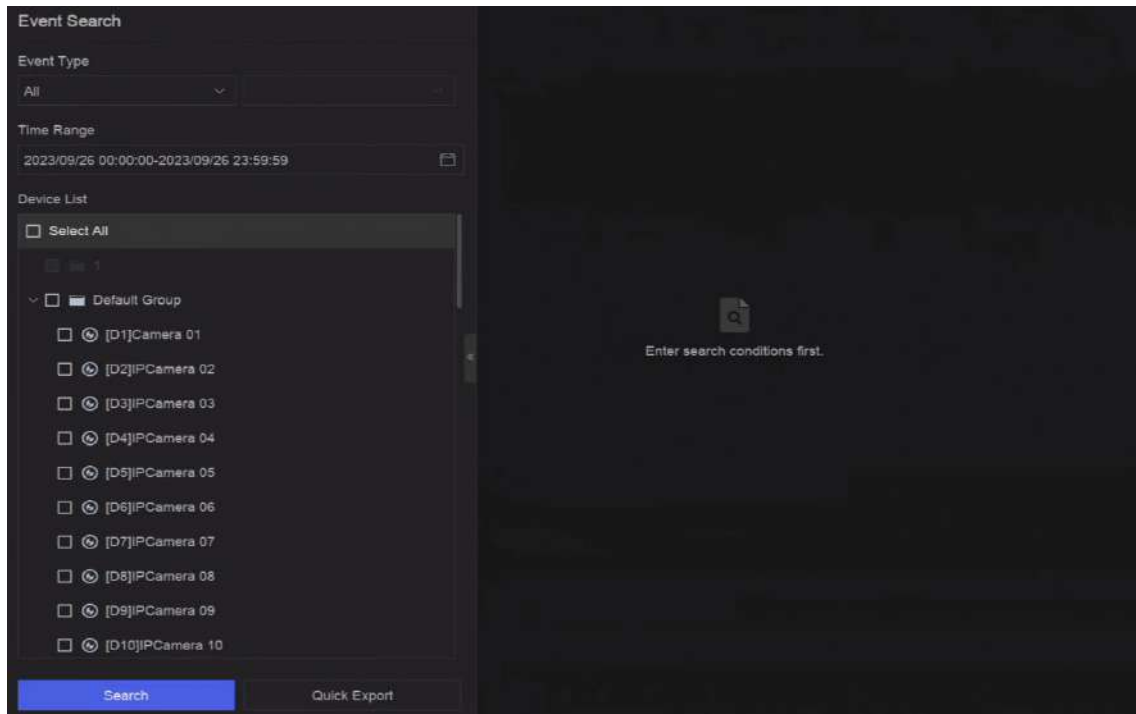


Figure 13-8 Event Search

2. Specify detailed conditions, including event type, time, channel, etc.
3. Click **Search**.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

1. Go to **Event Center** → .
2. Click **Real-Time Alarm**.
3. Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

4. Click **Playback**, and the alarm recording video would be played back.
5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to **Backup**.

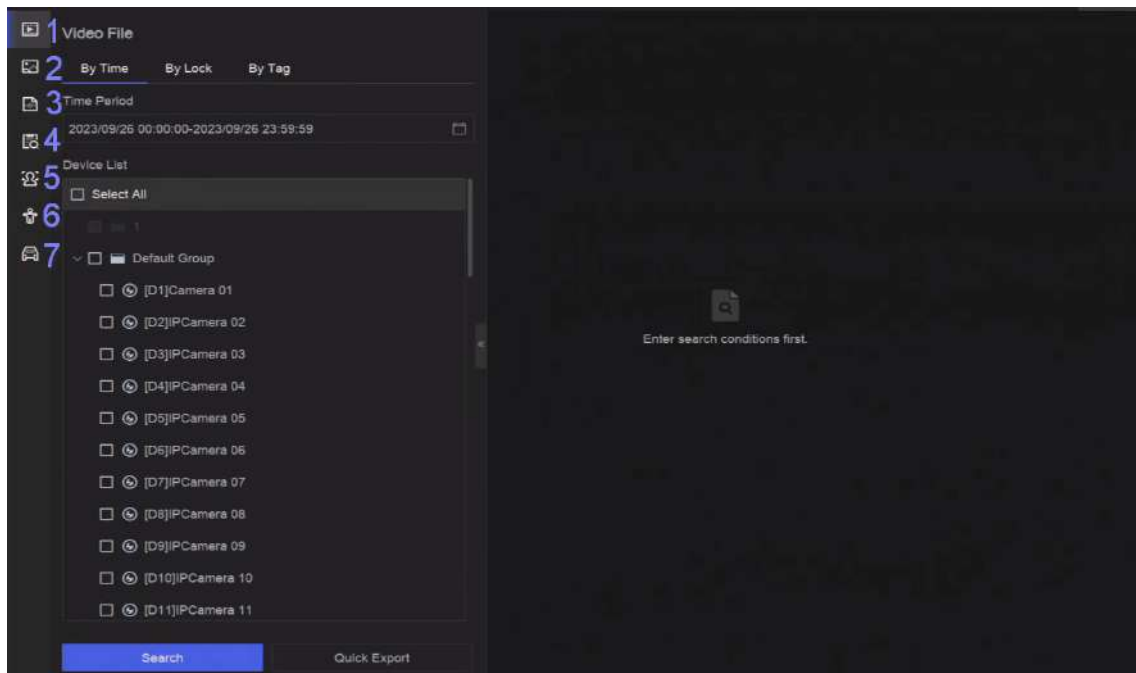


Figure 14-1 Search and Backup

2. Choose a searching method from at the left side as your desire, 7 types are supported.



Note

The searching conditions would vary according to the selected searching method.

3. Set the searching conditions.
4. Click **Search**.

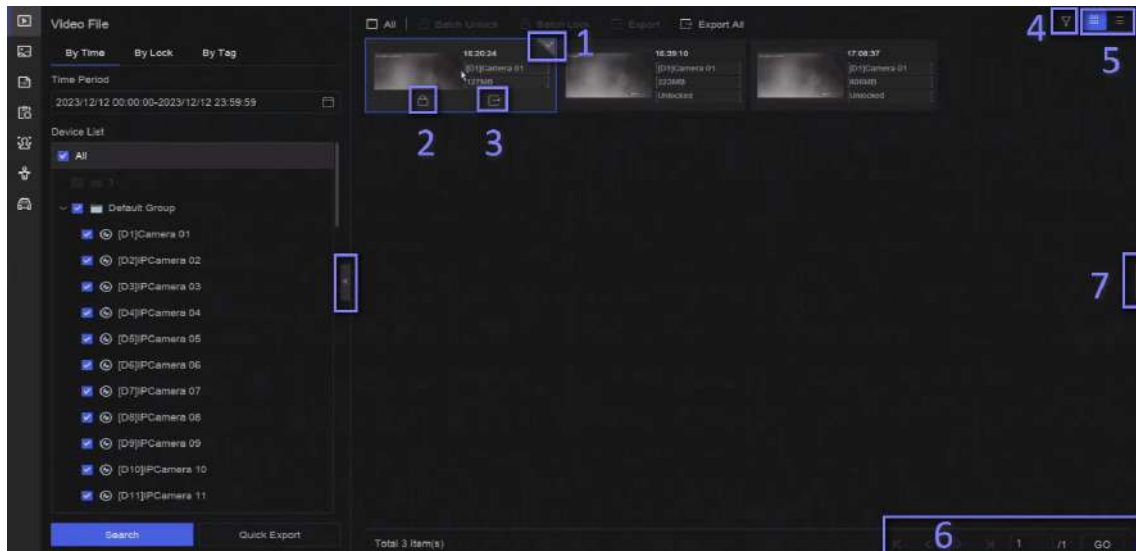


Figure 14-2 Searching Result

5. Optional: Perform the following operations.

- 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - 3 Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - 5 Use the tool bar at the top to switch display effect.
 - 6 Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6.** Insert a USB flash drive to the device for backup.
- 7.** Export files to the USB flash drive.
- Select file(s) in the result list and click **Export**.
 - Click **Export All** to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

1. Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable AcuSearch algorithm.
 - **AI by Camera:** The camera will perform the AcuSearch analysis.
 - **AI by NVR:** The device will perform the AcuSearch analysis, and engine resource is required for analysis.
2. Go to Live View or Playback, and click  at the lower-left corner during video playing.



Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** () to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking  , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.

-
3. Click  of the selected target.



Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

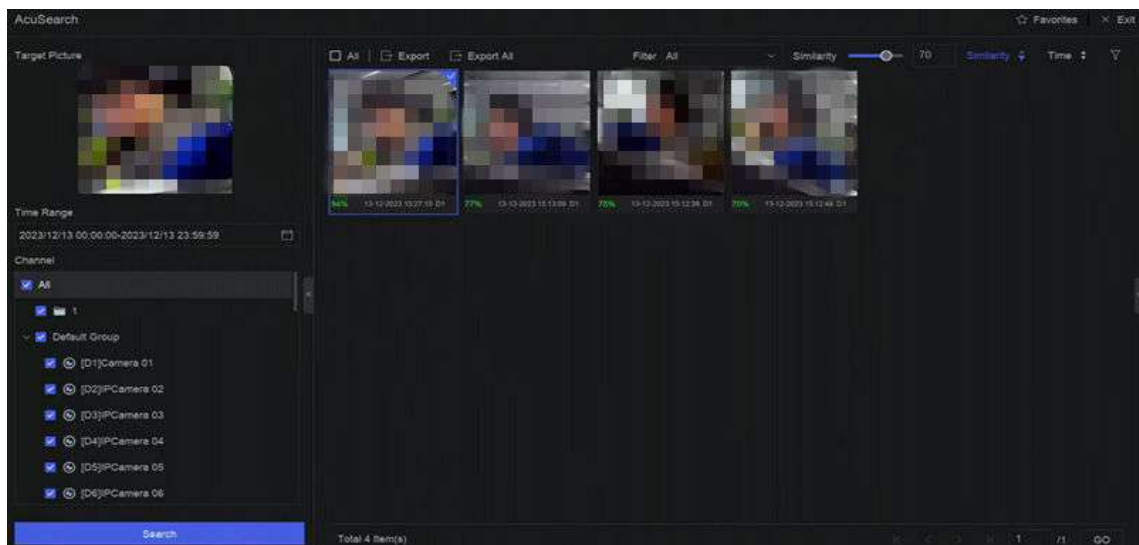


Figure 15-2 AcuSearch Result

5. **Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
6. **Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

Algorithms are used for device engines to analyze different smart functions. Smart function would be usable after allocating the corresponding algorithm to an engine.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Algorithm Management** or **Event Center → Event Configuration → Smart Settings → Algorithm Management**. The available algorithms would be listed, and you can click the required algorithm to link engine(s).

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Engine Status** or **Event Center → Event Configuration → Smart Settings → Engine Status**. If you need to switch the algorithm, refer to ***Algorithm Management***.

16.3 Task Plan Management

You can view the task status in task configuration. Smart analysis results are used for filtering the pictures when searching interested human body and vehicle pictures.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Task Plan Management** or **Event Center → Event Configuration → Smart Settings → Task Plan Management**. For **Non-Real-Time Target Comparison**, you can view the progress of each day.

Task status mainly includes 3 conditions: **Disabled**, **Waiting**, and **Enabled**.

Disabled

No analysis task is enabled on the camera.

Waiting

The analysis task of the camera is enabled. Device is waiting to analyze data.

Enabled

The analysis task of the camera is enabled and device is analyzing data of the camera.

16.4 List library Management

List library is mainly used for target picture storage and target comparison. **Strangers** library is used to store pictures for strangers, and it cannot be deleted.

16.4.1 Add a List Library

Steps

1. Go to **System → Event Configuration → Event Configuration → Data Archive → List Library** or **Event Center → Event Configuration → Data Archive → List Library**.
2. Click **Add**.
3. Enter the library name.
4. Click **Confirm**.



Note

- After a list library, you can move the cursor on the library to edit or delete it.
 - You can click **Delete in Batch** to delete selected libraries, or clear all pictures in the selected libraries.
-

16.4.2 Upload Face Pictures to the Library

Target picture comparison is based on target pictures in the library. You can upload a single target picture or import multiple target pictures to the library.

Before You Start

- Ensure the picture format is JPEG or JPG.
- Import all pictures to a backup device in advance.

Steps

1. Double click a list library.
2. **Optional:** Click **Custom Tag** to add tags to pictures. The tag can be edit as your desire, for example, personal information, organization, position, etc.
3. Click **Add** or **Import**.
4. Import picture(s).
 - **Add:** Click  to upload a picture at a time. If the picture has multiple targets, you have to pick one from them.
 - **Import:** Multiple pictures can be imported at a time. The device will use the file name as its picture name and leave other attributes empty, or import picture files by specified rules. If a picture has multiple targets in the image, the device will choose the target at the center by default.
5. **Optional:** Perform the following operations.

Delete Pictures from the Library

- Select a picture and delete it.
- Select pictures and click **Delete in Batch** to delete the select ones.

Search Pictures in the Library

Click  at the tool bar to search pictures.

**Copy Pictures to
Another Library**

Select pictures and click **Copy to** to copy the uploaded pictures of the current library to another library.

Edit Pictures

Click the picture name, and edit its attributes.

Export Pictures

Select pictures, and click **Export** to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

The human and vehicle information will be displayed for the selected channel at real-time.

Human and vehicle detection should be configured in advance. Go to **Event Center** →  to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

No.	Description
1	Right-click shortcut menu.
2	Human and vehicle detection settings. You can set the layout, comparison succeeded prompt, and resource channels.
3	Enter/exit full screen.

17.2 Person Check-In

After check-in tasks are added, you can view the live check-in information and search check-in results.

17.2.1 Add Check-In Task

Before starting person check-in, the corresponding task should be properly configured.

Before You Start

- A camera for person check-in is properly connected.
- Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** .
Allocate **Target Recognition** to at least one engine.
- The list library for check-in comparison is properly configured. Refer to [Add a List Library](#) for details.

Steps

1. Click **Person Check-In** .
2. Right click to display the menu at left side.
3. Click  .
4. Click **Add**.

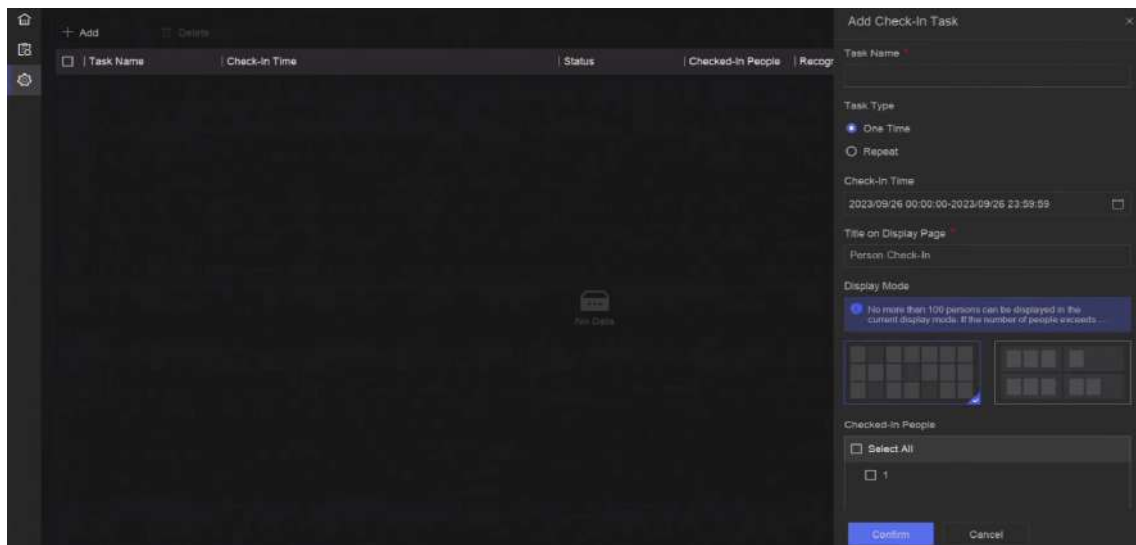


Figure 17-2 Add Check-In Task

5. Set **Task**.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

6. Configure other parameters, including **Task Name**, **Check-In Time**, **Recognition Channel**, etc.
7. Click **Confirm**.

17.2.2 Search Check-In Records

After check-in tasks are configured, you can search the records by day or month.

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to **Person Check-In**.
2. Right click to display the menu at the left side.
3. Click .

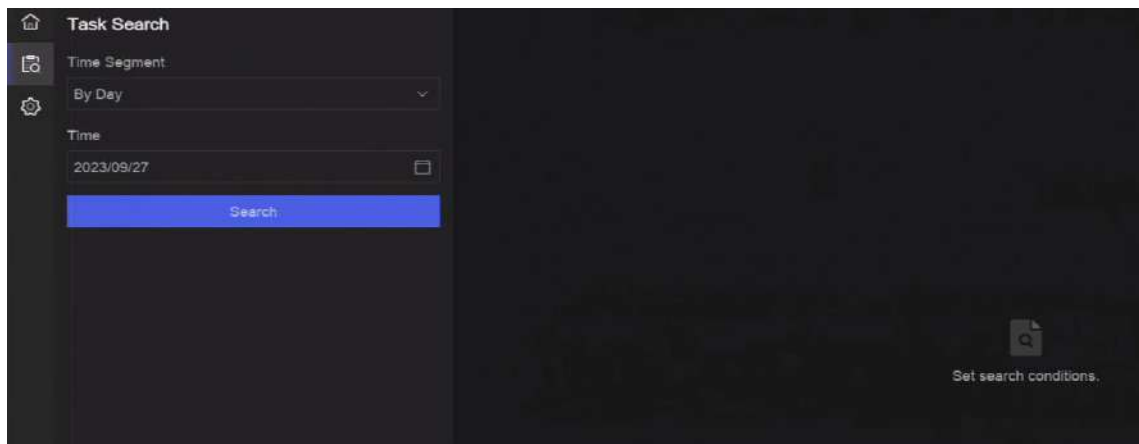


Figure 17-3 Search Check-In Records

4. Set time.
5. Click **Search**.

17.3 Statistic Report

You can view reports of people counting and heat map.

Table 17-2 Statistic Report Introduction

Function Name	Icon	Condition	Description
People Counting		The function must be supported by the connected IP camera. For example, a people counting	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

Function Name	Icon	Condition	Description
		camera is connected to your device. • Camera statistic data can be stored to the device HDD.	
Heat Map		• The function must be supported by the connected IP camera. • Camera statistic data can be stored to the device HDD.	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Table 18-1 Parameter Description

Type	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time Configuration	Time Sync Mode	NTP Time Sync You can select NTP Time Sync and configure NTP Server, NTP Server Port, NTP Client Port, and Interval. Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization. Manual Time Sync Manually set the system time. Hik-Connect Server Time Sync The device will sync time with Hik-Connect instead of NTP server. DST DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest. We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of

Type	Parameter Name	Description
		DST, and move them back the same period when we return to standard time (ST).
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console After connecting it to PC with a convertor, PC can set the device parameters. Transparent Channel It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System



Note

- Up to 32 working devices and 32 hot spare devices are allowed.
 - It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
 - Only certain models support this function.
-

19.1 Set Working Device

Steps

1. Go to **System** → **System Management** → **N+M Hot Spare** .
2. Set **Working Mode** as **Normal Mode**.
3. Turn on **Enable**.
4. Click **Save**.
5. **Optional:** View **Hot Spare Device IP Address** and **Hot Spare Device Working Status**.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

1. Go to **System** → **System Management** → **N+M Hot Spare** .
2. Set **Working Mode** as **Hot Spare Mode**.
3. Click **Save**. Your device will restart automatically.



Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

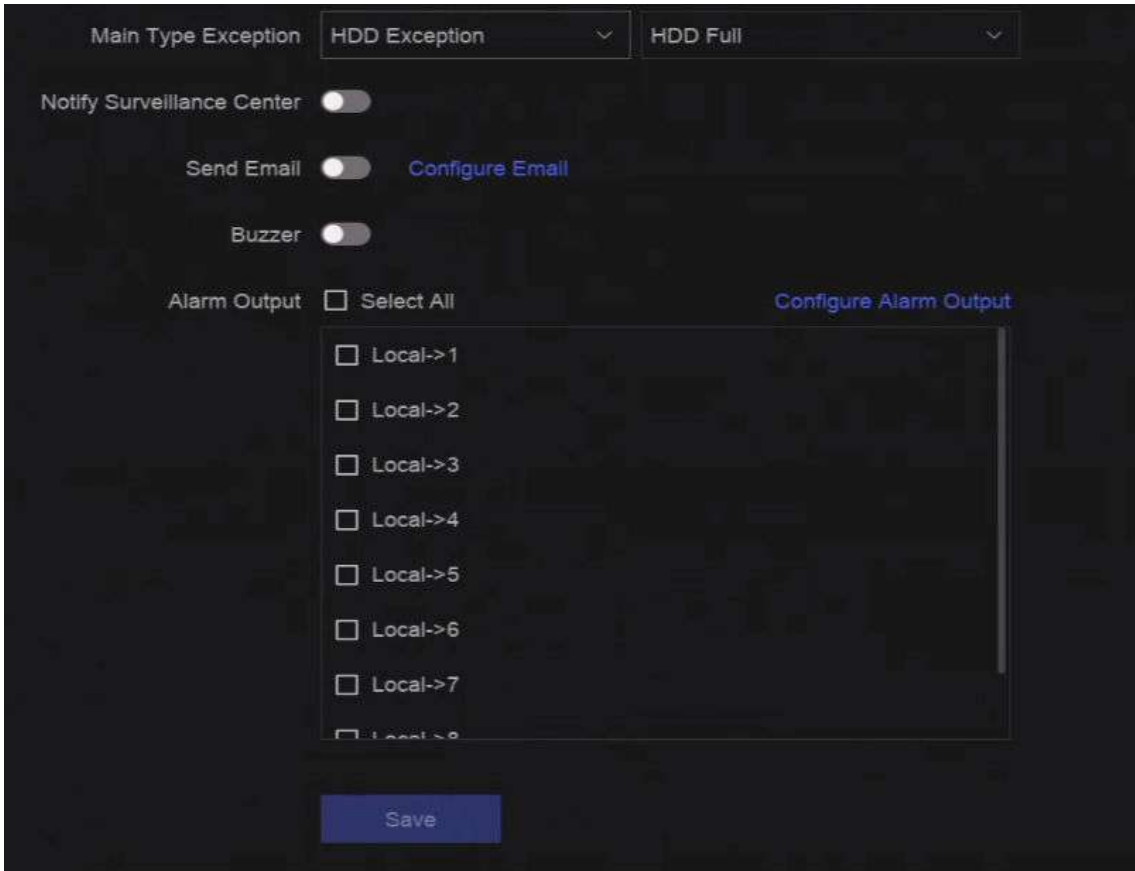
-
4. Go to **System → System Management → N+M Hot Spare** again.
 5. Add working devices to the hot spare system.
 6. Add hot spare devices to the hot spare system.
 7. Click **Save**.

Chapter 20 Configure Exception Event

Exception events can be configured to take the event hint in the live view interface and trigger alarm output and linkage actions.

Steps

1. Go to **System** → **System Settings** → **Exception** .



The screenshot shows the 'Exception' configuration page. At the top, there are two dropdown menus: 'Main Type Exception' set to 'HDD Exception' and 'HDD Full'. Below these are three toggle switches: 'Notify Surveillance Center' (off), 'Send Email' (off), and 'Buzzer' (on). To the right of the 'Send Email' toggle is a blue link 'Configure Email'. Below the toggles is the 'Alarm Output' section, which includes a checkbox for 'Select All' and a blue link 'Configure Alarm Output'. A list of checkboxes follows, labeled 'Local->1' through 'Local->8'. At the bottom center is a blue 'Save' button.

Figure 20-1 Exception Event Configuration

2. Select exception type.
3. Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.



Note

When exception events occur,  at the upper-right corner would notify, and you can click  to view.

4. Click **Save.**

Chapter 21 View System Info

Go to **System** → **System Maintenance** → **Running Info** → **System Info** to view the system information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to **System** → **System Maintenance** → **Maintenance** → **Schedule Reboot** to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** → **System Maintenance** → **Maintenance** → **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** → **System Maintenance** → **Maintenance** → **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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, and leave all settings unchanged except restoring user accounts.

22.4 Log Info

Go to **System → System Maintenance → Maintenance → Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

1. Go to **System → CX → System Settings → Network → Network → Log Server**.
2. Turn on **Enable**.
3. Set **Upload Time**, **Server IP Address**, and **Port**.
4. **Optional**: Click **Test** to test if parameters are valid.
5. Click **Save**.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

1. Go to **System → System Maintenance → Maintenance → Maintenance Tools**.
2. Select tools according to your requirement.

Table 22-1 Tool Description

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping The ping test is used to detect whether the destination IP address is reachable. NIC Packet Capture

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.

**Note**

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

1. Go to **System → System Maintenance → Security Management → Address Filter**.
2. Turn on **Enable**.
3. Set **Filtering Type**. Choose to filter by IP address or MAC Address.
4. Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
5. **Optional**: Set **Restriction List**. You can add, edit or delete address.
6. Click **Save**.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

1. Go to **System → System Maintenance → Security Management → Stream Encryption**.
2. Turn on **Enable**.
3. Set **Encryption Key**.



Note

The stream encryption key is synchronized with the Hik-Connect service verification code. After enabling the encryption code, the Hik-Connect stream will be forcedly encrypted.

4. Click **Save**.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to **System → System Maintenance → Security Management → TLS** to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, $\Phi 2.1$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 Glossary

Dual-Stream

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 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

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.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

PPPoE

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.

DDNS

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 hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

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.

NVR

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.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

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.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?

Reason

1. Sub-stream resolution or bitrate settings is inappropriate.
2. Connecting sub-stream failed.

Solution

1. Go to **Camera → Video Parameters → Sub-Stream** . Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).



Note

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.



Warning

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: 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.

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

1. The camera does not support coaxitron.
2. The coaxitron protocol is incorrect.
3. The signal is affected by video optical transceiver.

Solution

1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

1. The RS-485 cable is not properly connected.
2. The RS-485 interface is broken.
3. The control protocol is not correct.

Solution

1. Check if RS-485 cable is properly connected.
2. Change RS-485 interface, and try again.
3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

1. The audio input device does not have a good effect in sound collection.
2. Interference in transmission.
3. The audio parameter is not properly set.

Solution

1. Check if the audio input device is working properly. You can change another audio input device, and try again.
2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Table 24-1 Corrosive Gas Concentration Limit

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCl (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _x (Nitrogen Oxides)	0.5	1.0

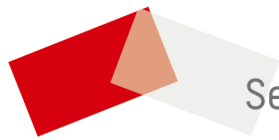


Note

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Table 24-2 Common Categories and Sources of Corrosive Gases

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _x (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.



See Far, Go Further

DS-96128NXI-S16

- Up to 32×1080p decoding capacity
- H.265+/H.265/H.264+/H.264 video formats
- Up to 128-ch IP cameras can be connected
- Intelligent analytics supports facial recognition, perimeter protection, video structuralization, AcuSearch
- Up to 8-ch IP speakers can be connected
- Supports RAID 0, 1, 5, 6, 10 and N+M hot spare for even more reliable data storage, effectively avoids data loss risks
- HDMI video output at up to 8K resolution

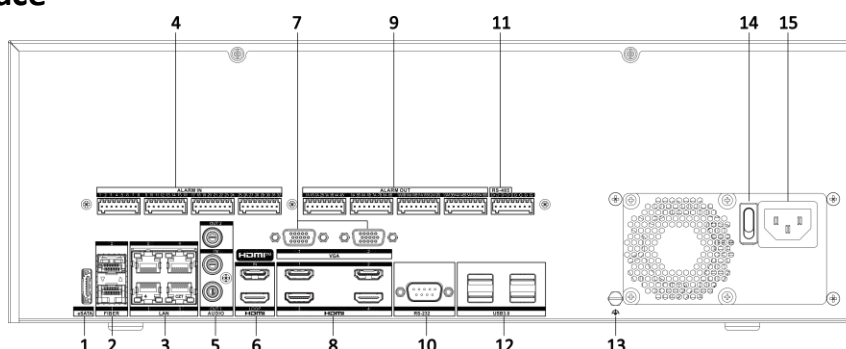
▪ Specification

Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization
AI by Camera	Facial recognition, perimeter protection, video structuralization, AcuSearch, motion detection2.0, ANPR, people counting, VCA
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 64 face picture libraries, up to 300,000 face pictures in list library (each picture ≤ 4 MB, total capacity ≤ 10 GB)
Face Picture Comparison (Captured from Camera)	16-ch Comparison speed: 24 pictures per second
Facial Detection and Analytics Performance	Simultaneous mode: 8-ch, up to 2 MP independent mode: 4-ch, up to 2 MP.
AcuSearch	
By Camera	All channels , up to 345,600 targets per day Note: The camera should enable AcuSearch function.
Perimeter Protection	
By NVR	Simultaneous mode: 8-ch, up to 2 MP independent mode: 4-ch, up to 2 MP.
By Camera	All channels
Video Structuralization	
Structured Analysis	Simultaneous mode: 8-ch, up to 2 MP independent mode: 4-ch, up to 2 MP.
Face Picture Library	Up to 64 face picture libraries, up to 300,000 face pictures in list library (each picture ≤ 4 MB, total capacity ≤ 10 GB)
Face Picture Comparison	16-ch; Comparison speed: 24 pictures per second
Video and Audio	
IP Video Input	128-ch Up to 32 MP resolution
Incoming Bandwidth	1280 Mbps
Outgoing Bandwidth	1024 Mbps
Incoming Bandwidth (RAID Mode)	640 Mbps
Outgoing Bandwidth (RAID mode)	512 Mbps
HDMI 1 Output	4K (4096 × 2160)/30 Hz, 4K (3840 × 2160)/60 Hz, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1080P (1920 × 1080)/60 Hz
HDMI 2 Output	4K (4096 × 2160)/30 Hz, 4K (3840 × 2160)/60 Hz, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1080P (1920 × 1080)/60 Hz
HDMI 3 Output	8K (7680 × 4320)/30 Hz, 4K (4096 × 2160)/30 Hz, 4K (3840 × 2160)/60 Hz, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1080P (1920 × 1080)/60 Hz
HDMI 4 Output	1080P (1920 × 1080)/60 Hz
VGA 1 Output	1080P (1920 × 1080)/60 Hz
VGA 2 Output	1080P (1920 × 1080)/60 Hz

Video Output Mode	Mode 1 (default output mode): simultaneous output with 1080p resolution; Mode 2 (simultaneous output): HDMI 1, VGA 1, HDMI 2, VGA 2, HDMI 3, and HDMI 4 provides simultaneous output, the maximum resolution for VGA 1/VGA 2/HDMI 4 is 1080p, the maximum resolution for HDMI 1/HDMI 2/HDMI 3 is 4K; Mode 3 (independent output and 8K HDMI 3 output resolution): HDMI 1/VGA 1/HDMI 2/VGA 2, HDMI 3, and HDMI 4 provide independent output respectively. The maximum resolution is 8K + 4K + 1080p; Mode 4 (independent output and HDMI 3 output resolution ≤ 4K): HDMI 1/VGA 1, HDMI 2/VGA 2, HDMI 3, and HDMI 4 provide independent output respectively. The maximum resolution is 4K + 4K + 4K + 1080p.
HDMI Input	1-ch
HDMI Loopback	1-ch (matching the HDMI input)
Audio Output	2-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 k Ω)
Decoding	
Decoding Format	H.265/H.265+/H.264/H.264+
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30fps)/4-ch@16 MP (30fps)/8-ch@8 MP (30fps)/16-ch@4 MP (30fps)/32-ch@2 MP (30fps)
Synchronous Playback	16-ch
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA/4CIF/DCIF/ 2CIF/CIF/QCIF
Network	
Remote Connection	256
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMP, NFS, iSCSI, ISUP, UPnP™, HTTP, HTTPS, ONVIF (version 2.2), OTAP
API	ONVIF (profile S/T); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	4, RJ-45 10/100/1000/2500 Mbps self-adaptive Ethernet interface 2, SFP 1000 Mbps
Camera Access Protocol	ONVIF (version 2.5), RTSP
RAID	
RAID Type	RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Auxiliary Interface	
SATA	16 SATA interfaces; 3.5-inch HDD
eSATA	1 eSATA interface
Capacity	Up to 20 TB capacity for each HDD
Serial Interface	1 RS-232, 2 RS-485 (half-duplex)
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 4 × USB 3.0
Alarm In/Out	32/16
General	
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian
Power Supply	100 to 240 VAC, 50 to 60 Hz

Consumption	≤ 100 W (without HDD)
Working Temperature	-10 to 55°C (14 to 131° F)
Working Humidity	10 to 90%
Dimension (W × D × H)	442 mm × 497 mm × 146 mm (17.4 × 19.5 × 5.7 inch)
Weight	≤ 12 kg (without HDD, 28.7 lb.)
Certification	
Obtained Certification	CE, IC, CB, Rohs, Reach, WEEE, RCM, UKCA, LOA
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:2019, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020

▪ Physical Interface



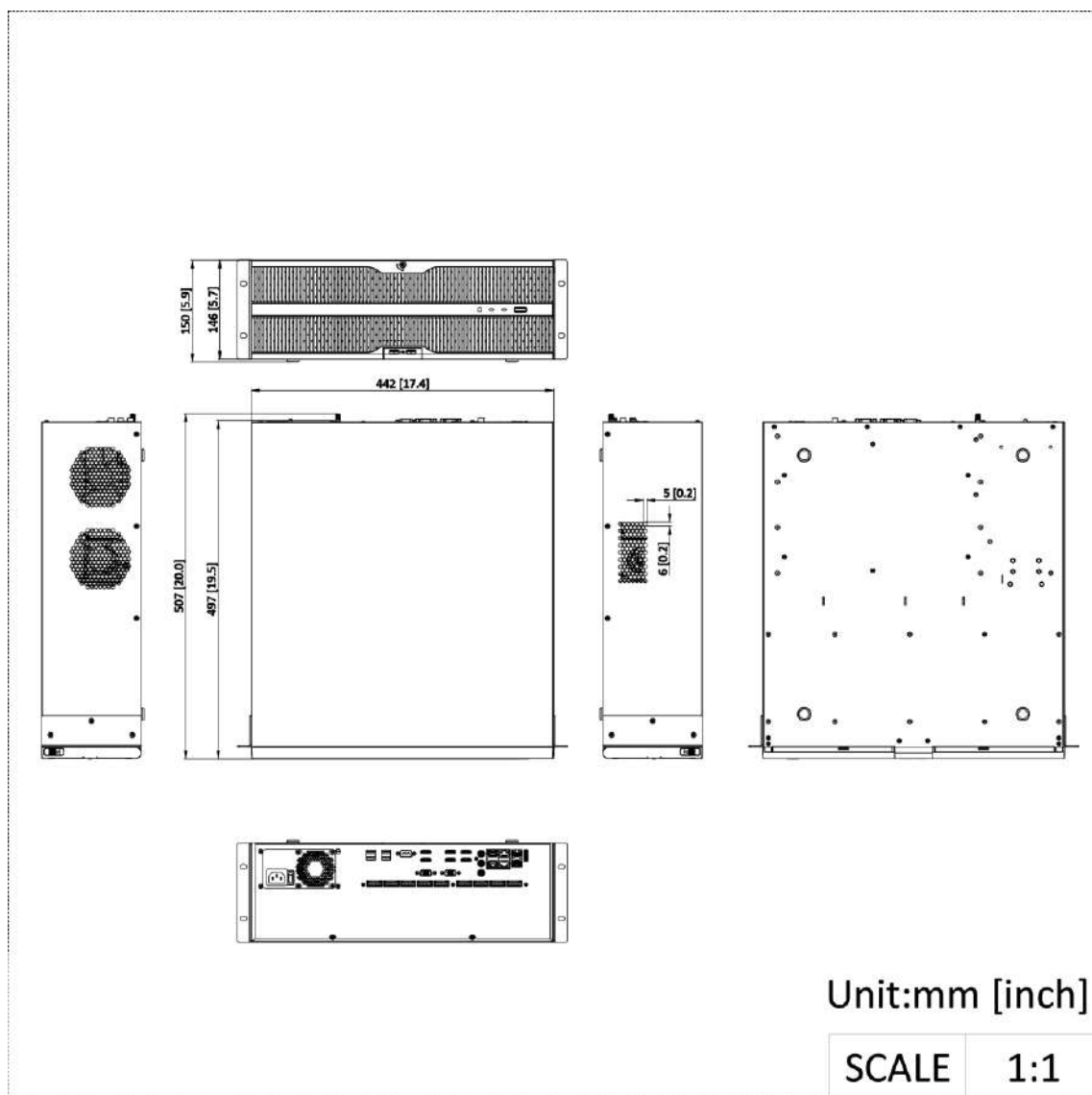
No.	Description	No.	Description
1	eSATA interface	9	Alarm out
2	Fiber	10	RS-232 serial interface
3	LAN interfaces	11	RS-485 serial interface
4	Alarm in	12	USB 3.0 interfaces
5	Audio in and out	13	GND
6	HDMI input and HDMI loopback	14	Power switch
7	VGA 1 and VGA 2 interfaces	15	Power supply
8	HDMI interfaces		

▪ Available Model

DS-96128NXI-S16(STD)

DS-96128NXI-S16(NEU)

▪ Dimension



See Far, Go Further



www.hikvision.com
support@hikvision.com





Network Video Recorder

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Conditions

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

- This device may not cause harmful interference.
- 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 2014/30/EU, LVD Directive 2014/35/EU, 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 see: <http://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 see: <http://www.recyclethis.info> .

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Table 1-1 Applicable Model

Series	Model
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P

Series	Model
	DS-7716NI-M4/16P
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-7700NXI-M4/VPro	DS-7716NXI-M4/VPro
	DS-7732NXI-M4/VPro
DS-7700NXI-M4/16P/VPro	DS-7716NXI-M4/16P/VPro
	DS-7732NXI-M4/16P/VPro
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro

Series	Model
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-I2/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-I2/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-I4/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-I8/S	DS-8616NXI-I8/S
	DS-8632NXI-I8/S
	DS-8664NXI-I8/S
DS-8600NXI-I8/24P/S	DS-8632NXI-I8/24P/S
DS-9600NXI-I8/S	DS-9616NXI-I8/S

Series	Model
	DS-9632NXI-I8/S
	DS-9664NXI-I8/S
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X
DS-9600NXI-S16	DS-9632NXI-S16
	DS-9664NXI-S16

Series	Model
	DS-9664NXI-S16(LCD)
DS-96000NXI-S16	DS-96128NXI-S16
	DS-96128NXI-S16(LCD)
	DS-96256NXI-S16
DS-9600NXI-S16R	DS-9632NXI-S16R
	DS-9664NXI-S16R
DS-96000NXI-S16R	DS-96128NXI-S16R
	DS-96128NXI-S16R(LCD)
	DS-96256NXI-S16R
	DS-96256NXI-S16R(LCD)
DS-96000NXI-S24R	DS-96128NXI-S24R
	DS-96128NXI-S24R(LCD)
	DS-96256NXI-S24R
	DS-96256NXI-S24R(LCD)
DS-96000NXI-S36R	DS-96128NXI-S36R
	DS-96256NXI-S36R
DS-9600NXI-S8	DS-9616NXI-S8
	DS-9632NXI-S8
	DS-9664NXI-S8
DS-96000NXI-S8	DS-96128NXI-S8
DS-9600NXI-S8R	DS-9632NXI-S8R
	DS-9664NXI-S8R
DS-96000NXI-S8R	DS-96128NXI-S8R

Safety Instruction

- 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.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the device and shall be easily accessible.
- For the device with the sign ⚡ indicating hazardous live, the external wiring connected to the terminals requires installation by an instructed person.
- Never place the device in an unstable location. The device may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC62368.
- High touch current! Connect to earth before connecting to the power supply.
- 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.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Do not ingest battery. Chemical Burn Hazard!
- This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- Use only power supplies same with the original model, or LPS power supplies with the same voltage and electric current.

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
-  identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- If the device has been powered off or placed for a long time, its coin/button cell battery may run out power.
- When the coin/button cell battery runs out power, the system time would be incorrect, please contact the after-sales service to replace the battery.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.
- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- Do not touch the bare components (such as the metal contacts of the inlets) and wait for at least 5 minutes, since electricity may still exist after the device is powered off.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only. The current for the connected device shall be not more than 0.1 A.
- The serial port of the device is used for debugging only.
- If the power output port of the device does not comply with Limited Power Source, the connected device powered by this port shall be equipped with a fire enclosure.
- If a power adapter is provided in the device package, use the provided adapter only.

- For the device with sticker  or  , pay attention to the following cautions: CAUTION: Hot parts! Do not touch. Burned fingers when handling the parts. Wait one-half hour after switching off before handling the parts.
- If the device needs to be installed on the wall or ceiling,
 1. Install the device according to the instructions in this manual.
 2. To prevent injury, this device must be securely attached to the installation surface in accordance with the installation instructions.
- Under high working temperature (40 °C (104 °F) to 55 °C (131 °F)), the power of some power adapters may decrease.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device.
- If the device needs to be wired by yourself, select the corresponding wire to supply power according to the electric parameters labeled on the device. Strip off wire with a standard wire stripper at corresponding position. To avoid serious consequences, the length of stripped wire shall be appropriate, and conductors shall not be exposed.
- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

Content Convention

In order to simplify description, please read the following conventions.

- Recorder or device mainly refers to video recorder.
- IP device mainly refers to network camera (IP camera), IP dome (speed dome), DVS (Digital Video Server), or NVS (Network Video Server).
- Channel mainly refers to the video channel in video recorder.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Indicator and Interface Description

Front Panel Indicator Description

The indicators at the front panel indicates different working status of your device.

Table 1-1 Common Indicator Description

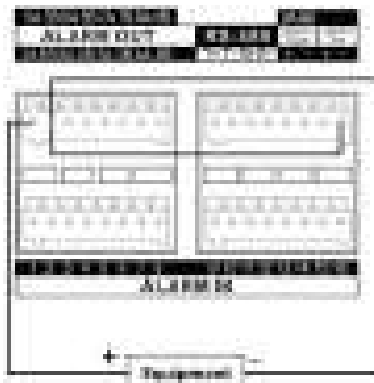
Indicator	Description
	The indicator turns on when device is powered up.
	The indicator flashes when data is being read from or written to HDD.
	The indicator flashes when network connection is functioning properly.

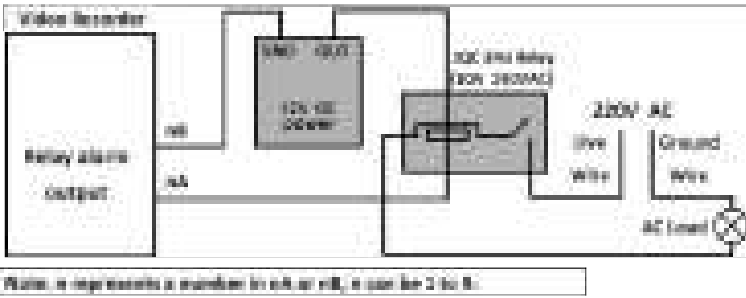
Interface Description

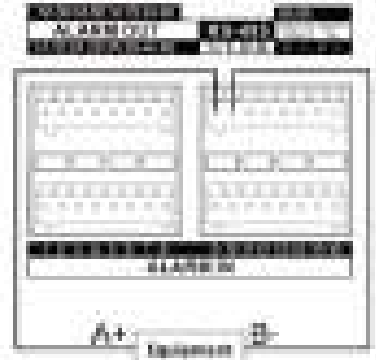
The panel interfaces vary with different models. Refer to the following table for common interface description.

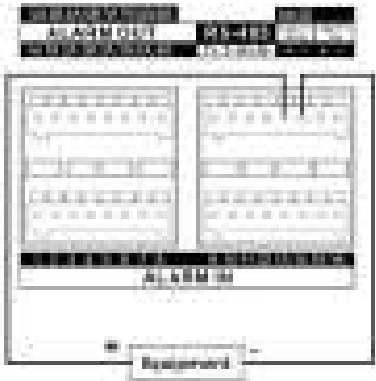
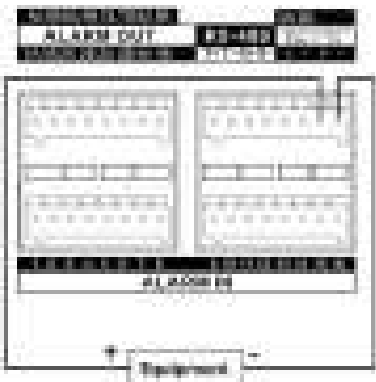
Table 1-2 Common Indicator Description

Item	Description
VIDEO IN	BNC interface for Turbo HD and analog video input.
VIDEO OUT	BNC connector for video output.
AUDIO IN	RCA connector for audio input.
AUDIO OUT	RCA connector for audio output.
LINE IN	RCA connector for two-way audio input.
USB	Universal Serial Bus (USB) interface for additional device.
VGA	DB15 connector for local video output and menu display.
HDMI	HDMI interface for video output.
RS-485	RS-485 serial interface for pan/tilt unit, speed dome, etc.
RS-232	RS-232 interface for parameter configuration, or transparent channel.
LAN	RJ-45 self-adaptive Ethernet interface.
eSATA	Storage and expansion interface for record or backup.
GND	Ground.

Item	Description
Power Switch	Switch for turning on/off the device.
Power Supply	100 to 240 VAC, 48 VDC, or 12 VDC power supply.
USIM Card	UIM/SIM card slot.
	SMA antenna interface.
ALARM IN	The alarm input receives alarm input signal. The equipment positive terminal (+) should connect to a number, and the equipment negative terminal (-) should connect to “-” or “G”. Use the following diagram as a connection example for alarm input. 
ALARM OUT	The alarm output sends out alarm signal. When an equipment uses DC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should both connect to the corresponding number with “B”, and then connect to “-” or “G”. Use the following diagram as an alarm output connection example for DC equipment. 

Item	Description
	When an equipment uses AC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should connect to the corresponding number with “B”. Use the following diagram as an alarm output connection example for AC equipment.   Note For the reason that the AC load voltage could be high, please use an external relay for safety. Use the following diagram for reference. 
KB	KB represents keyboard. Connect “D+” and “D-” to “T+” and “T-” respectively. Use the following diagram for reference.

Item	Description
	
RS-485	RS-485 is an electrical specification of a two-wire, half-duplex, multipoint serial connection. Connect “T+” and “T-” to “A+” and “B-” respectively. Use the following diagram for reference. 
Ctrl 12V/ $\frac{12V}{0.5A}$	Controllable 12 VDC and 0.5/1 A power output for external alarm device. The power will be turned on when the corresponding alarm output is triggered. Use the following diagram for reference.

Item	Description
	 The diagram shows a terminal block with three main sections. The top section is labeled 'ALARM OUT' and 'RS-485'. The middle section is labeled 'ALARM IN'. The bottom section is labeled 'Equipment'. Wires are connected to the terminals, and a ground symbol is shown at the bottom.
DC 12V/ $\frac{12V}{1A}$	It provides 12 VDC and 1 A power output. Use the following diagram for reference.  This diagram is identical to the one in the first row, showing the terminal block connections for Alarm Out, RS-485, Alarm In, and Equipment, with a ground symbol at the bottom.

HDD Installation

If your device does not support HDD hot swapping, disconnect the power from the device before installing a hard disk drive (HDD). A factory recommended HDD should be used for this installation.

Scan the QR code below to view HDD installation videos.



Figure 1-1 HDD Installation

Bracket Installation

Bracket installation is applicable when it requires to remove the device cover, and install HDD on the internal bracket.

Steps

1. Unfasten screws on the back, and push the cover backwards to remove the cover.

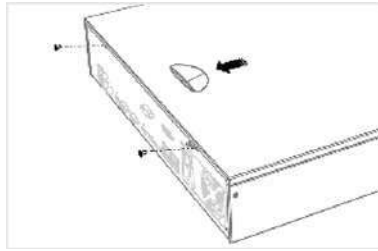


Figure 1-2 Remove Cover

2. Fix the HDD on the bracket with screws.



Note

Please uninstall the upper layer bracket first before installing HDD on the lower layer bracket.

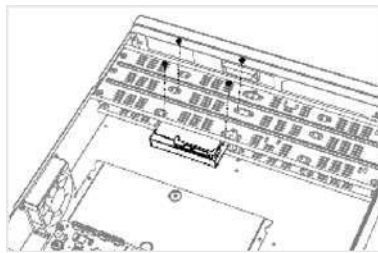


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

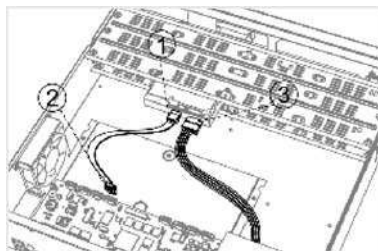


Figure 1-4 Connect Cable



Note

You can repeat the steps above to install other HDDs.

4. Reinstall the device cover and fasten screws.

Front Panel Plug-Pull Installation

Front panel plug-pull installation is applicable when you need to open the device front panel with key and install the HDD.

Steps

1. Fix mounting ears to HDD with screws.

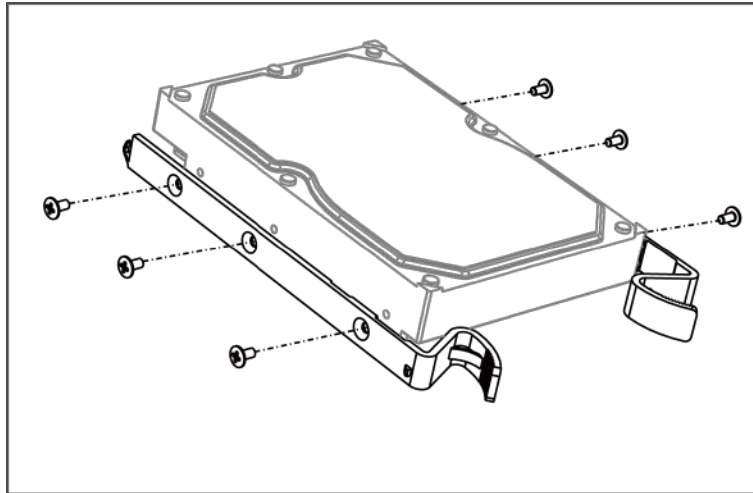


Figure 1-5 Fix Mounting Ears to HDD

2. Unlock the front panel with the attached key, and press the buttons on both sides of the front panel to open it.

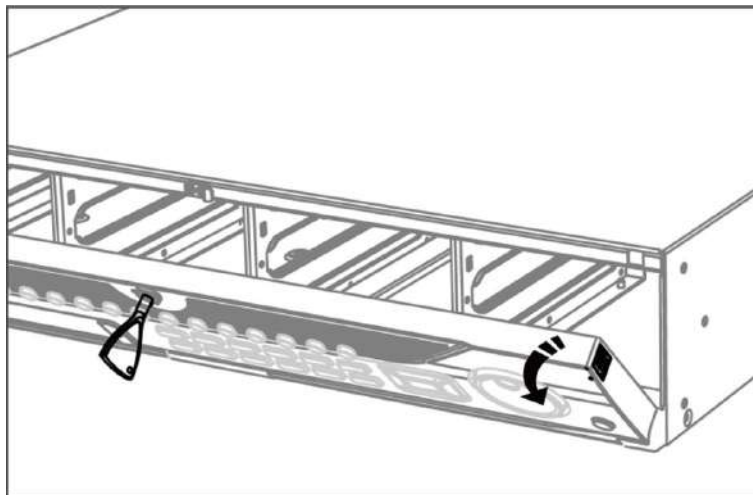


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

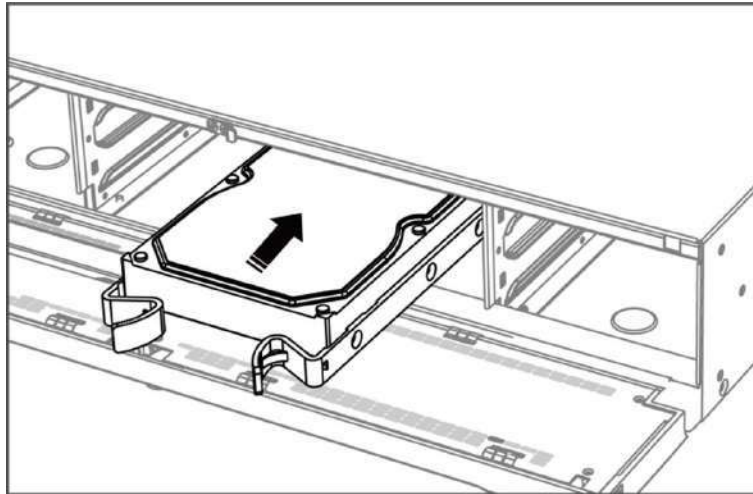


Figure 1-7 Insert HDD

4. **Optional:** Repeat the steps above to install other HDDs.
5. Close the front panel and lock it with key.

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

1. Unlock the front panel with panel key.
2. Pull the front panel out of the device and make it a little above the left handle.



Note

The angle between the front panel and the device must be within 10°.

3. Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
4. Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

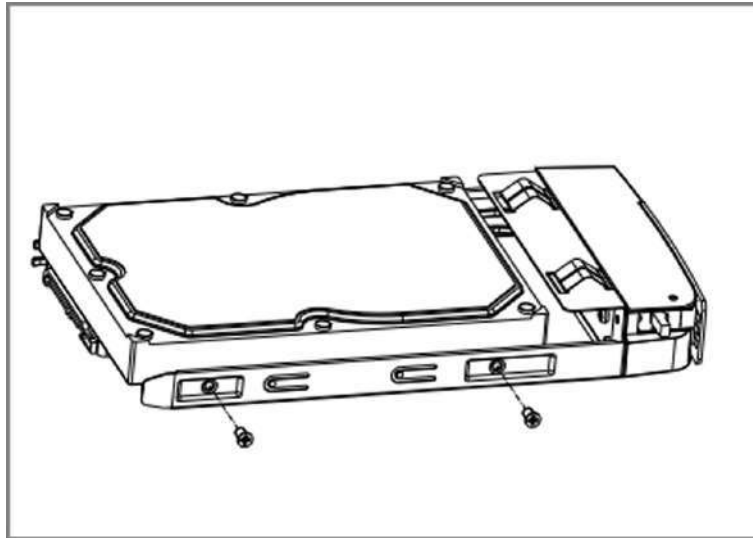


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

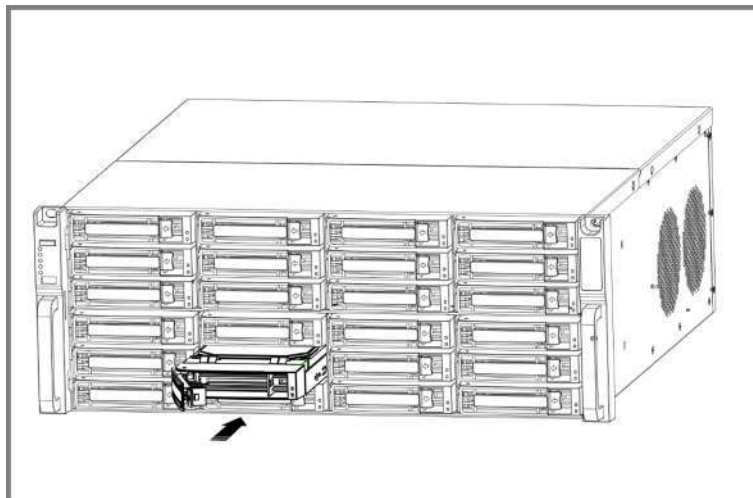


Figure 1-9 Push HDD Case into Slot

6. Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
7. Close the front panel, and lock it with the panel key.

Fix-on-Bottom Installation

Fix-on-bottom installation is applicable when you need to install and fix the HDD on the device bottom.

Steps

1. Remove the cover from device by unfastening the screws on panels.

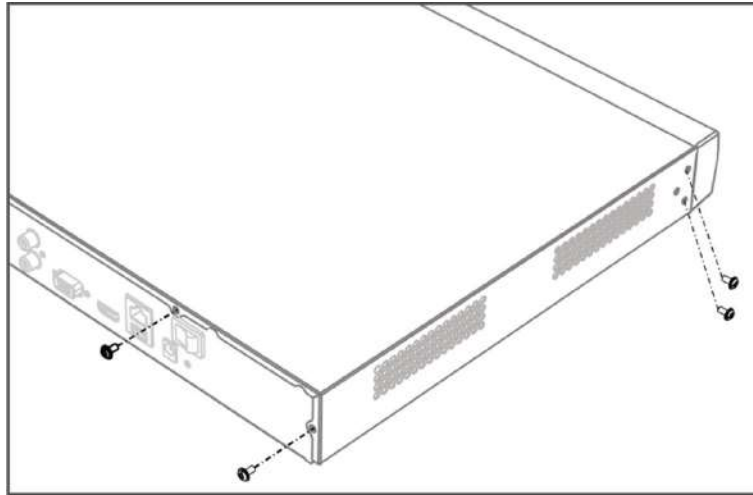


Figure 1-10 Remove Cover

2. Connect the data cable and power cable.
 - 1) Connect one end of data cable to the device motherboard.
 - 2) Connect the other end of data cable to HDD.
 - 3) Connect one end of power cable to HDD.
 - 4) Connect the other end of power cable to the device motherboard.

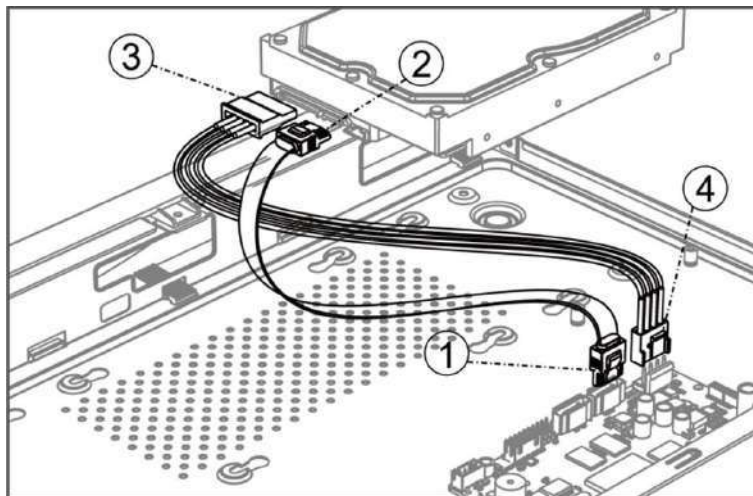


Figure 1-11 Connect Cables

3. Set the device up, match HDD screw threads with the reserved holes on the device bottom, and fix HDD with screws.

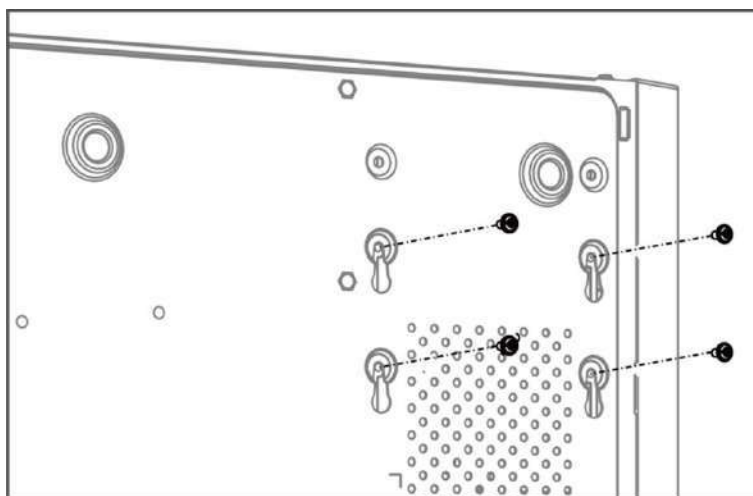


Figure 1-12 Fix HDD to Device Bottom

- 4. Optional:** Repeat the steps above to install other HDDs.
- 5.** Reinstall the device cover and fasten screws.

Coin/Button Cell Battery Replacement

The coin/button cell battery should be replaced when the device has been powered off or placed for a long time, and the system time is incorrect.

Before You Start

Power off your device.

Steps

1. Remove the device chassis cover.
2. Find the coin/button cell battery on motherboard.
3. Use tweezers to push the metal latch at the middle from its inside, and the battery would automatically pop up.

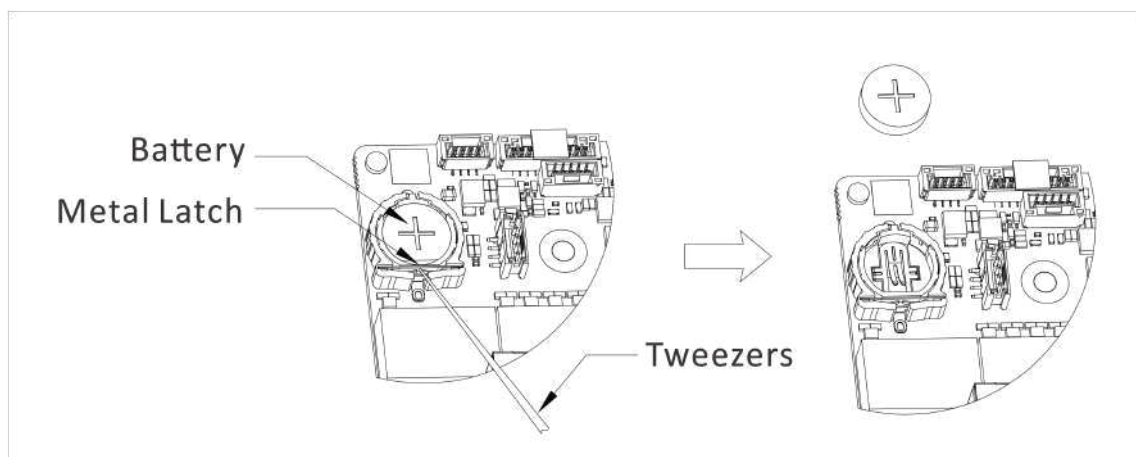


Figure 1-1 Remove Battery

4. Take out the old battery and press a new battery with the same model in to the battery slot.

Note

The battery positive terminal (+ identifies the positive terminal) should be placed upward.

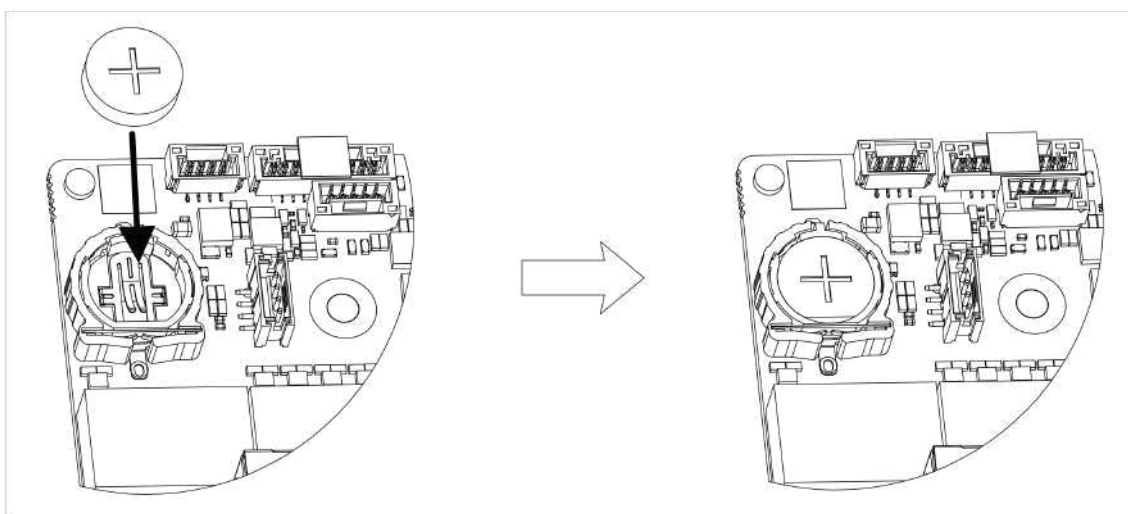


Figure 1-2 Replace Battery

5. Reinstall the device chassis cover.

What to do next

If the system time is incorrect, please go to configure the time.

Contents

Chapter 1 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	9
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP	11
4.2.3 Configure ISUP	12
4.2.4 Configure SDK Service	13
4.2.5 Enable ISAPI	14
4.2.6 Configure ONVIF	14
4.2.7 Configure Log Server	15
4.3 Network Service Settings	16
4.3.1 Configure HTTP(S)	16
4.3.2 Configure RTSP	17
4.3.3 Configure WebSocket(s)	18
4.3.4 Configure Port Mapping (NAT)	18
4.3.5 Configure IoT	20
Chapter 5 User Management	21
Chapter 6 Device Access	22
6.1 Access Video Device	22

6.1.1 Add Automatically Searched Online Network Camera	22
6.1.2 Add Network Camera Manually	22
6.1.3 Add Network Camera through PoE	24
6.1.4 Add Solar-Powered Camera through OTAP Protocol	24
6.1.5 Add Network Camera via Custom Protocol	25
6.1.6 Add Network Camera through Camera Configuration File	26
6.2 Add Access Control Device	26
6.3 Add Audio Device	26
6.4 Add POS Device	27
6.5 Channel Management	28
Chapter 7 Device Grouping	29
Chapter 8 Video or Audio Device Settings	30
8.1 Enable H.265 Stream Access	30
8.2 Configure Display Settings	30
8.3 Configure Video Parameters	31
8.4 Configure Privacy Mask	31
8.5 Configure Audio Parameter	32
8.6 Configure OTAP Service	33
8.7 Batch Configuration	33
8.8 Configure PoE (Power over Ethernet) Interface	34
Chapter 9 Storage Management	36
9.1 Manage HDD	36
9.2 RAID Configuration	36
9.2.1 Create Disk Array	37
9.2.2 Rebuild Array	39
9.2.3 Delete Array	39
9.2.4 View Firmware Info	39
9.3 Configure Storage Mode	40

9.4 Configure Other Storage Parameters	40
9.5 Manage USB Flash Drive	41
Chapter 10 Schedule Configuration	42
10.1 Configure Schedule Template	42
10.2 Configure Recording Schedule	44
10.3 Configure Picture Capture Schedule	46
10.4 Configure Audio Recording	48
Chapter 11 Live View	49
11.1 Configure Live View Layout	49
11.2 GUI Introduction	49
11.3 PTZ Control	51
Chapter 12 Playback	52
12.1 GUI Introduction	52
12.2 Normal Playback	54
12.3 Event Playback	54
12.4 Slice Playback	55
12.5 Sub-Period Playback	55
Chapter 13 Event Center	57
13.1 Event Settings	57
13.1.1 Basic/Generic Event	57
13.1.2 Perimeter Protection	59
13.1.3 Abnormal Behavior Event	70
13.1.4 Target Event	72
13.1.5 Thermal Camera Detection	74
13.1.6 Alarm Input Event	76
13.1.7 Audio Analysis Event	78
13.2 Linkage Configuration	79
13.3 Disarming Configuration	81

13.4 Batch Configuration	82
13.5 Event Search	82
13.6 View Alarms	83
Chapter 14 Search and Backup	84
Chapter 15 AcuSearch	86
Chapter 16 Smart Settings	88
16.1 Algorithm Management	88
16.2 Engine Status	88
16.3 Task Plan Management	88
16.4 List library Management	88
16.4.1 Add a List Library	89
16.4.2 Upload Face Pictures to the Library	89
Chapter 17 Application Center	91
17.1 Human and Vehicle Detection	91
17.2 Person Check-In	91
17.2.1 Add Check-In Task	92
17.2.2 Search Check-In Records	93
17.3 Statistic Report	93
Chapter 18 System Parameter Settings	95
Chapter 19 Hot Spare Device Backup	97
19.1 Set Working Device	97
19.2 Set Hot Spare Device	97
Chapter 20 Configure Exception Event	99
Chapter 21 View System Info	101
Chapter 22 System Maintenance	102
22.1 Schedule Reboot	102
22.2 Upgrade Device	102
22.3 Backup and Restore	102

22.4 Log Info	103
22.5 Configure Log Server	103
22.6 Maintenance Tools	103
Chapter 23 Security Management	105
23.1 Address Filter	105
23.2 Stream Encryption	105
23.3 Select TLS Version	105
Chapter 24 Appendix	106
24.1 List of Applicable Power Adapter	106
24.2 Glossary	107
24.3 Frequently Asked Questions	108
24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?	108
24.3.2 Why is the video recorder notifying risky password after a network camera is added?	109
24.3.3 Why is the video recorder notifying the stream type is not supported?	109
24.3.4 How to confirm the video recorder is using H.265 to record video?	109
24.3.5 Why is the video recorder notifying IP conflict?	109
24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?	110
24.3.7 Why is the device not able to control PTZ camera via coaxitron?	110
24.3.8 Why does the PTZ seem unresponsive via RS-485?	110
24.3.9 Why is the video sound quality not good?	110
24.4 Notification for Corrosive Gas	111

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

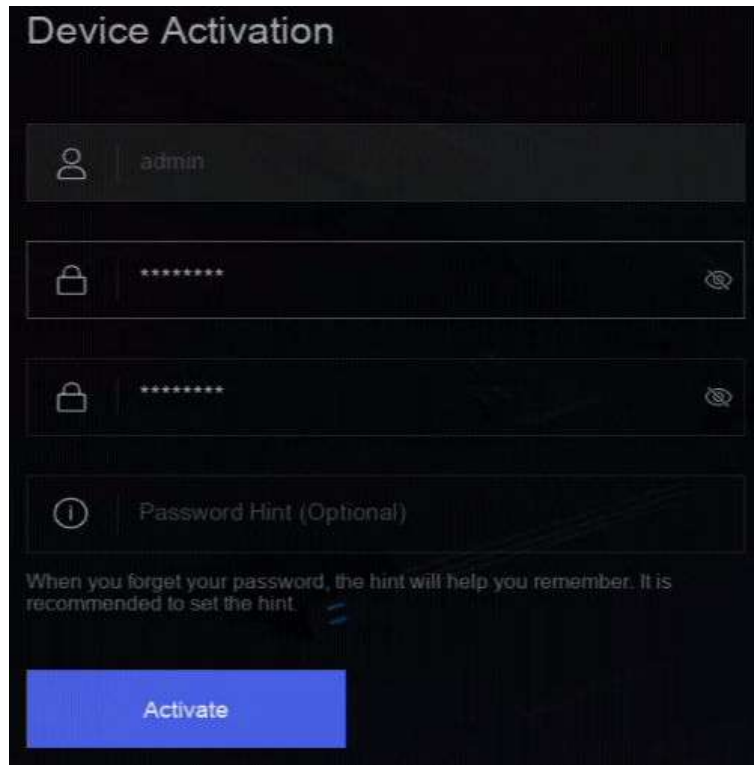
Steps

1. Power on your device.
2. Select a system language.
3. Enter the admin password twice.



Caution

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.



The image shows a 'Device Activation' screen with a dark background. At the top, the title 'Device Activation' is displayed. Below it, there are three input fields. The first field is for the username, with a person icon and the text 'admin' entered. The second and third fields are for passwords, each with a lock icon and masked text '*****'. To the right of each password field is an eye icon for toggling visibility. Below the password fields is a field for a 'Password Hint (Optional)' with an information icon. A note below this field states: 'When you forget your password, the hint will help you remember. It is recommended to set the hint'. At the bottom of the screen is a large blue button labeled 'Activate'.

Figure 1-1 Activate via Local Menu

4. **Optional:** Enter a password hint. It will help you remember your password when you forget.
5. Click **Activate**.



Note

After the device is activated, you should properly keep the password.

-
6. **Optional:** Draw an unlock pattern.
 7. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

1. Power on your device.
2. Right click to display the shortcut menu.
3. Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

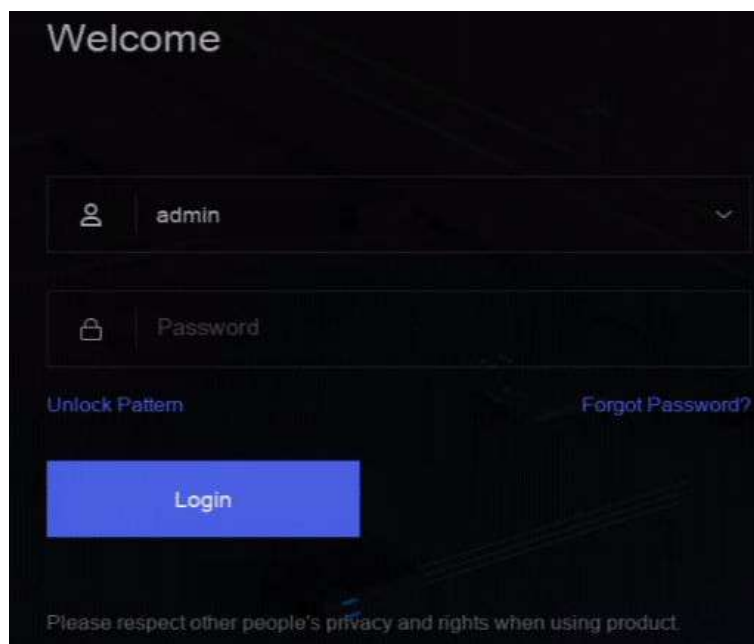


Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.



Note

- Unlock pattern is only available for admin user.
 - If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.
-

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

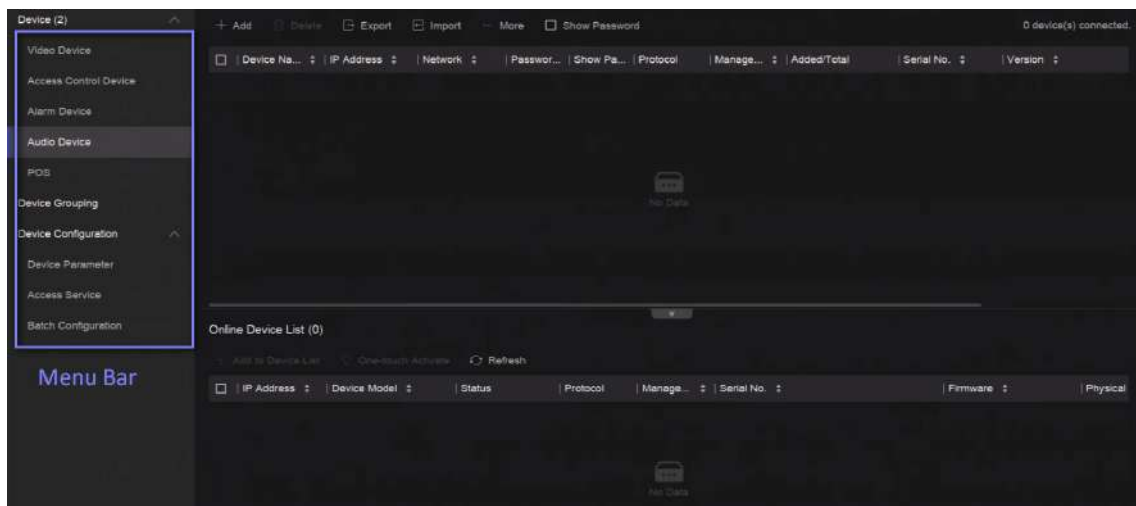


Figure 3-2 Menu Bar Example

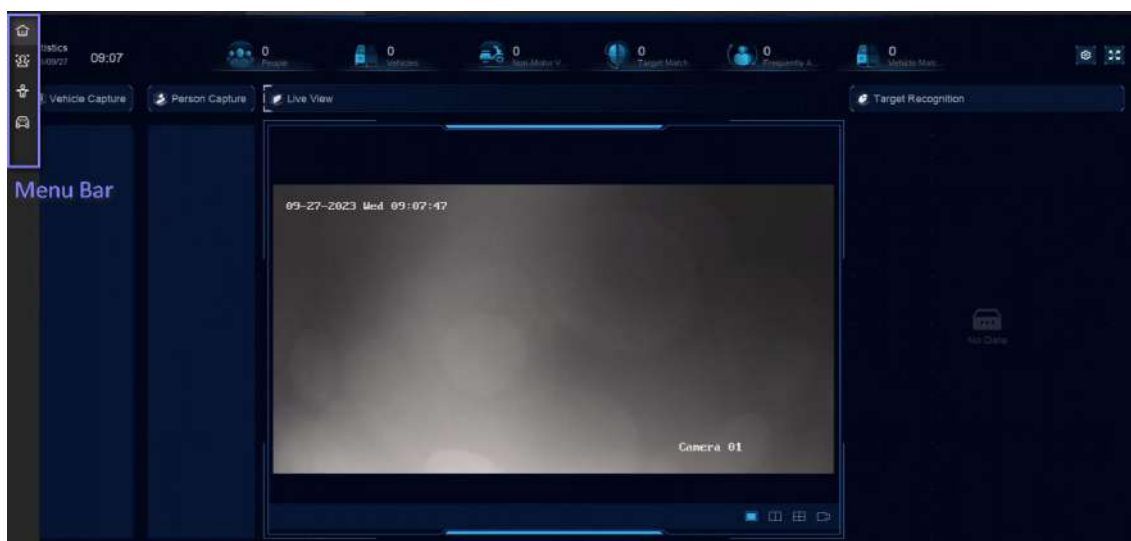


Figure 3-3 Human and Vehicle Detection Example of Application Center

Table 3-1 Interface Introduction

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab. Icon introduction : •  : Main menu. •  : Event center. Event alarms can be searched and viewed. •  : The download progress of each download task can be viewed here. •  : Shut down, log out, or reboot your device.
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.  Note For applications in Application Center, you can click  , or right click to display the menu bar.

Chapter 4 Network Settings

Network parameters, platform access settings, and network services are configurable.

4.1 Network Parameter Settings

You shall configure network parameters before using functions that require network access.

4.1.1 Configure TCP/IP

TCP/IP must be properly configured before you operate video recorder over network or access network devices.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **TCP/IP** .

Figure 4-1 TCP/IP Settings

2. Set **Working Mode** and **Select NIC**.

Multi-address

The parameters of the two NIC cards can be configured independently. You can select **LAN1** or **LAN2** in the NIC type field for parameter settings. You can select one NIC card as default route. And then the system is connecting with the extranet and the data will be forwarded through the default route.

Net-fault Tolerance

The two NIC cards use the same IP address, and you can set **Main NIC** to **LAN1** or **LAN2**. By this way, in case of one NIC card failure, the video recorder will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.



Note

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

If the DHCP server is available, you can enable **DHCP** to automatically obtain an IP address and other network settings from that server.

MTU

The maximum transmission unit (MTU) is the size of the largest network layer protocol data unit that can be communicated in a single network transaction.

Auto Obtain DNS Server

If **DHCP** is enabled. You can check **Auto Obtain DNS Server** to obtain **Preferred DNS Server** and **Alternate DNS Server**.

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click **Save**.

4.1.2 Configure DDNS

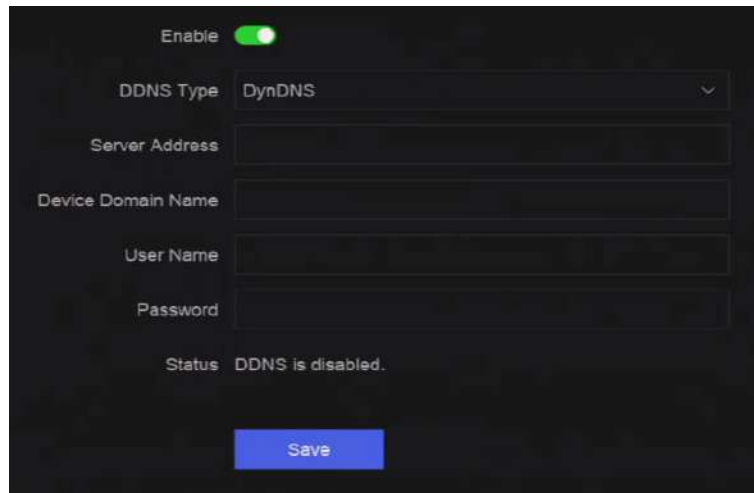
Dynamic domain name server (DDNS) maps dynamic user IP addresses to a fixed domain name server.

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **DDNS** .



Enable ☒

DDNS Type: DynDNS

Server Address:

Device Domain Name:

User Name:

Password:

Status: DDNS is disabled.

Save

Figure 4-2 DDNS

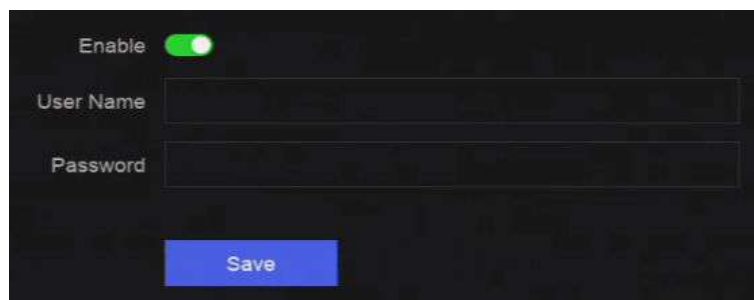
2. Turn on **Enable**.
3. Select a DDNS type.
4. Set parameters, including service address, domain name, etc.
5. Click **Save**.

4.1.3 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly. Contact your Internet service provider for details about PPPoE service.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **PPPoE** .



Enable ☒

User Name:

Password:

Save

Figure 4-3 PPPoE

2. Turn on **Enable**.
3. Enter user name and password.
4. Click **Save**.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

1. Go to **System → System Settings → Network → Network → Other**.
2. Set **Multicast** parameters.



Note

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the CMS software, the multicast address must be the same as that of the device.

-
3. Click **Save**.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

Hik-Connect provides mobile phone application and platform service to access and manage your video recorder, which enables you to get a convenient remote access to the video security system.

Steps

1. Go to **System → System Settings → Network → Hik-Connect**.

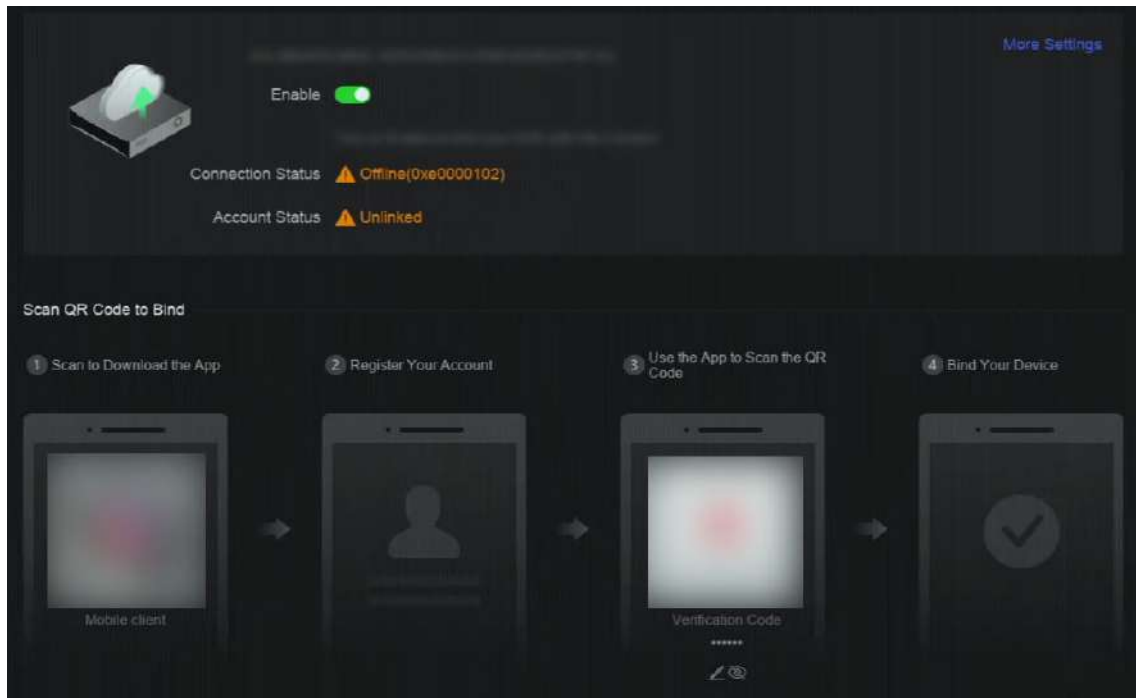


Figure 4-4 Hik-Connect

2. Turn on **Enable**, and the service terms will pop up.
3. Accept the service terms.
4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.
 - Download the app from <https://appstore.hikvision.com>.



Figure 4-5 Download Hik-Connect

5. Register an account at the app.
6. **Optional:** Click **More Settings** to enable **Stream Encryption**, **Platform Time Sync**, and **Adaptive Bitrate Streaming**, or edit **Server IP Address**.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

7. Click  to set verification code.
8. Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.



Note

If the device is already bound with an account, you can click **Unbind** to unbind with the current account.

Result

- If your device is connected with Hik-Connect, **Connection Status** will be **Online**.
- If your device is bound with a Hik-Connect account, **Account Status** will be **Linked**.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

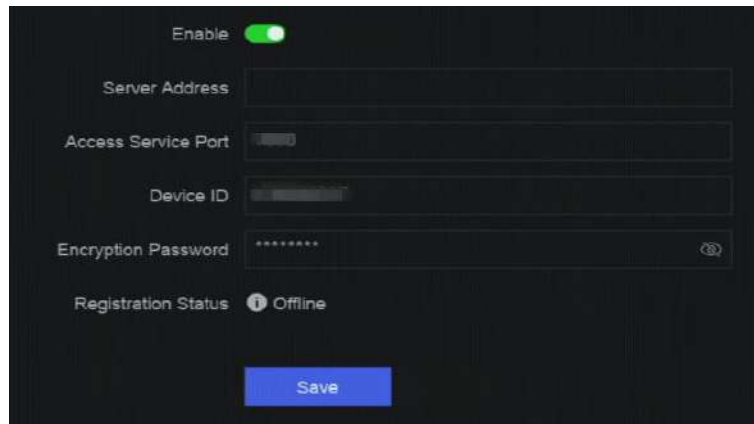
OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

1. Go to **System** → **System Settings** → **Network** → **Platform Access** → **OTAP** .



Enable ☒

Server Address

Access Service Port

Device ID

Encryption Password

Registration Status Offline

Save

Figure 4-6 OTAP

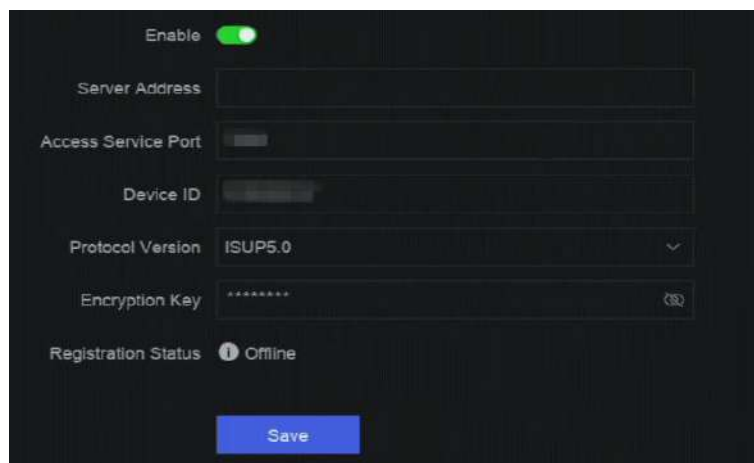
2. Turn on **OTAP**.
3. Set the parameters.
4. Click **Save**.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the third-party platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to **System → CX → System Settings → Network → Platform Access → ISUP**.



Enable ☒

Server Address

Access Service Port

Device ID

Protocol Version ISUP5.0

Encryption Key

Registration Status Offline

Save

Figure 4-7 ISUP

2. Turn on **Enable**.



Note

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click **Save**.

You can see the registration status (online or offline) after the device is restarted.

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to **System → System Settings → Network → Platform Access → SDK**.

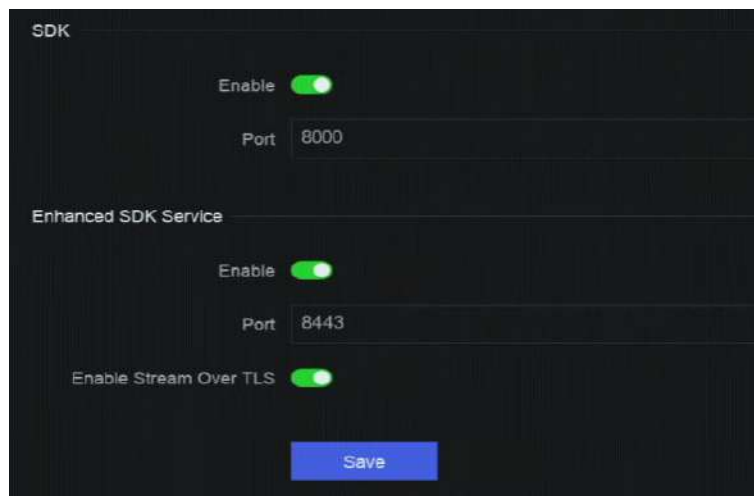


Figure 4-8 SDK Service

2. Configure **SDK** and **Enhanced SDK Service** according to your requirement.



Note

The port for **Enhanced SDK Service** is 8443 by default.

3. **Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
4. Click **Save**.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to **System → System Settings → Network → Platform Access → ISAPI** to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to **System → CX → System Settings → Network → Platform Access → ONVIF**.

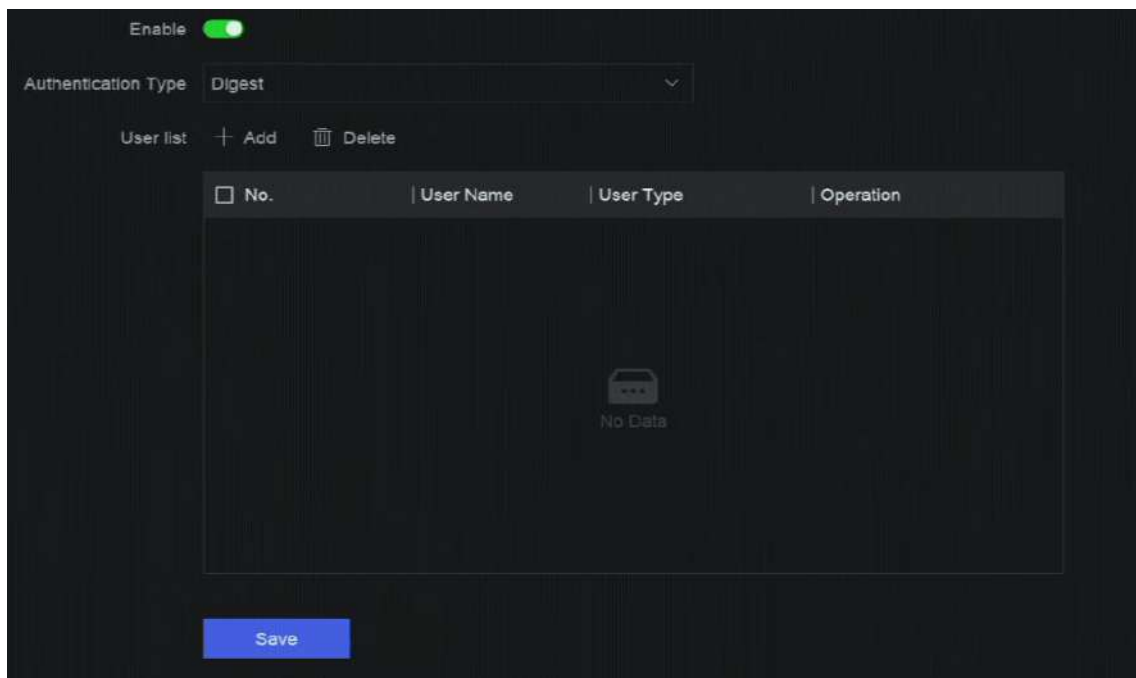


Figure 4-9 ONVIF

2. Turn on **Enable**.
3. Select an authentication type.
4. Click **Add** to add a user.
5. Set the user name and password.



Caution

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: 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

6. Click **Save**.
-

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to **System → System Settings → Network → Platform Access → Log Server**.

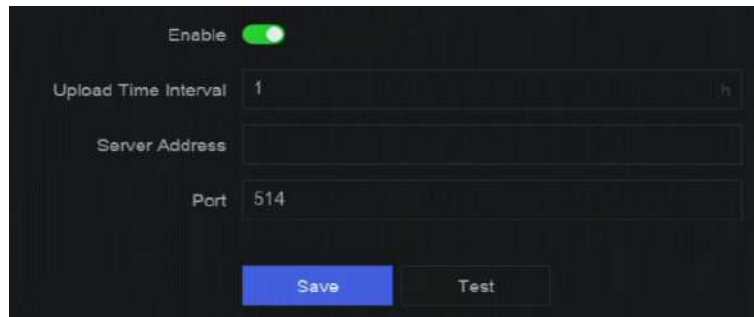


Figure 4-10 Log Server

2. Turn on **Enable**.
3. Set **Upload Time Interval**, **Server IP Address**, and **Port**.
4. **Optional**: Click **Test** to check if parameters are valid.
5. Click **Save**.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **HTTP(S)**.

The screenshot shows a configuration page with three main sections: HTTP, HTTPS, and HTTP/HTTPS Authentication. In the HTTP section, the 'Enable' toggle is turned on (green) and the 'Port' is set to 80. In the HTTPS section, the 'Enable' toggle is also turned on (green), with a note 'Ensure the client TLS version is enabled.' and a link to 'TLS Settings'. The 'Port' is set to 443. Below this, the 'Enable HTTPS Browsing' toggle is turned off (grey). The 'HTTP/HTTPS Authentication' section has 'Authentication Type' set to 'Digest' and 'Digest Algorithm' set to 'MD5'. A note states 'Authentication type and digest algorithm are valid for both HTTP and HTTPS.' At the bottom is a blue 'Save' button.

Figure 4-11 HTTP(S)

2. **Optional:** Turn on HTTP or HTTPS.
3. View or edit **Port** of HTTP or HTTPS.
4. Set **HTTP/HTTPS Authentication**.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click **Save**.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

1. Go to **System → System Settings → Network → Network Service → RTSP**.



Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

Two authentication types are selectable, if you select **Digest**, only the request with digest authentication can access the video stream by RTSP via the IP address. For security reasons, it is recommended to select **Digest** as the authentication type.

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click **Save**.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **WebSocket(s)** .
2. Turn on **Enable**.
3. Set **Port**.
4. Click **Save**.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ (Universal Plug and Play), and manual mapping. UPnP™ can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

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.

Steps

1. Go to **System → System Settings → Network → Network Service → NAT**.

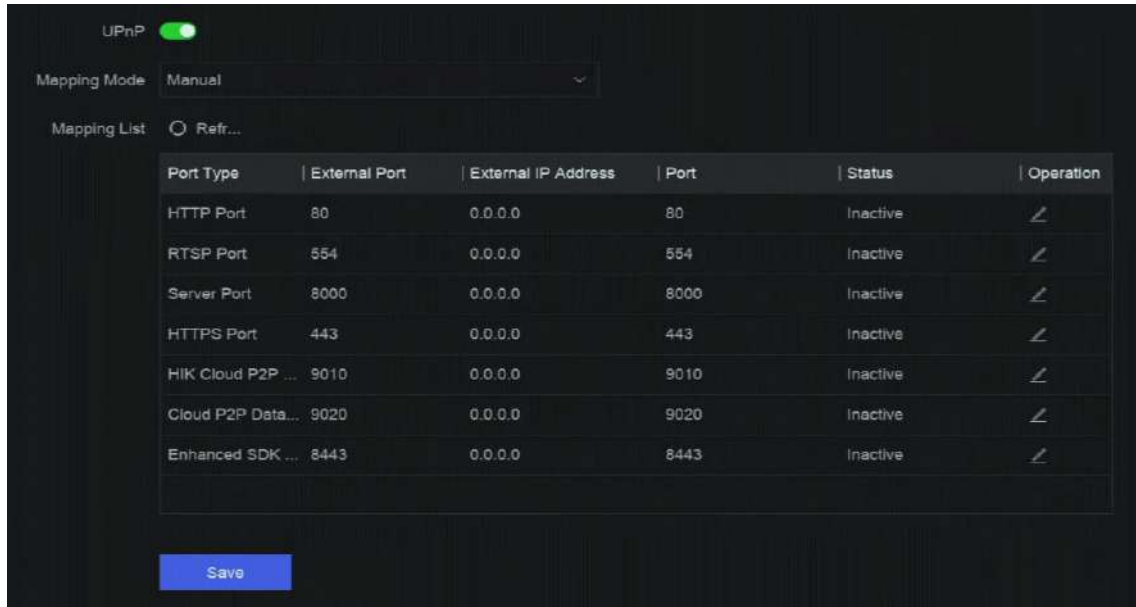


Figure 4-13 Port Mapping (NAT)

2. Turn on **Enable**.
3. Set **Mapping Mode**.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If **Mapping Mode** is selected as **Manual**, click  to edit corresponding ports.



Note

- The value of the RTSP port number 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.
- **External Port** indicates the internal port number for port mapping in the router.

5. Click **Save**.

What to do next

Enter the virtual server settings page of router, then fill in the blank of internal/external source port with the internal/external port value, and other required contents.

4.3.5 Configure IoT

You can configure the network port through which the NVR will receive alarms from a security control panel.

Go to **System → System Settings → Network → Network Service → IoT** to enable the function and configure the port number.



Note

The port number you configured here should be the same as the alarm sending port on the security control panel.

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to **System → System Settings → User Management**.

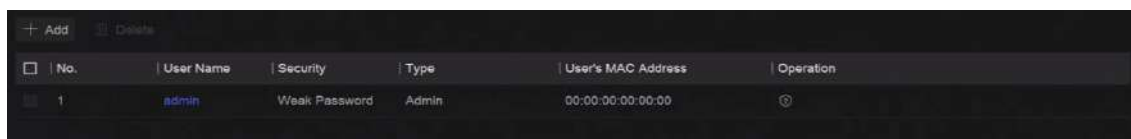


Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description
	Set account security.
Add	Add a new guest or operator user.
	Delete the selected user.

Note

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to **System → Device Access → Device → Video Device → Online Device List**.
2. Select the device(s) from the list.

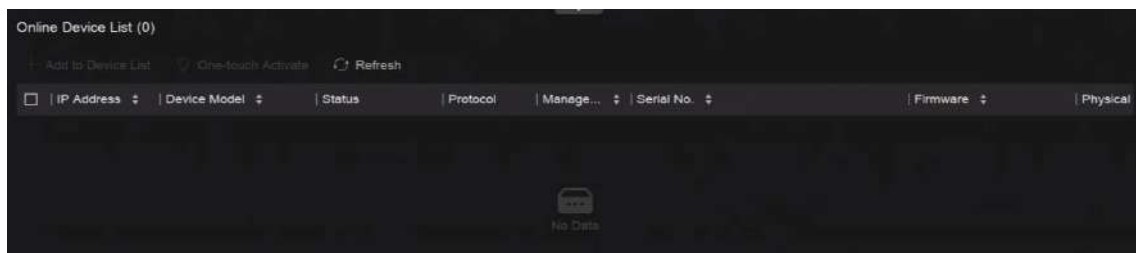


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click **Add to Device List**.



Note

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password.
- If the network camera to add has not been activated, you can activate it in the network camera list of camera management interface.
- When a network camera is successfully added, its status would be **Online**.
- You can click the device name to add its parameters.

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with that of your video recorder.
- Ensure the network connection is valid and correct.
- Ensure the network camera is activated.

Steps

1. Go to **System → Device Access → Device → Video Device**.

The screenshot shows the 'Add Device' window. At the top, there's a title bar 'Add Device' with a close button. Below it is a section 'Online Device List (0)' with a 'Refresh' button and a circular arrow icon. Under this section is a table with columns: No., IP Address, Device Model, Status, Protocol, Manag..., and Serial No. The table is empty, showing 'No Data' with a camera icon. Below the table are several input fields: 'IP Address' with a 'Test' button, 'Device Name' (containing 'IPCamera 01'), 'Protocol' (a dropdown menu showing 'ONVIF' and a 'Protocol Manag...' button), 'Management Port' (containing '80'), 'User Name' (containing 'admin'), 'Password' (empty), and 'Transfer Protocol' (a dropdown menu showing 'Auto'). There is also a checkbox labeled 'Use Channel Default Password' which is currently unchecked.

Figure 6-2 Add Network Camera Manually

2. Click **Add**.
3. Enter network camera parameters.

Use Channel Default Password

If it is enabled, the video recorder will add the camera by the set channel default password.

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

4. **Optional:** Click **Continue to Add** to add other network cameras.
5. Click **Add**.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to **Configure PoE (Power over Ethernet) Interface** for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

1. Go to **System → Device Access → Device Configuration → Access Service → OTAP Service**.
2. Turn on **Enable**.
3. Set **OTAP Server Port** and **Encryption Key**.
4. **Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.
5. Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



Note

The solar-powered camera OTAP protocol parameters shall be the same as the device.

6. Add solar-powered camera(s) to your device.
 - If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
 - Select solar-powered camera(s) from **Online Device List**, and click **Quick Add**.
7. Click **Add** in **System → Device Access → Device → Video Device**, select **Protocol** as **OTAP**, and click **Add**.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to **Configure Recording Schedule**.

6.1.5 Add Network Camera via Custom Protocol

For network cameras that are not using standard protocols, you can configure custom protocols to add them. The system provides 8 custom protocols.

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

1. Go to **System → Device Access → Device → Video Device**.
2. Click **More → Custom Protocol Management**, or **Add → Protocol Management**.

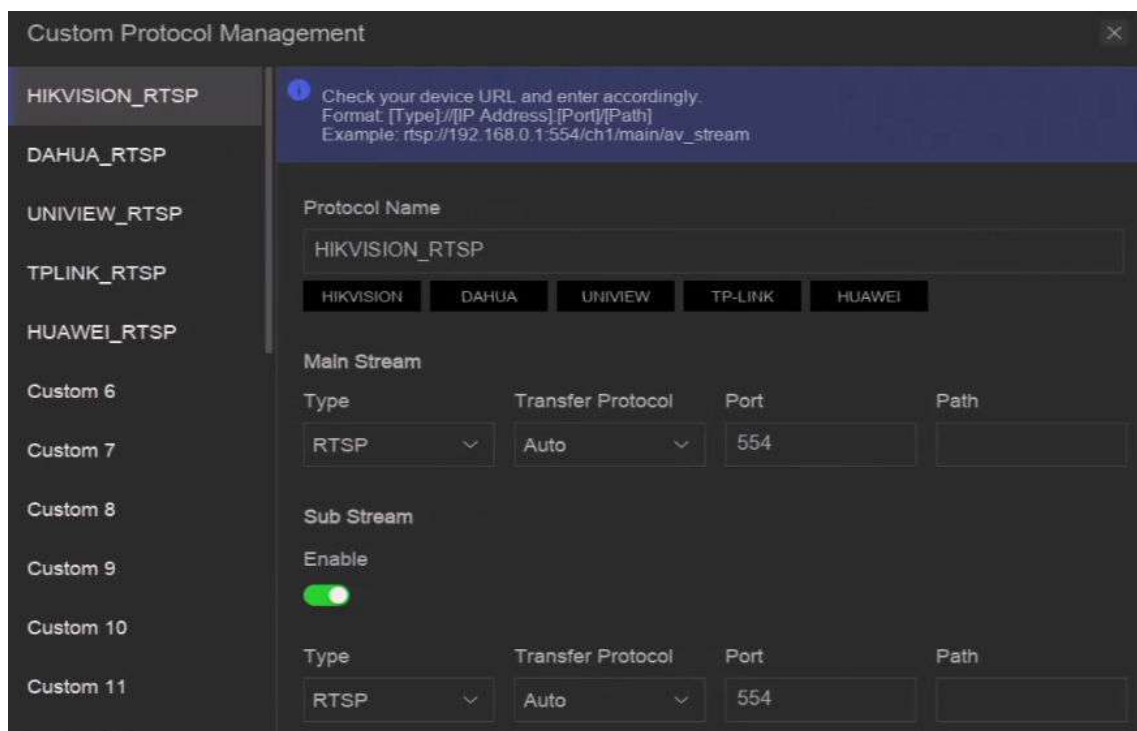


Figure 6-3 Add Network Camera via Customized Protocol

3. Select a protocol type at the left side.
4. Set protocol parameters.

Type

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

Transfer Protocol

3 types are selectable, including **Auto**, **UDP**, and **RTP Over RTSP**.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and sub-stream. The general format is *[Type]://[IP Address]:[Port]/[Resource Path]*, for example, *rtsp://192.168.0.1:554/ch1/main/av_stream*.



Note

- **Protocol Name** and **Path** can be automatically generated if you click a brand name below **Protocol Name**.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.

-
5. Click **OK**.
 6. Click **Add** in **System** → **Device Access** → **Device** → **Video Device** to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

1. Go to **System** → **Device Access** → **Device** → **Video Device**.
2. Click **Import** to import the configuration file in USB flash drive.
3. Set the folder path.
4. Click **Confirm**.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with [Access Video Device](#).

6.3 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with **Access Video Device** . If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.4 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

1. Go to **System → Device Access → Device → POS** .
2. Click **Add** to add a POS device.

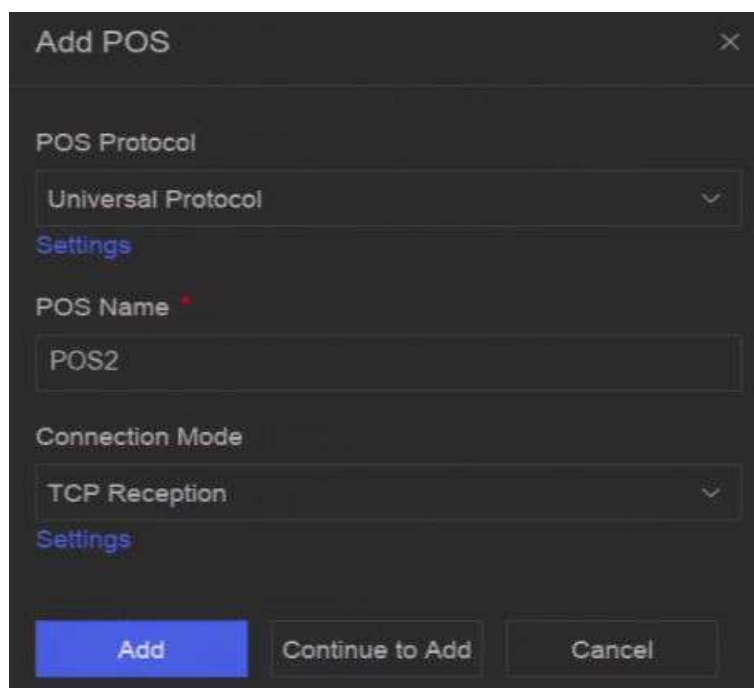


Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported.

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click **Add.**



Note

After a POS device is add, you can click  in **Operation** to configure POS text overlay.

6.5 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System → Device Access → Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to **System** → **Device Access** → **Device Grouping** .

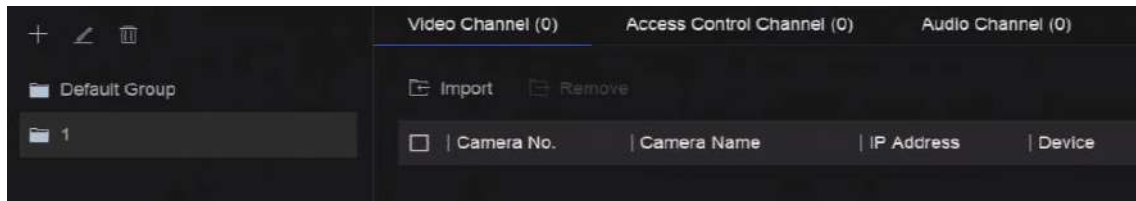


Figure 7-1 Device Grouping

2. Click  to add a group.

Note

After a group is added, you can click  /  to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.
-

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

1. Go to **System → Device Access → Device → Video Device**.
2. Click **More → Auto Switch to H.265**.
3. Enable this function.
4. Click **Save**.

8.2 Configure Display Settings

Configure the OSD (On-Screen Display), image settings, exposure settings, day/night switch settings, etc.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Display Settings**. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

Customize the image parameters including the brightness, contrast, and saturation for the live view and recording effect.

Exposure Time

Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.

Day/Night Switch

The camera can be set to day, night, or auto switch mode according to the surrounding illumination conditions.

Backlight

Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you should set the WDR value.

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Video Parameters**. Select a camera, and configure parameters as your desire.

Main Stream

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your video quality and image size. Comparing with the sub-stream, the main stream provides a higher quality video with higher resolution and frame rate.

Sub-Stream

Sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

It refers to the number of frames captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Privacy Mask**.

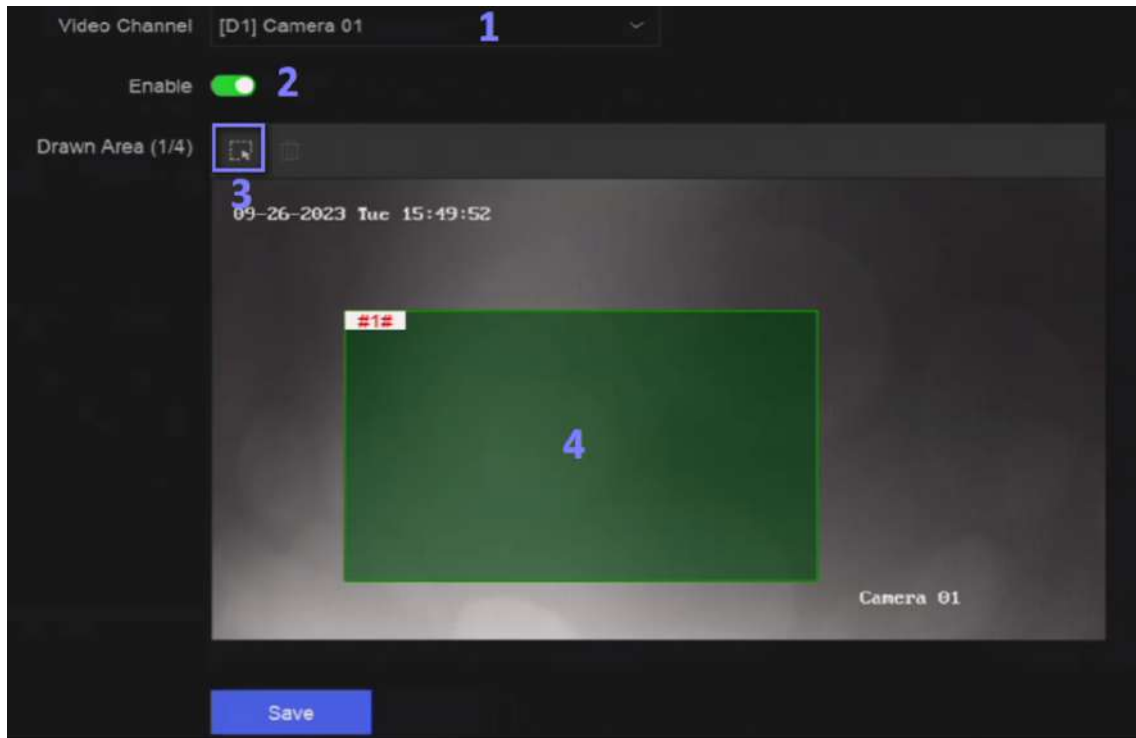


Figure 8-1 Privacy Mask

2. Select a camera.
3. Turn on **Enable**.
4. Draw mask areas on the preview window. The areas will be marked with different frame colors.



Note

Up to 4 privacy mask areas can be configured and the size of each area can be adjusted.

5. Click **Save**.

8.5 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System → Device Access → Device Configuration → Device Parameter → Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.6 Configure OTAP Service

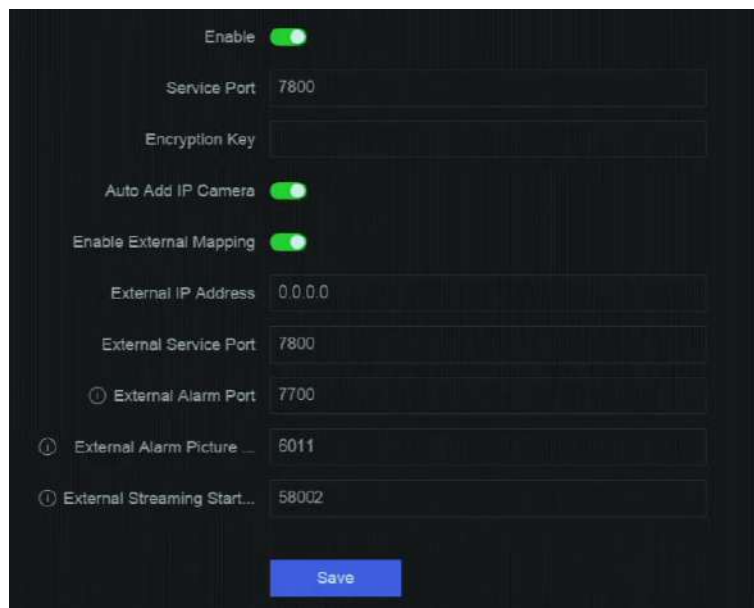
OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to **System → Device Access → Device Configuration → Access Service → OTAP Service**.



The screenshot shows the OTAP Service configuration page. At the top, there is an 'Enable' toggle switch which is turned on. Below it are several configuration fields: 'Service Port' (7800), 'Encryption Key' (empty), 'Auto Add IP Camera' (toggle on), 'Enable External Mapping' (toggle on), 'External IP Address' (0.0.0.0), 'External Service Port' (7800), 'External Alarm Port' (7700), 'External Alarm Picture' (8011), and 'External Streaming Start...' (58002). Each field has a small information icon to its left. At the bottom right, there is a blue 'Save' button.

Figure 8-2 Configure OTAP Service

2. Turn on **Enable**.
3. Set the parameters.
4. Click **Save**.

8.7 Batch Configuration

Connected devices can be configured in a batch.

Steps

1. Go to **System → Device Access → Device Configuration → Batch Configuration**.

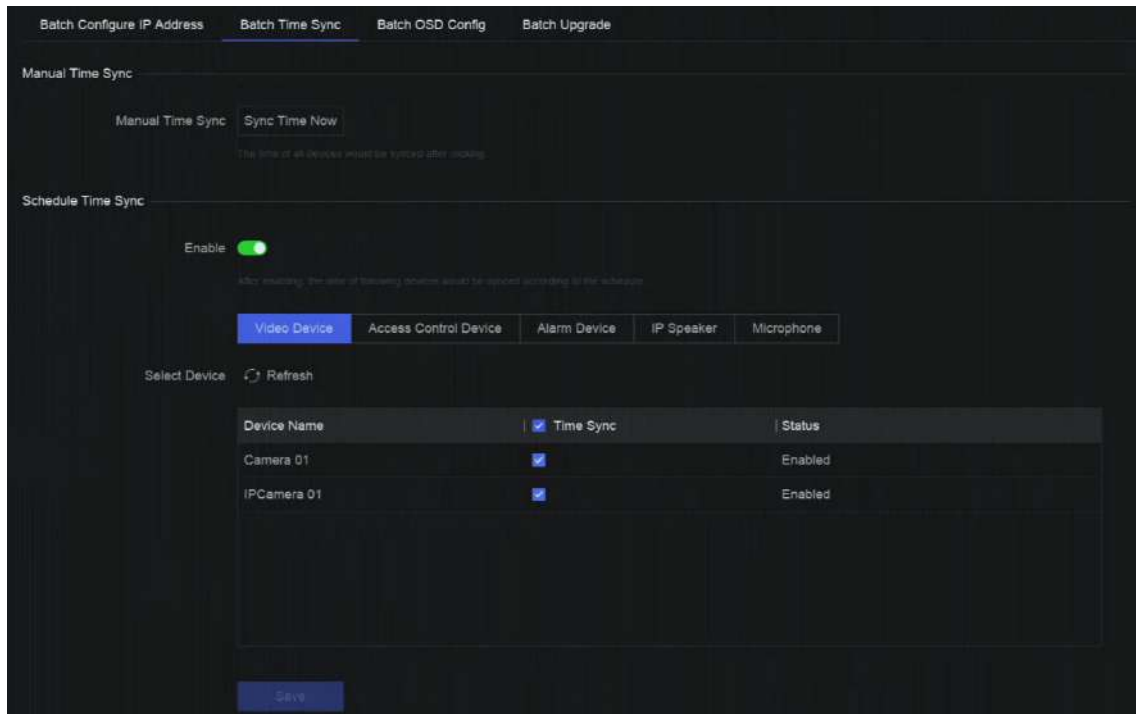


Figure 8-3 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule.

3. For IP address configuration and time sync, click **Save**.

8.8 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

1. Go to **System → Device Access → Device Configuration → PoE**.
2. Enable **Plug-and-Play** function of PoE interfaces according to your requirement.

3. Select the device type as **IP Speaker** or **Camera**.

4. If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.



Note

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click **Save**.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

A newly installed hard disk drive (HDD) must be initialized before using. You can format HDD, repair database, and view HDD status through HDD management interface.

Before You Start

Ensure the HDD is properly installed to your device.

Steps

1. Go to **System → Storage Management → Storage HDD → Storage HDD**.



HDD No.	Free Space (GB)	Capacity (GB)	Status	Type	Property	Operation
1	166	466	Sleeping	Local	R/W	[Icon]
3	3685	3726	Sleeping	Local	R/W	[Icon]
5	3685	3726	Sleeping	Local	R/W	[Icon]

Figure 9-1 Manage HDD

2. **Optional:** Perform the following operations as your desire.

Add Network HDD Add a NAS or IP SAN.

Format Format the selected HDD.

Repair Database Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Note

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out the drive, or shut down the device during the process.



Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed

across the drives in one of several ways called "RAID levels", based the redundancy and performance required.



Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

Table 9-1 HDD Requirement for Each RAID Type

RAID Type	Required Number of HDDs
RAID0	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8



Note

- The function is only available for certain models.
 - When array exception event occurs, the corresponding linkage actions can be configured in **System → System Settings → Exception** .
-

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- **Storage Mode** is set to **Quota** in **System → Storage Management → Storage Mode** .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Enable Array Mode**, or enable **Array Mode**.

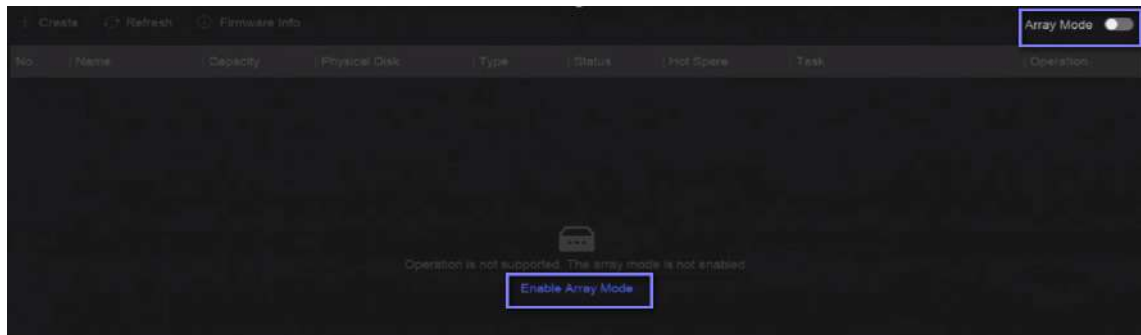


Figure 9-2 Enable RAID

- Wait for the device to restart.
- Go to **System → Storage Management → Storage HDD → Array Management** again.

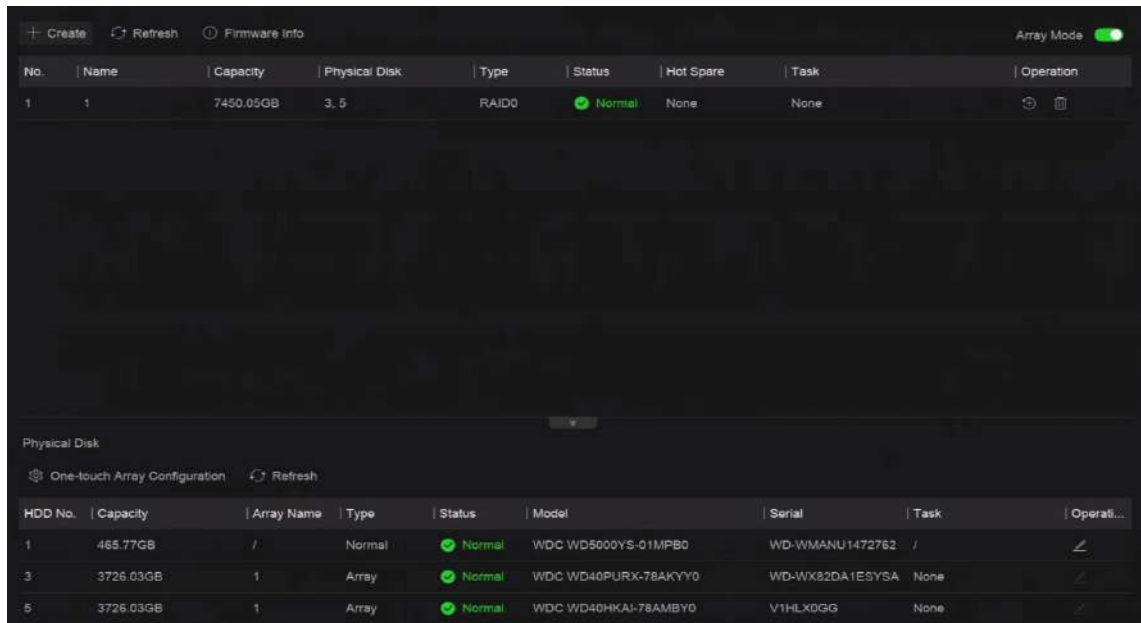


Figure 9-3 Array Management

- Create an array.

Creation Method

Description

One-touch Array Configuration

Click **One-touch Array Configuration**.



Note

By default, the array type created by one-touch configuration is RAID 5.

Manual Creation

Click **Create** to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

9.2.2 Rebuild Array

The array status includes **Functional**, **Degraded**, and **Offline**. To ensure the high security and reliability of the data stored in an array, take immediate and proper maintenance of the arrays according its status.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management**.
2. Rebuild an array.

Table 9-2 Rebuilding Method

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click  in Operation column under Physical Disk to set a hot spare disk. When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.  Note After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array. Go to System → Storage Management → Storage HDD → Array Management, and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to **System → Storage Management → Storage HDD** to click  to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Firmware Info**.
3. **Optional**: Set **Back Ground Task Speed**.

9.3 Configure Storage Mode

Steps

1. Go to **System → Storage Management → Storage Mode** .

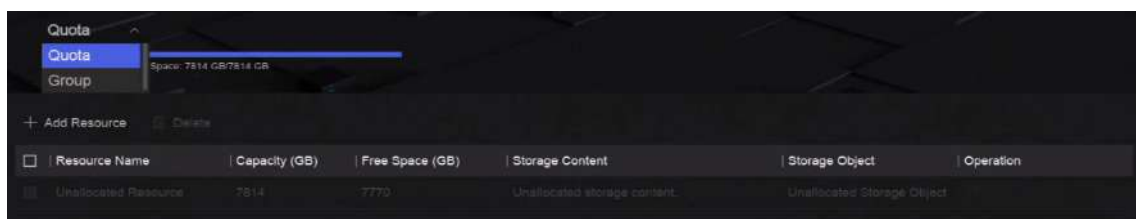


Figure 9-4 Storage Mode

2. Select **Quota** or **Group**.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

3. Set corresponding parameters.
 - **Quota**: Allocate space for storage objects.
 - **Group**: Link channels to HDD groups.

9.4 Configure Other Storage Parameters

Go to **System → Storage Management → Advanced Settings** .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.  Note - You can click  during live view or playback to add a tag. - For searching tag videos, go to  → Backup → By Tag.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.

9.5 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon  displayed at the upper-right corner.

Chapter 10 Schedule Configuration

The device will follow the schedule to store files to the disk.

10.1 Configure Schedule Template

After a schedule template is configured, you can use the template as the recording schedule.

Steps

1. Go to **System → System Settings → Template Configuration → Holiday Schedule** .
2. Click **Add**.

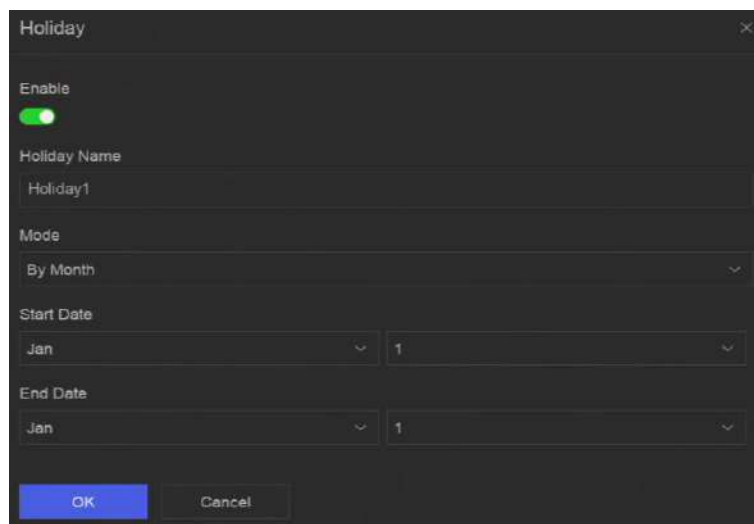


Figure 10-1 Add Holiday

3. Turn on **Enable**.
4. Configure the holiday.

Note

After holidays are configured, you will be able to set the holiday schedule independently. Holiday schedule has higher priority than normal schedule (from Mon to Sun).

-
5. Set **Storage Schedule**.
 - 1) Click **Storage Schedule**.
 - 2) Select a template name.

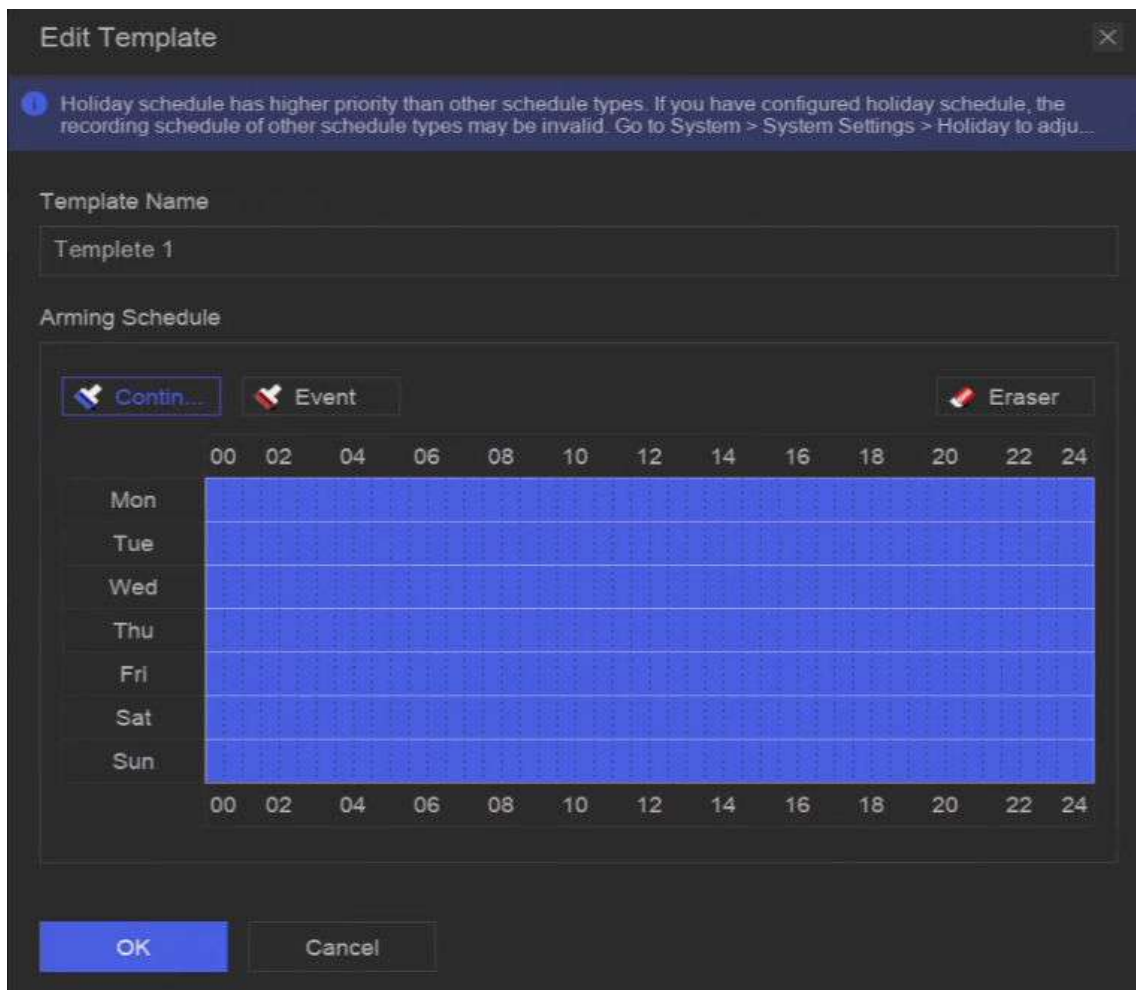


Figure 10-2 Edit Template

- 3) Select a recording type. For example, **Event**.
- 4) Drag the cursor on time bar to draw the schedule.



Note

- After moving the cursor on time bar, you can also click **00:00-24:00**  to set specified time schedule.
- You can click **Eraser** to clear schedule.



Note

You can also click **Configure Template** to configure template in **System → Storage Management → Storage Schedule → Video Recording / Picture Capture / Audio Recording**.

6. Click **OK**.

10.2 Configure Recording Schedule

The camera would automatically start/stop recording according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Video Recording** .

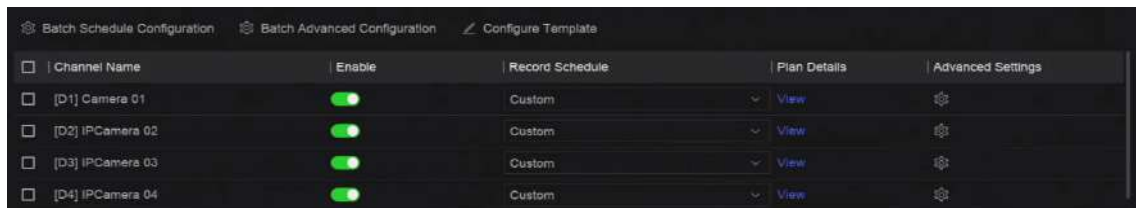


Figure 10-3 Video Recording Configuration

2. Turn on **Enable** for a camera.
3. Select a schedule type.



Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

4. Click **View** to view the schedule.



Figure 10-4 View Schedule

5. **Optional:** Click  under **Advanced Settings** to set other advanced parameters.

Table 10-1 Advanced Parameter Description

Parameter	Description
Record Audio	Enable or disable audio recording.  Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.

Parameter	Description
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

- Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
- Click **Save**.

10.3 Configure Picture Capture Schedule

The device would automatically capture live pictures according to the schedule.

Steps

- Go to **System → Storage Management → Storage Schedule → Picture Capture**.

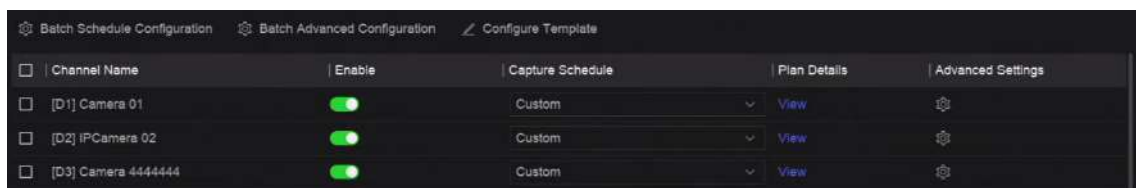


Figure 10-5 Picture Capture Configuration

- Turn on **Enable** for a camera.
- Select a schedule type.

Note

If you set **Capture Schedule** as **Custom**, you can drag the cursor on time bar to set customized picture capture schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

- Click **View** to view the schedule.



Figure 10-6 View Schedule

5. Click under **Advanced Settings** to set advanced picture parameters.

Table 10-2 Advanced Parameter Description

Parameter	Description
Capture Delay	The duration for picture capture.
Resolution	Set the resolution of the picture to capture.
Picture Quality	Set the picture quality to low, medium or high. High picture quality requires more storage space.
Interval	The time interval of capturing each live picture.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

10.4 Configure Audio Recording

The device would automatically record audios according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Audio Recording**.
2. Turn on **Enable** for a channel.
3. Select a schedule type.



Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

-
4. Click **View** to view the schedule.
 5. **Optional:** Click under **Advanced Settings** to set other advanced parameters.

Table 10-3 Advanced Parameter Description

Parameter	Description
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the channel records 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 recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

Chapter 11 Live View

11.1 Configure Live View Layout

Live view displays the video image of each camera in real time.

Steps

1. Go to **Live View**.
2. Click  at the lower-right corner.
3. Select a window division type, or click **Custom** to customize a new type as your desire.
4. Move the cursor on **Default View** in **View**.
5. Click  at the right side of **View**.
6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
7. Click .

11.2 GUI Introduction

You can view live image, play live audio, capture pictures, perform instant playback, etc.

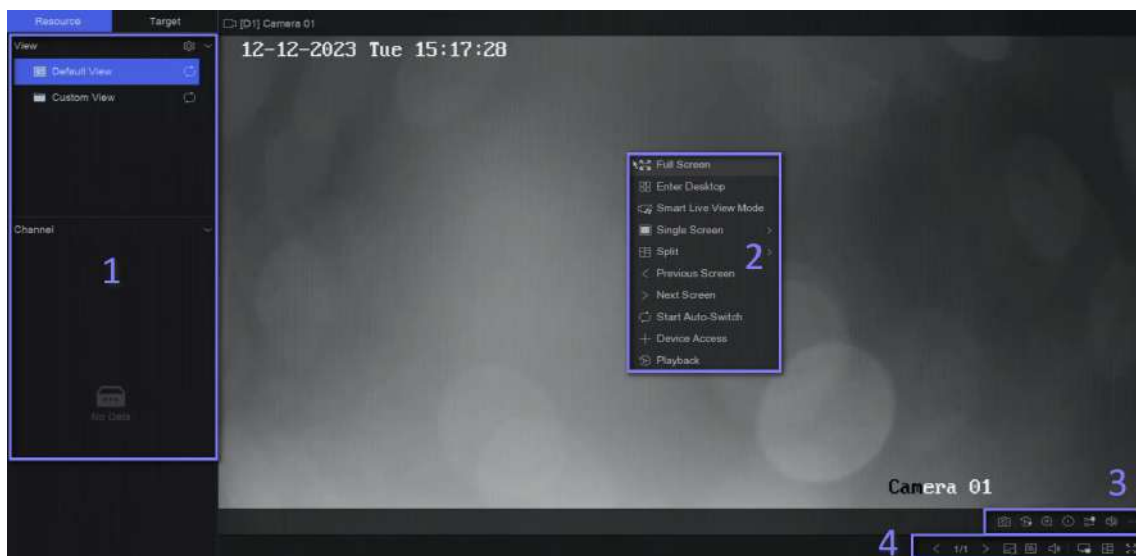


Figure 11-1 Live View (Type 1)

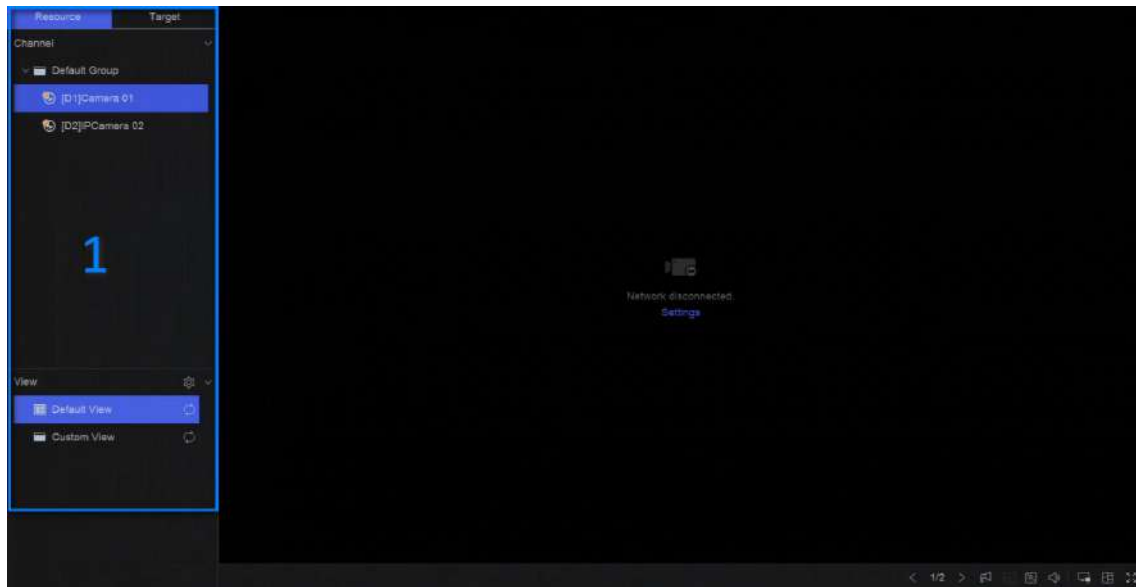


Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window. If you click Target , you can view live target detection results in the list, and click  to configure the corresponding settings.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	Channel tool bar. - Click  to add a tag go the channel. After adding, you can go to  → Backup → By Tag to search videos by tag. - You can select  → Show VCA Info to display rule frames.
4	Live view tool bar. Functions like Voice Broadcast , Display VCA Info and Switch Output can be performed here.

Note

- You can scroll up/down your mouse to turn to previous/next screen.
- If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Table 11-2 PTZ Operation

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click  .
		Call a preset: Click  .
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click  .
		3. Add presets for the patrol. 4. Click OK . Call a patrol: Click  .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	Set a pattern: 1. Click  .
		2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click  .

Note

If the PTZ panel cannot be used, please click  to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.



Figure 12-1 Playback

Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	Channel tool bar. - Click  to add a tag to the channel. After adding, you can go to  → Backup → By Tag to search videos by tag. - Click  to lock the video. After a video is locked, it will not be overwritten. After locking, you can go to  → Backup → By Tag to search videos by lock.

No.	Description
	- Select  → Dual-VCA to search videos that can trigger the corresponding event rule. Refer to the event configuration steps for details of each event type.  Note In order to use this function, go to Configuration → Device Access → Device Configuration → Device Parameter → Display Info. on Screen to turn on Enable Dual-VCA via web browser, and go to System → Storage Management → Advanced Settings to turn on Save Camera VCA Data via local GUI interface. - You can select  → Show VCA Info to display rule frames.
5	Playback timeline. - Position the cursor on the timeline, drag the timeline to position to a certain time. - Period marked with blue bar contains video. Red bar indicates the video in the period is event video. - Scroll up/down to zoom out/in timeline.
6	Playback tool bar. - Click  to set normal video and smart video (the video that contains smart data) playback strategy. - Click  (Smart Search), then follow the pop-up tips to draw event rule and search videos that can trigger the corresponding event rule. The operations are similar with Dual-VCA function. - Click  to perform AcuSearch function. Refer to AcuSearch for details. - Click  /  to show videos that contain human/vehicle.  Note In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types.

12.2 Normal Playback

Play back videos for a channel. For certain devices, synchronous playback may be allowed for several channels.

Steps

1. Go to **Playback** → .
2. Select channel(s) in the list at the left side.



Group playback: Select a group in the list, and channels in the group can be played back.

3. Select a date in the calendar.



The blue triangle at the calendar date corner indicates there are available videos.

4. **Optional:** Play back videos that contain human or vehicle targets.
 -  : Videos that contain human would be marked in red.
 -  : Videos that contain vehicle would be marked in red.

12.3 Event Playback

When you select the event playback mode, the system will analyze and mark videos that contain the motion detection, line crossing detection, or intrusion detection information

Before You Start

- Ensure the camera has enabled **Dual-VCA**. You can enable it via the camera web browser interface in **Configuration** → **Video/Audio** → **Display Info. on Stream**.
- Ensure your video recorder has enabled **Save Camera VCA Data** in **Storage management** → **Advanced Settings**.

Steps

1. Select **Playback** → .
2. Select a date in the calendar.



The blue triangle at the calendar date corner indicates there are available videos.

3. Click  → **Dual-VCA** at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
4. Click **Search**.

Videos meet the detection rule requirement will be marked in red.
5. Click  to set normal video and smart video (the video that contains smart data) playback strategy.



Note

If **Dual-VCA** is not used, red segments in progress bar means the smart videos are generated by the original event.

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

1. Go to **Playback** →
2. Select a camera from the camera list.
3. Select a date on the calendar.
4. Click **Search**.
The retrieved video will be divided into one-hour slices for playback.
5. **Optional:** Select an one-hour slice and click to divide it into one-minute slices for playback.

12.5 Sub-Period Playback

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

Steps

1. Go to **Playback** →
2. Select a camera.
3. Set the start time and end time.
4. Click **Search**.

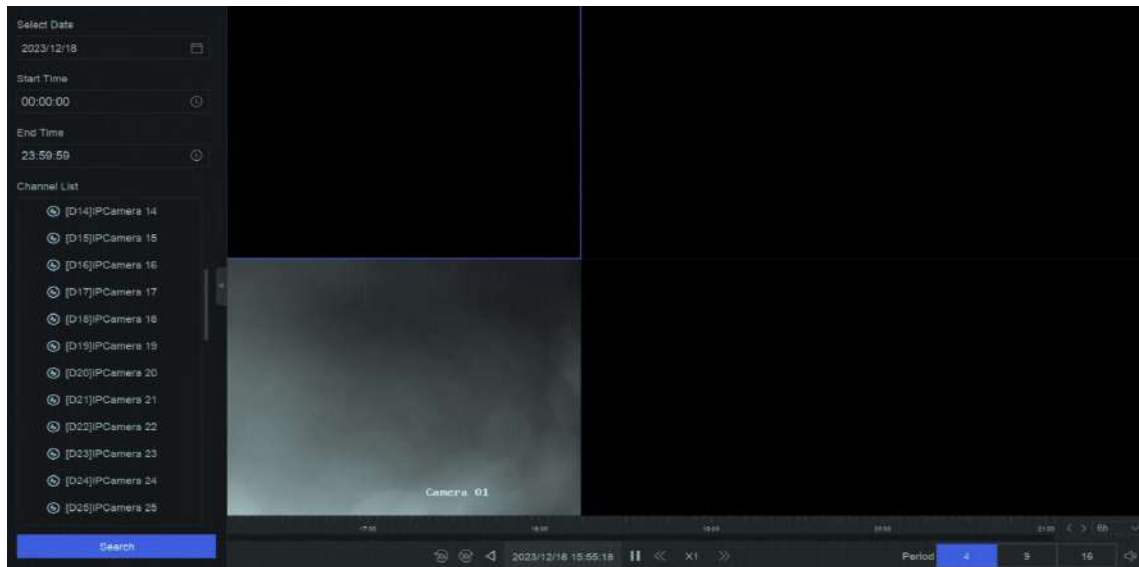


Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.



Note

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.

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Basic Event / Generic Event** .
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Configuration	
Motion Detection	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. • AI by NVR: The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects. • AI by Camera: The motion detection event will be analyzed by camera. • Detection Target: Human and Vehicle are selectable, apart from false alarms, only the	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.

Event Name	Event Description	Rule Configuration	
		selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-2 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.2 Perimeter Protection

Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

Configure Line Crossing Detection

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Steps



Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center →  → Event Configuration → Perimeter Protection**.

2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Line Crossing**.
6. Turn on **Enable**.

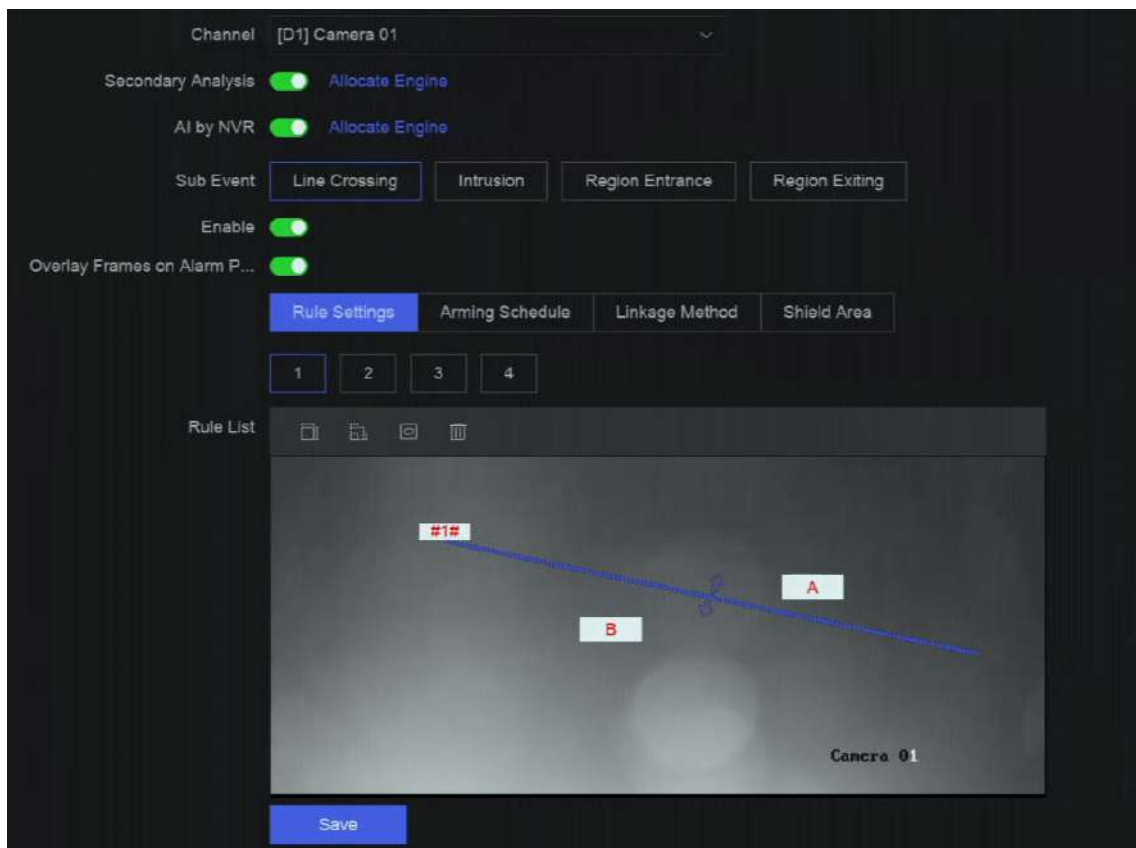


Figure 13-1 Line Crossing Detection

7. Click **Rule Settings** to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set **Direction**, **Sensitivity**, and **Detection Target**.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions 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.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Click  /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-3 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Intrusion Detection

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

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Intrusion**.

6. Turn on **Enable**.

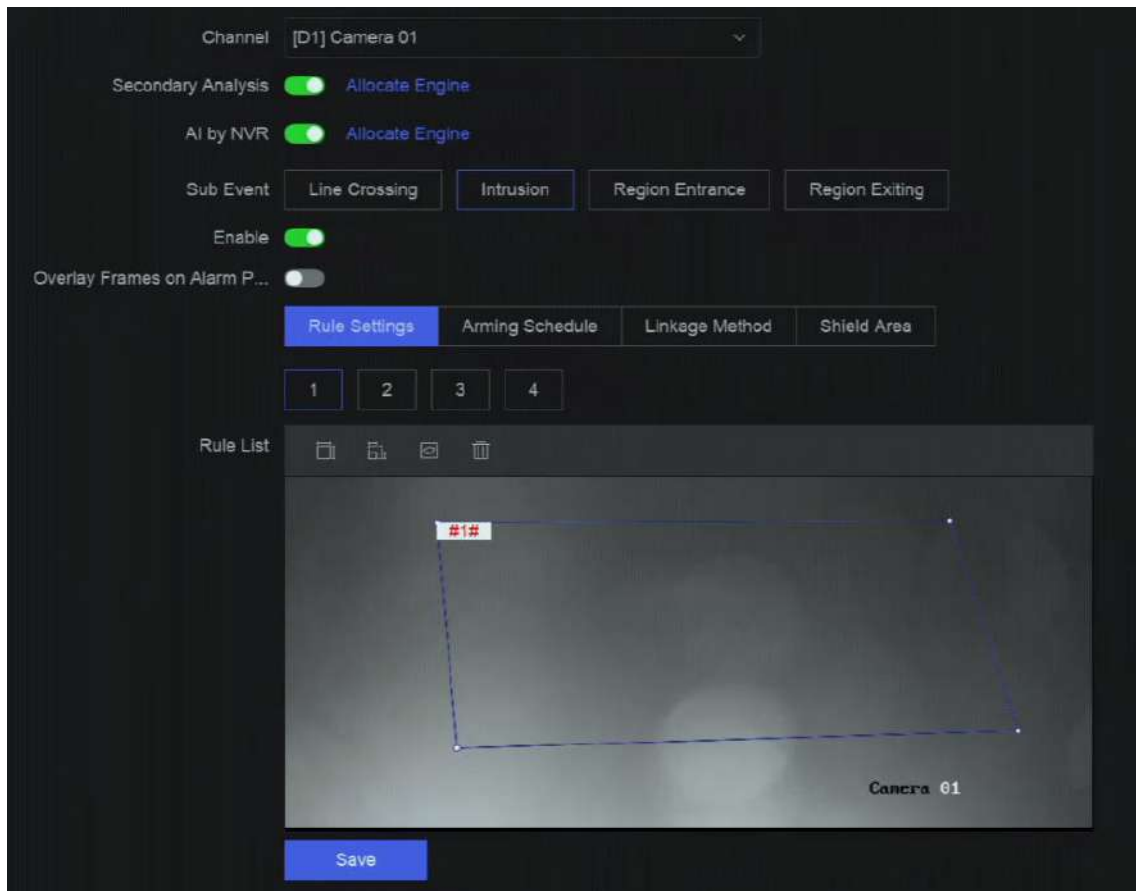


Figure 13-2 Intrusion Detection

7. Click **Rule Settings** to detection rules.

1) Select a rule number. For example, select **1**.

2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.

3) Set **Time Threshold**, **Sensitivity**, and **Detection Target**.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

4) **Optional:** Click  /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.

5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supported.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-4 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Steps



Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.



Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Region Entrance**.
6. Turn on **Enable**.

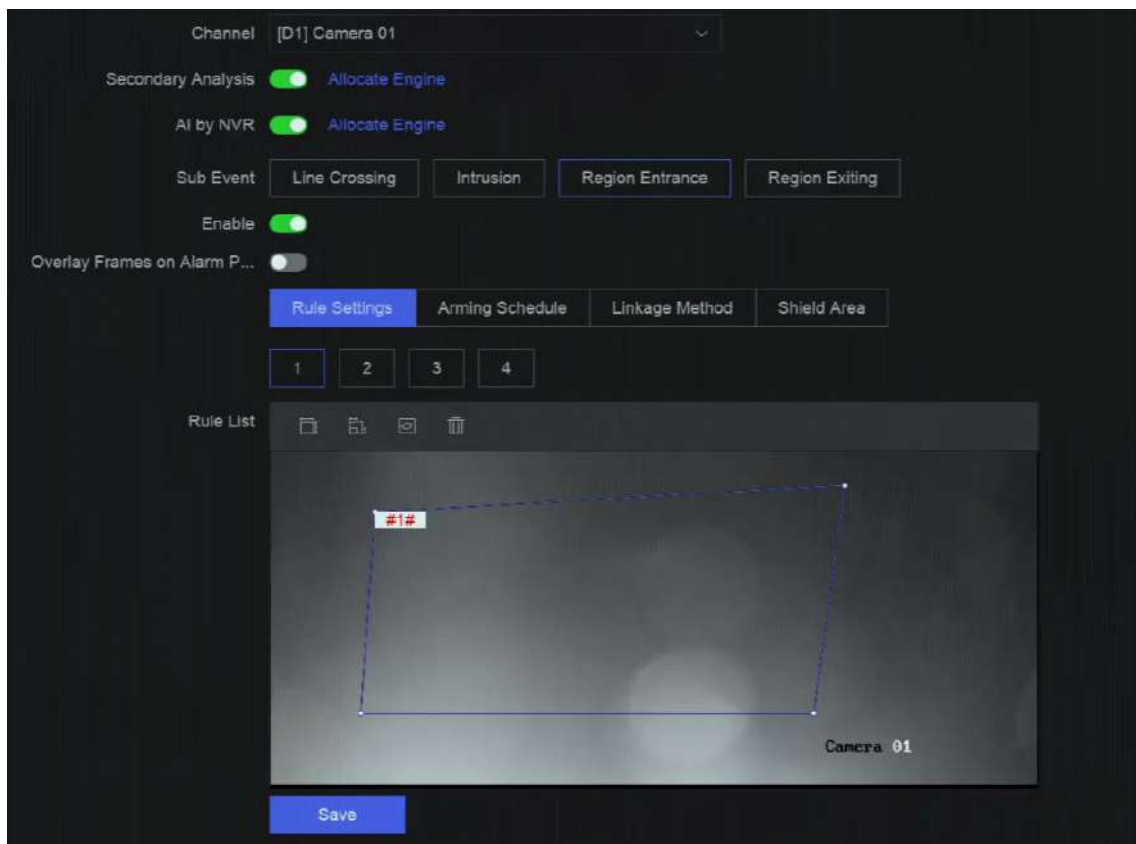


Figure 13-3 Region Entrance Detection

7. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set **Sensitivity** and **Detection Target**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click Arming Schedule to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

9. Click Linkage Method to set linkage methods.

Table 13-5 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.

3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Region Exiting**.

6. Turn on **Enable**.

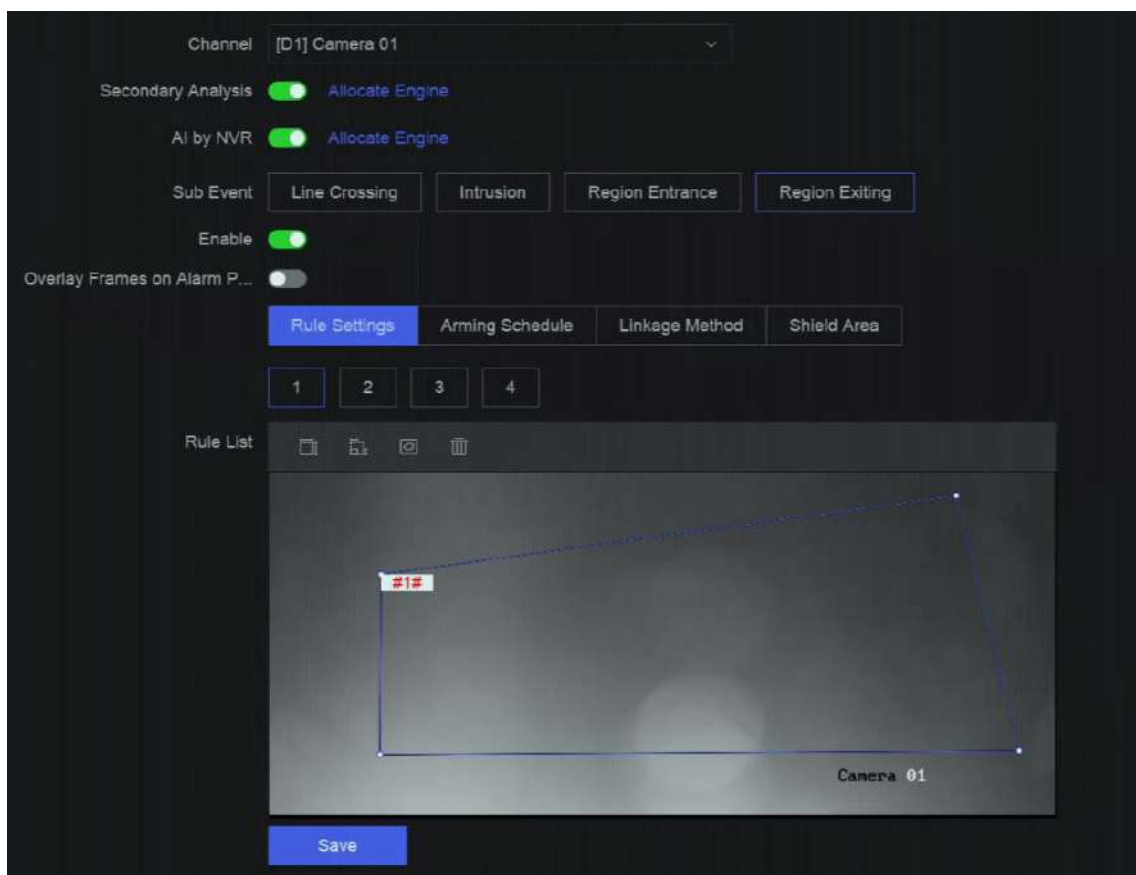


Figure 13-4 Region Exiting Detection

7. Click **Rule Settings** to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral area.
- 3) Set **Sensitivity** and **Detection Target**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

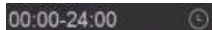
Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

- 4) **Optional**: Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-6 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System →

Linkage Method	Description
	Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Abnormal Behavior Event** .
2. Select a camera
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10]. Sensitivity Similarity of the background image to the object. The higher the value is, more
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions	

Event Name	Event Description	Rule Configuration
	can be taken when the alarm is triggered.	easily the detection alarm will be triggered.
Object Removal Detection	The object removal detection function detects the objects removed from a predefined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	d. Optional: Repeat the above steps to set another one.
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Percentage . Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. d. Optional: Repeat the above steps to set another one.

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **Event Center → Event Configuration → Smart Settings → Algorithm Configuration → Algorithm Management**.

Steps

1. Go to **Event Center →  → Event Configuration → Target Event**.
2. Select a camera.
3. Select an event.
4. Turn on **Enable**.
5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can be triggered when a human face is detected.	-
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	• Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). • Supports configuring prompts for failed and succeeded comparisons.
Stranger Detection	Faces not in the list library appearing in the video will be identified as strangers.	• Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). • Supports configuring the prompt for detecting strangers.
Multi-Target-Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Thermal Event** .
2. Select a camera.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature Detection	An alarm would be triggered when the temperature exceeds the threshold value.
Perimeter Protection	Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

- Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

- Click **Linkage Method** to set linkage methods.

Table 13-11 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System →

Linkage Method	Description
	Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Alarm Input Event** .
2. Select an alarm input name.

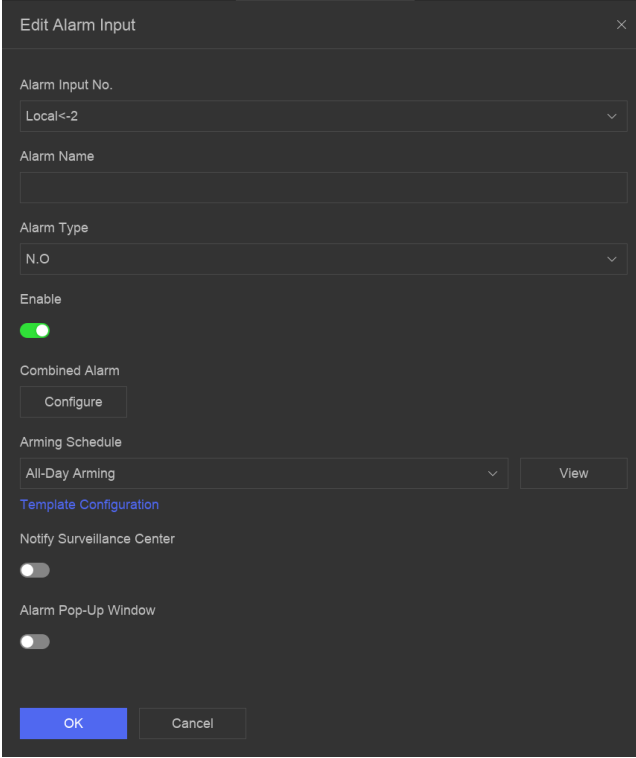


Figure 13-5 Configure Alarm Input

Note

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

3. Edit **Alarm Name**.
4. Set **Alarm Type**.
N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

5. Turn on **Enable**.

6. **Optional**: If you select **Local<-1** in Step 2, select the processing method.

- Select **Process Alarm Input**, and then you can set the corresponding arming schedule, linkage methods, etc.



Note

The operations below are all available when you select this processing method.

- Select **Quick Disarming**, and then linkage methods of all events will be disabled.

7. Click **Configure** to configure combined alarm.

- 1) Select a channel.
- 2) Select combined alarm events such as motion detection and video tampering detection.
- 3) Click **OK**.

The combined alarm will be triggered when it receives alarms from both alarm input and events.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click 00:00-24:00 to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-12 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Click **Save**.

13.1.7 Audio Analysis Event

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Audio Analysis**.
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-13 Audio Analysis Event

Event Name	Event Description	Rule Configuration
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	Sudden Increase of Sound Intensity Detection Detects a steep sound increase in the scene. Sudden Decrease of Sound Intensity Detection Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered. Sound Intensity Threshold It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

- Click **Linkage Method** to set linkage methods.

Table 13-14 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

- Click **Save**.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

- Go to **Event Center** → → **Event Configuration** → **Linkage Configuration** or **System** → **Event Configuration** → → **Event Configuration** → **Linkage Configuration**.
- Click **Email** to configure email parameters.

Table 13-15 Email Linkage

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

3. Click **Audio Management** to manage audio files for alarm linkage.



Note

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.



Note

- This linkage action is only available for few event types.
- The uploaded audio file should be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.

5. Click **Alarm Output** to set alarm output parameters.



Note

- Click the name of each alarm output to edit it.
- The alarm output No. is the same as the one at the device rear panel. For example, **Local->1** means the alarm out No. 1 at the device rear panel.

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

- If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.



Note

This linkage action is only available for few event types.

- Click **Security Control Panel** to set the connected security control panel parameters.

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

- Go to **Event Center** → → **Event Configuration** → **Linkage Configuration** or **System** → **Event Configuration** → → **Event Configuration** → **Linkage Configuration**.

Batch Schedule Configuration		Disarming Template Configuration			
☐ Channel Name	☐ Allow Disarming ⓘ	Disarming Status	Disarming Method	Disarming Template	Details
☐ [D1] Camera 01	☒	Disabled	Quick Disarming	Mute Disarming	
☐ [D2] IPCamera 02	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D3] IPCamera 03	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D4] IPCamera 04	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D5] IPCamera 05	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D6] IPCamera 06	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D7] IPCamera 07	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D8] IPCamera 08	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D9] IPCamera 09	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D10] IPCamera 10	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D11] IPCamera 11	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D12] IPCamera 12	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D13] IPCamera 13	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D14] IPCamera 14	☐	Disabled	Quick Disarming	Mute Disarming	
☐ [D15] IPCamera 15	☐	Disabled	Quick Disarming	Mute Disarming	

Figure 13-6 Disarming Configuration

- Select channel(s) that are allowed for disarming.
- Click **Batch Schedule Configuration**.
- Turn on **Enable**.
- Select **Disarming Template**. Only two types are available



Note

Currently, only two template types are available and each template parameters cannot configured.

6. Click **OK**.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center** → → **Event Configuration** → **Batch Configuration** or **System** → **Event Configuration** → → **Event Configuration** → **Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

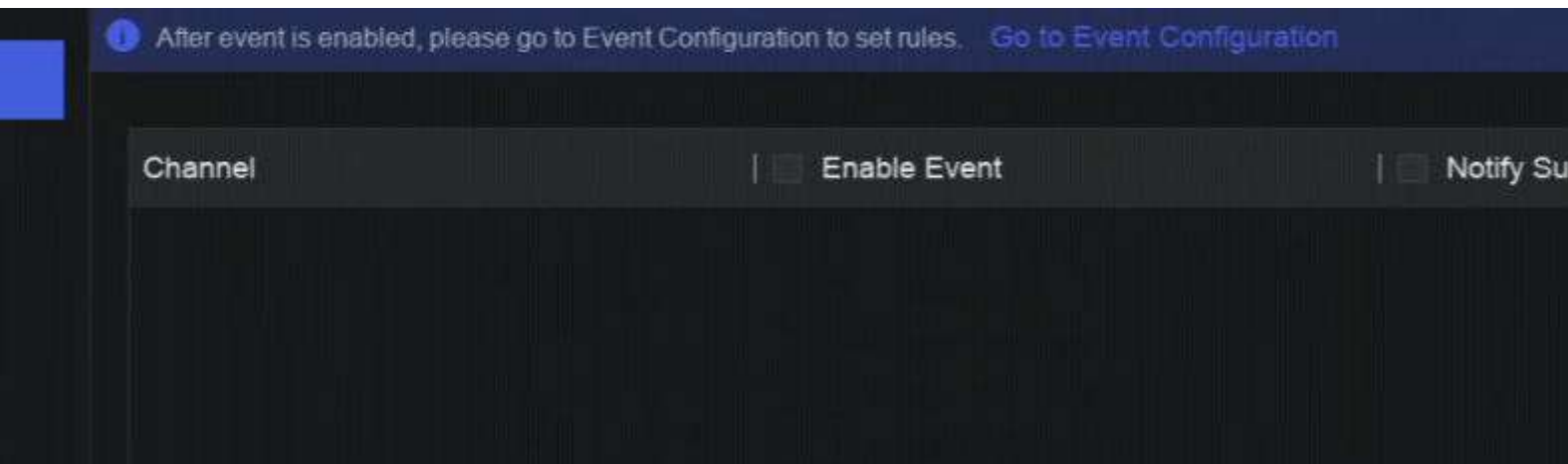


Figure 13-7 Batch Configuration

13.5 Event Search

You can search event files like videos and pictures according to the searching condition.

Steps

1. Go to **Event Center** → .

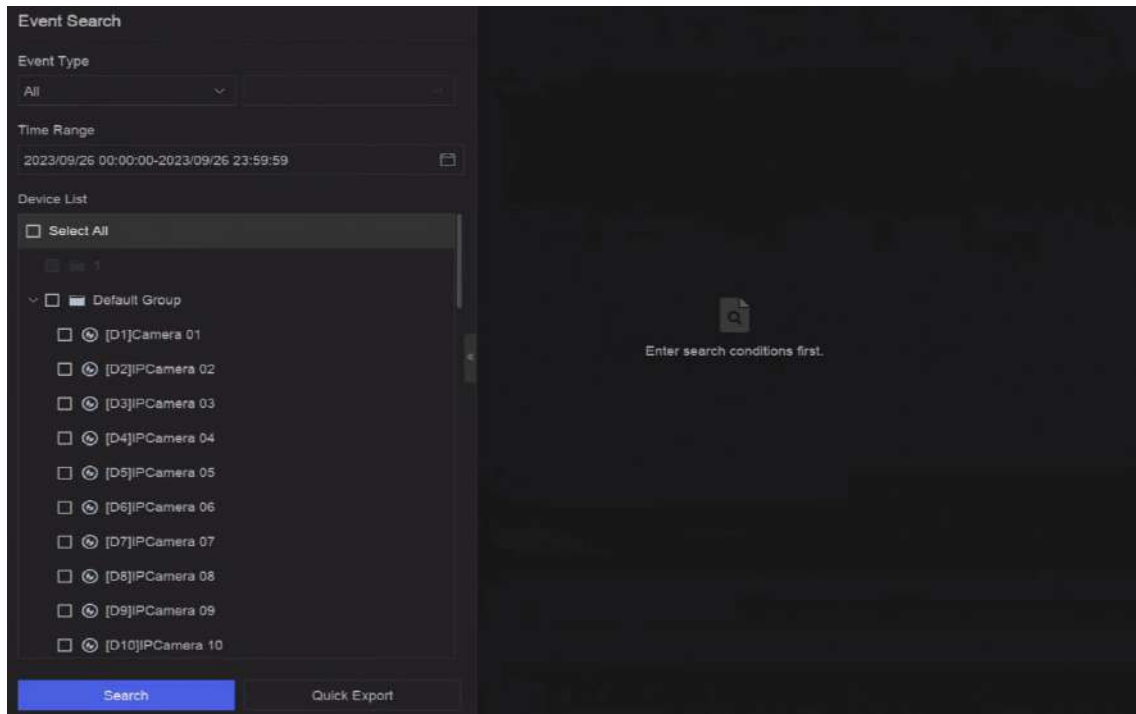


Figure 13-8 Event Search

2. Specify detailed conditions, including event type, time, channel, etc.
3. Click **Search**.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

1. Go to **Event Center** → .
2. Click **Real-Time Alarm**.
3. Select the alarm from the list.

If there are too many alarms, click **Filter** to search and find the alarm.

4. Click **Playback**, and the alarm recording video would be played back.
5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to **Backup**.

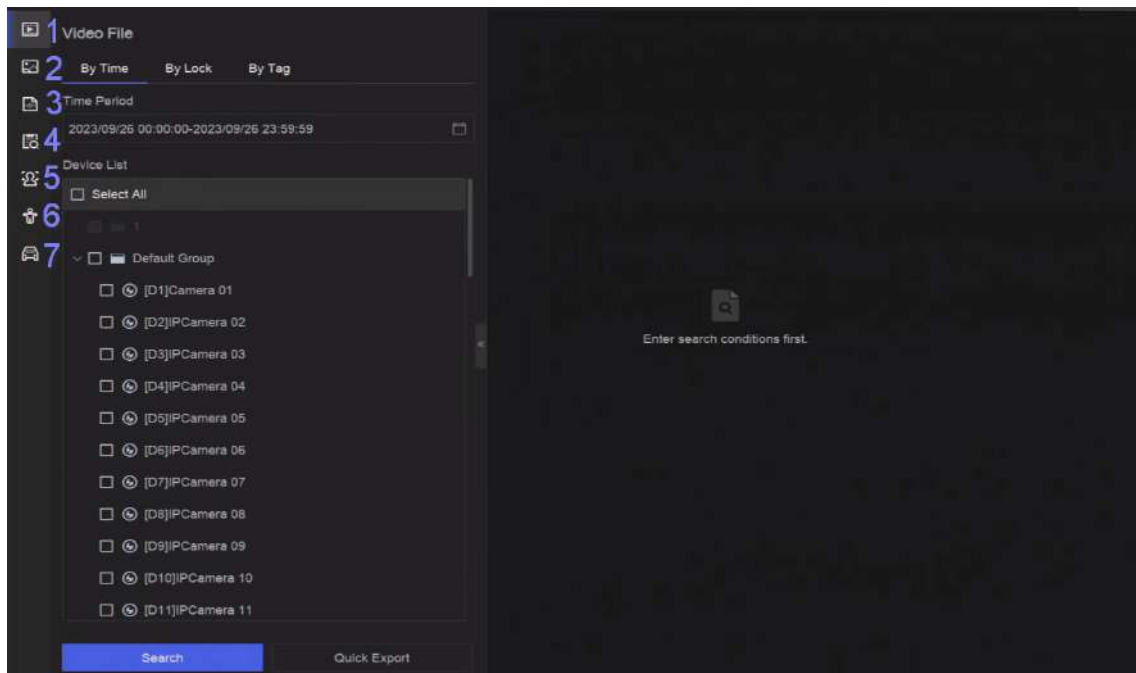


Figure 14-1 Search and Backup

2. Choose a searching method from at the left side as your desire, 7 types are supported.



Note

The searching conditions would vary according to the selected searching method.

3. Set the searching conditions.
4. Click **Search**.

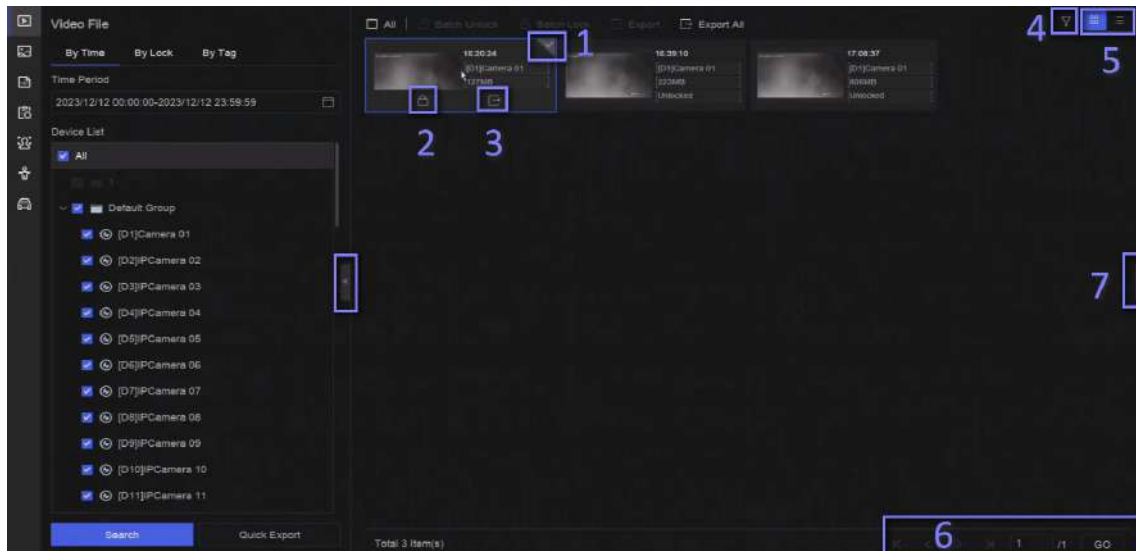


Figure 14-2 Searching Result

5. Optional: Perform the following operations.

- 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - 3 Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - 5 Use the tool bar at the top to switch display effect.
 - 6 Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6.** Insert a USB flash drive to the device for backup.
- 7.** Export files to the USB flash drive.
- Select file(s) in the result list and click **Export**.
 - Click **Export All** to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

1. Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable AcuSearch algorithm.
 - **AI by Camera:** The camera will perform the AcuSearch analysis.
 - **AI by NVR:** The device will perform the AcuSearch analysis, and engine resource is required for analysis.
2. Go to Live View or Playback, and click  at the lower-left corner during video playing.



Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** () to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking  , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.

-
3. Click  of the selected target.



Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

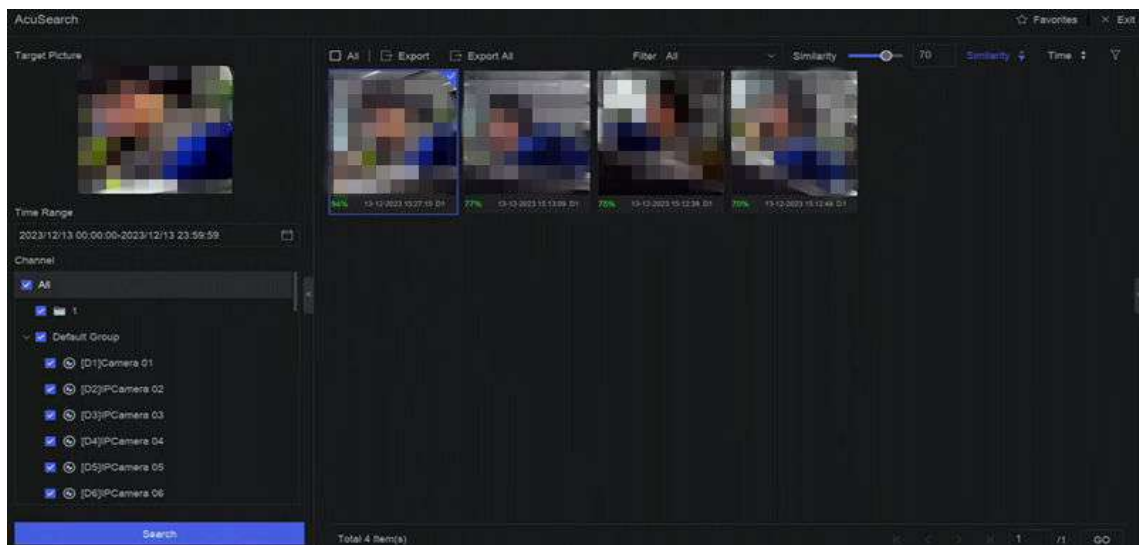


Figure 15-2 AcuSearch Result

5. **Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
6. **Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

Algorithms are used for device engines to analyze different smart functions. Smart function would be usable after allocating the corresponding algorithm to an engine.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Algorithm Management** or **Event Center → Event Configuration → Smart Settings → Algorithm Management**. The available algorithms would be listed, and you can click the required algorithm to link engine(s).

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Engine Status** or **Event Center → Event Configuration → Smart Settings → Engine Status**. If you need to switch the algorithm, refer to ***Algorithm Management***.

16.3 Task Plan Management

You can view the task status in task configuration. Smart analysis results are used for filtering the pictures when searching interested human body and vehicle pictures.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Task Plan Management** or **Event Center → Event Configuration → Smart Settings → Task Plan Management**. For **Non-Real-Time Target Comparison**, you can view the progress of each day.

Task status mainly includes 3 conditions: **Disabled**, **Waiting**, and **Enabled**.

Disabled

No analysis task is enabled on the camera.

Waiting

The analysis task of the camera is enabled. Device is waiting to analyze data.

Enabled

The analysis task of the camera is enabled and device is analyzing data of the camera.

16.4 List library Management

List library is mainly used for target picture storage and target comparison. **Strangers** library is used to store pictures for strangers, and it cannot be deleted.

16.4.1 Add a List Library

Steps

1. Go to **System → Event Configuration → Event Configuration → Data Archive → List Library** or **Event Center → Event Configuration → Data Archive → List Library**.
2. Click **Add**.
3. Enter the library name.
4. Click **Confirm**.



Note

- After a list library, you can move the cursor on the library to edit or delete it.
 - You can click **Delete in Batch** to delete selected libraries, or clear all pictures in the selected libraries.
-

16.4.2 Upload Face Pictures to the Library

Target picture comparison is based on target pictures in the library. You can upload a single target picture or import multiple target pictures to the library.

Before You Start

- Ensure the picture format is JPEG or JPG.
- Import all pictures to a backup device in advance.

Steps

1. Double click a list library.
2. **Optional:** Click **Custom Tag** to add tags to pictures. The tag can be edit as your desire, for example, personal information, organization, position, etc.
3. Click **Add** or **Import**.
4. Import picture(s).
 - **Add:** Click  to upload a picture at a time. If the picture has multiple targets, you have to pick one from them.
 - **Import:** Multiple pictures can be imported at a time. The device will use the file name as its picture name and leave other attributes empty, or import picture files by specified rules. If a picture has multiple targets in the image, the device will choose the target at the center by default.
5. **Optional:** Perform the following operations.

Delete Pictures from the Library	• Select a picture and delete it. • Select pictures and click Delete in Batch to delete the select ones.
Search Pictures in the Library	Click  at the tool bar to search pictures.

**Copy Pictures to
Another Library**

Select pictures and click **Copy to** to copy the uploaded pictures of the current library to another library.

Edit Pictures

Click the picture name, and edit its attributes.

Export Pictures

Select pictures, and click **Export** to export them to a USB flash drive.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

The human and vehicle information will be displayed for the selected channel at real-time.

Human and vehicle detection should be configured in advance. Go to **Event Center** →  to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

No.	Description
1	Right-click shortcut menu.
2	Human and vehicle detection settings. You can set the layout, comparison succeeded prompt, and resource channels.
3	Enter/exit full screen.

17.2 Person Check-In

After check-in tasks are added, you can view the live check-in information and search check-in results.

17.2.1 Add Check-In Task

Before starting person check-in, the corresponding task should be properly configured.

Before You Start

- A camera for person check-in is properly connected.
- Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** .
Allocate **Target Recognition** to at least one engine.
- The list library for check-in comparison is properly configured. Refer to [Add a List Library](#) for details.

Steps

1. Click **Person Check-In** .
2. Right click to display the menu at left side.
3. Click  .
4. Click **Add**.

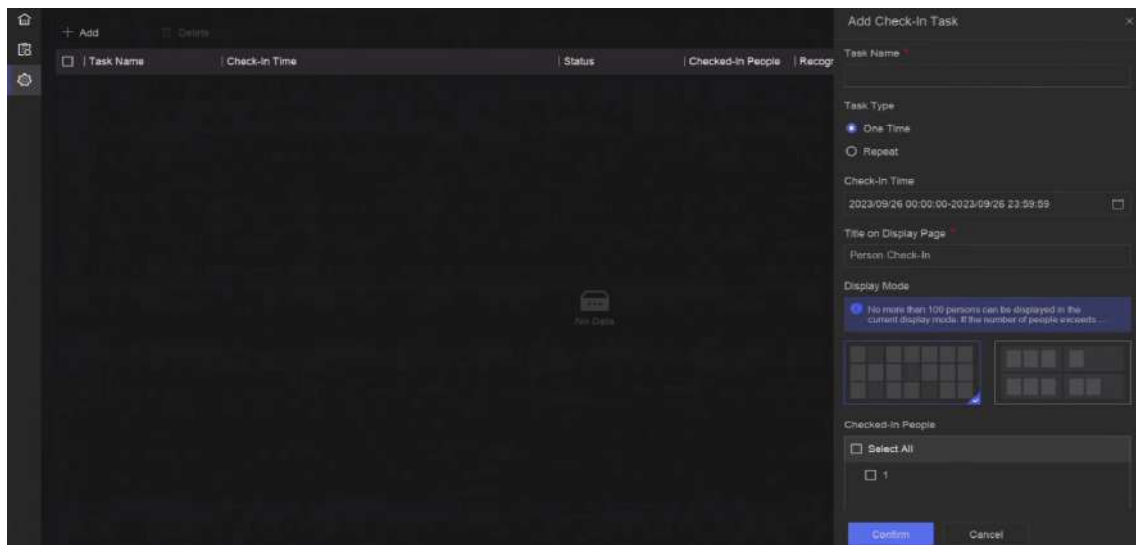


Figure 17-2 Add Check-In Task

5. Set **Task**.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

6. Configure other parameters, including **Task Name**, **Check-In Time**, **Recognition Channel**, etc.
7. Click **Confirm**.

17.2.2 Search Check-In Records

After check-in tasks are configured, you can search the records by day or month.

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to **Person Check-In** .
2. Right click to display the menu at the left side.
3. Click  .

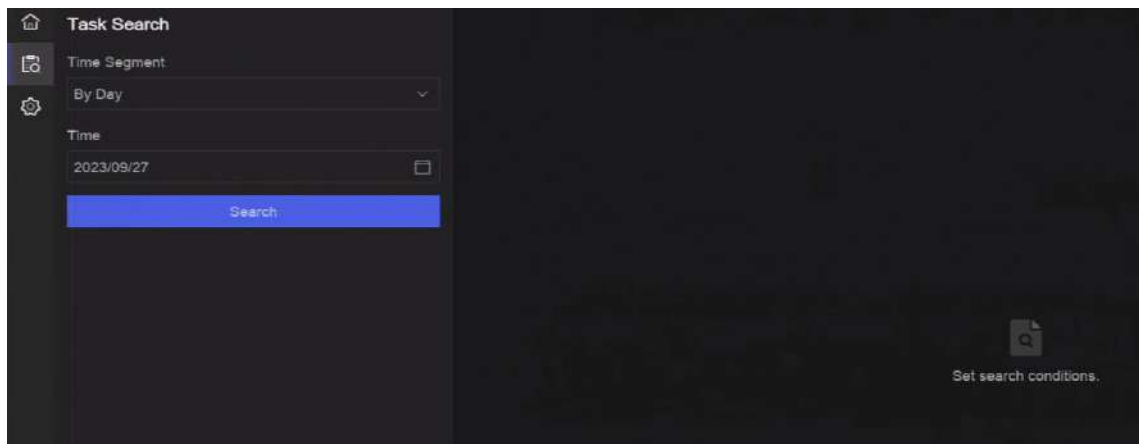


Figure 17-3 Search Check-In Records

4. Set time.
5. Click **Search**.

17.3 Statistic Report

You can view reports of people counting and heat map.

Table 17-2 Statistic Report Introduction

Function Name	Icon	Condition	Description
People Counting		The function must be supported by the connected IP camera. For example, a people counting	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

Function Name	Icon	Condition	Description
		camera is connected to your device. • Camera statistic data can be stored to the device HDD.	
Heat Map		• The function must be supported by the connected IP camera. • Camera statistic data can be stored to the device HDD.	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Chapter 18 System Parameter Settings

System parameters include device name, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Table 18-1 Parameter Description

Type	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Time Configuration	Time Sync Mode	NTP Time Sync You can select NTP Time Sync and configure NTP Server, NTP Server Port, NTP Client Port, and Interval. Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization. Manual Time Sync Manually set the system time. Hik-Connect Server Time Sync The device will sync time with Hik-Connect instead of NTP server. DST DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest. We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of

Type	Parameter Name	Description
		DST, and move them back the same period when we return to standard time (ST).
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console After connecting it to PC with a convertor, PC can set the device parameters. Transparent Channel It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System



Note

- Up to 32 working devices and 32 hot spare devices are allowed.
 - It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
 - Only certain models support this function.
-

19.1 Set Working Device

Steps

1. Go to **System → System Management → N+M Hot Spare**.
2. Set **Working Mode** as **Normal Mode**.
3. Turn on **Enable**.
4. Click **Save**.
5. **Optional:** View **Hot Spare Device IP Address** and **Hot Spare Device Working Status**.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

1. Go to **System → System Management → N+M Hot Spare**.
2. Set **Working Mode** as **Hot Spare Mode**.
3. Click **Save**. Your device will restart automatically.



Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

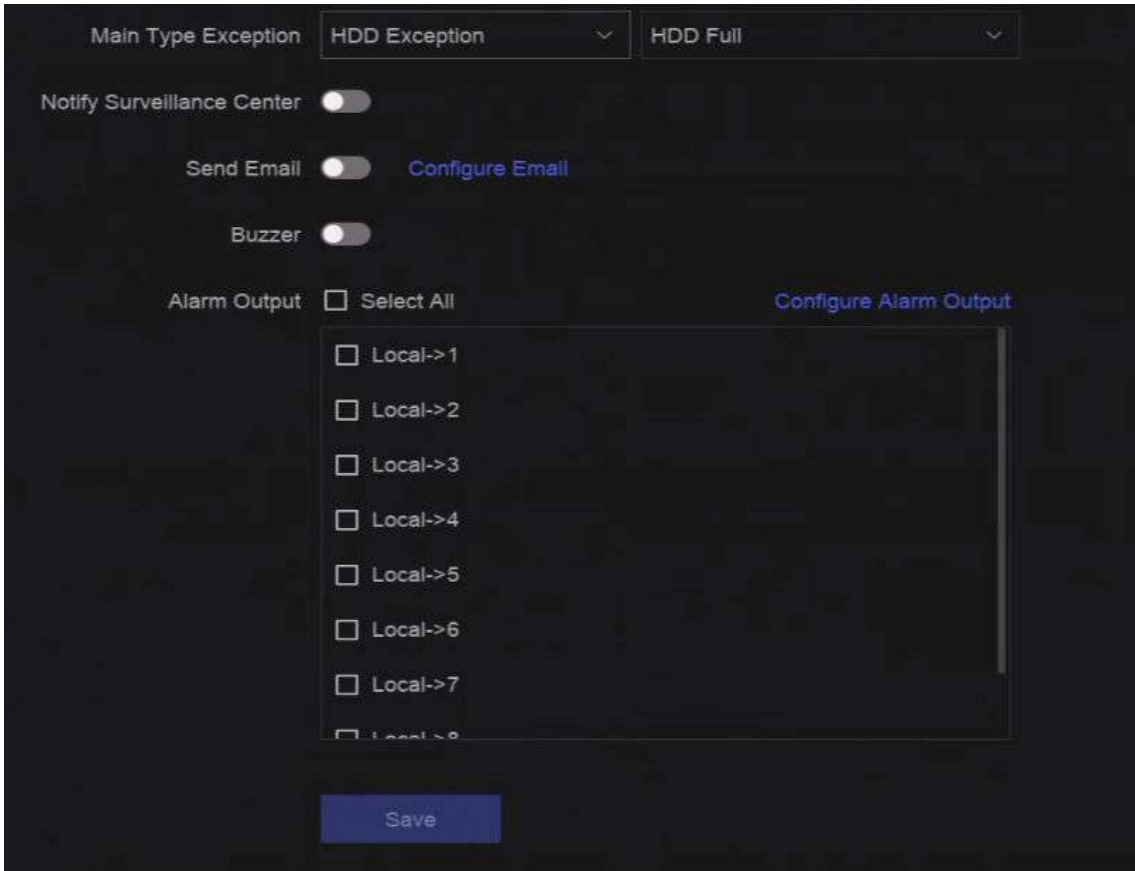
-
4. Go to **System → System Management → N+M Hot Spare** again.
 5. Add working devices to the hot spare system.
 6. Add hot spare devices to the hot spare system.
 7. Click **Save**.

Chapter 20 Configure Exception Event

Exception events can be configured to take the event hint in the live view interface and trigger alarm output and linkage actions.

Steps

1. Go to **System** → **System Settings** → **Exception** .



The screenshot displays the 'Exception Event Configuration' window. At the top, 'Main Type Exception' is set to 'HDD Exception' and 'HDD Full'. Below this, there are three toggle switches: 'Notify Surveillance Center' (off), 'Send Email' (off), and 'Buzzer' (on). To the right of the 'Send Email' toggle is a blue link 'Configure Email'. Under the 'Alarm Output' section, there is a checkbox for 'Select All' and a blue link 'Configure Alarm Output'. A list of local outputs is shown with checkboxes: 'Local->1' through 'Local->8'. At the bottom center is a blue 'Save' button.

Figure 20-1 Exception Event Configuration

2. Select exception type.
3. Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.



Note

When exception events occur,  at the upper-right corner would notify, and you can click  to view.

4. Click **Save.**

Chapter 21 View System Info

Go to **System** → **System Maintenance** → **Running Info** → **System Info** to view the system information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to **System** → **System Maintenance** → **Maintenance** → **Schedule Reboot** to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** → **System Maintenance** → **Maintenance** → **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** → **System Maintenance** → **Maintenance** → **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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, and leave all settings unchanged except restoring user accounts.

22.4 Log Info

Go to **System → System Maintenance → Maintenance → Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

1. Go to **System → CX → System Settings → Network → Network → Log Server**.
2. Turn on **Enable**.
3. Set **Upload Time**, **Server IP Address**, and **Port**.
4. **Optional**: Click **Test** to test if parameters are valid.
5. Click **Save**.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

1. Go to **System → System Maintenance → Maintenance → Maintenance Tools**.
2. Select tools according to your requirement.

Table 22-1 Tool Description

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping The ping test is used to detect whether the destination IP address is reachable. NIC Packet Capture

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.

**Note**

It is recommended to use maintenance tools with the help of technical support.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

1. Go to **System → System Maintenance → Security Management → Address Filter**.
2. Turn on **Enable**.
3. Set **Filtering Type**. Choose to filter by IP address or MAC Address.
4. Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
5. **Optional**: Set **Restriction List**. You can add, edit or delete address.
6. Click **Save**.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

1. Go to **System → System Maintenance → Security Management → Stream Encryption**.
2. Turn on **Enable**.
3. Set **Encryption Key**.



Note

The stream encryption key is synchronized with the Hik-Connect service verification code. After enabling the encryption code, the Hik-Connect stream will be forcedly encrypted.

4. Click **Save**.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to **System → System Maintenance → Security Management → TLS** to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, $\Phi 2.1$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 Glossary

Dual-Stream

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 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

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.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

PPPoE

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.

DDNS

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 hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

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.

NVR

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.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

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.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?

Reason

1. Sub-stream resolution or bitrate settings is inappropriate.
2. Connecting sub-stream failed.

Solution

1. Go to **Camera → Video Parameters → Sub-Stream** . Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).



Note

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.



Warning

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: 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.

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

1. The camera does not support coaxitron.
2. The coaxitron protocol is incorrect.
3. The signal is affected by video optical transceiver.

Solution

1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

1. The RS-485 cable is not properly connected.
2. The RS-485 interface is broken.
3. The control protocol is not correct.

Solution

1. Check if RS-485 cable is properly connected.
2. Change RS-485 interface, and try again.
3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

1. The audio input device does not have a good effect in sound collection.
2. Interference in transmission.
3. The audio parameter is not properly set.

Solution

1. Check if the audio input device is working properly. You can change another audio input device, and try again.
2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Table 24-1 Corrosive Gas Concentration Limit

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCl (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _x (Nitrogen Oxides)	0.5	1.0

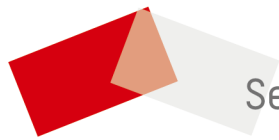


Note

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Table 24-2 Common Categories and Sources of Corrosive Gases

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _x (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.



See Far, Go Further

DS-9664NXI-S16(LCD)
S Series NVR with AcuSense



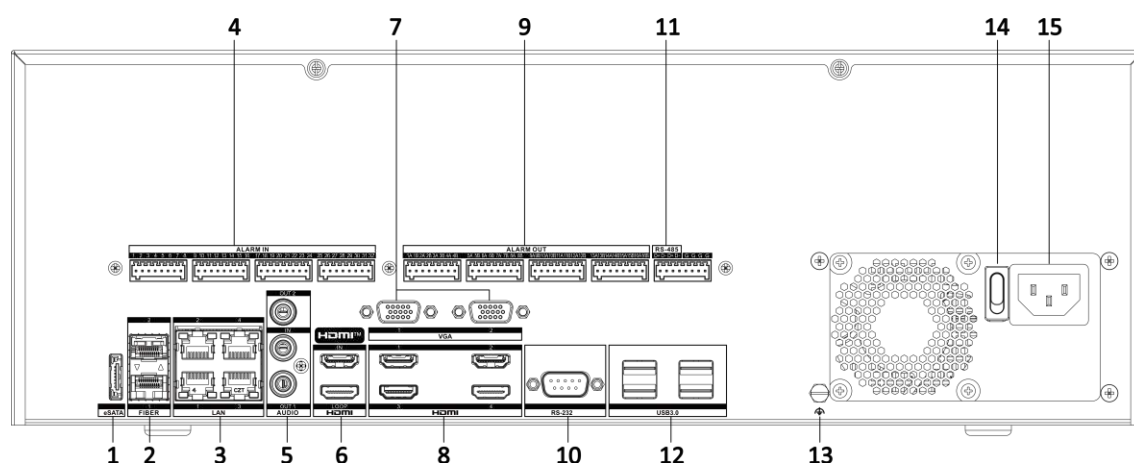
▪ Specification

Intelligent Analytics	
AI by NVR	Facial recognition, perimeter protection, video structuralization
AI by Camera	Facial recognition, perimeter protection, video structuralization, AcuSearch, motion detection2.0, ANPR, people counting, VCA
Facial Recognition	
Facial Detection and Analytics	Face picture comparison, human face capture, face picture search
Face Picture Library	Up to 64 face picture libraries, up to 300,000 face pictures in list library (each picture ≤ 4 MB, total capacity ≤ 10 GB)
Face Picture Comparison (Captured from Camera)	16-ch Comparison speed: 24 pictures per second
Facial Detection and Analytics Performance	Simultaneous mode: 8-ch, up to 2 MP independent mode: 4-ch, up to 2 MP.
AcuSearch	
By NVR	Up to 32-ch
By Camera	All channels , up to 345,600 targets per day Note: The camera should enable AcuSearch function.
Perimeter Protection	
By NVR	Simultaneous mode: 8-ch, up to 2 MP independent mode: 4-ch, up to 2 MP.
By Camera	All channels
Video Structuralization	
Structured Analysis	Simultaneous mode: 8-ch, up to 2 MP independent mode: 4-ch, up to 2 MP.
Face Picture Library	Up to 64 face picture libraries, up to 300,000 face pictures in list library (each picture ≤ 4 MB, total capacity ≤ 10 GB)
Face Picture Comparison	16-ch; Comparison speed: 24 pictures per second
Video and Audio	
IP Video Input	64-ch Up to 32 MP resolution
Incoming Bandwidth	1280Mbps
Outgoing Bandwidth	1024Mbps
Incoming Bandwidth (RAID Mode)	640Mbps
Outgoing Bandwidth (RAID mode)	512Mbps
HDMI 1 Output	4K (4096 × 2160)/30 Hz, 4K (3840 × 2160)/60 Hz, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1080P (1920 × 1080)/60 Hz
HDMI 2 Output	4K (4096 × 2160)/30 Hz, 4K (3840 × 2160)/60 Hz, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1080P (1920 × 1080)/60 Hz
HDMI 3 Output	8K (7680 × 4320)/30 Hz, 4K (4096 × 2160)/30 Hz, 4K (3840 × 2160)/60 Hz, 4K (3840 × 2160)/30 Hz, 2K (2560 × 1440)/60 Hz, 1080P (1920 × 1080)/60 Hz
HDMI 4 Output	1080P (1920 × 1080)/60 Hz
VGA 1 Output	1080P (1920 × 1080)/60 Hz

VGA 2 Output	1080P (1920 × 1080)/60 Hz
Video Output Mode	Mode 1 (default output mode): simultaneous output with 1080p resolution; Mode 2 (simultaneous output): HDMI 1, VGA 1, HDMI 2, VGA 2, HDMI 3, and HDMI 4 provide simultaneous output, the maximum resolution for VGA 1/VGA 2/HDMI 4 is 1080p, the maximum resolution for HDMI 1/HDMI 2/HDMI 3 is 4K; Mode 3 (independent output and 8K HDMI 3 output resolution): HDMI 1/VGA 1/HDMI 2/VGA 2, HDMI 3, and HDMI 4 provide independent output respectively. The maximum resolution is 8K + 4K + 1080p; Mode 4 (independent output and HDMI 3 output resolution ≤ 4K): HDMI 1/VGA 1, HDMI 2/VGA 2, HDMI 3, and HDMI 4 provide independent output respectively. The maximum resolution is 8K × 4K + 1080p.
HDMI Input	1-ch
HDMI Loopback	1-ch (matching the HDMI input)
Audio Output	2-ch, RCA (Linear, 1 kΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 kΩ)
Decoding	
Decoding Format	H.265/H.265+/H.264/H.264+
Decoding Capability	2-ch@32 MP (30 fps)/2-ch@24 MP (30fps)/4-ch@16 MP (30fps)/8-ch@8 MP (30fps)/16-ch@4 MP (30fps)/32-ch@2 MP (30fps)
Synchronous Playback	16-ch
Recording Resolution	32 MP/24 MP/12 MP/8 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA/4CIF/DCIF/ 2CIF/CIF/QCIF
Network	
Remote Connection	128
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMP, NFS, iSCSI, ISUP, UPnP™, HTTP, HTTPS, ONVIF (version 2.2), OTAP
API	ONVIF (profile S/G); SDK; ISAPI
Compatible Browser	IE11, Chrome V57, Firefox V52, Safari V12, Edge V89, or above version
Network Interface	4, RJ-45 10/100/1000/2500 Mbps self-adaptive Ethernet interface
Camera Access Protocol	ONVIF (version 2.5), RTSP
RAID	
RAID Type	RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Auxiliary Interface	
SATA	16 SATA interfaces; 3.5-inch HDD
eSATA	1 eSATA interface
Capacity	Up to 20 TB capacity for each HDD
Serial Interface	1 RS-232, 2 RS-485 (half-duplex)
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 4 × USB 3.0
Alarm In/Out	32/16
General	
GUI Language	English, Russian, Bulgarian, Hungarian, Greek, German, Italian, Czech, Slovak, French, Polish, Dutch, Portuguese, Spanish, Romanian, Turkish, Japanese, Danish, Swedish, Norwegian, Finnish, Korean, Traditional Chinese, Thai, Estonian, Vietnamese, Croatian, Slovenian, Serbian, Latvian, Lithuanian, Uzbek, Kazakh, Arabic, Ukrainian, Kyrgyz, Brazilian Portuguese, Indonesian

Power Supply	100 to 240 VAC, 50 to 60 Hz, redundant power supply
Consumption	≤ 100 W (without HDD)
Working Temperature	-10 to 55°C (14 to 131° F)
Working Humidity	10 to 90%
Dimension (W × D × H)	442 mm × 497 mm × 146 mm (17.4 × 19.5 × 5.7 inch)
Weight	≤ 12 kg (without HDD, 28.7 lb.)
Certification	
Obtained Certification	CE, IC, CB, Rohs, Reach, WEEE, RCM, UKCA, LOA
CE	EN 55032:2015+A1:2020, ENIEC61000-3-2:2019+A1:2021, EN 61000-3-3:2013+A1:2019, EN 50130-4:2011+A1:2014, EN 55035:2017+A11:2020

▪ Physical Interface



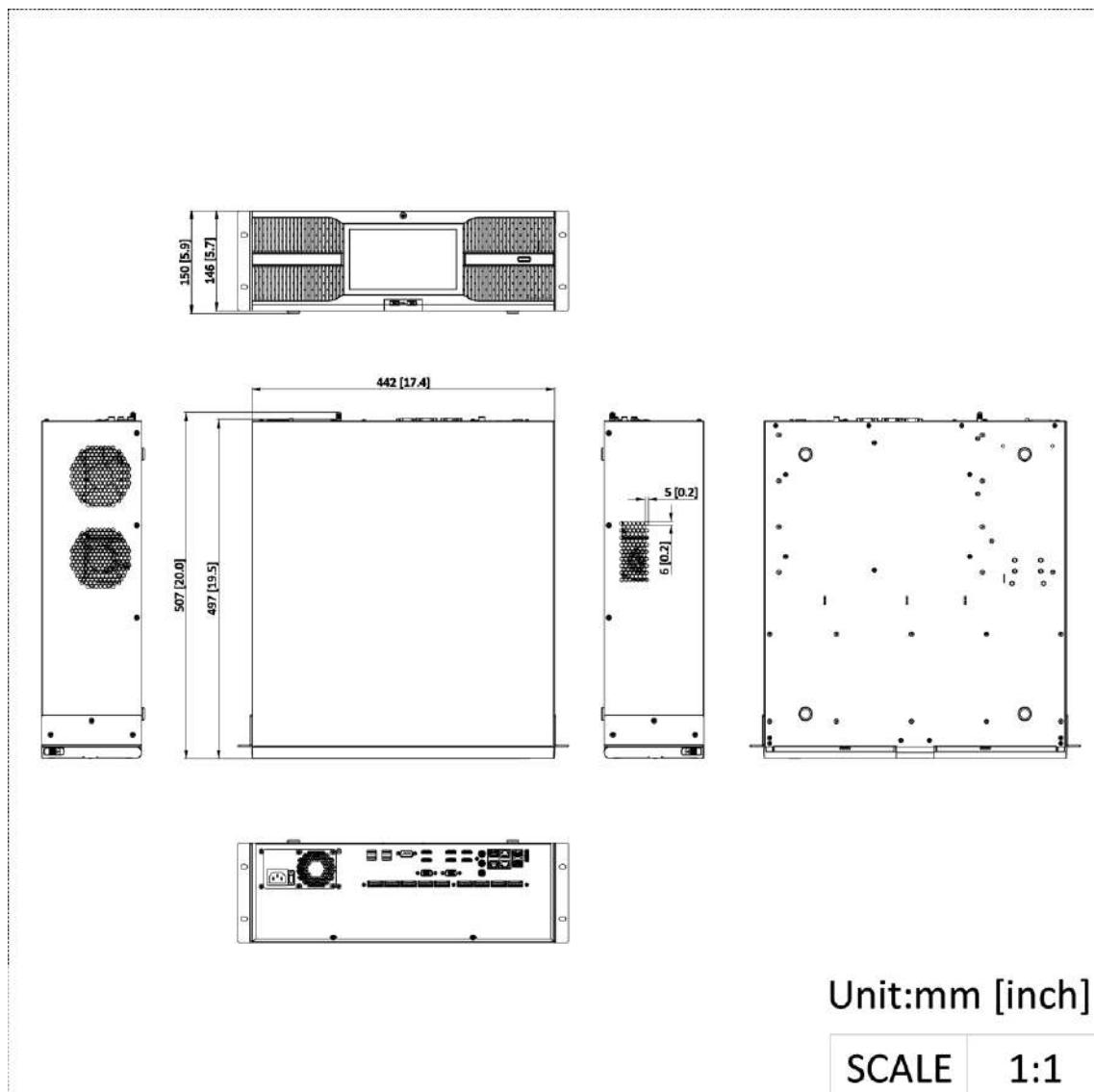
No.	Description	No.	Description
1	eSATA interface	9	Alarm out
2	Fiber	10	RS-232 serial interface
3	LAN interfaces	11	RS-484 serial interface
4	Alarm in	12	USB 3.0 interfaces
5	Audio in and out	13	GND
6	HDMI input and HDMI loopback	14	Power switch
7	VGA 1 and 2 interfaces	15	Power supply
8	HDMI interfaces		

▪ Available Model

DS-9664NXI-S16

DS-9664NXI-S16R

▪ Dimension



See Far, Go Further



www.hikvision.com
support@hikvision.com





Network Video Recorder

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.



Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Conditions

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

- This device may not cause harmful interference.
- 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 2014/30/EU, LVD Directive 2014/35/EU, 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 see: <http://www.recyclethis.info> .



Regulation (EU) 2023/1542(Battery Regulation): This product contains a battery and it is in conformity with the Regulation (EU) 2023/1542. The battery 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), or lead (Pb). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: <http://www.recyclethis.info> .

Applicable Model

This manual is applicable to the following models. But not all the functions in this manual are supported for each model.

Table 1-1 Applicable Model

Series	Model
DS-7600NI-I2	DS-7608NI-I2
	DS-7616NI-I2
	DS-7632NI-I2
DS-7600NI-I2/P	DS-7608NI-I2/8P
	DS-7616NI-I2/16P
	DS-7632NI-I2/16P
DS-7700NI-I4	DS-7708NI-I4
	DS-7716NI-I4
	DS-7732NI-I4
DS-7700NI-I4/P	DS-7708NI-I4/8P
	DS-7716NI-I4/16P
	DS-7732NI-I4/16P
	DS-7732NI-I4/24P
DS-7600NI-M1/P	DS-7604NI-M1/4P
DS-7608NI-M2	DS-7608NI-M2
	DS-7616NI-M2
	DS-7632NI-M2
DS-7600NI-M2/P	DS-7608NI-M2/8P
	DS-7616NI-M2/16P
DS-7700NI-M4	DS-7716NI-M4
	DS-7732NI-M4
	DS-7764NI-M4
DS-7700NI-M4/P	DS-7708NI-M4/8P

Series	Model
	DS-7716NI-M4/16P
	DS-7732NI-M4/16P
	DS-7732NI-M4/24P
DS-9600NI-M8	DS-9616NI-M8
	DS-9632NI-M8
	DS-9664NI-M8
	DS-96128NI-M8
DS-9600NI-M8/R	DS-9616NI-M8/R
	DS-9632NI-M8/R
	DS-9664NI-M8/R
	DS-96128NI-M8/R
DS-9600NI-M16	DS-9616NI-M16
	DS-9632NI-M16
	DS-9664NI-M16
	DS-96128NI-M16
DS-9600NI-M16/R	DS-9616NI-M16/R
	DS-9632NI-M16/R
	DS-9664NI-M16/R
	DS-96128NI-M16/R
DS-7600NXI-M2/P/VPro	DS-7608NXI-M2/8P/VPro
	DS-7616NXI-M2/16P/VPro
DS-7600NXI-M2/VPro	DS-7608NXI-M2/VPro
	DS-7616NXI-M2/VPro
DS-7700NXI-M4/VPro	DS-7716NXI-M4/VPro
	DS-7732NXI-M4/VPro
DS-7700NXI-M4/16P/VPro	DS-7716NXI-M4/16P/VPro
	DS-7732NXI-M4/16P/VPro
DS-8600NI-M16	DS-86128NI-M16

Series	Model
DS-9600NXI-M8/VPro	DS-9616NXI-M8/VPro
	DS-9632NXI-M8/VPro
	DS-9664NXI-M8/VPro
	DS-96128NXI-M8/VPro
DS-9600NXI-M8R/VPro	DS-9616NXI-M8R/VPro
	DS-9632NXI-M8R/VPro
	DS-9664NXI-M8R/VPro
	DS-96128NXI-M8R/VPro
DS-9600NXI-M16/VPro	DS-9632NXI-M16/VPro
	DS-9664NXI-M16/VPro
	DS-96128NXI-M16/VPro
DS-9600NXI-M16R/VPro	DS-9632NXI-M16R/VPro
	DS-9664NXI-M16R/VPro
	DS-96128NXI-M16R/VPro
DS-7600NXI-I2/S	DS-7608NXI-I2/S
	DS-7616NXI-I2/S
	DS-7632NXI-I2/S
DS-7600NXI-I2/P/S	DS-7608NXI-I2/8P/S
	DS-7616NXI-I2/16P/S
	DS-7632NXI-I2/16P/S
DS-7700NXI-I4/S	DS-7716NXI-I4/S
	DS-7732NXI-I4/S
DS-7700NXI-I4/P/S	DS-7716NXI-I4/16P/S
	DS-7732NXI-I4/16P/S
DS-8600NXI-I8/S	DS-8616NXI-I8/S
	DS-8632NXI-I8/S
	DS-8664NXI-I8/S
DS-8600NXI-I8/24P/S	DS-8632NXI-I8/24P/S

Series	Model
DS-9600NXI-I8/S	DS-9616NXI-I8/S
	DS-9632NXI-I8/S
	DS-9664NXI-I8/S
DS-96000NI-H16R	DS-96256NI-H16R
	DS-96256NI-H16R/LCD
DS-96000NI-H20R	DS-96128NI-H20R
	DS-96128NI-H20R/LCD
	DS-96256NI-H20R
	DS-96256NI-H20R/LCD
DS-96000NI-H30R	DS-96128NI-H30R
	DS-96128NI-H30R/LCD
	DS-96256NI-H30R
	DS-96256NI-H30R/LCD
DS-9600NI-G8R	DS-9632NI-G8R
iDS-6700NXI-M1/X	iDS-6704NXI-M1/X
	iDS-6708NXI-M1/X
	iDS-6716NXI-M1/X
iDS-7600NXI-M1/X	iDS-7608NXI-M1/X
	iDS-7616NXI-M1/X
iDS-7600NXI-M2/X	iDS-7608NXI-M2/X
	iDS-7616NXI-M2/X
	iDS-7632NXI-M2/X
iDS-7600NXI-M2/P/X	iDS-7608NXI-M2/8P/X
	iDS-7616NXI-M2/16P/X
iDS-7700NXI-M4/X	iDS-7716NXI-M4/X
	iDS-7732NXI-M4/X
iDS-7700NXI-M4/16P/X	iDS-7716NXI-M4/16P/X
	iDS-7732NXI-M4/16P/X

Series	Model
iDS-9632NXI-M8/X	iDS-9632NXI-M8/X
	iDS-9664NXI-M8/X
	iDS-96128NXI-M8/X
iDS-9600NXI-M8R/X	iDS-9632NXI-M8R/X
	iDS-9664NXI-M8R/X
	iDS-96128NXI-M8R/X
iDS-9600NXI-M16/X	iDS-9632NXI-M16/X
	iDS-9664NXI-M16/X
iDS-9600NXI-M16R/X	iDS-9632NXI-M16R/X
	iDS-9664NXI-M16R/X
iDS-96000NXI-H16R	iDS-96064NXI-H16R
	iDS-96128NXI-H16R
	iDS-96128NXI-H16R/LCD
iDS-96000NXI-H24R	iDS-96128NXI-H24R
	iDS-96128NXI-H24R/LCD
	iDS-96256NXI-H24R
	iDS-96256NXI-H24R/LCD
iVMS-9000NI-S8/C128	iVMS-9000NI-S8/C128
iVMS-9000NI-S16R/C1000	iVMS-9000NI-S16R/C1000

Safety Instruction

- 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.
- Firmly connect the plug to the power socket. Do not connect several devices to one power adapter. Power off the device before connecting and disconnecting accessories and peripherals.
- Shock hazard! Disconnect all power sources before maintenance.
- The equipment must be connected to an earthed mains socket-outlet.
- The socket-outlet shall be installed near the device and shall be easily accessible.
- For the device with the sign ⚡ indicating hazardous live, the external wiring connected to the terminals requires installation by an instructed person.
- Never place the device in an unstable location. The device may fall, causing serious personal injury or death.
- Input voltage should meet the SELV (Safety Extra Low Voltage) and the LPS (Limited Power Source) according to the IEC62368.
- High touch current! Connect to earth before connecting to the power supply.
- 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.
- Use the device in conjunction with an UPS, and use factory recommended HDD if possible.
- This equipment is not suitable for use in locations where children are likely to be present.
- CAUTION: Risk of explosion if the battery is replaced by an incorrect type.
- Do not ingest battery. Chemical Burn Hazard!
- This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
- Improper replacement of the battery with an incorrect type may defeat a safeguard (for example, in the case of some lithium battery types).
- Do not dispose of the battery into fire or a hot oven, or mechanically crush or cut the battery, which may result in an explosion.
- Do not leave the battery in an extremely high temperature surrounding environment, which may result in an explosion or the leakage of flammable liquid or gas.
- Do not subject the battery to extremely low air pressure, which may result in an explosion or the leakage of flammable liquid or gas.
- Dispose of used batteries according to the instructions.
- Keep body parts away from fan blades and motors. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- Use only power supplies same with the original model, or LPS power supplies with the same voltage and electric current.

Preventive and Cautionary Tips

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

- The device is designed for indoor use only. Install it in a well-ventilated, dust-free environment without liquids.
- Ensure recorder is properly secured to a rack or shelf. Major shocks or jolts to the recorder as a result of dropping it may cause damage to the sensitive electronics within the recorder.
- The device shall not be exposed to water dripping or splashing, and no objects filled with liquids, such as vases, shall be placed on the device.
- No naked flame sources, such as lighted candles, should be placed on the device.
- The ventilation should not be impeded by covering the ventilation openings with items, such as newspapers, table-cloths, curtains. The openings shall never be blocked by placing the device on a bed, sofa, rug, or other similar surface.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- For certain models, the equipment has been designed, when required, modified for connection to an IT power distribution system.
-  identifies the battery holder itself and identifies the positioning of the cell(s) inside the battery holder.
- + identifies the positive terminal(s) of the device which is used with, or generates direct current, and - identifies the negative terminal(s) of the device which is used with, or generates direct current.
- If the device has been powered off or placed for a long time, its coin/button cell battery may run out power.
- When the coin/button cell battery runs out power, the system time would be incorrect, please contact the after-sales service to replace the battery.
- Keep a minimum 200 mm (7.87 inch) distance around the equipment for sufficient ventilation.
- For certain models, ensure correct wiring of the terminals for connection to an AC mains supply.
- Do not touch the sharp edges or corners.
- When the device is running above 45 °C (113 °F), or its HDD temperature in S.M.A.R.T. exceeds the stated value, please ensure the device is running in a cool environment, or replace HDD(s) to make the HDD temperature in S.M.A.R.T. below the stated value.
- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- Do not touch the bare components (such as the metal contacts of the inlets) and wait for at least 5 minutes, since electricity may still exist after the device is powered off.
- The USB port of the equipment is used for connecting to a mouse, keyboard, USB flash drive, or Wi-Fi dongle only. The current for the connected device shall be not more than 0.1 A.
- The serial port of the device is used for debugging only.
- If the power output port of the device does not comply with Limited Power Source, the connected device powered by this port shall be equipped with a fire enclosure.
- If a power adapter is provided in the device package, use the provided adapter only.

- For the device with sticker  or  , pay attention to the following cautions: CAUTION: Hot parts! Do not touch. Burned fingers when handling the parts. Wait one-half hour after switching off before handling the parts.
- If the device needs to be installed on the wall or ceiling,
 1. Install the device according to the instructions in this manual.
 2. To prevent injury, this device must be securely attached to the installation surface in accordance with the installation instructions.
- Under high working temperature (40 °C (104 °F) to 55 °C (131 °F)), the power of some power adapters may decrease.
- Make sure that the power has been disconnected before you wire, install, or disassemble the device.
- If the device needs to be wired by yourself, select the corresponding wire to supply power according to the electric parameters labeled on the device. Strip off wire with a standard wire stripper at corresponding position. To avoid serious consequences, the length of stripped wire shall be appropriate, and conductors shall not be exposed.
- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

Content Convention

In order to simplify description, please read the following conventions.

- Recorder or device mainly refers to video recorder.
- IP device mainly refers to network camera (IP camera), IP dome (speed dome), DVS (Digital Video Server), or NVS (Network Video Server).
- Channel mainly refers to the video channel in video recorder.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Indicator and Interface Description

Front Panel Indicator Description

The indicators at the front panel indicates different working status of your device.

Table 1-1 Common Indicator Description

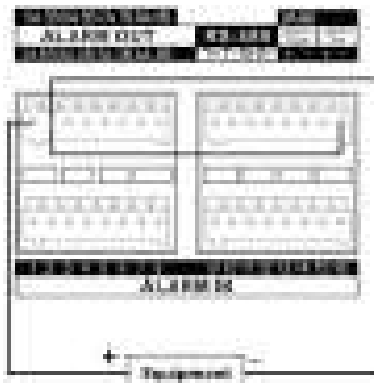
Indicator	Description
	The indicator turns on when device is powered up.
	The indicator flashes when data is being read from or written to HDD.
	The indicator flashes when network connection is functioning properly.

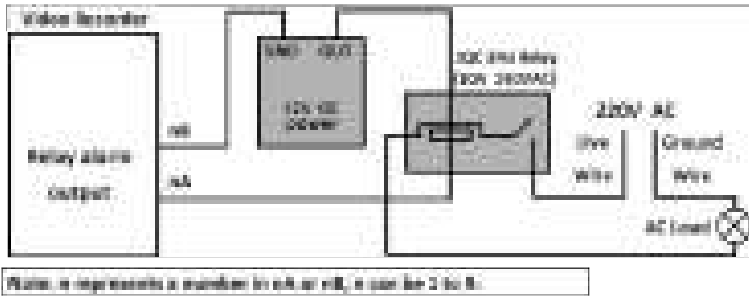
Interface Description

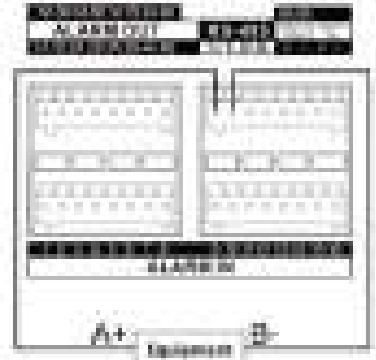
The panel interfaces vary with different models. Refer to the following table for common interface description.

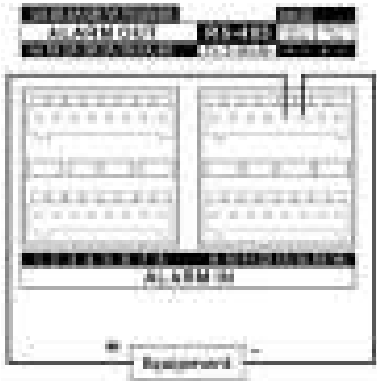
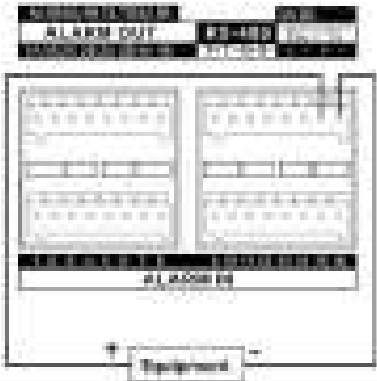
Table 1-2 Common Indicator Description

Item	Description
VIDEO IN	BNC interface for Turbo HD and analog video input.
VIDEO OUT	BNC connector for video output.
AUDIO IN	RCA connector for audio input.
AUDIO OUT	RCA connector for audio output.
LINE IN	RCA connector for two-way audio input.
USB	Universal Serial Bus (USB) interface for additional device.
VGA	DB15 connector for local video output and menu display.
HDMI	HDMI interface for video output.
RS-485	RS-485 serial interface for pan/tilt unit, speed dome, etc.
RS-232	RS-232 interface for parameter configuration, or transparent channel.
LAN	RJ-45 self-adaptive Ethernet interface.
eSATA	Storage and expansion interface for record or backup.
GND	Ground.

Item	Description
Power Switch	Switch for turning on/off the device.
Power Supply	100 to 240 VAC, 48 VDC, or 12 VDC power supply.
USIM Card	UIM/SIM card slot.
	SMA antenna interface.
ALARM IN	The alarm input receives alarm input signal. The equipment positive terminal (+) should connect to a number, and the equipment negative terminal (-) should connect to “-” or “G”. Use the following diagram as a connection example for alarm input. 
ALARM OUT	The alarm output sends out alarm signal. When an equipment uses DC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should both connect to the corresponding number with “B”, and then connect to “-” or “G”. Use the following diagram as an alarm output connection example for DC equipment. 

Item	Description
	When an equipment uses AC power supply, its positive terminal (+) should connect to a number with “A”, and its negative terminal (-) should connect to the corresponding number with “B”. Use the following diagram as an alarm output connection example for AC equipment.  Note For the reason that the AC load voltage could be high, please use an external relay for safety. Use the following diagram for reference. 
KB	KB represents keyboard. Connect “D+” and “D-” to “T+” and “T-” respectively. Use the following diagram for reference.

Item	Description
	
RS-485	RS-485 is an electrical specification of a two-wire, half-duplex, multipoint serial connection. Connect “T+” and “T-” to “A+” and “B-” respectively. Use the following diagram for reference. 
Ctrl 12V/ $\frac{12V}{0.5A}$	Controllable 12 VDC and 0.5/1 A power output for external alarm device. The power will be turned on when the corresponding alarm output is triggered. Use the following diagram for reference.

Item	Description
	
DC 12V/ $\frac{12V}{1A}$	It provides 12 VDC and 1 A power output. Use the following diagram for reference. 

HDD Installation

If your device does not support HDD hot swapping, disconnect the power from the device before installing a hard disk drive (HDD). A factory recommended HDD should be used for this installation.

Scan the QR code below to view HDD installation videos.



Figure 1-1 HDD Installation

Bracket Installation

Bracket installation is applicable when it requires to remove the device cover, and install HDD on the internal bracket.

Steps

1. Unfasten screws on the back, and push the cover backwards to remove the cover.

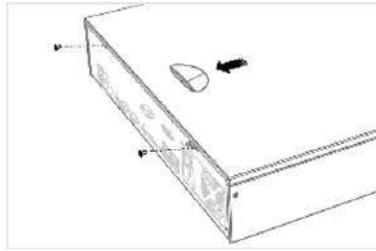


Figure 1-2 Remove Cover

2. Fix the HDD on the bracket with screws.



Note

Please uninstall the upper layer bracket first before installing HDD on the lower layer bracket.

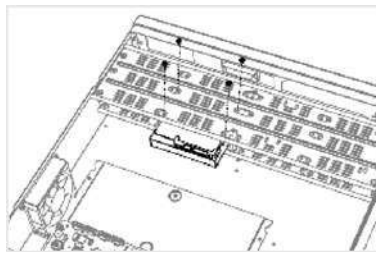


Figure 1-3 Fix HDD

3. Connect the data cable and power cable.

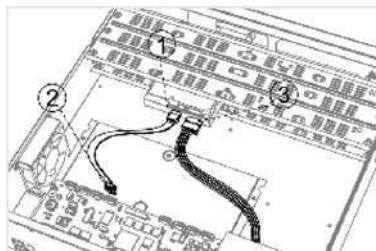


Figure 1-4 Connect Cable



Note

You can repeat the steps above to install other HDDs.

4. Reinstall the device cover and fasten screws.

Front Panel Plug-Pull Installation

Front panel plug-pull installation is applicable when you need to open the device front panel with key and install the HDD.

Steps

1. Fix mounting ears to HDD with screws.

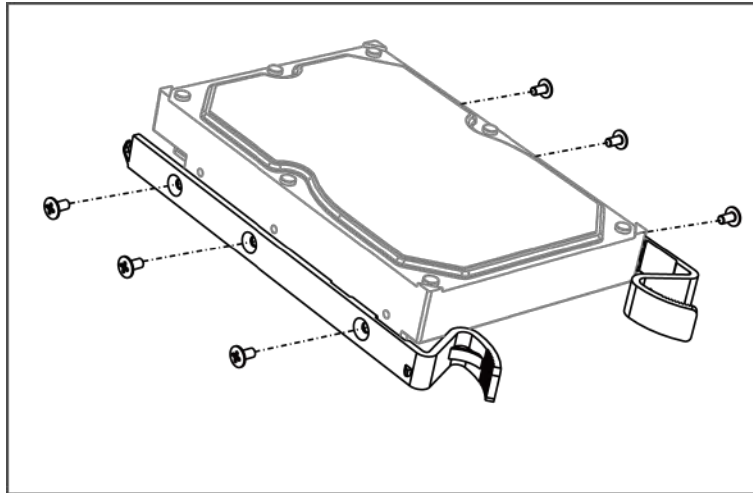


Figure 1-5 Fix Mounting Ears to HDD

2. Unlock the front panel with the attached key, and press the buttons on both sides of the front panel to open it.

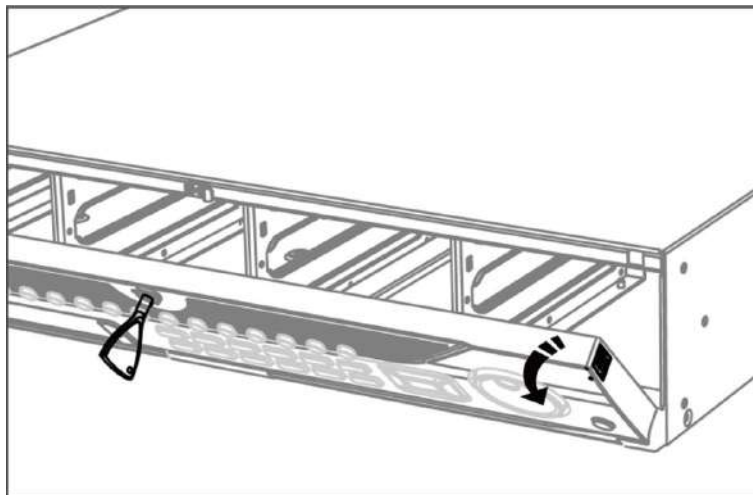


Figure 1-6 Open Front Panel

3. Insert the HDD until it is fixed firmly.

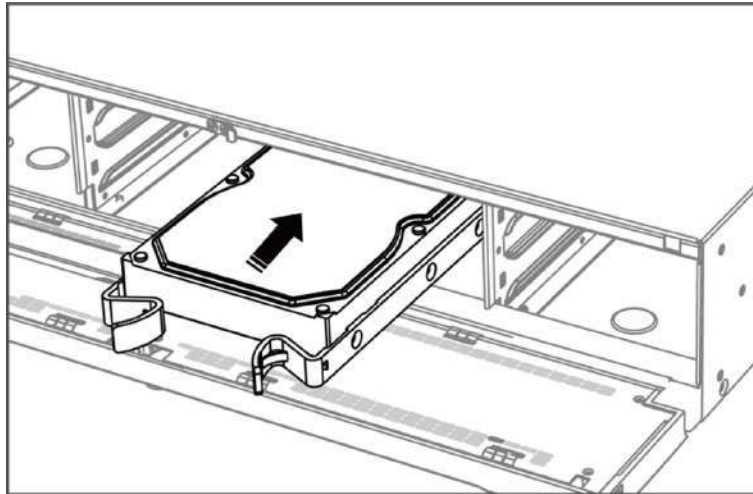


Figure 1-7 Insert HDD

4. **Optional:** Repeat the steps above to install other HDDs.
5. Close the front panel and lock it with key.

HDD Case Installation

HDD case installation refers to the method that you install the HDD in the case, and then plug the HDD case into the slot.

Steps

1. Unlock the front panel with panel key.
2. Pull the front panel out of the device and make it a little above the left handle.



The angle between the front panel and the device must be within 10°.

3. Press the blue button to pop up the handle and hold the handle and pull the HDD case out of the slot.
4. Fix the hard disk in the HDD case.
 - 1) Place a HDD in the case. The SATA interface must face the case bottom.
 - 2) Adjust the HDD position. Ensure the hard disk rear aligns with HDD bottom.
 - 3) Use a screwdriver to fasten the four screws into the screw holes in both sides.

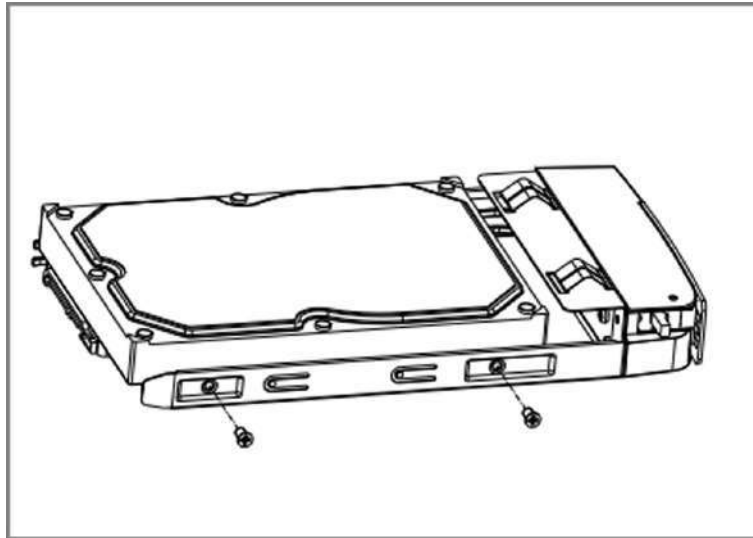


Figure 1-8 Fix HDD

5. Push the HDD case back into the slot.

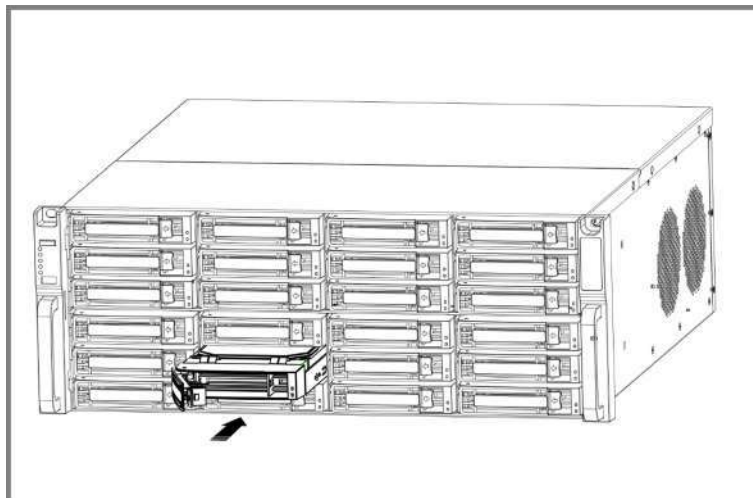


Figure 1-9 Push HDD Case into Slot

6. Press the handle until you hear a click. Thus to fix the HDD case. Repeat above steps to install the rest hard disk boxes.
7. Close the front panel, and lock it with the panel key.

Fix-on-Bottom Installation

Fix-on-bottom installation is applicable when you need to install and fix the HDD on the device bottom.

Steps

1. Remove the cover from device by unfastening the screws on panels.

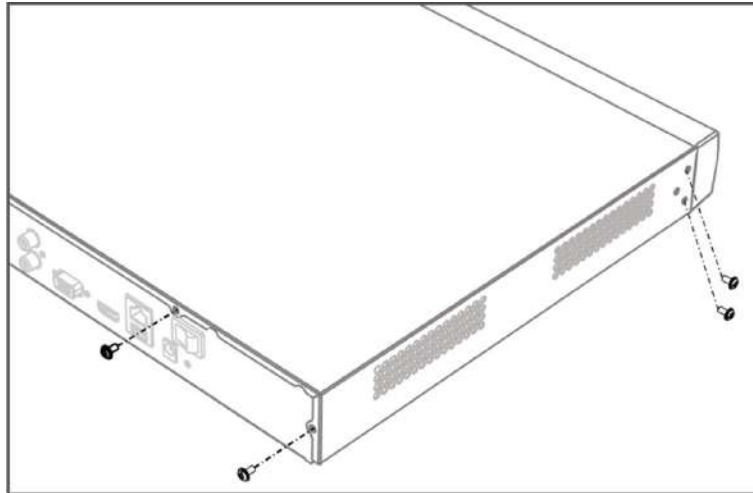


Figure 1-10 Remove Cover

2. Connect the data cable and power cable.
 - 1) Connect one end of data cable to the device motherboard.
 - 2) Connect the other end of data cable to HDD.
 - 3) Connect one end of power cable to HDD.
 - 4) Connect the other end of power cable to the device motherboard.

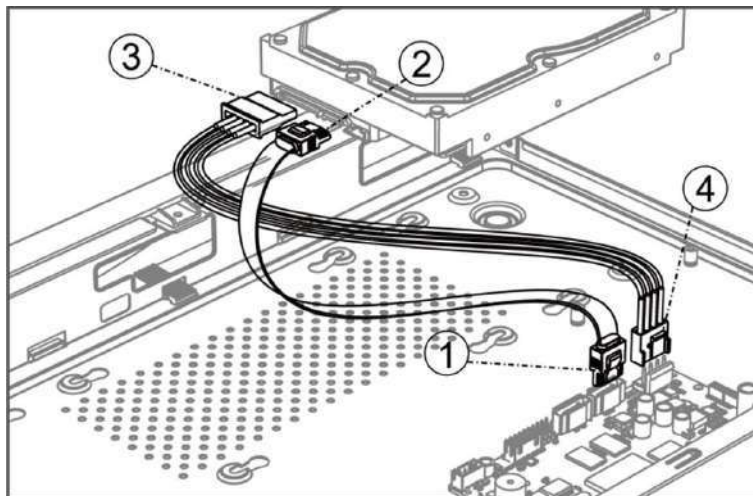


Figure 1-11 Connect Cables

3. Set the device up, match HDD screw threads with the reserved holes on the device bottom, and fix HDD with screws.

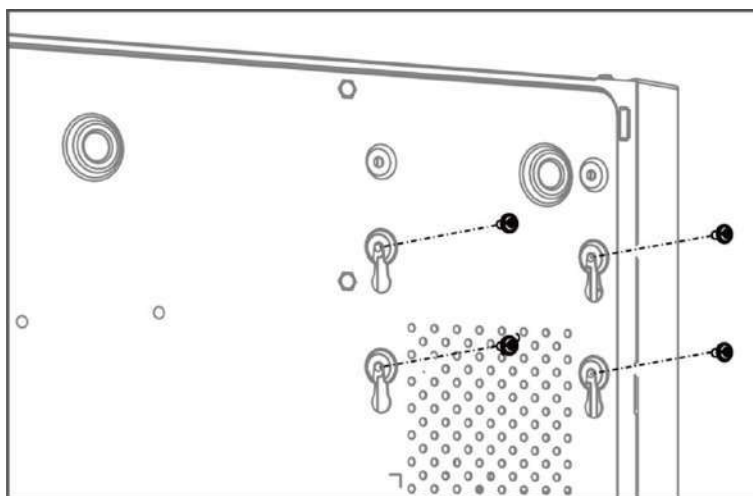


Figure 1-12 Fix HDD to Device Bottom

- 4. Optional:** Repeat the steps above to install other HDDs.
- 5.** Reinstall the device cover and fasten screws.

Coin/Button Cell Battery Replacement

The coin/button cell battery should be replaced when the device has been powered off or placed for a long time, and the system time is incorrect.

Before You Start

Power off your device.

Steps

1. Remove the device chassis cover.
2. Find the coin/button cell battery on motherboard.
3. Put the thumb outside the battery slot, and use the index finger to push the positive contact spring outward gently. The battery will pop up automatically.

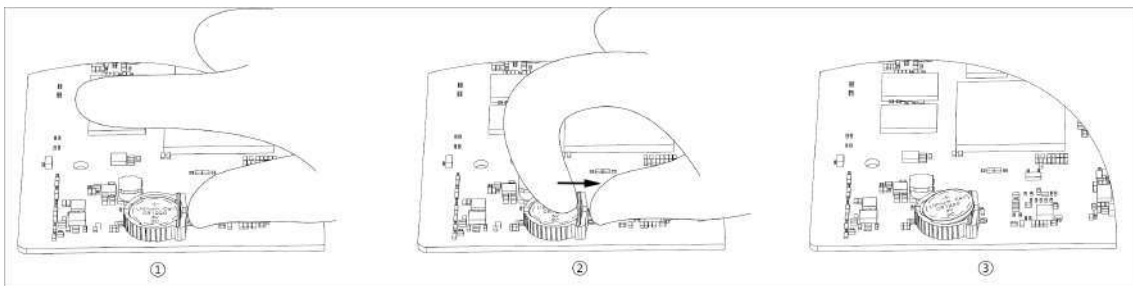


Figure 1-1 Remove Battery



Note

- You should wear anti-static gloves when removing the battery.
 - If the spring is deformed due to excessive force when pushing outward, it needs to be adjusted back into its original position before inserting the battery.
4. Insert the battery diagonally towards the side with the plastic snap point in the battery slot, and then press the battery near the positive contact spring to snap it beneath the spring.

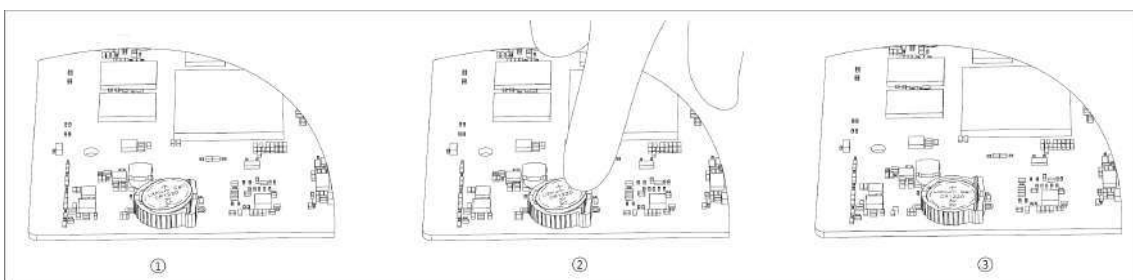


Figure 1-2 Replace Battery



Note

You should wear anti-static gloves when replacing the battery.

5. Reinstall the device chassis cover.

What to do next

If the system time is incorrect, please go to configure the time.

Contents

Chapter 1 Activate via Local Menu	1
Chapter 2 Log In to Your Device	3
Chapter 3 User Interface Introduce	4
Chapter 4 Network Settings	6
4.1 Network Parameter Settings	6
4.1.1 Configure TCP/IP	6
4.1.2 Configure DDNS	7
4.1.3 Configure PPPoE	8
4.1.4 Configure Multicast	9
4.1.5 Enable SVC Network Transmission Frame Extraction	9
4.2 Platform Access Settings	9
4.2.1 Configure Hik-Connect	9
4.2.2 Configure OTAP	11
4.2.3 Configure ISUP	12
4.2.4 Configure SDK Service	13
4.2.5 Enable ISAPI	14
4.2.6 Configure ONVIF	14
4.2.7 Configure Log Server	15
4.3 Network Service Settings	16
4.3.1 Configure HTTP(S)	16
4.3.2 Configure RTSP	17
4.3.3 Configure WebSocket(s)	18
4.3.4 Configure Port Mapping (NAT)	18
4.3.5 Configure IoT	20
Chapter 5 User Management	21
Chapter 6 Device Access	22

6.1 Access Video Device	22
6.1.1 Add Automatically Searched Online Network Camera	22
6.1.2 Add Network Camera Manually	23
6.1.3 Add Network Camera through PoE	24
6.1.4 Add Solar-Powered Camera through OTAP Protocol	24
6.1.5 Add Network Camera via Custom Protocol	25
6.1.6 Add Network Camera through Camera Configuration File	26
6.2 Add Access Control Device	26
6.3 Add Security Control Panel	27
6.4 Add Audio Device	27
6.5 Add POS Device	27
6.6 Channel Management	29
Chapter 7 Device Grouping	30
Chapter 8 Video or Audio Device Settings	31
8.1 Enable H.265 Stream Access	31
8.2 Configure Display Settings	31
8.3 Configure Video Parameters	32
8.4 Configure Privacy Mask	32
8.5 Configure Privacy Protection	33
8.6 Configure Audio Parameter	35
8.7 Configure OTAP Service	35
8.8 Configure ISUP Service	36
8.9 Batch Configuration	36
8.10 Configure PoE (Power over Ethernet) Interface	37
Chapter 9 Storage Management	39
9.1 Manage HDD	39
9.2 RAID Configuration	39
9.2.1 Create Disk Array	40

9.2.2 Rebuild Array	42
9.2.3 Delete Array	42
9.2.4 View Firmware Info	42
9.3 Configure Storage Mode	43
9.4 Configure Auto Backup	43
9.5 Configure Other Storage Parameters	44
9.6 Mange USB Flash Drive	44
Chapter 10 Schedule Configuration	46
10.1 Configure Schedule Template	46
10.2 Configure Recording Schedule	48
10.3 Configure Picture Capture Schedule	50
10.4 Configure Audio Recording	52
Chapter 11 Live View	53
11.1 Configure Live View Layout	53
11.2 GUI Introduction	53
11.3 PTZ Control	55
Chapter 12 Playback	56
12.1 GUI Introduction	56
12.2 Normal Playback	57
12.3 Event Playback	58
12.4 Slice Playback	59
12.5 Sub-Period Playback	59
Chapter 13 Event Center	61
13.1 Event Settings	61
13.1.1 Basic/Generic Event	61
13.1.2 Perimeter Protection	63
13.1.3 Abnormal Behavior Event	74
13.1.4 Target Event	77

13.1.5 Thermal Camera Detection	79
13.1.6 Alarm Input Event	80
13.1.7 Audio Analysis Event	82
13.2 Linkage Configuration	84
13.3 Disarming Configuration	86
13.4 Batch Configuration	87
13.5 Event Search	88
13.6 View Alarms	89
Chapter 14 Search and Backup	90
Chapter 15 AcuSearch	92
Chapter 16 Smart Settings	94
16.1 Algorithm Management	94
16.2 Engine Status	94
16.3 Task Plan Management	94
16.4 List library Management	95
16.4.1 Add a List Library	95
16.4.2 Upload Face Pictures to the Library	95
16.5 Self-Learning Settings	96
16.5.1 Self-Learning Task Management	96
16.5.2 Model Management	97
16.5.3 Smart Status	97
Chapter 17 Application Center	98
17.1 Human and Vehicle Detection	98
17.2 Person Check-In	98
17.2.1 Add Check-In Task	99
17.2.2 Search Check-In Records	100
17.3 Statistic Report	100
Chapter 18 System Parameter Settings	102

Chapter 19 Hot Spare Device Backup	104
19.1 Set Working Device	104
19.2 Set Hot Spare Device	104
Chapter 20 Configure Exception Event	106
Chapter 21 View System Info	108
Chapter 22 System Maintenance	109
22.1 Schedule Reboot	109
22.2 Upgrade Device	109
22.3 Backup and Restore	109
22.4 Log Info	110
22.5 Configure Log Server	110
22.6 Maintenance Tools	110
22.7 Soft Power Off Configuration	111
Chapter 23 Security Management	113
23.1 Address Filter	113
23.2 Stream Encryption	113
23.3 Select TLS Version	113
Chapter 24 Appendix	114
24.1 List of Applicable Power Adapter	114
24.2 Glossary	115
24.3 Frequently Asked Questions	116
24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?	116
24.3.2 Why is the video recorder notifying risky password after a network camera is added?	117
24.3.3 Why is the video recorder notifying the stream type is not supported?	117
24.3.4 How to confirm the video recorder is using H.265 to record video?	117
24.3.5 Why is the video recorder notifying IP conflict?	117

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?	118
24.3.7 Why is the device not able to control PTZ camera via coaxitron?	118
24.3.8 Why does the PTZ seem unresponsive via RS-485?	118
24.3.9 Why is the video sound quality not good?	118
24.4 Notification for Corrosive Gas	119

Chapter 1 Activate via Local Menu

For the first-time access, you have to set an admin password to activate your device. No operation is allowed before activation. You can also activate the device via web browser, SADP or client software.

Before You Start

Ensure your device is connected with a monitor and mouse.

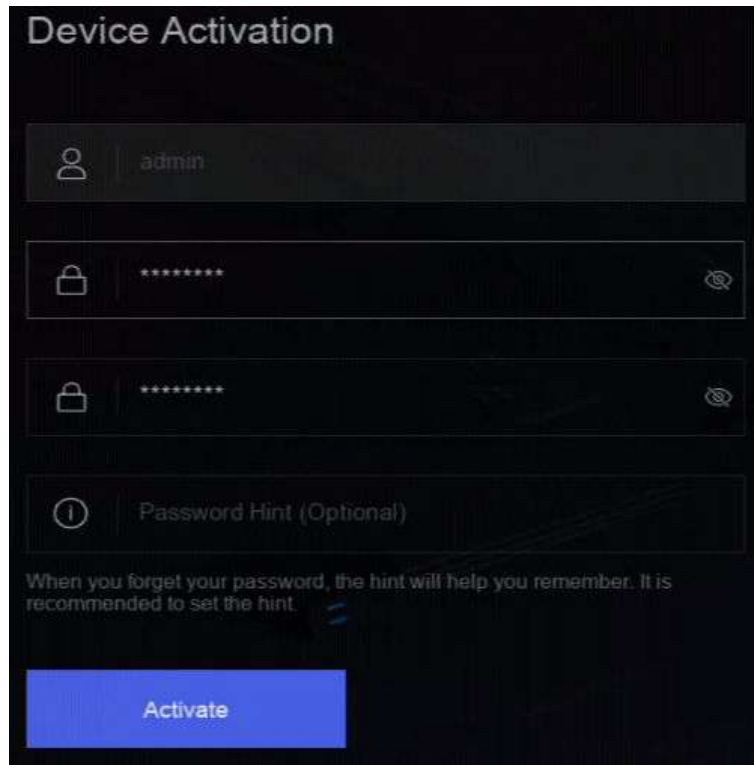
Steps

1. Power on your device.
2. Set the region or DST (Daylight Saving Time) parameters.
3. Select a system language.
4. Enter the admin password twice.



Caution

We highly recommend you to create a strong password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.



The image shows a 'Device Activation' screen with a dark background. At the top, the title 'Device Activation' is displayed. Below it, there are three input fields. The first field is for the username, with a person icon and the text 'admin' entered. The second and third fields are for passwords, each with a lock icon and masked text '*****'. To the right of each password field is an eye icon for toggling visibility. Below the password fields is a section for a 'Password Hint (Optional)' with an information icon. A note below this section states: 'When you forget your password, the hint will help you remember. It is recommended to set the hint'. At the bottom of the screen is a large blue button labeled 'Activate'.

Figure 1-1 Activate via Local Menu

5. **Optional:** Enter a password hint. It will help you remember your password when you forget.
6. Click **Activate**.



Note

After the device is activated, you should properly keep the password.

7. **Optional:** Draw an unlock pattern.
8. Configure at least one password recovery method.

What to do next

Follow the wizard to set basic parameters.

Chapter 2 Log In to Your Device

You have to log in to your device before operating the menu and other functions.

Before You Start

Ensure your device is activated.

Steps

1. Power on your device.
2. Right click to display the shortcut menu.
3. Select an item as needed. For example, select **Exit Full Screen**, and you would automatically enter the login interface.

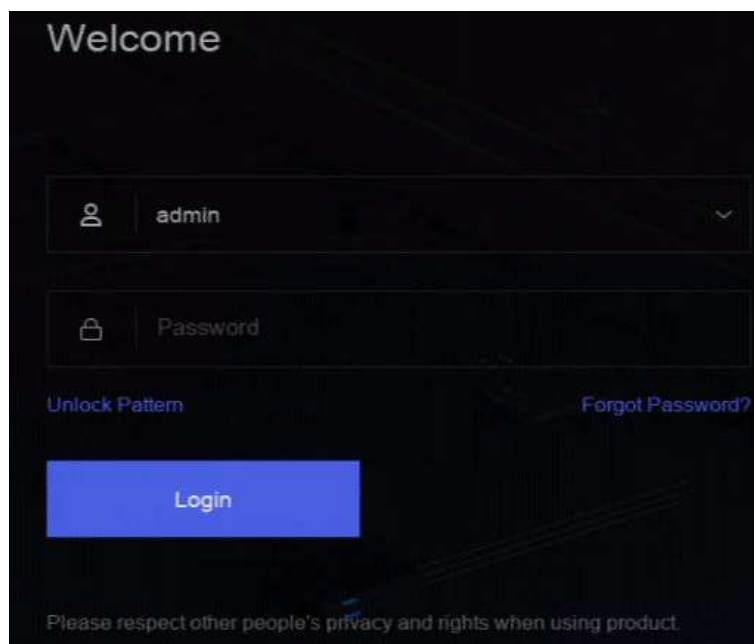


Figure 2-1 Login

4. Use the unlock pattern to log in, or click **Password Login** to log in via user name and password.



Note

- Unlock pattern is only available for admin user.
 - If you forget your unlock pattern or login password, click **Forget Password** at the password login interface to reset your password, or use the password hint to remember.
-

Chapter 3 User Interface Introduce

The device will enter the live view interface after it is powered on. Right click your mouse and select **Exit Full Screen** through the shortcut menu.



Figure 3-1 Main Function Page

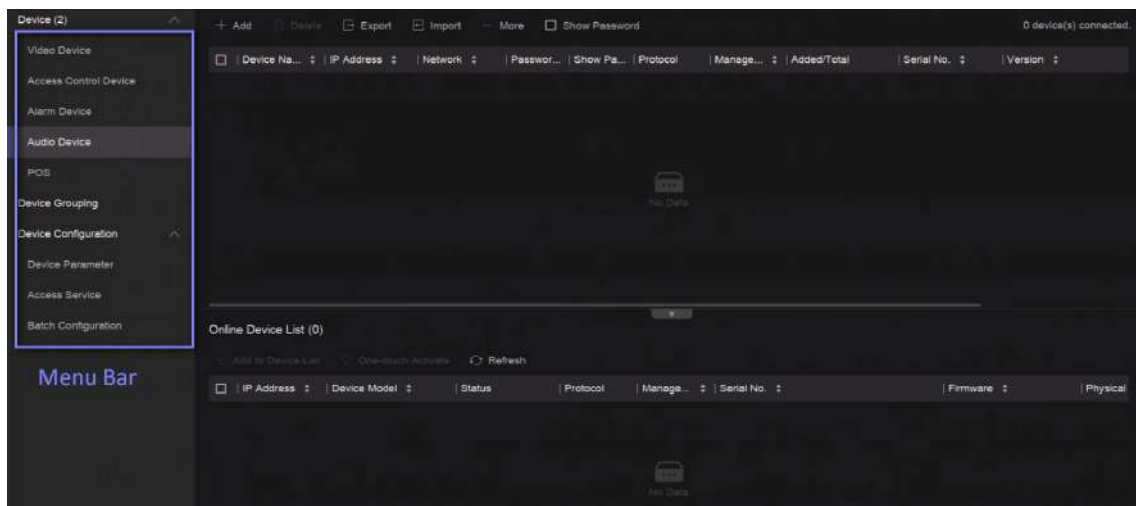


Figure 3-2 Menu Bar Example

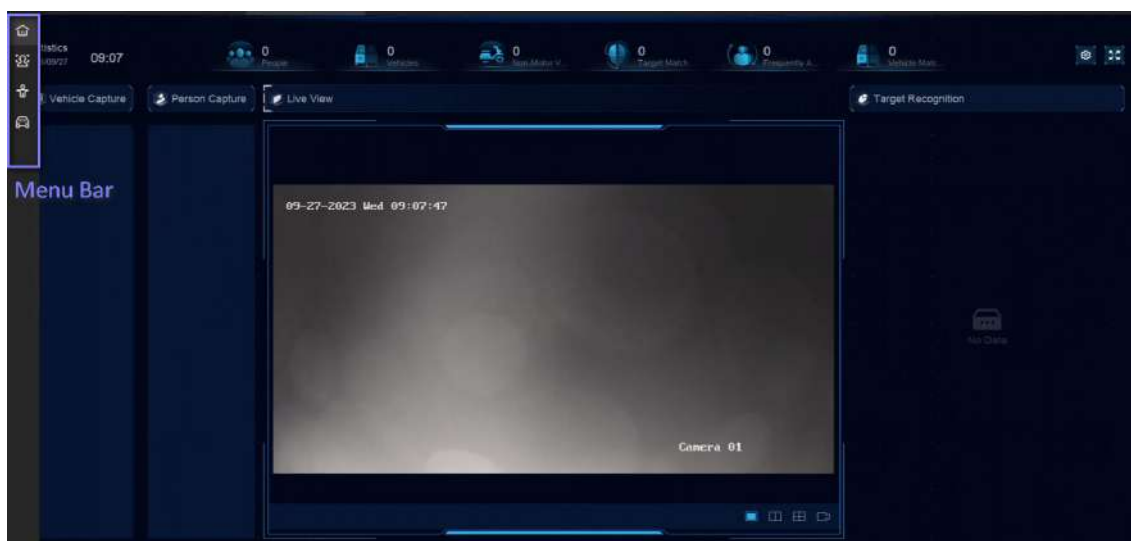


Figure 3-3 Human and Vehicle Detection Example of Application Center

Table 3-1 Interface Introduction

Interface Name	Introduction
Task Bar	The opened applications are listed in the task bar. You can move and close each application tab. Icon introduction : •  : Main menu. •  : Event center. Event alarms can be searched and viewed. •  : The download progress of each download task can be viewed here. •  : Shut down, log out, or reboot your device.
Application List	All applications are displayed here. You can click one to configure it.
Navigation Bar	Click to configure each function of the system.
Menu Bar	Configurable items of each application are listed here.  Note For applications in Application Center, you can click  , or right click to display the menu bar.

Chapter 4 Network Settings

Network parameters, platform access settings, and network services are configurable.

4.1 Network Parameter Settings

You shall configure network parameters before using functions that require network access.

4.1.1 Configure TCP/IP

TCP/IP must be properly configured before you operate video recorder over network or access network devices.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **TCP/IP** .

Figure 4-1 TCP/IP Settings

2. Set **Working Mode** and **Select NIC**.

Multi-address

The parameters of the two NIC cards can be configured independently. You can select **LAN1** or **LAN2** in the NIC type field for parameter settings. You can select one NIC card as default route. And then the system is connecting with the extranet and the data will be forwarded through the default route.

Net-fault Tolerance

The two NIC cards use the same IP address, and you can set **Main NIC** to **LAN1** or **LAN2**. By this way, in case of one NIC card failure, the video recorder will automatically enable the other standby NIC card so as to ensure the normal running of the whole system.



Note

Working mode is only available for certain models.

3. Configure network parameters.

- IPv4

DHCP

If the DHCP server is available, you can enable **DHCP** to automatically obtain an IP address and other network settings from that server.

MTU

The maximum transmission unit (MTU) is the size of the largest network layer protocol data unit that can be communicated in a single network transaction.

Auto Obtain DNS Server

If **DHCP** is enabled. You can check **Auto Obtain DNS Server** to obtain **Preferred DNS Server** and **Alternate DNS Server**.

- IPv6

Router Advertisement

If the router in the network supports IPv6, it is recommended to use this mode as default.

Auto

If there is a DHCPv6 device in the network, it is recommended to use this mode

Manual Configuration

You shall use this mode if you are going to manually enter IPv6 parameters.

4. Click **Save**.

4.1.2 Configure DDNS

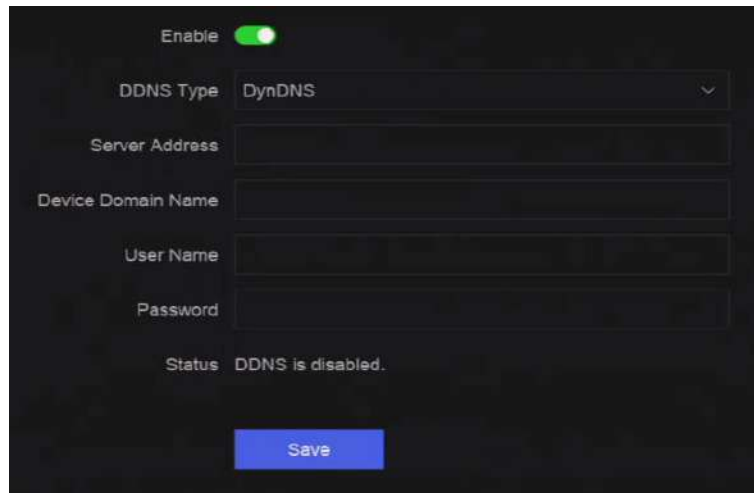
Dynamic domain name server (DDNS) maps dynamic user IP addresses to a fixed domain name server.

Before You Start

Ensure you have registered DynDNS, PeanutHull, and NO-IP services with your ISP.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **DDNS** .



Enable ☒

DDNS Type: DynDNS

Server Address:

Device Domain Name:

User Name:

Password:

Status: DDNS is disabled.

Save

Figure 4-2 DDNS

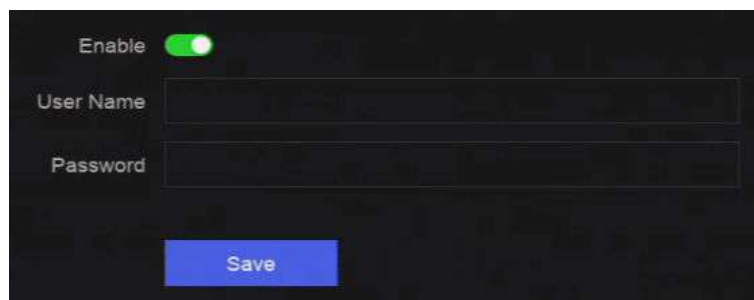
2. Turn on **Enable**.
3. Select a DDNS type.
4. Set parameters, including service address, domain name, etc.
5. Click **Save**.

4.1.3 Configure PPPoE

If the device is connected to Internet through PPPoE, you need to configure user name and password accordingly. Contact your Internet service provider for details about PPPoE service.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network** → **PPPoE** .



Enable ☒

User Name:

Password:

Save

Figure 4-3 PPPoE

2. Turn on **Enable**.
3. Enter user name and password.
4. Click **Save**.

What to do next

Go to **System** → **System Maintenance** → **Running Info** → **Network Status** to view PPPoE status.

4.1.4 Configure Multicast

Multicast can be configured to enable live view for cameras that exceed the maximum number allowed through network.

Steps

1. Go to **System → System Settings → Network → Network → Other**.
2. Set **Multicast** parameters.



Note

- When adding device through network video security client, multicast group IP address should be the same as the device multicast IP address.
- For IPv4, it covers Class-D IP ranging from 224.0.0.0 to 239.255.255.255 and it is recommended to use an IP address ranging from 239.252.0.0 to 239.255.255.255. When adding a device to the CMS software, the multicast address must be the same as that of the device.

-
3. Click **Save**.

4.1.5 Enable SVC Network Transmission Frame Extraction

Enabling SVC network transmission frame extraction allows for efficient transmission of video streams over networks with varying bandwidth conditions. It can save network bandwidth by reducing frame rates during live view and playback.



Note

Make sure you have enabled SVC Network Transmission Frame Extraction on the Web page of the related camera.

Go to **System → System Settings → Network → Network → Other** to enable the function.

4.2 Platform Access Settings

4.2.1 Configure Hik-Connect

Hik-Connect provides mobile phone application and platform service to access and manage your video recorder, which enables you to get a convenient remote access to the video security system.

Steps

1. Go to **System → System Settings → Network → Hik-Connect**.

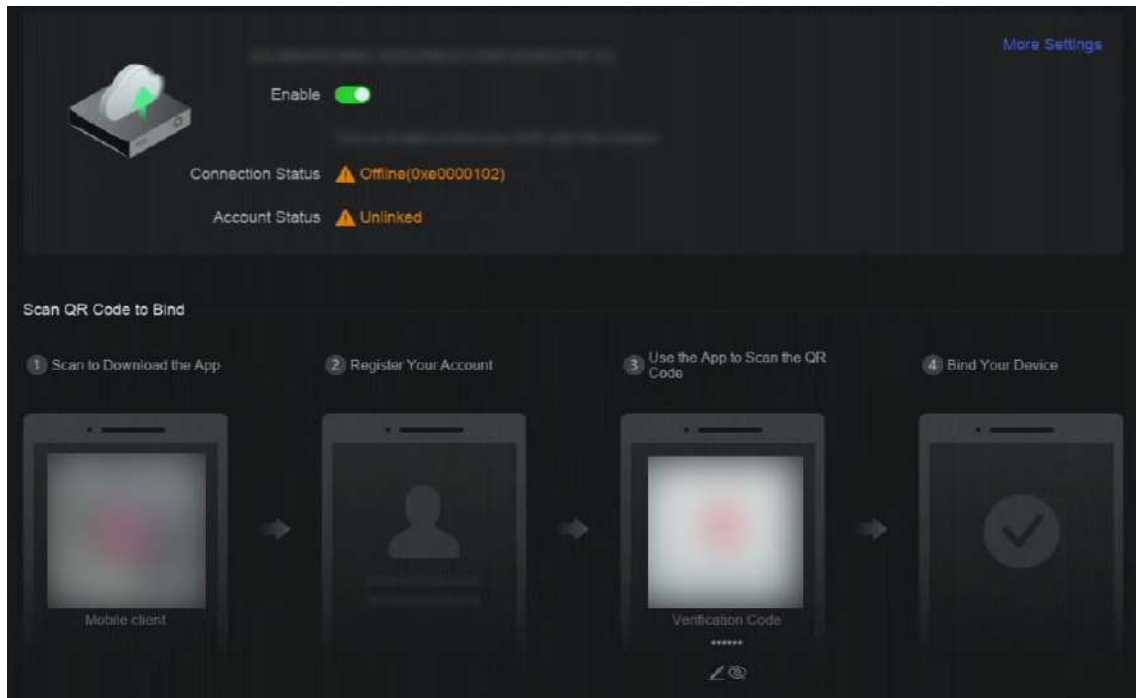


Figure 4-4 Hik-Connect

2. Turn on **Enable**, and the service terms will pop up.
3. Accept the service terms.
4. Download Hik-Connect app.
 - Use a smart phone to scan the QR code, and download Hik-Connect app.
 - Download the app from <https://appstore.hikvision.com>.



Figure 4-5 Download Hik-Connect

5. Register an account at the app.
6. **Optional:** Click **More Settings** to enable **Stream Encryption**, **Platform Time Sync**, and **Adaptive Bitrate Streaming**, or edit **Server IP Address**.

Stream Encryption

It requires to enter verification code in remote access and live view after this function is enabled.

Platform Time Sync

The device will sync time with Hik-Connect instead of NTP server.

Adaptive Bitrate Streaming

When the network environment is poor, the device would automatically adjust video bitrate to ensure playing fluency.

Server IP Address

The Hik-Connect server IP address.

7. Click  to set verification code.
8. Use Hik-Connect app to scan the device QR, and bind the device with your Hik-Connect account.



Note

If the device is already bound with an account, you can click **Unbind** to unbind with the current account.

Result

- If your device is connected with Hik-Connect, **Connection Status** will be **Online**.
- If your device is bound with a Hik-Connect account, **Account Status** will be **Linked**.

What to do next

You can access your video recorder via Hik-Connect.

4.2.2 Configure OTAP

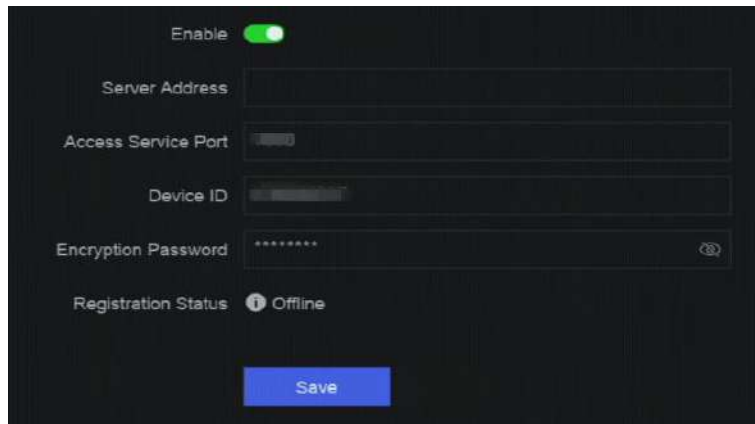
OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP.

Steps

1. Go to **System** → **System Settings** → **Network** → **Platform Access** → **OTAP** .



Enable ☒

Server Address

Access Service Port

Device ID

Encryption Password

Registration Status Offline

Save

Figure 4-6 OTAP

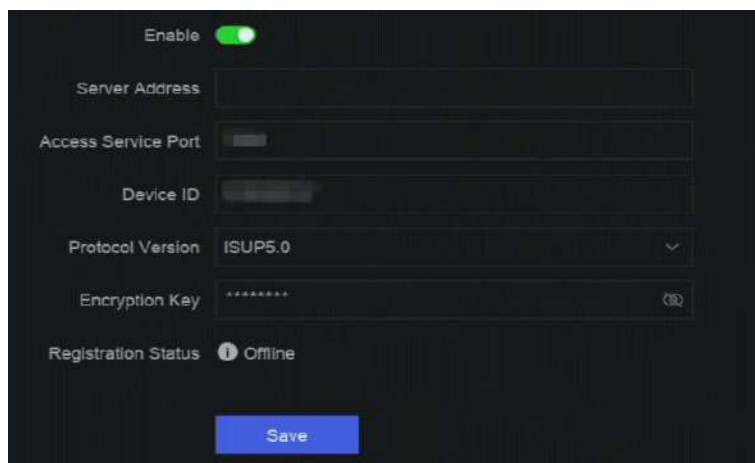
2. Turn on **OTAP**.
3. Set the parameters.
4. Click **Save**.

4.2.3 Configure ISUP

ISUP (Intelligent Security Uplink Protocol) provides APIs, library files, and commands for the third-party platform to access devices such as NVRs, speed domes, DVRs, network cameras, mobile NVRs, mobile devices, decoding devices, etc. With this protocol, the third-party platform can realize functions like live view, playback, two-way audio, PTZ control, etc.

Steps

1. Go to **System** → **CX** → **System Settings** → **Network** → **Platform Access** → **ISUP**.



Enable ☒

Server Address

Access Service Port

Device ID

Protocol Version ISUP5.0

Encryption Key

Registration Status Offline

Save

Figure 4-7 ISUP

2. Turn on **Enable**.



Note

If ISUP is enabled, the Hik-Connect access will automatically be disabled.

3. Set the related parameters.

Server Address

The platform server IP address.

Access Server Port

The platform server port, ranges from 1024 to 65535. The actual port shall be provided by the platform.

Device ID

Device ID shall be provided by the platform.

Protocol Version

ISUP protocol version, only ISUP 5.0 is available.

Encryption Key

Encryption password is required when using ISUP V5.0 version, it provides more secure communication between the device and platform. Enter it for verification after the device is registered to the ISUP platform. It cannot be empty, or "ABCDEF".

4. Click **Save**.

You can see the registration status (online or offline) after the device is restarted.

4.2.4 Configure SDK Service

SDK (Software Development Kit) service is used for third-party partners to integrate different functions. The enhanced SDK service adopts TLS protocol over the SDK service that provides safer data transmission.

Steps

1. Go to **System → System Settings → Network → Platform Access → SDK**.

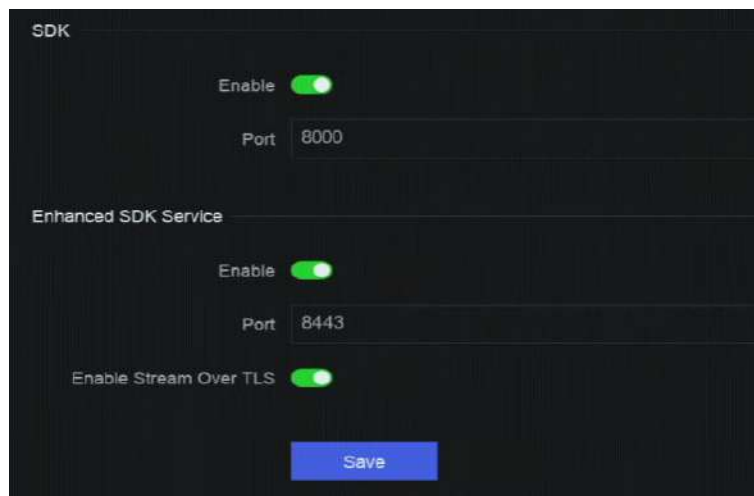


Figure 4-8 SDK Service

2. Configure **SDK** and **Enhanced SDK Service** according to your requirement.



Note

The port for **Enhanced SDK Service** is 8443 by default.

3. **Optional:** Enable **Stream Over TLS**. The stream over TLS encryption technology provides more secure stream transmission service.
4. Click **Save**.

4.2.5 Enable ISAPI

ISAPI (Internet Server Application Programming Interface) is an open protocol based on HTTP, which can realize the communication between the system devices (e.g., network camera, NVR, etc.).

Go to **System → System Settings → Network → Platform Access → ISAPI** to enable the function.

4.2.6 Configure ONVIF

ONVIF protocol allows the connection with third-party cameras. The added user accounts have the permission to connect other devices via ONVIF protocol.

Steps

1. Go to **System → CX → System Settings → Network → Platform Access → ONVIF**.

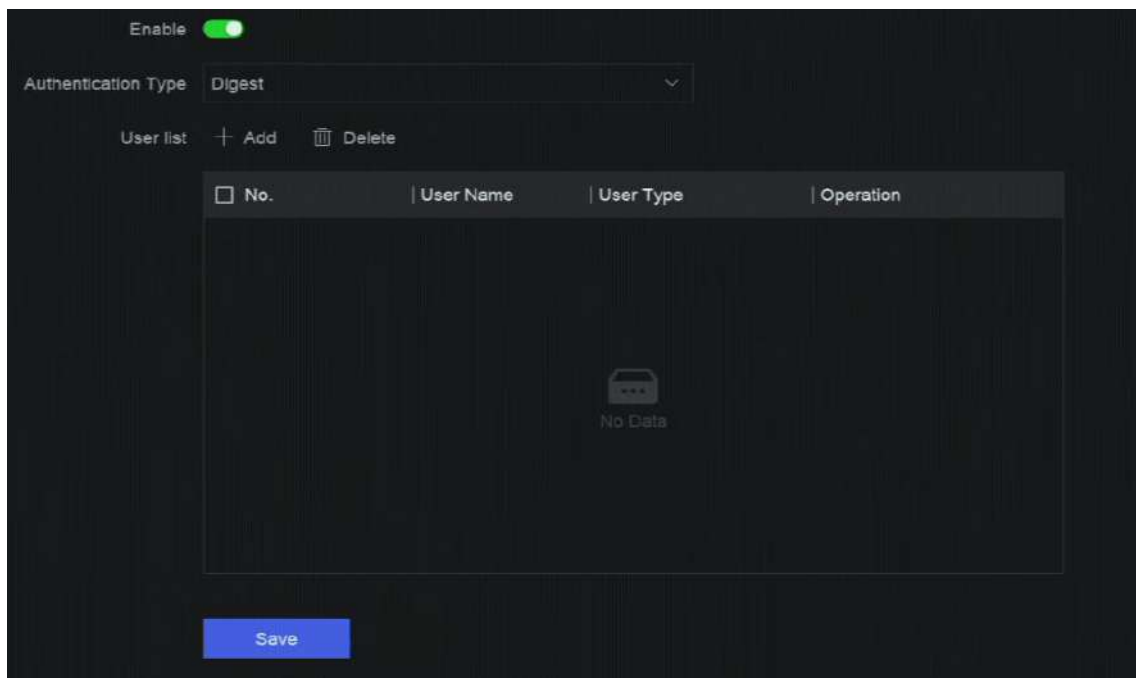


Figure 4-9 ONVIF

2. Turn on **Enable**.
3. Select an authentication type.
4. Click **Add** to add a user.
5. Set the user name and password.



Caution

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: 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

6. Click **Save**.
-

4.2.7 Configure Log Server

Logs can be uploaded to the log server for backup.

Steps

1. Go to **System → System Settings → Network → Platform Access → Log Server**.

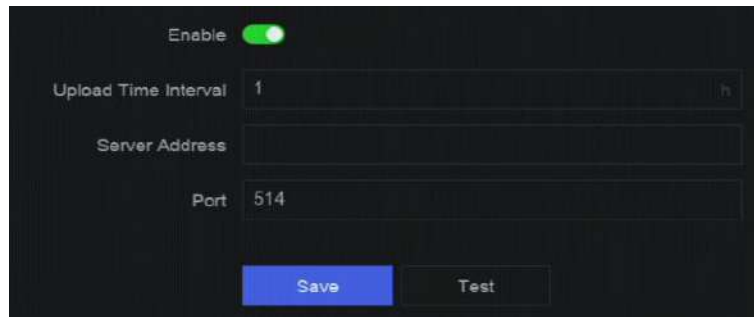


Figure 4-10 Log Server

2. Turn on **Enable**.
3. Set **Upload Time Interval**, **Server IP Address**, and **Port**.
4. **Optional**: Click **Test** to check if parameters are valid.
5. Click **Save**.

4.3 Network Service Settings

4.3.1 Configure HTTP(S)

HTTP ((Hyper Text Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) ports are used for remote access through web browser. HTTPS protocol enables encrypted transmission and identity authentication, which improves the security of remote access.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **HTTP(S)**.

The screenshot shows the configuration page for HTTP and HTTPS services. It is divided into three main sections: HTTP, HTTPS, and HTTP/HTTPS Authentication. In the HTTP section, the 'Enable' toggle is turned on (green) and the 'Port' is set to 80. In the HTTPS section, the 'Enable' toggle is also turned on (green), with a note 'Ensure the client TLS version is enabled.' and a link to 'TLS Settings'. The 'Port' is set to 443, and the 'Enable HTTPS Browsing' toggle is turned off (grey). The 'HTTP/HTTPS Authentication' section has 'Authentication Type' set to 'Digest' and 'Digest Algorithm' set to 'MD5'. A note states 'Authentication type and digest algorithm are valid for both HTTP and HTTPS.' A blue 'Save' button is at the bottom.

Section	Setting	Value
HTTP	Enable	On
	Port	80
HTTPS	Enable	On
	Client TLS Version	Ensure the client TLS version is enabled.
	Port	443
	Enable HTTPS Browsing	Off
HTTP/HTTPS Authentication	Authentication Type	Digest
	Digest Algorithm	MD5

Figure 4-11 HTTP(S)

2. **Optional:** Turn on HTTP or HTTPS.
3. View or edit **Port** of HTTP or HTTPS.
4. Set **HTTP/HTTPS Authentication**.

Authentication Type

Two authentication types are selectable, for security reasons, it is recommended to select **Digest** as the authentication type.

Digest Algorithm

Digest algorithms are based on HTTP/HTTPS and are mainly used for the digest authentication of user authentication.

5. Click **Save**.

4.3.2 Configure RTSP

RTSP (Real Time Streaming Protocol) is a network control protocol designed to control streaming media servers. You can specifically secure the stream data of live view by setting the RTSP authentication.

Steps

1. Go to **System → System Settings → Network → Network Service → RTSP**.



Figure 4-12 RTSP

2. Set parameters.

Port

The port is 554 by default.

Authentication Type

Two authentication types are selectable, if you select **Digest**, only the request with digest authentication can access the video stream by RTSP via the IP address. For security reasons, it is recommended to select **Digest** as the authentication type.

RTSP Digest Algorithm

RTSP digest algorithm is based on RTSP, it is an algorithm for digest authentication of the user authentication.

3. Click **Save**.

4.3.3 Configure WebSocket(s)

WebSocket protocol, based on TCP, aims to provide full-duplex communication between web browsers and servers. It allows to open a two-way interactive communication session.

Steps

1. Go to **System** → **System Settings** → **Network** → **Network Service** → **WebSocket(s)** .
2. Turn on **Enable**.
3. Set **Port**.
4. Click **Save**.

4.3.4 Configure Port Mapping (NAT)

Two ways are provided for port mapping to realize the remote access via the cross-segment network, UPnP™ (Universal Plug and Play), and manual mapping. UPnP™ can permit the device seamlessly discover the presence of other network devices on the network and establish functional network services for data sharing, communications, etc. You can use the UPnP™ function to enable the fast connection of the device to the WAN via a router without port mapping.

Before You Start

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.

Steps

1. Go to **System → System Settings → Network → Network Service → NAT**.

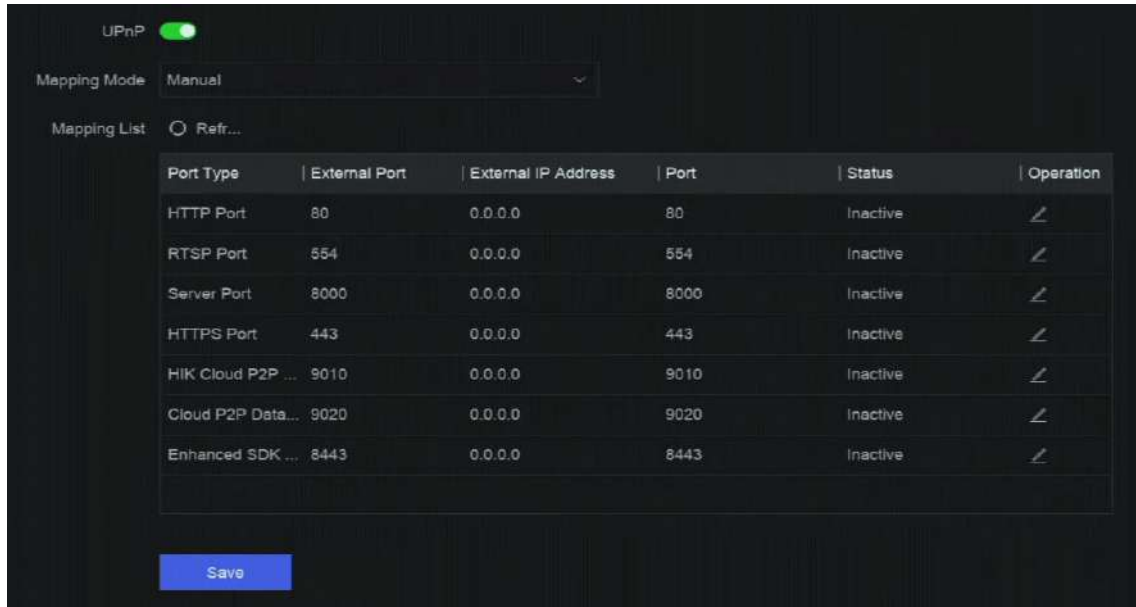


Figure 4-13 Port Mapping (NAT)

2. Turn on **Enable**.
3. Set **Mapping Mode**.

Auto

The port mapping items are read-only, and the external ports are set by the router automatically.

Manual

You can manually edit the external port.

4. If **Mapping Mode** is selected as **Manual**, click  to edit corresponding ports.



Note

- The value of the RTSP port number 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.
- **External Port** indicates the internal port number for port mapping in the router.

5. Click **Save**.

What to do next

Enter the virtual server settings page of router, then fill in the blank of internal/external source port with the internal/external port value, and other required contents.

4.3.5 Configure IoT

You can configure the network port through which the NVR will receive alarms from a security control panel.

Go to **System → System Settings → Network → Network Service → IoT** to enable the function and configure the port number.



Note

The port number you configured here should be the same as the alarm sending port on the security control panel.

Chapter 5 User Management

There is a default account for administrator. The administrator user name is **admin**. Administrator has the permission to add, delete, and edit user. Guest and operator users only have limited permissions.

Go to **System → System Settings → User Management** .

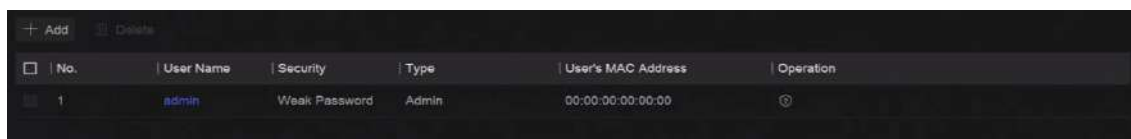


Figure 5-1 User Management

Table 5-1 Icon/Button Description

Icon/Button	Description
	Set account security.
Add	Add a new guest or operator user.
	Delete the selected user.

Note

Before operation, you have to confirm the admin password.

Chapter 6 Device Access

The video recorder may be able to access multiple device types, such as network camera, access control device, and alarm device. Please refer to the actual device for the access capability of your video recorder.

6.1 Access Video Device

There are several ways to access a video device.

6.1.1 Add Automatically Searched Online Network Camera

Network cameras on the same network segment can be automatically searched and added to the device.

Steps

1. Go to **System → Device Access → Device → Video Device → Online Device List**.
2. Select the device(s) from the list.

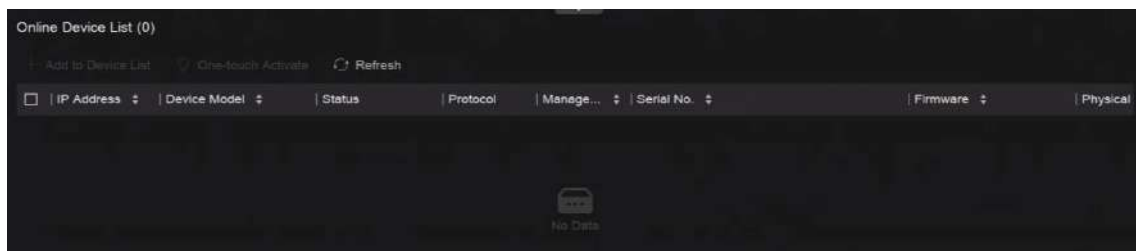


Figure 6-1 Add Automatically Searched Online Network Camera

3. Click **Add to Device List**.



Note

- The device will use a default password to add network cameras, ensure the camera password is the same as the default password. The default password can be configured in **More → Default Password Settings**.
 - If the searched network cameras are not activated, the device will use a default password to activate and add inactive network cameras. The default password can be configured in **More → Default Password Settings**.
 - When a network camera is successfully added, its status would be **Online**.
 - You can click the device name to add its parameters.
-

6.1.2 Add Network Camera Manually

Manually add the network cameras to your video recorder.

Before You Start

- Ensure your network camera is on the same network segment with that of your video recorder.
- Ensure the network connection is valid and correct.
- Ensure the network camera is activated.

Steps

1. Go to **System → Device Access → Device → Video Device** .

The screenshot shows the 'Add Device' window. At the top, there's a title bar with 'Add Device' and a close button. Below it is a section titled 'Online Device List (0)' with a 'Refresh' button. A table with 7 columns (No., IP Address, Device Model, Status, Protocol, Manag..., Serial No.) is shown, but it's empty, displaying 'No Data' with a camera icon. Below the table, there are several input fields: 'IP Address' with a 'Test' button, 'Device Name' (containing 'IPCamera 01'), 'Protocol' (a dropdown menu showing 'ONVIF'), 'Management Port' (containing '80'), 'User Name' (containing 'admin'), 'Password' (empty), and 'Transfer Protocol' (a dropdown menu showing 'Auto'). There is also a checkbox labeled 'Use Channel Default Password'.

Figure 6-2 Add Network Camera Manually

2. Click **Add**.
3. Enter network camera parameters.

Use Channel Default Password

If it is enabled, the video recorder will add the camera by the set channel default password.

More Settings

You can enable **Verify Certificate** to verify the camera with certificate. The certificate is a form of identification for the camera that provides more secure camera authentication. It requires to import the network camera certificate to the device first when you use this function.

4. **Optional:** Click **Continue to Add** to add other network cameras.

5. Click **Add**.

6.1.3 Add Network Camera through PoE

A PoE (Power over Ethernet) network camera can be directly connected to your device through the PoE interface at the rear panel.

After using a network cable to connect a PoE network camera with your device, you shall configure the corresponding PoE interface. Refer to **Configure PoE (Power over Ethernet) Interface** for details.

6.1.4 Add Solar-Powered Camera through OTAP Protocol

Solar-powered cameras can be added to your device through OTAP protocol.

Before You Start

Ensure the network between your device and solar-powered camera is accessible through OTAP protocol.

Enter the context of your task here (optional).

Steps

1. Go to **System → Device Access → Device Configuration → Access Service → OTAP Service**.

2. Turn on **Enable**.

3. Set **OTAP Server Port** and **Encryption Key**.

4. **Optional:** Enable **Auto Add IP Camera**. After the device OTAP parameters are configured, the newly signed network cameras (through OTAP protocol) can be automatically added to your device.

5. Configure the solar-powered camera OTAP protocol parameters through web browser. Refer to the camera user manual for details.



Note

The solar-powered camera OTAP protocol parameters shall be the same as the device.

6. Add solar-powered camera(s) to your device.

- If you have enabled **Auto Add IP Camera**, the newly signed network cameras (through OTAP protocol) would automatically be added to your device.
- Select solar-powered camera(s) from **Online Device List**, and click **Quick Add**.

7. Click **Add** in **System → Device Access → Device → Video Device**, select **Protocol** as **OTAP**, and click **Add**.

What to do next

- After a solar-powered camera is add to your device, you can wake it up, view its battery power, view its live video, configure its parameters through web browser, etc.
- Set ANR (Automatic Network Replenishment) for the camera. Refer to **Configure Recording Schedule** .

6.1.5 Add Network Camera via Custom Protocol

For network cameras that are not using standard protocols, you can configure custom protocols to add them. The system provides 8 custom protocols.

Before You Start

- Ensure the network camera supports RTSP streaming.
- Prepare the URL (Uniform Resource Locator) for getting the main stream or sub-stream of network cameras.

Steps

1. Go to **System → Device Access → Device → Video Device** .
2. Click **More → Custom Protocol Management** , or **Add → Protocol Management** .

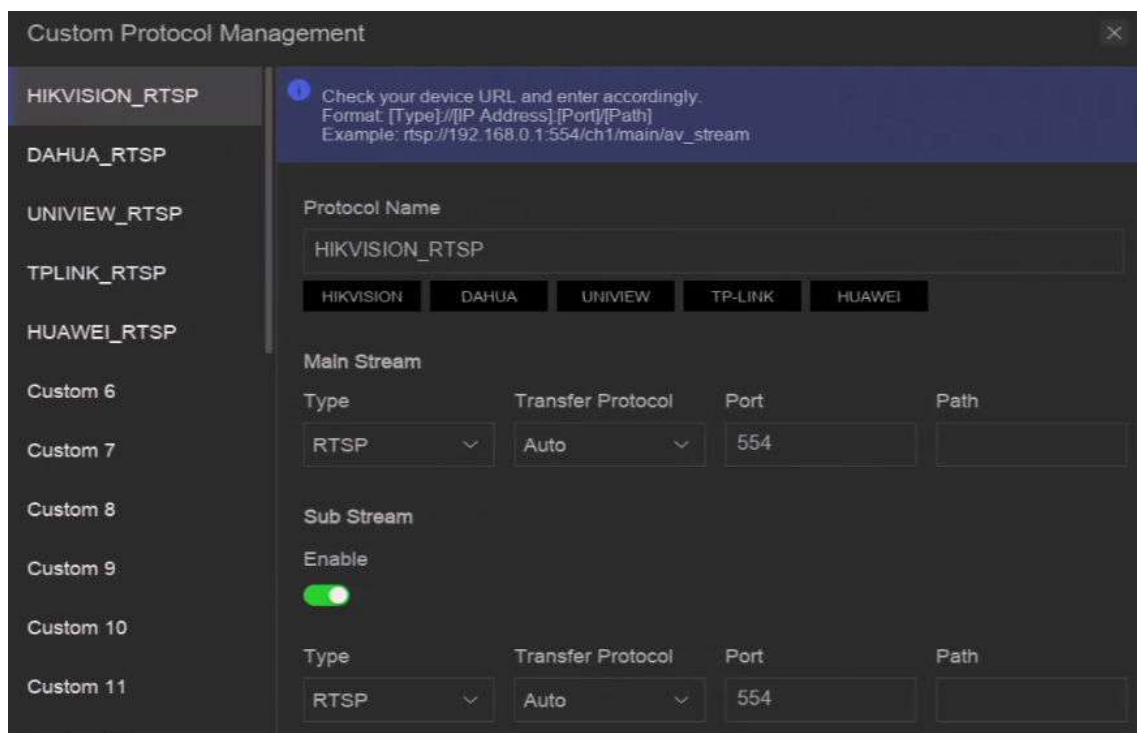


Figure 6-3 Add Network Camera via Customized Protocol

3. Select a protocol type at the left side.
4. Set protocol parameters.

Type

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

Transfer Protocol

3 types are selectable, including **Auto**, **UDP**, and **RTP Over RTSP**.

Port

The port for RTSP streaming, its default value is 554.

Path

Contact the manufacturer of network camera for the URL of getting main stream and sub-stream. The general format is *[Type]://[IP Address]:[Port]/[Resource Path]*, for example, *rtsp://192.168.0.1:554/ch1/main/av_stream*.



Note

- **Protocol Name** and **Path** can be automatically generated if you click a brand name below **Protocol Name**.
- You can disable sub-stream if the camera does not support sub-stream or does not have to use the sub-stream.

5. Click **OK**.

6. Click **Add** in **System → Device Access → Device → Video Device** to manually add a network camera.

6.1.6 Add Network Camera through Camera Configuration File

The information of added network cameras can be exported, including the IP address, port, password of admin, etc. And the exported camera configuration file content can be edited on your computer. After editing, the file can also be imported to other devices to add the cameras in the file.

Before You Start

Connect your video recorder to a USB flash drive that contains camera configuration file in it.

Steps

1. Go to **System → Device Access → Device → Video Device**.
2. Click **Import** to import the configuration file in USB flash drive.
3. Set the folder path.
4. Click **Confirm**.

6.2 Add Access Control Device

Access control devices can be added to your video recorder.

The adding process is similar with **Access Video Device**.

6.3 Add Security Control Panel

Steps

1. Go to **System → Device Access → Device → Security Control Panel** .
2. Click **Add**.
3. **Optional:** Select a protocol.
4. Enter device IP address, name, and IoT service port.
5. **Optional:** Select a transfer protocol if you select **OPTEX** as the protocol type.
6. **Optional:** Click  in the Operation column to set OSD parameters including character encoding, overlay mode, font size, etc.



Note

The Linked Channel cannot be edited. Go to **Event Center → Event Configuration → Event Configuration → Security Control Panel Event** to edit the linked channel.

OSD information you have set will be displayed on the video image.

6.4 Add Audio Device

Audio devices can be added to your video recorder, such as IP speakers, and microphones.

The adding process is similar with [Access Video Device](#) . If you link video channels with an IP speaker, the IP speaker could be used for voice broadcast. If you link video channels with a microphone, the microphone would be used as the audio input of the linked video channels for video recording.

6.5 Add POS Device

POS machine/server can be connected for certain device models. The device can receive transaction messages from POS machine/server, overlay transaction messages on the video image, and trigger POS event alarms.

Steps

1. Go to **System → Device Access → Device → POS** .
2. Click **Add** to add a POS device.

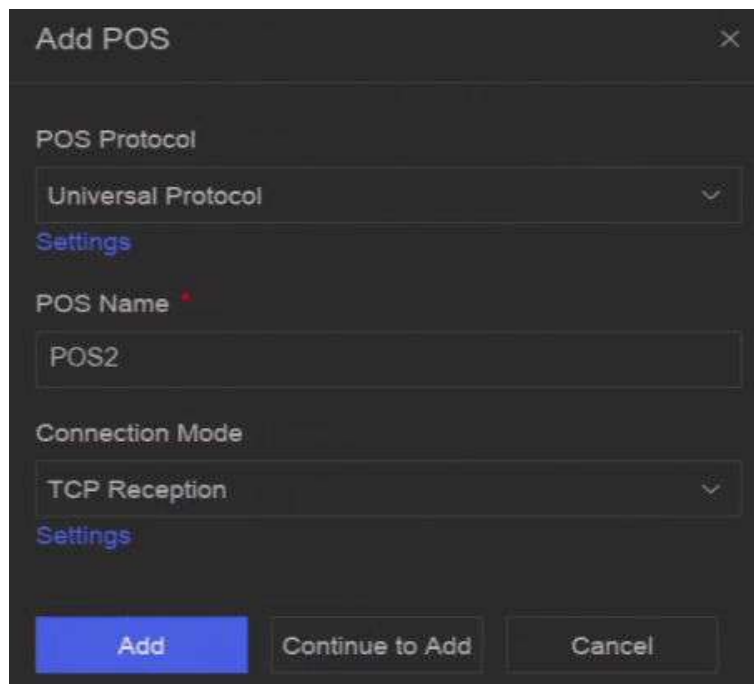


Figure 6-4 Add POS Device

3. Set the POS device parameters.

POS Protocol

Universal Protocol

You can set the start line identifier, line break tag, and end line tag for the POS overlay characters, and the case-sensitive property of the characters. You can also optionally check the filtering identifier and the XML protocol.

EPSON

The fixed start and end line tag are used for EPSON protocol.

AVE

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported.

NUCLEUS

The fixed start and end line tag are used for AVE protocol. Serial port and virtual serial port connection types are supported. The NUCLEUS protocol must be used in the RS-232 connection communication.

Connection Mode

TCP Connection

When using TCP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

UDP Connection

When using UDP connection, the port must be set from 1 to 65535, and the port for each POS machine must be unique.

USB-to-RS-232 Connection

Configure the USB-to-RS-232 convertor port parameters, including the port serial number, baud rate, data bit, stop bit, and parity.

RS-232 Connection

Connect the device and the POS machine via RS-232.

Multicast Connection

When connecting the device and the POS machine via Multicast protocol, set the multicast address and port.

Sniff Connection

Connect the device and the POS machine via Sniff. Configure the source address and destination address settings.

4. Click **Add**.



Note

After a POS device is added, you can click  in **Operation** to configure POS text overlay.

6.6 Channel Management

After a video device is added, you can view its channel number and channel name, and manage its parameters. This function is mainly used for a video device that contains more than one channel.

Go to **System → Device Access → Channel** to manage channels of video devices.

Chapter 7 Device Grouping

The added devices can be classified into different customized groups.

Steps

1. Go to **System** → **Device Access** → **Device Grouping**.

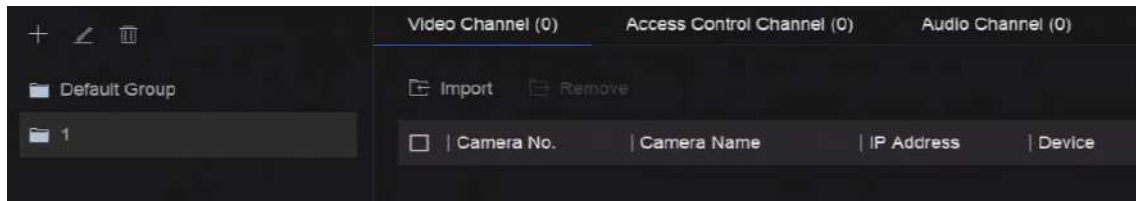


Figure 7-1 Device Grouping

2. Click  to add a group.



Note

After a group is added, you can click  /  to edit/delete it.

3. Click **Import** to add channel(s) to the selected group.

Chapter 8 Video or Audio Device Settings

You can configure the added video or audio device, such as privacy mask, image parameters, etc.

8.1 Enable H.265 Stream Access

The device can automatically switch to the H.265 stream of IP camera (which supports H.265 video format) for the initial access.

Steps

1. Go to **System → Device Access → Device → Video Device**.
2. Click **More → Auto Switch to H.265**.
3. Enable this function.
4. Click **Save**.

8.2 Configure Display Settings

Configure the OSD (On-Screen Display), image settings, exposure settings, day/night switch settings, etc.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Display Settings**. Select a camera, and configure parameters as your desire.

OSD Settings

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

Image Settings

Customize the image parameters including the brightness, contrast, and saturation for the live view and recording effect.

Exposure Time

Set the camera exposure time (1/10000 to 1 sec). A larger exposure value results in a brighter image.

Day/Night Switch

The camera can be set to day, night, or auto switch mode according to the surrounding illumination conditions.

Backlight

Set the camera's wide dynamic range (0 to 100). When the surrounding illumination and the object have large differences in brightness, you should set the WDR value.

Image Enhancement

For optimized image contrast enhancement.

8.3 Configure Video Parameters

Video parameters would affect the live view image and recording file.

Go to **System → Device Access → Device Configuration → Device Parameter → Video Device → Video Parameters**. Select a camera, and configure parameters as your desire.

Main Stream

Main stream refers to the primary stream that affects data recorded to the hard disk drive and will directly determine your video quality and image size. Comparing with the sub-stream, the main stream provides a higher quality video with higher resolution and frame rate.

Sub-Stream

Sub-stream is a second codec that runs alongside the mainstream. It allows you to reduce the outgoing internet bandwidth without sacrificing your direct recording quality. Sub-stream is often exclusively used by smartphone applications to view live video. Users with limited internet speeds may benefit most from this setting.

Resolution

Image resolution is a measure of how much detail a digital image can hold. The greater the resolution, the greater the level of detail. Resolution can be specified as the number of pixel-columns (width) by the number of pixel-rows (height), e.g., 1024 × 768.

Bitrate Type

The bit rate (in kbit/s or Mbit/s) is often referred to as speed, but actually defines the number of bits/time unit rather than distance/time unit. Two types including variable or constant are available.

Frame Rate

It refers to the number of frames captured each second. A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

I-Frame Interval

I-Frame also referred as intra picture, I-Frame is the first frame of every GOP (a video compression technology of MPEG). It can be viewed as pictures after compression. I-Frame interval is the amount of frames between two continuous I-Frames.

8.4 Configure Privacy Mask

The privacy mask protects personal privacy by concealing parts of the image from live view or recording with a masked area.

Steps

1. Go to **System** → **Device Access** → **Device Configuration** → **Device Parameter** → **Video Device** → **Privacy Mask**.

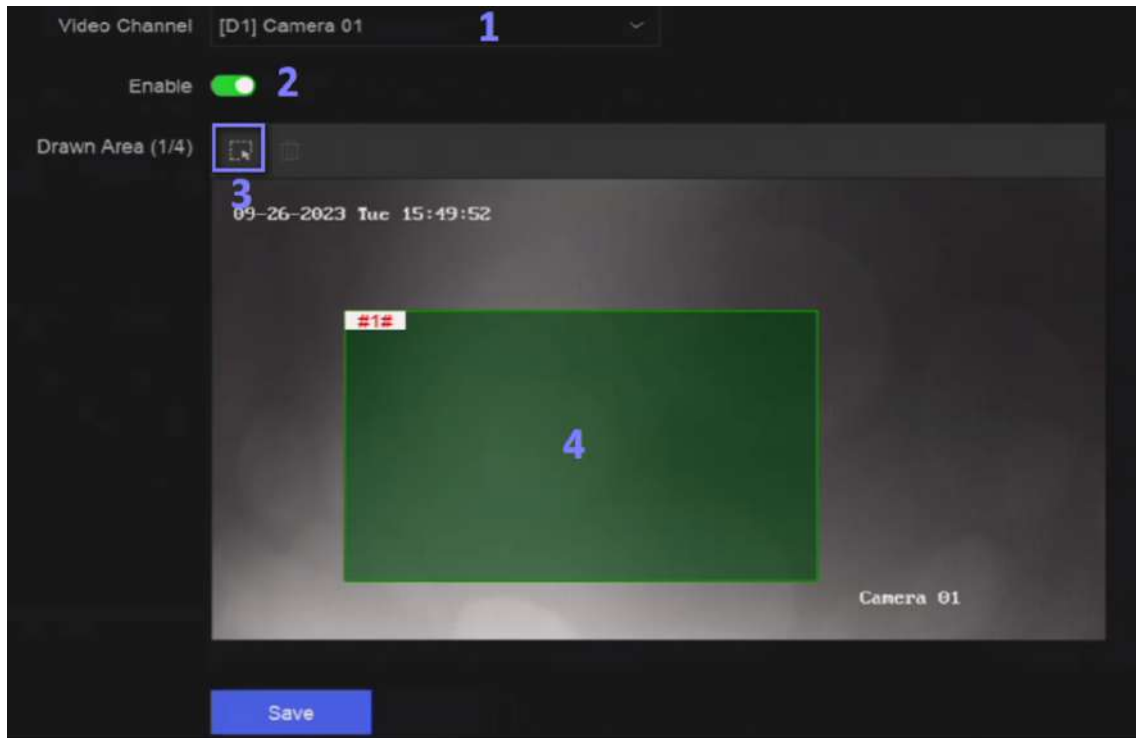


Figure 8-1 Privacy Mask

2. Select a camera.
3. Turn on **Enable**.
4. Draw mask areas on the preview window. The areas will be marked with different frame colors.



Note

Up to 4 privacy mask areas can be configured and the size of each area can be adjusted.

5. Click **Save**.

8.5 Configure Privacy Protection

This function allows for the automatic obscuring or blurring of specific areas (including human faces, human bodies, and vehicles) on the video footage to protect personal privacy or sensitive information.

Before You Start

This function should be supported by the camera.

Steps

1. Go to **System** → **Device Access** → **Device Configuration** → **Device Parameter** → **Video Device** → **Privacy Protection** .

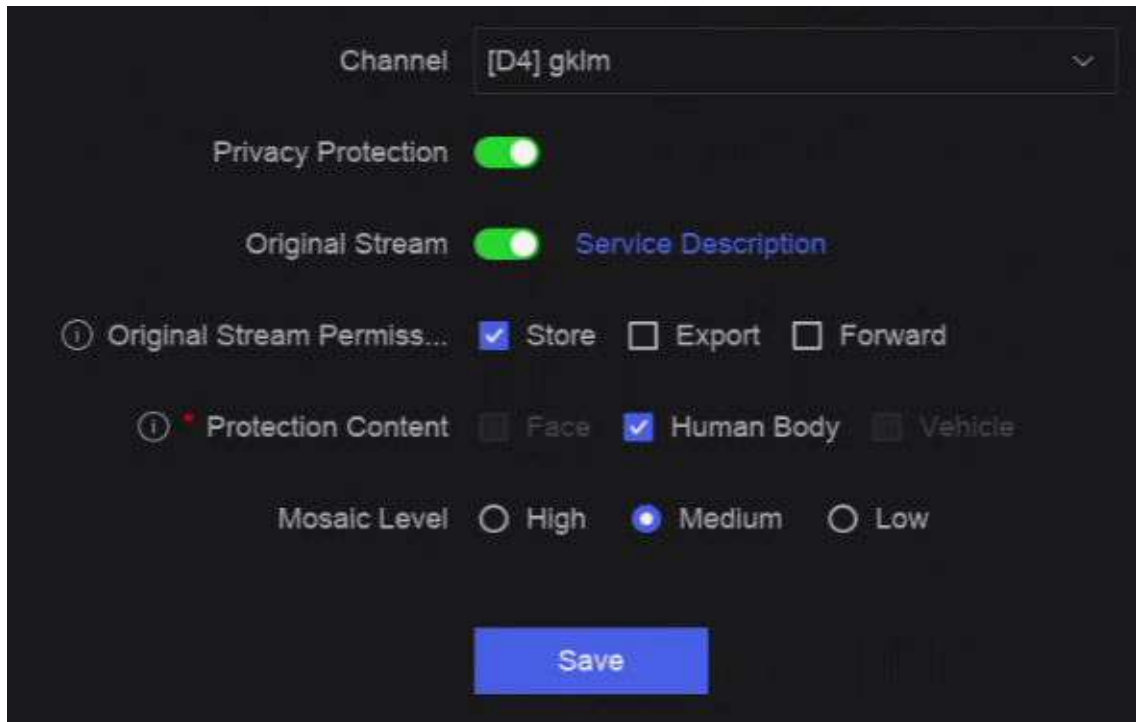


Figure 8-2 Privacy Protection

2. Select a camera.
3. Enable **Privacy Protection**.
4. **Optional:** Enable **Original Stream** and set the stream permission.

Note

Original stream means the video stream without mosaic.

Store

The original stream can be stored. Storing original stream will cost more storage space or decrease the recording storage period of the channel. The original stream bitrate is the same as the camera, which is not configurable.

Export

The channel original stream can be exported.

Forward

The original stream can be forwarded.



Note

You should check Store permission before checking Export and/or Forward permissions.

5. Set **Protection Content**. The selected protection content will be blurred during live view and playback.
6. Set **Mosaic Level**. Higher the level, more blurred the target image.
7. Click **Save**.

8.6 Configure Audio Parameter

After an audio device is added, you can configure its parameters in **System** → **Device Access** → **Device Configuration** → **Device Parameter** → **Audio Device**. For example, if an IP speaker is added, its name, audio output volume and audio quality can be configured.

8.7 Configure OTAP Service

OTAP (Open Thing Access Protocol) is an unified integrated standard and push-pull mode of Hikvision protocol in the public network and private network. After OTAP is enabled, other applications may be able to remotely view videos through this protocol.

Before You Start

Ensure your device network is accessible through OTAP protocol.

Steps

1. Go to **System** → **Device Access** → **Device Configuration** → **Access Service** → **OTAP Service**.

Enable ☒

Service Port 7800

Encryption Key

Auto Add IP Camera ☒

Enable External Mapping ☒

External IP Address 0.0.0.0

External Service Port 7800

① External Alarm Port 7700

① External Alarm Picture ... 6011

① External Streaming Start... 58002

Save

Figure 8-3 Configure OTAP Service

2. Turn on **Enable**.
3. Set the parameters.
4. Click **Save**.

8.8 Configure ISUP Service

Before adding cameras to NVR via ISUP, you should enable ISUP service for camera registration by configuring service port and encryption key.

Before You Start

Make sure you have configured service port number and encryption key on cameras.

Steps

1. Go to **System → Device Access → Device Configuration → Access Service → ISUP Service** .
2. Enable **Enable**.
3. Enter the service port number and encryption key, which should be the same as that are configured on the cameras.
4. **Optional:** Enable **Enable Auto Add Network Camera**, and then network cameras can be added to the NVR automatically after being registered via ISUP.
5. **Optional:** Enable **Enable External Mapping** and configure the related parameters.
6. Set the streaming mode as **Continuous Streaming** or **Scheduled Streaming**.
7. Click **Save**.

8.9 Batch Configuration

Connected devices can be configured in a batch.

Steps

1. Go to **System → Device Access → Device Configuration → Batch Configuration** .

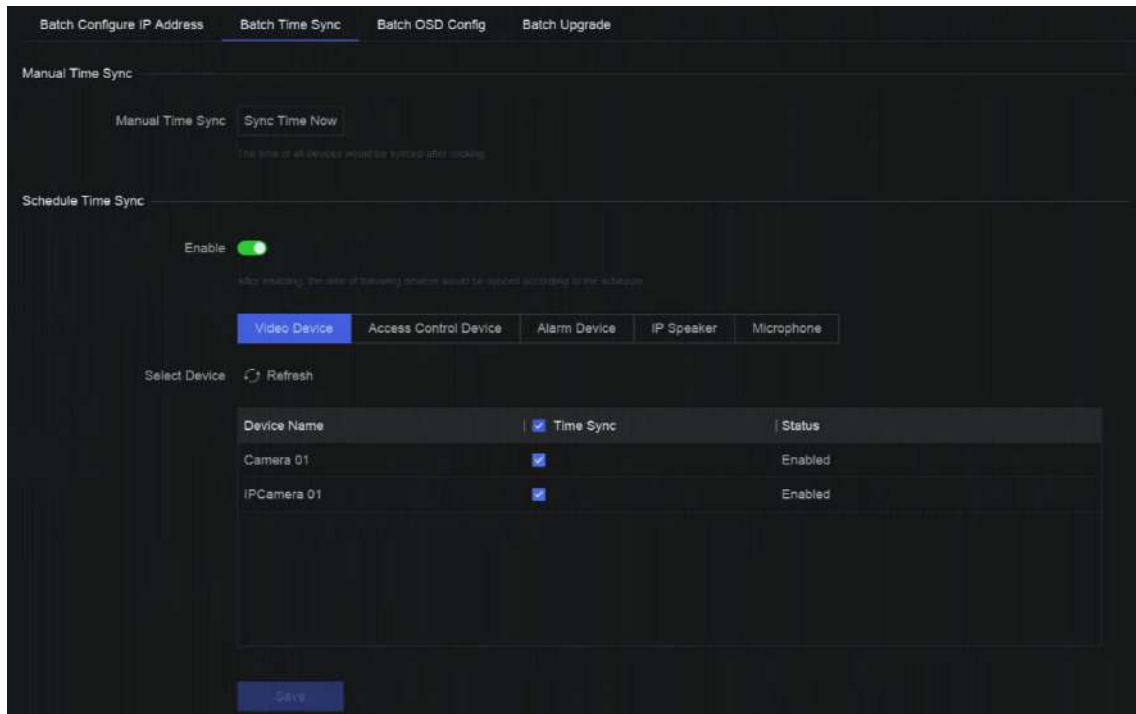


Figure 8-4 Batch Configuration

2. Configure IP address, time sync, OSD, or upgrade firmware as your desire.

Manual Time Sync

Click **Sync Time Now** to manually sync time of all connected devices. This operation is just for once.

Schedule Time Sync

The recorder would sync time of the selected devices according a fixed schedule.

3. For IP address configuration and time sync, click **Save**.

8.10 Configure PoE (Power over Ethernet) Interface

The PoE interfaces enable the device to transfer electrical power and data to connected PoE devices. And the PoE interface supports the Plug-and-Play function. Connectable PoE device number varies with device models. If you disable a PoE interface, you can also use it to connect to an online device.

Before You Start

Ensure your NVR support PoE function.

Steps

1. Go to **System → Device Access → Device Configuration → PoE**.
2. Enable **Plug-and-Play** function of PoE interfaces according to your requirement.

3. Select the device type as **IP Speaker** or **Camera**.

4. If a PoE interface is used to connect a PoE camera, select the connection distance of network cable.

Long Distance

Long-distance (100 to 300 meters) network transmissions via PoE interface.

Short Distance

Short-distance (< 100 meters) network transmission via PoE interface.



Note

- The PoE interfaces are enabled with the short distance mode by default.
- The bandwidth of IP camera connected to the PoE via long network cable (100 to 300 meters) cannot exceed 6 MP.
- The allowed max. long network cable may be less than 300 meters depending on different IP camera models and cable materials.
- When the transmission distance reaches 100 to 250 meters, you must use the CAT5E or CAT6 network cable to connect with the PoE interface.
- When the transmission distance reaches 250 to 300 meters, you must use the CAT6 network cable to connect with the PoE interface.

5. Click **Save**.

What to do next

When PoE devices are connected, you can view the status and power of each PoE interface.

Chapter 9 Storage Management

9.1 Manage HDD

A newly installed hard disk drive (HDD) must be initialized before using. You can format HDD, repair database, and view HDD status through HDD management interface.

Before You Start

Ensure the HDD is properly installed to your device.

Steps

1. Go to **System → Storage Management → Storage HDD → Storage HDD**.



HDD No.	Free Space (GB)	Capacity (GB)	Status	Type	Property	Operation
1	166	466	Sleeping	Local	R/W	[Icon]
3	3685	3726	Sleeping	Local	R/W	[Icon]
5	3685	3726	Sleeping	Local	R/W	[Icon]

Figure 9-1 Manage HDD

2. **Optional:** Perform the following operations as your desire.

Add Network HDD Add a NAS or IP SAN.

Format Format the selected HDD.

Repair Database Repairing database will rebuild all databases. It might help to improve your system speed after upgrade.

Note

- Repairing database will rebuild all databases. Existing data will not be affected, but local search and playback functions will not be available during the process, you can still achieve search and playback functions remotely via web browser, client software, etc.
- Do not pull out the drive, or shut down the device during the process.



Remove/load HDD.

9.2 RAID Configuration

A disk array is a data storage virtualization technology that combines multiple physical disk drives into a single logical unit. Also known as a "RAID", an array stores data over multiple HDDs to provide enough redundancy so that data can be recovered if one disk fails. Data is distributed

across the drives in one of several ways called "RAID levels", based the redundancy and performance required.



Caution

RAID requires enterprise-level HDDs.

The functions in this section are only available for certain models. It is recommended to use the same model and capacity HDDs.

There are two ways to create RAID. For one-touch creation, the default RAID type is RAID5. For manual creation, RAID0, RAID1, RAID5, RAID6, and RAID10 can be configured.

Table 9-1 HDD Requirement for Each RAID Type

RAID Type	Required Number of HDDs
RAID0	≥2
RAID1	2
RAID5	≥3
RAID6	≥4
RAID10	4 or 8



Note

- The function is only available for certain models.
 - When array exception event occurs, the corresponding linkage actions can be configured in **System → System Settings → Exception** .
-

9.2.1 Create Disk Array

A disk array can be created after enabling array mode.

Before You Start

- **Storage Mode** is set to **Quota** in **System → Storage Management → Storage Mode** .
- Enough HDDs are correctly installed to the device. And HDDs for array creation are AI or enterprise level.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Enable Array Mode**, or enable **Array Mode**.

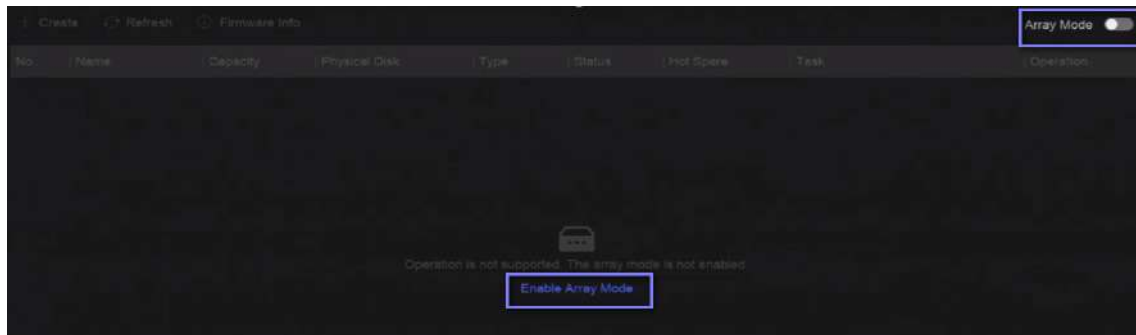


Figure 9-2 Enable RAID

3. Wait for the device to restart.
4. Go to **System → Storage Management → Storage HDD → Array Management** again.

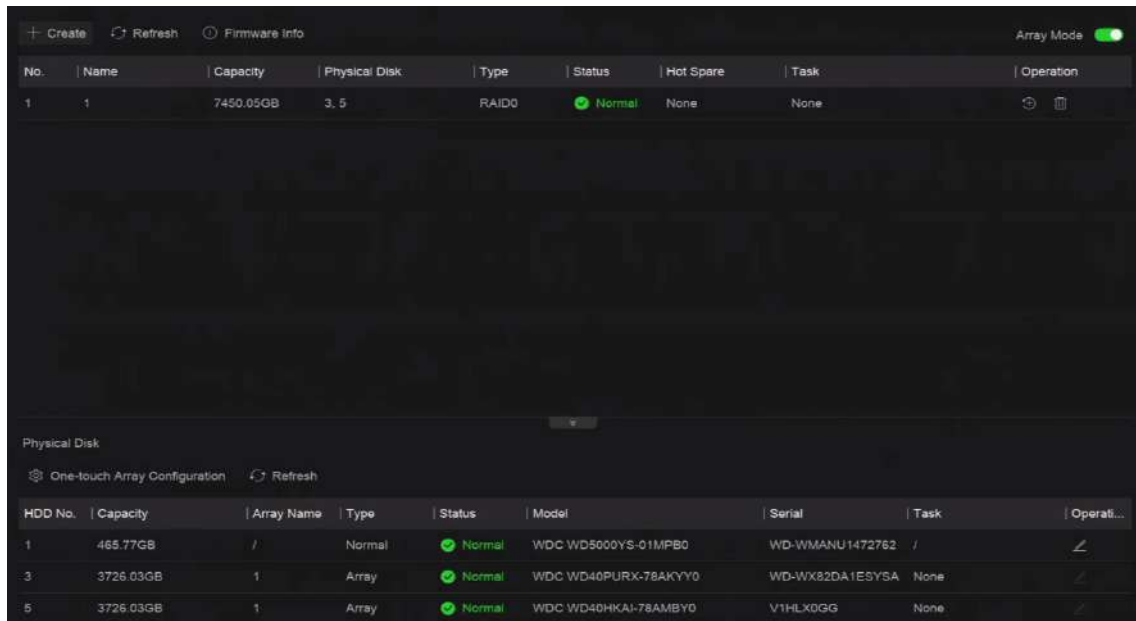


Figure 9-3 Array Management

5. Create an array.

Creation Method

Description

One-touch Array Configuration

Click **One-touch Array Configuration**.



Note

By default, the array type created by one-touch configuration is RAID 5.

Manual Creation

Click **Create** to manually create a RAID 0, RAID 1, RAID 5, RAID 6, or RAID 10 array.

9.2.2 Rebuild Array

The array status includes **Functional**, **Degraded**, and **Offline**. To ensure the high security and reliability of the data stored in an array, take immediate and proper maintenance of the arrays according its status.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management**.
2. Rebuild an array.

Table 9-2 Rebuilding Method

Rebuilding Method	Description
Auto Rebuild	There should be a hot spare disk in the array, and the hot spare disk capacity is not less than the disk with the minimum capacity in the array. Click  in Operation column under Physical Disk to set a hot spare disk. When an HDD in the array in the array is not working, the hot spare disk would be activated, and the array would be automatically rebuilt.  Note After auto rebuild finishes, it is recommended to install another HDD, and configure it as the hot spare disk.
Manual Rebuild	If there is no hot spare disks in the array, you have to manually rebuild the array. Go to System → Storage Management → Storage HDD → Array Management, and select the hot spare disk in the list to rebuild.

9.2.3 Delete Array

Go to **System → Storage Management → Storage HDD** to click  to delete the selected array.

9.2.4 View Firmware Info

You can view array firmware information and set the background task speed.

Before You Start

Ensure disk array is enabled.

Steps

1. Go to **System → Storage Management → Storage HDD → Array Management** .
2. Click **Firmware Info**.
3. **Optional**: Set **Back Ground Task Speed**.

9.3 Configure Storage Mode

Steps

1. Go to **System → Storage Management → Storage Mode** .

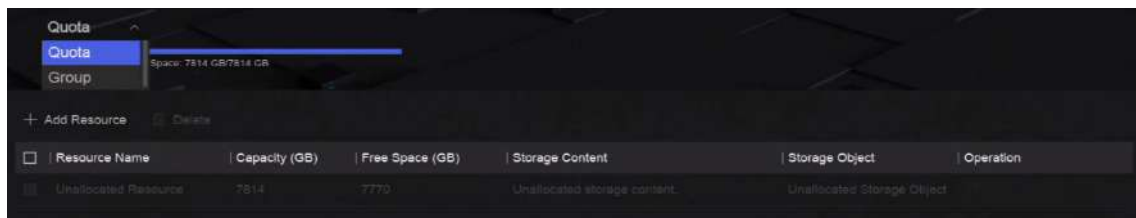


Figure 9-4 Storage Mode

2. Select **Quota** or **Group**.

Quota

Each camera or audio device can be configured with an allocated quota for storing videos, pictures, or audios.

Group

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

3. Set corresponding parameters.
 - **Quota**: Allocate space for storage objects.
 - **Group**: Link channels to HDD groups.

9.4 Configure Auto Backup

You can enable auto backup so that specific channels will start backing up recordings at the configured time.



Note

This function should be supported by the device. Before using the function, make sure the eSATA storage device have been connected.

Go to **System → Storage Management → Backup Configuration → Auto Backup Configuration** , and enable **Auto Backup**.

Stop Writing

When the HDD space used for backup is full, new recording data will stop being written to HDD.

Overwrite

When the HDD space used for backup is full, the older recordings will be overwritten so that new recording data can be written to HDD.

9.5 Configure Other Storage Parameters

Go to **System → Storage Management → Advanced Settings** .

Table 9-3 Parameter Description

Parameter Name	Description
HDD Sleeping	Select a mode for HDDs. Performance Mode , Balanced Mode , and Energy Saving Mode are selectable.
Overwriting	When HDD is full, it will continue to write new files by deleting the oldest files.
Save Camera VCA Data	After saving VCA data of camera to your device, you will be able to search it in Event Center .
Max. Length per Video	It is the time length of each video file when you exporting videos from the device.
Tag Video Post-Record	After adding a tag to a video, it is the time you set to record after the scheduled time.  Note - You can click  during live view or playback to add a tag. - For searching tag videos, go to  → Backup → By Tag.
eSATA	For devices with eSATA interface at the rear panel.
Usage	Set the usage for eSATA.

9.6 Mange USB Flash Drive

After inserting a USB flash drive in to your device, you can view its remaining storage capacity, manage its content, or format it.

When a USB flash drive is connected to your device for the first time, short operations can be performed, such as device upgrade and backup. Meanwhile, there would be a new icon  displayed at the upper-right corner.

Chapter 10 Schedule Configuration

The device will follow the schedule to store files to the disk.

10.1 Configure Schedule Template

After a schedule template is configured, you can use the template as the recording schedule.

Steps

1. Go to **System → System Settings → Template Configuration → Holiday Schedule** .
2. Click **Add**.

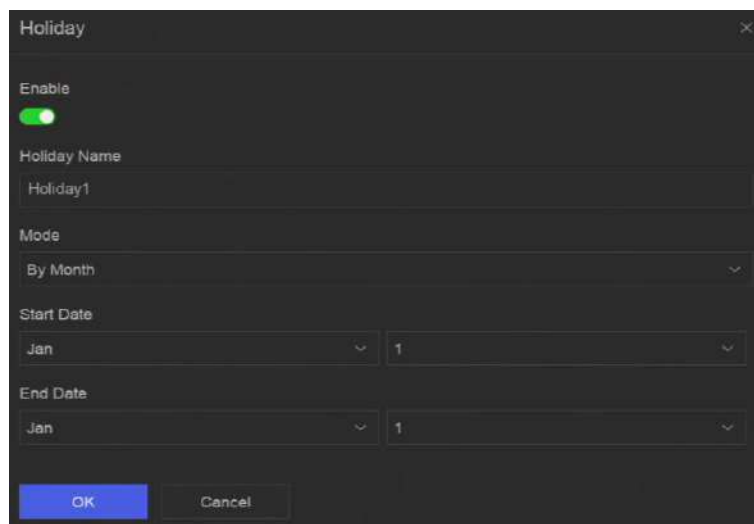


Figure 10-1 Add Holiday

3. Turn on **Enable**.
4. Configure the holiday.



Note

After holidays are configured, you will be able to set the holiday schedule independently. Holiday schedule has higher priority than normal schedule (from Mon to Sun).

-
5. Set **Storage Schedule**.
 - 1) Click **Storage Schedule**.
 - 2) Select a template name.

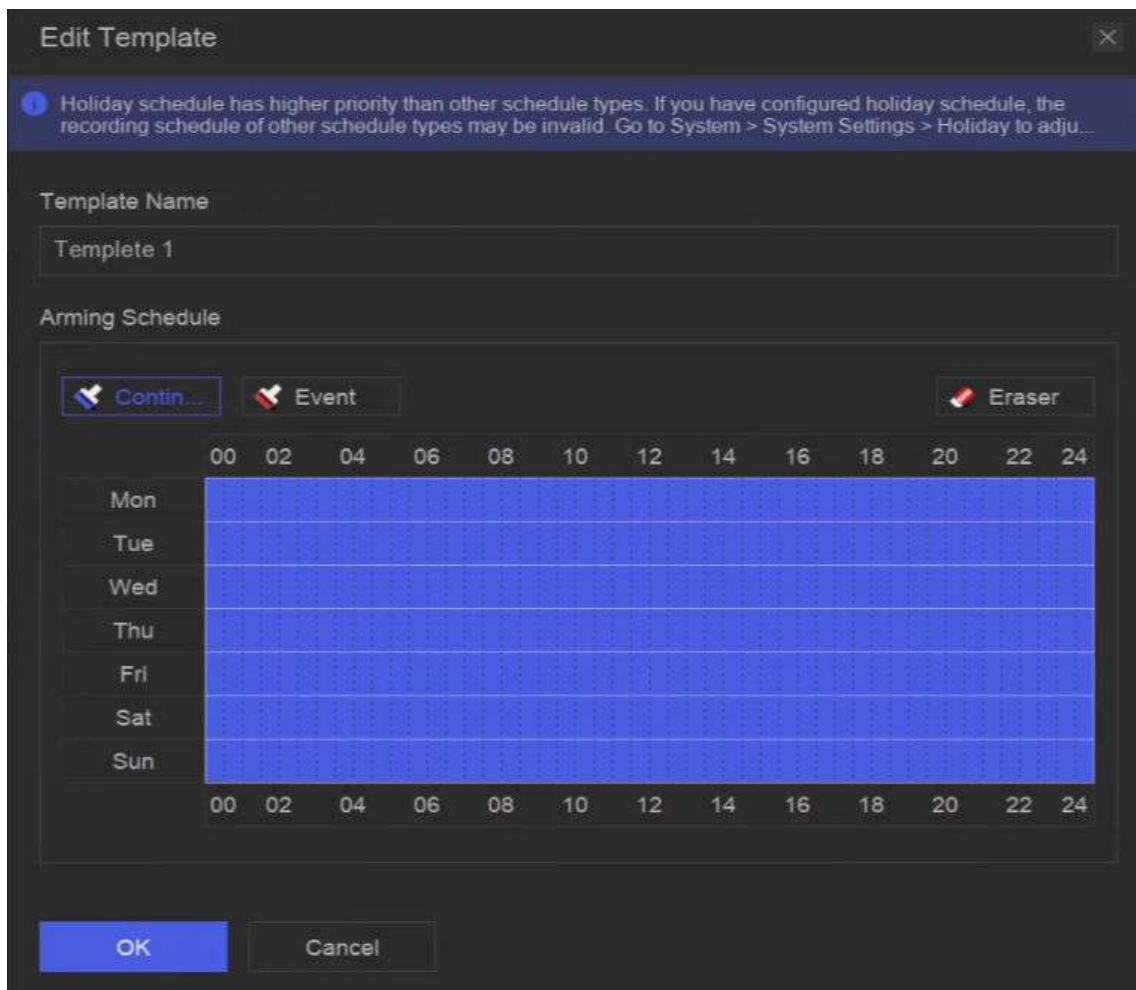


Figure 10-2 Edit Template

- 3) Select a recording type. For example, **Event**.
- 4) Drag the cursor on time bar to draw the schedule.



Note

- After moving the cursor on time bar, you can also click **00:00-24:00**  to set specified time schedule.
- You can click **Eraser** to clear schedule.



Note

You can also click **Configure Template** to configure template in **System → Storage Management → Storage Schedule → Video Recording / Picture Capture / Audio Recording**.

6. Click **OK**.

10.2 Configure Recording Schedule

The camera would automatically start/stop recording according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Video Recording** .

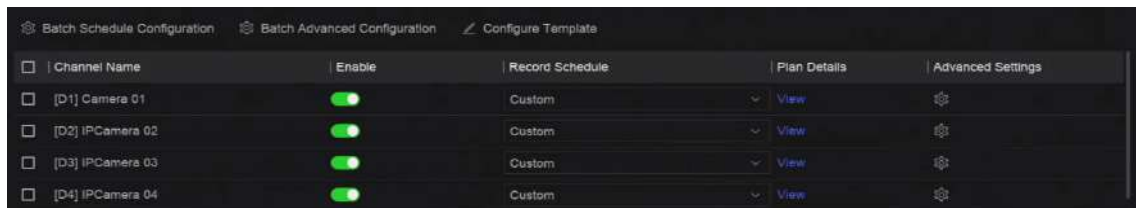


Figure 10-3 Video Recording Configuration

2. Turn on **Enable** for a camera.
3. Select a schedule type.



Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

4. Click **View** to view the schedule.



Figure 10-4 View Schedule

5. **Optional:** Click  under **Advanced Settings** to set other advanced parameters.

Table 10-1 Advanced Parameter Description

Parameter	Description
Record Audio	Enable or disable audio recording.  Note The channel shall have audio function, or have connected an audio device.
ANR	ANR (Automatic Network Replenishment) can automatically enable SD card of network camera to save the video in the condition of network disconnection, and can synchronize data after the network is recovered.
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the camera records at 9:59:55.

Parameter	Description
Post-Record	The time you set to record after the event or the scheduled time. For example, when an alarm triggered recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.
Stream Type	For Main Stream , its resolution is usually higher. For Sub-Stream , you can record for a longer time with the same storage space, but its resolution would be low. For Dual Stream , the device will record both main stream and sub-stream.
Video/Picture Expired Time	The expired time is period for a file to be kept in the HDD. When the deadline is reached, the file will be deleted. If you set the expired time to 0, the file will not be deleted. The actual keeping time for the file should be determined by the capacity of the HDD.

- Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
- Click **Save**.

10.3 Configure Picture Capture Schedule

The device would automatically capture live pictures according to the schedule.

Steps

- Go to **System → Storage Management → Storage Schedule → Picture Capture**.

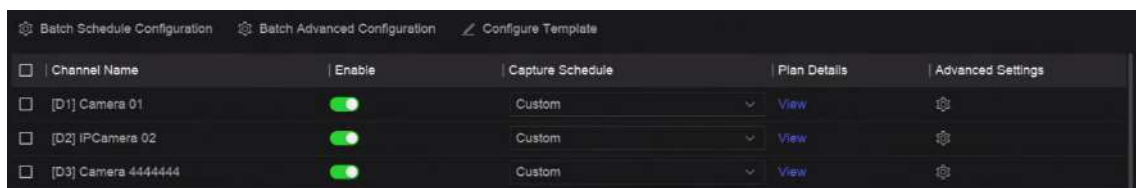


Figure 10-5 Picture Capture Configuration

- Turn on **Enable** for a camera.
- Select a schedule type.

Note

If you set **Capture Schedule** as **Custom**, you can drag the cursor on time bar to set customized picture capture schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

- Click **View** to view the schedule.



Figure 10-6 View Schedule

5. Click under **Advanced Settings** to set advanced picture parameters.

Table 10-2 Advanced Parameter Description

Parameter	Description
Capture Delay	The duration for picture capture.
Resolution	Set the resolution of the picture to capture.
Picture Quality	Set the picture quality to low, medium or high. High picture quality requires more storage space.
Interval	The time interval of capturing each live picture.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

10.4 Configure Audio Recording

The device would automatically record audios according to the configured recording schedule.

Steps

1. Go to **System → Storage Management → Storage Schedule → Audio Recording** .
2. Turn on **Enable** for a channel.
3. Select a schedule type.



Note

If you set **Record Schedule** as **Custom**, you can drag the cursor on time bar to set customized record schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

-
4. Click **View** to view the schedule.
 5. **Optional:** Click under **Advanced Settings** to set other advanced parameters.

Table 10-3 Advanced Parameter Description

Parameter	Description
Pre-Record	The time you set to record before the scheduled time or event. For example, when an alarm triggers the recording at 10:00, and if you set the pre-record time as 5 seconds, the channel records 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 recording ends at 11:00, and if you set the post-record time as 5 seconds, it records till 11:00:05.

6. **Optional:** Select channels in the list, and use **Batch Schedule Configuration** and **Batch Advanced Settings** to configure channels in a batch.
7. Click **Save**.

Chapter 11 Live View

11.1 Configure Live View Layout

Live view displays the video image of each camera in real time.

Steps

1. Go to **Live View**.
2. Click  at the lower-right corner.
3. Select a window division type, or click **Custom** to customize a new type as your desire.
4. Move the cursor on **Default View** in **View**.
5. Click  at the right side of **View**.
6. Follow the step descriptions to adjust the live view image output interface. Besides the two ways that are mentioned on the user interface, you can drag a channel from one window to another.
7. Click .

11.2 GUI Introduction

You can view live image, play live audio, capture pictures, perform instant playback, etc.

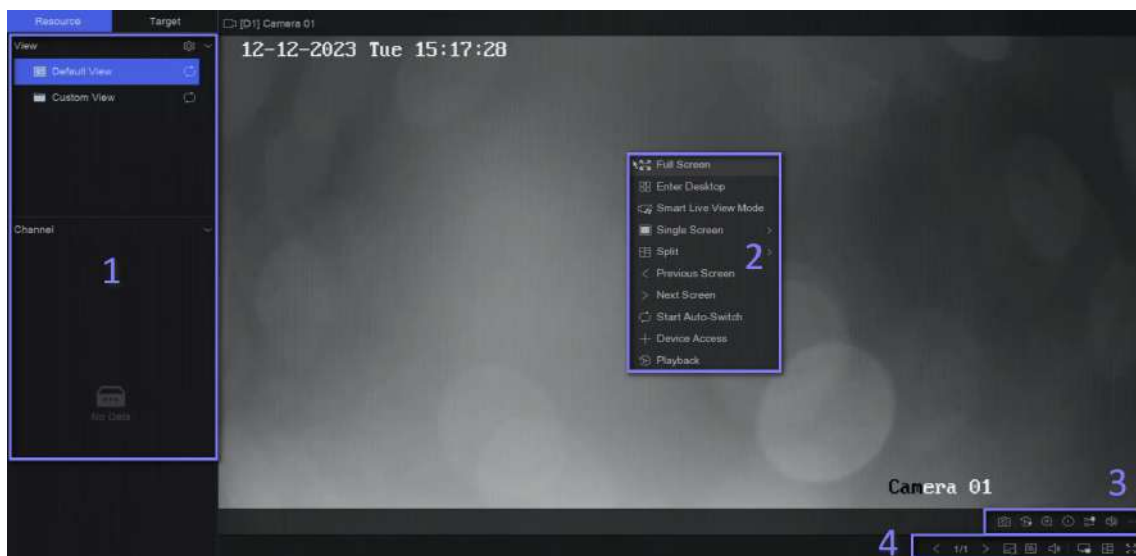


Figure 11-1 Live View (Type 1)

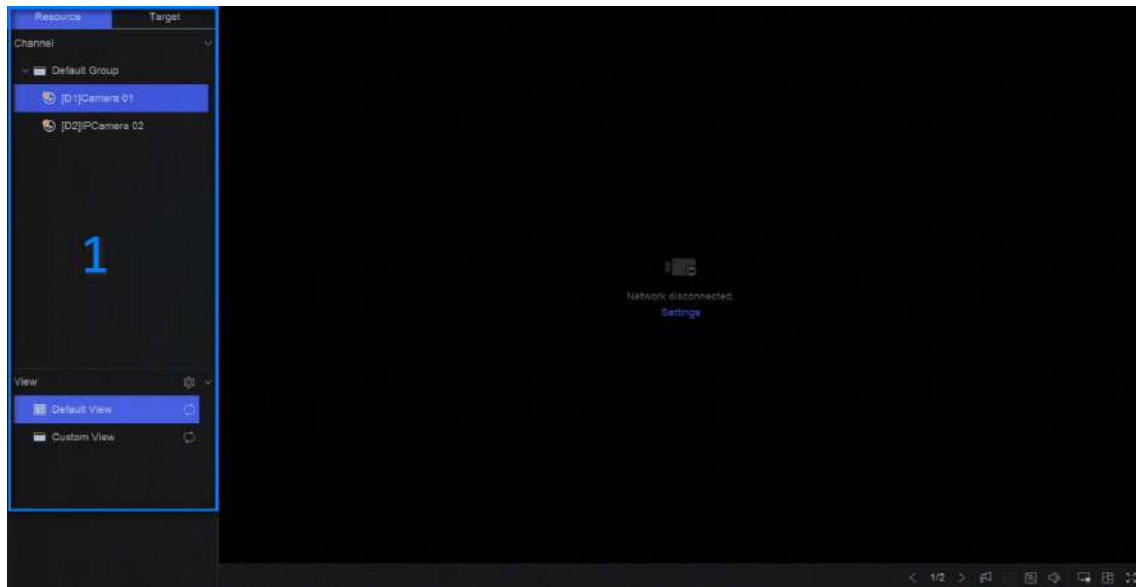


Figure 11-2 Live View (Type 2)

Table 11-1 Interface Description

No.	Description
1	Channel list, PTZ control panel, and target detection list. If you select a channel from the channel list, the device will redirect to the corresponding window. If you click Target , you can view live target detection results in the list, and click  to configure the corresponding settings.
2	Right-click shortcut menu. It will appear after right clicking the cursor on the image area.
3	Channel tool bar. - Click  to add a tag go the channel. After adding, you can go to  → Backup → By Tag to search videos by tag. - You can select  → Show VCA Info to display rule frames.
4	Live view tool bar. Functions like Voice Broadcast , Display VCA Info and Switch Output can be performed here.

Note

- You can scroll up/down your mouse to turn to previous/next screen.
- If channel image display exception occurs, the corresponding window would show the error message, and you can directly click the text (in blue color) to edit the device settings.

11.3 PTZ Control

PTZ is the acronym for Pan, Tilt, and Zoom. After a PTZ camera is add to your device, the device would be allowed to pan left and right, tilt up and down, and zoom in and out.

Select a PTZ camera, and expend the PTZ control menu at the lower-left corner.

Table 11-2 PTZ Operation

Task	Description	Operation
Preset	Presets record the PTZ position and the status of zoom, focus, iris, etc. You can call a preset to quickly move the camera to the predefined position.	Set a preset: 1. Select a preset. 2. Use to direction buttons to adjust the image. 3. Click  .
		Call a preset: Click  .
Patrol	Patrols can be set to move the PTZ to key points and have it stay there for a set duration before moving on to the next key point. The key points are correspond to the presets.	Set a patrol: 1. Select a patrol. 2. Click  .
		3. Add presets for the patrol. 4. Click OK . Call a patrol: Click  .
Pattern	Patterns can be set by recording the movement of the PTZ. You can call the pattern to make the PTZ move according to the predefined path.	Set a pattern: 1. Click  .
		2. Use to direction buttons to adjust the image, the device will record the movement. 3. Stop recording. Call a pattern: Click  .

Note

If the PTZ panel cannot be used, please click  to check the settings.

Chapter 12 Playback

12.1 GUI Introduction

You can play back video or audio files.

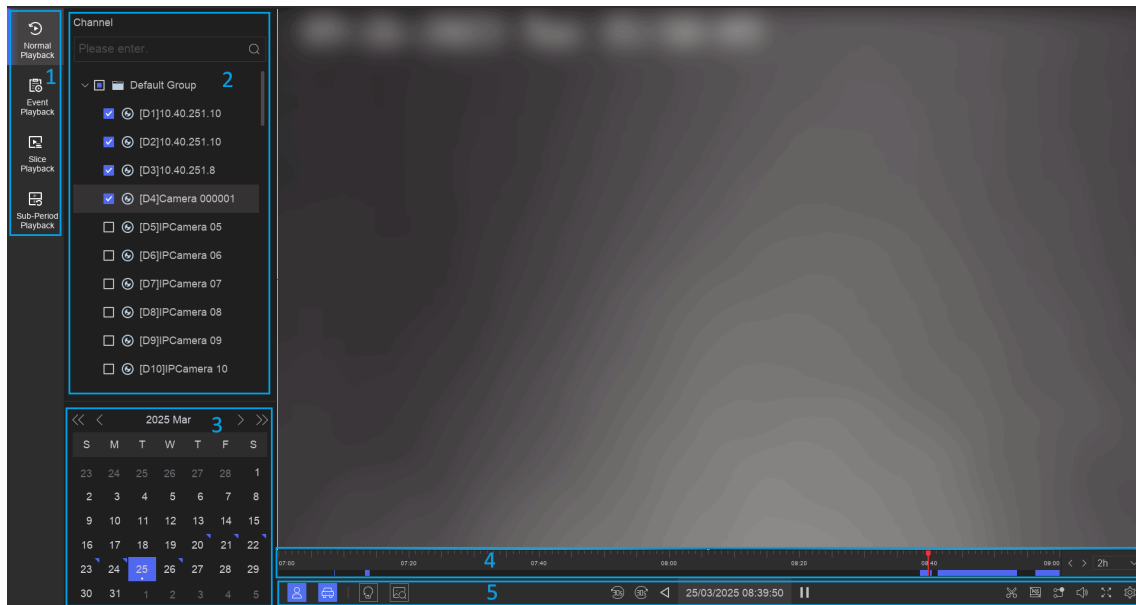


Figure 12-1 Playback

Table 12-1 Interface Description

No.	Description
1	Area for selecting playback type.
2	Channel list.
3	Calendar for time selection.
4	Playback timeline. - Position the cursor on the timeline, drag the timeline to position to a certain time. - Period marked with blue bar contains video. Red bar indicates the video in the period is event video. - Scroll up/down to zoom out/in timeline.
5	Playback tool bar.

No.	Description
	- Click  (Smart Search), then follow the pop-up tips to draw event rule and search videos that can trigger the corresponding event rule. The operations are similar with Dual-VCA function. - Click  to perform AcuSearch function. Refer to AcuSearch for details. - Click  /  to show videos that contain human/vehicle.  Note In order to use this function, ensure you have configured Detection Target as Human or Vehicle for certain event types. - Click , select channels, and set the start and end time to clip the video in the selected channels within specific time period. - Click  to set normal video and smart video (the video that contains smart data) playback strategy.

12.2 Normal Playback

Play back videos for a channel. For certain devices, synchronous playback may be allowed for several channels.

Steps

1. Go to **Playback** → .
2. Select channel(s) in the list at the left side.

Note

Group playback: Select a group in the list, and channels in the group can be played back.

3. Select a date in the calendar.

Note

The blue triangle at the calendar date corner indicates there are available videos.

4. **Optional:** Perform more operations.

Capture Click  to capture pictures during playback.

Digital Zoom Click  to zoom in a certain part of the video image.



Click to add a tag to the channel. After adding, you can go to → **Backup** → **By Tag** to search videos by tag.



Click to lock the video. After a video is locked, it will not be overwritten.

After locking, you can go to → **Backup** → **By Tag** to search videos by lock.

Dual-VCA

Select → **Dual-VCA** to search videos that can trigger the corresponding event rule. Refer to the event configuration steps for details of each event type.



Note

To use this function, go to **Configuration** → **Device Access** → **Device Configuration** → **Device Parameter** → **Display Info. on Screen** to turn on **Enable Dual-VCA** via web browser, and go to **System** → **Storage Management** → **Advanced Settings** to turn on **Save Camera VCA Data** via local GUI interface.

Show VCA Info

You can select → **Show VCA Info** to display rule frames.

Disable Privacy Protection

If privacy protection is enabled, the image may contain mosaics. You can select → **Display Privacy Protection** to display the original video (without mosaics) if the storage permission of privacy protection is enabled as well. Refer to [**Configure Privacy Protection**](#) for details about privacy protection function.

12.3 Event Playback

When you select the event playback mode, the system will analyze and mark videos that contain the motion detection, line crossing detection, or intrusion detection information

Before You Start

- Ensure the camera has enabled **Dual-VCA**. You can enable it via the camera web browser interface in **Configuration** → **Video/Audio** → **Display Info. on Stream**.
- Ensure your video recorder has enabled **Save Camera VCA Data** in **Storage management** → **Advanced Settings**.

Steps

1. Select **Playback** → .
2. Select a date in the calendar.



Note

The blue triangle at the calendar date corner indicates there are available videos.

3. Click  → **Dual-VCA** at the lower-right corner of playback image to select a event type. Refer to the event configuration steps for details of each event type.
4. Click **Search**.
Videos meet the detection rule requirement will be marked in red.
5. Click  to set normal video and smart video (the video that contains smart data) playback strategy.



Note

If **Dual-VCA** is not used, red segments in progress bar means the smart videos are generated by the original event.

12.4 Slice Playback

Divide the video into slices and play them back.

Steps

1. Go to **Playback** → .
2. Select a camera from the camera list.
3. Select a date on the calendar.
4. Click **Search**.
The retrieved video will be divided into one-hour slices for playback.
5. **Optional:** Select an one-hour slice and click  to divide it into one-minute slices for playback.

12.5 Sub-Period Playback

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

Steps

1. Go to **Playback** → .
2. Select a camera.
3. Set the start time and end time.
4. Click **Search**.

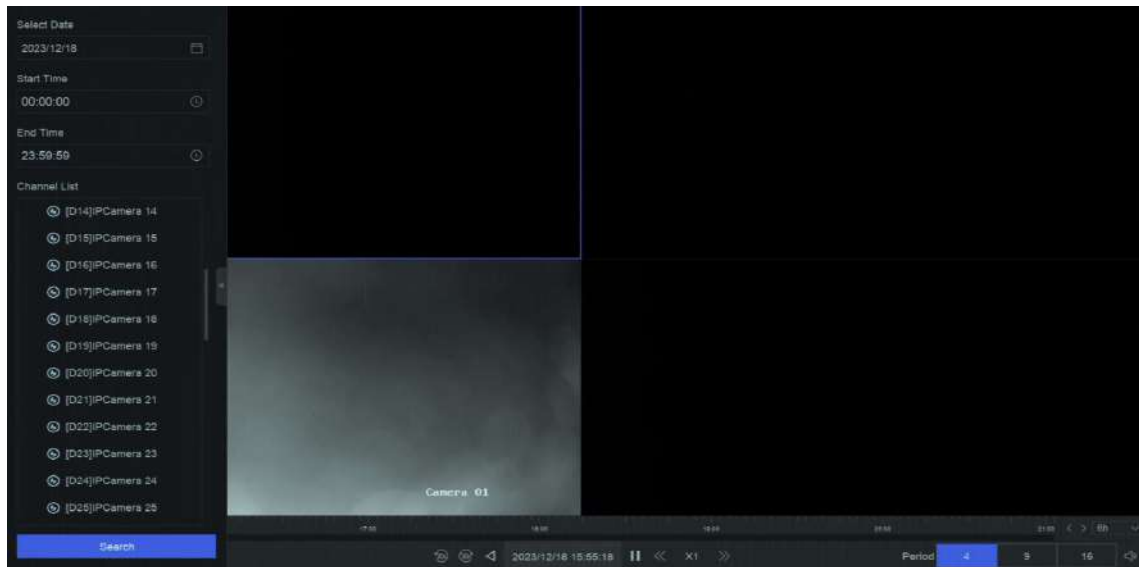


Figure 12-2 Sub-Period Playback

5. Select the period at the lower-right corner, e.g., 4.



Note

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.

Chapter 13 Event Center

13.1 Event Settings

13.1.1 Basic/Generic Event

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Basic Event / Generic Event** .
2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-1 Normal Event

Event Name	Event Description	Rule Configuration	
Motion Detection	Motion detection detects the moving objects in the monitored area.	Use the tool bar at the top of image to draw the detection area. • AI by NVR: The motion detection event will be analyzed by NVR. The device can analyze videos that contain human and vehicle. Only the target of selected type (human or vehicle) will trigger alarms, which can reduce false alarms that are caused by other objects. • AI by Camera: The motion detection event will be analyzed by camera. • Detection Target: Human and Vehicle are selectable, apart from false alarms, only the	Sensitivity allows you to calibrate how easily movement could trigger the alarm. A higher value results in the more readily to triggers motion detection.

Event Name	Event Description	Rule Configuration	
		selected target(s) can triggered alarms.	
Video Tampering Detection	Video tampering detection triggered an alarm when the camera lens is covered and takes alarm response action(s).	Use the tool bar at the top of image to draw the detection area.	
Video Loss Detection	Video loss detection detects video loss of a channel and takes alarm response action(s).	-	
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	-	
Defocus Detection	Image blur caused by lens defocus can be detected.	-	
Sudden Scene Change Detection	Scene change detection detects the change of the video security environment affected by external factors, such as the intentional rotation of the camera.	-	

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-2 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.2 Perimeter Protection

Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

Configure Line Crossing Detection

Line crossing detection detects people, vehicles, and objects crossing a set virtual line. The detection direction can be set as bidirectional, from left to right or from right to left.

Steps



Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center →  → Event Configuration → Perimeter Protection**.

2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.

Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Line Crossing**.
6. Turn on **Enable**.

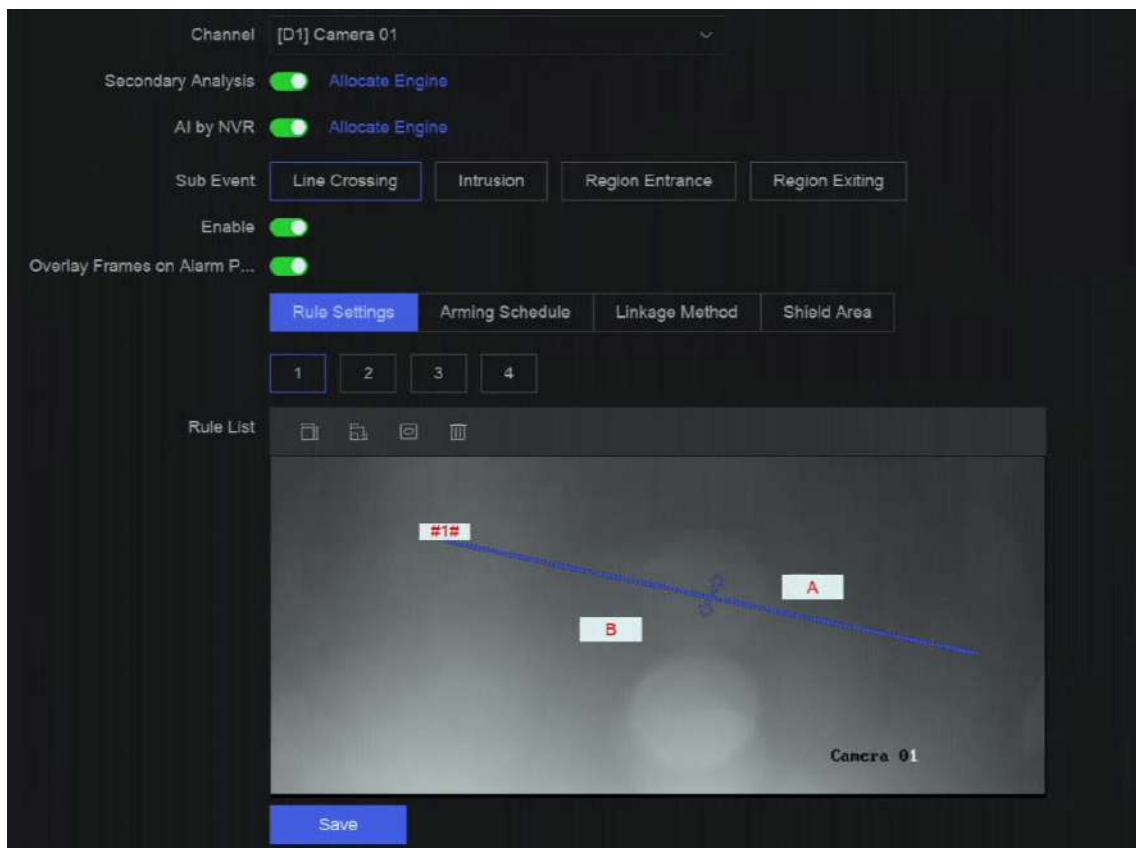


Figure 13-1 Line Crossing Detection

7. Click **Rule Settings** to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image twice respectively to draw the start point and end point of the detection line.
- 3) Set **Direction**, **Sensitivity**, **Detection Target**, and **Target Confidence**.

A<->B

Only the arrow on the B side shows. When an object goes across the configured line with both directions 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.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

Target Confidence

It is used to indicate the level of certainty or reliability in detecting line crossing events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

- 4) **Optional:** Click  /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
- 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-3 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.

Linkage Method	Description
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Intrusion Detection

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

Steps



Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.



Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Intrusion**.
6. Turn on **Enable**.

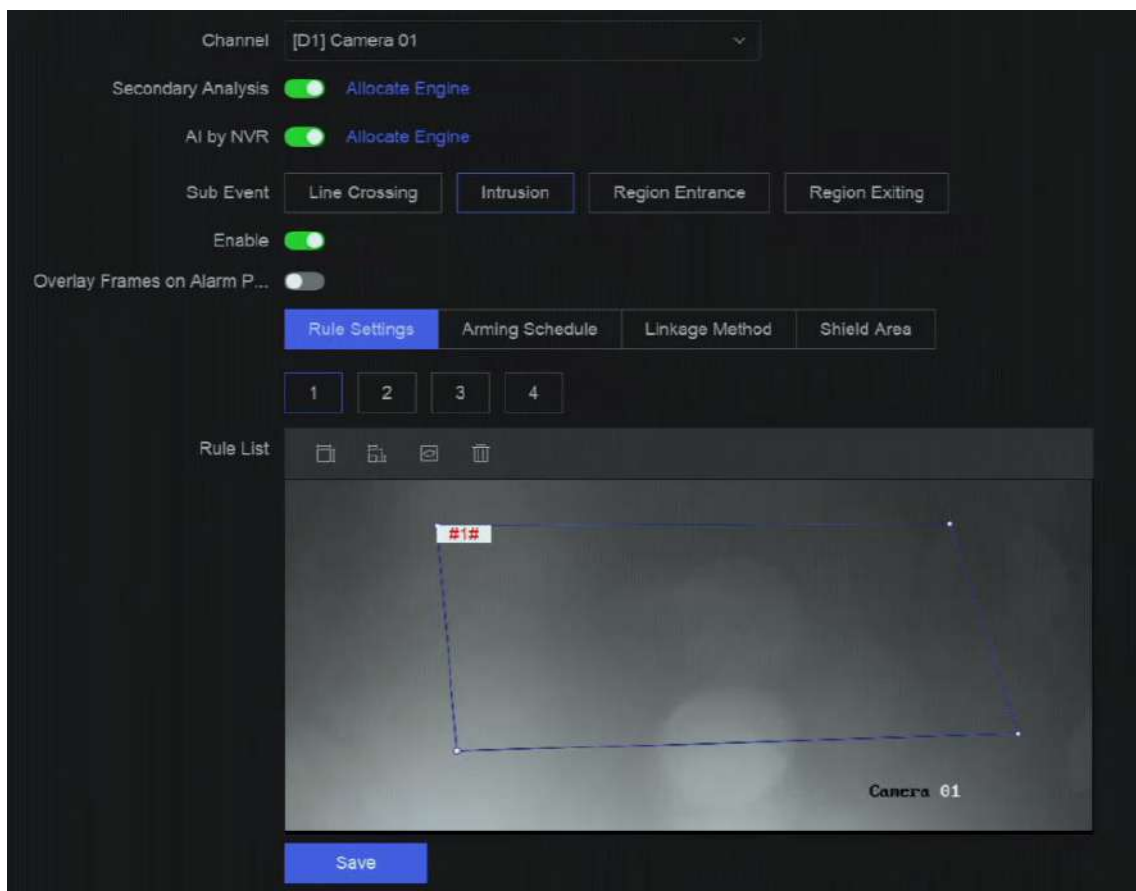


Figure 13-2 Intrusion Detection

7. Click **Rule Settings** to detection rules.
 - 1) Select a rule number. For example, select **1**.

- 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral or decagonal area.
- 3) Set **Time Threshold**, **Sensitivity**, **Detection Target**, and **Target Confidence**.

Time Threshold

The time an object loiter in the region. When the duration of the object in the defined detection area exceeds the threshold, the device will trigger an alarm.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

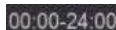
Target Confidence

It is used to indicate the level of certainty or reliability in detecting intrusion events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

- 4) **Optional:** Click  /  to draw **Max. Size** or **Min. Size**. Only targets that meet the size requirement can trigger alarms.
 - 5) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.
8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-4 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Optional: Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Entrance Detection

Region entrance detection detects objects that enter a predefined virtual region.

Steps

Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
2. Select a camera.
3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.

Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Region Entrance**.

6. Turn on **Enable**.

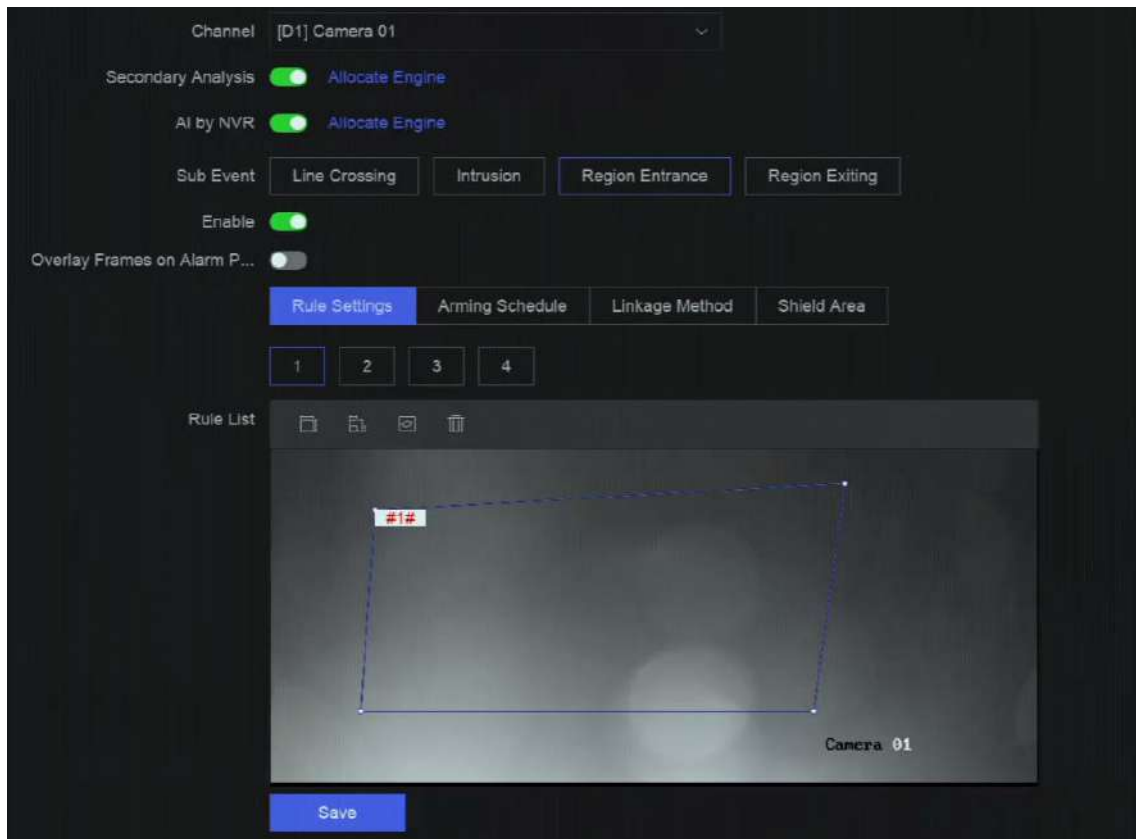


Figure 13-3 Region Entrance Detection

7. Click **Rule Settings** to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral or decagonal area.
- 3) Set **Sensitivity**, **Detection Target**, and **Target Confidence**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

Target Confidence

It is used to indicate the level of certainty or reliability in detecting region entrance events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-5 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

Configure Region Exiting Detection

Region exiting detection detects objects that exit from a predefined virtual region.

Steps



Note

A part of the following steps are only available for certain NVR or camera models.

1. Go to **Event Center** →  → **Event Configuration** → **Perimeter Protection**.
 2. Select a camera.
 3. **Optional:** Turn on **Secondary Analysis**. The corresponding device engine will analyze this event for a second time to reduce false alarms.
-



Note

At least one device engine should run **Secondary Analysis for Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Secondary Analysis for Perimeter Protection** algorithm.

4. **Optional:** Turn on **AI by NVR**. The corresponding device engine will analyze the video, and cameras only transmit video stream.
-



Note

At least one device engine should run **Perimeter Protection** algorithm. You can click **Allocate Engine** at the right side to quickly allocate engine, or go to **System** → **Smart Settings** → **Algorithm Configuration** → **Algorithm Management** to enable **Perimeter Protection** algorithm.

5. Select **Region Exiting**.
6. Turn on **Enable**.

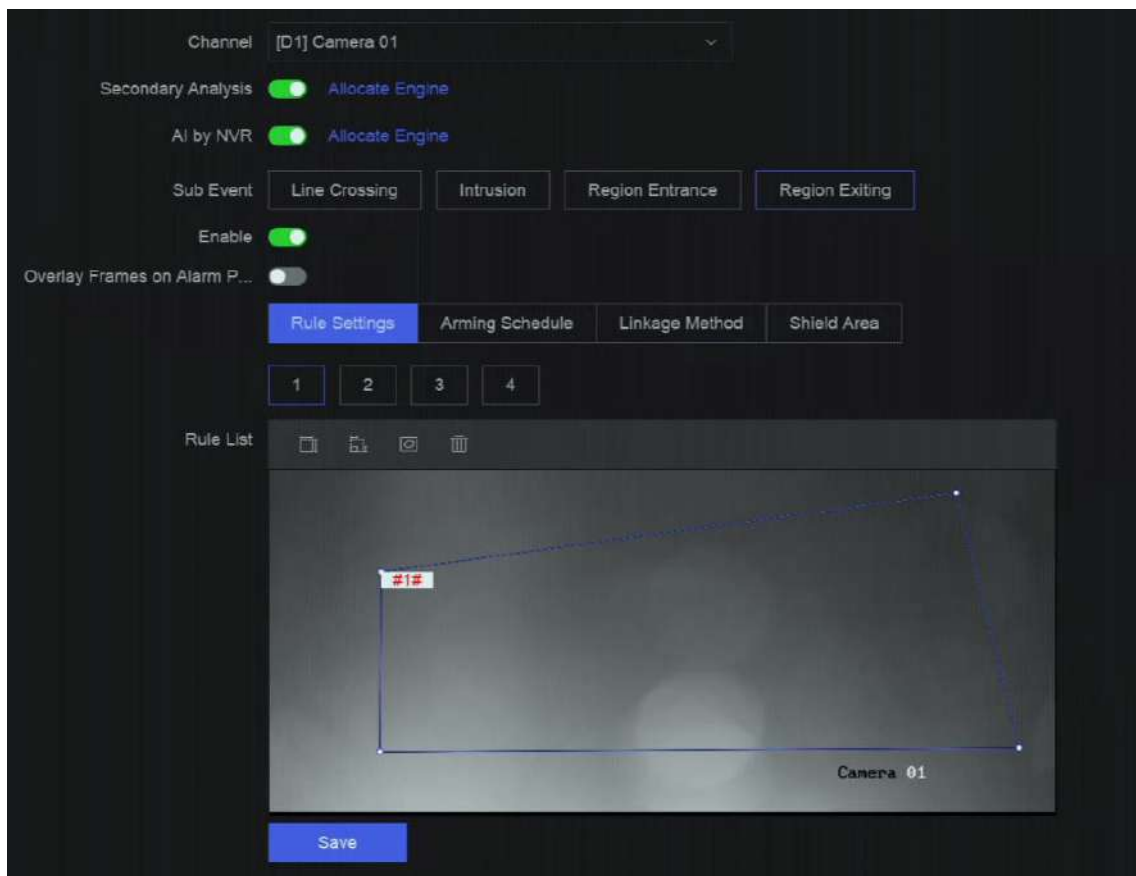


Figure 13-4 Region Exiting Detection

7. Click Rule Settings to detection rules.

- 1) Select a rule number. For example, select **1**.
- 2) Click , and click on the image 4 times respectively to draw each point of a quadrilateral or decagonal area.
- 3) Set **Sensitivity**, **Detection Target**, and **Target Confidence**.

Sensitivity

The higher the value is, the more easily the detection alarm can be triggered.

Detection Target

Select **Detection Target** as **Human** or **Vehicle** to discard alarms which are not triggered by human or vehicle. **Detection Target** is only available for certain models.

Target Confidence

It is used to indicate the level of certainty or reliability in detecting region exiting events. Setting higher confidence levels ensures that only highly reliable detections trigger events, reducing false alarms.

- 4) **Optional:** Repeat above steps to draw more rules. Up to 4 rules are supports.

8. Click Arming Schedule to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-6 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. **Optional:** Set **Shield Area** when **AI by NVR** is enabled. After a shield area is set, the device will not analyze target behavior in the area, so that the perimeter protection events will not be triggered within the area.

11. Click **Save**.

What to do next

You can go to **Live View** and click **Target** to view real-time alarms.

13.1.3 Abnormal Behavior Event

Before You Start

Ensure the camera supports this function.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Abnormal Behavior Event** .
2. Select a camera
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-7 Abnormal Behavior Events

Event Name	Event Description	Rule Configuration
Loitering Detection	Loitering detection is used to detect whether a target stays within a specified area longer than the set time and trigger alarm for linked actions.	a. Select a rule number. b. Use the tool bar at the top of image to draw the detection line. c. Set Time Threshold and Sensitivity. Time Threshold The time of the target staying in the region. If the value is 10, an alarm is triggered after the target has stayed in the region for 10 s. Range: [1-10]. Sensitivity Similarity of the background image to the object. The higher the value is, more easily the detection alarm will be triggered. d. Optional: Repeat the above steps to set another one.
Parking Detection	Parking detection is used to detect parking violation in the area, applicable in expressway and one-way street.	
Unattended Baggage Detection	Unattended baggage detection detects the objects left over in a predefined region such as the baggage, purses, dangerous materials, etc., and a series of actions can be taken when the alarm is triggered.	
Object Removal Detection	The object removal detection function detects the objects removed from a predefined region, such as the exhibits on display, and a series of actions can be taken when the alarm is triggered.	
Fast Moving Detection	Fast moving detection is used to detect suspicious running and chasing, over-speed, and fast moving. It will trigger alarm when an object is moving fast and send notification to arming host so	

Event Name	Event Description	Rule Configuration
	that necessary actions can be taken in advance.	
People Gathering Detection	People gathering detection is used to detect whether the density of human bodies within a specified area exceeds the set value and trigger alarm for linked actions.	- Select a rule number. - Use the tool bar at the top of image to draw the detection line. - Set Percentage. Percentage is the density of human bodies within the area. If it exceeds the threshold value, the device will trigger alarm. - Optional: Repeat the above steps to set another one.

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-8 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.

Linkage Method	Description
	 Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.4 Target Event

Before You Start

Ensure the connected camera supports this function, or the device engine has enabled **Target Recognition** or **Video Structuralization** algorithm in **Event Center → Event Configuration → Smart Settings → Algorithm Configuration → Algorithm Management**.

Steps

1. Go to **Event Center →  → Event Configuration → Target Event**.
2. Select a camera.
3. Select an event.
4. Turn on **Enable**.
5. Set event rules.

Event Name	Event Description	Rule Configuration
Face Capture	The face capture detects and captures faces appearing in the scene. Linkage actions can be triggered when a human face is detected.	-
Face Picture Comparison	The function compares detected face pictures with specified list library. Trigger alarm when comparison succeeded.	• Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). • Supports configuring prompts for failed and succeeded comparisons.

Event Name	Event Description	Rule Configuration
Stranger Detection	Faces not in the list library appearing in the video will be identified as strangers.	- Supports configuring target grading. Face picture comparison begins when the grade of target meets the comparison requirements (the pupil distance are bigger than the configured threshold, and the tilt angle and pan angle are smaller than the configured thresholds). - Supports configuring the prompt for detecting strangers.
Multi-Target-Type Detection	Multi-target-type detection enables the device to detect the faces, human bodies and vehicles simultaneously in a scene.	-

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-9 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.

Linkage Method	Description
	 Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.5 Thermal Camera Detection

The NVR supports the event detection modes of the thermal network cameras: fire and smoke detection, temperature detection, temperature difference detection, etc.

Before You Start

Add the thermal network camera to your device and make sure the camera is activated.

Steps

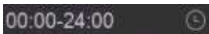
1. Go to **Event Center** →  → **Event Configuration** → **Thermal Event**.
2. Select a camera.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-10 Thermal Events

Event Name	Event Description
Fire Detection	An alarm would be triggered when fire is detected in the arming area.
Temperature Detection	An alarm would be triggered when the temperature exceeds the threshold value.
Perimeter Protection	Perimeter protection events include line crossing detection, intrusion detection, region entrance detection, and region exiting detection.

6. Click **Arming Schedule** to select an arming schedule type.

Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-11 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.1.6 Alarm Input Event

Set the handling action of an external sensor alarm.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Alarm Input Event**.
2. Select an alarm input name.

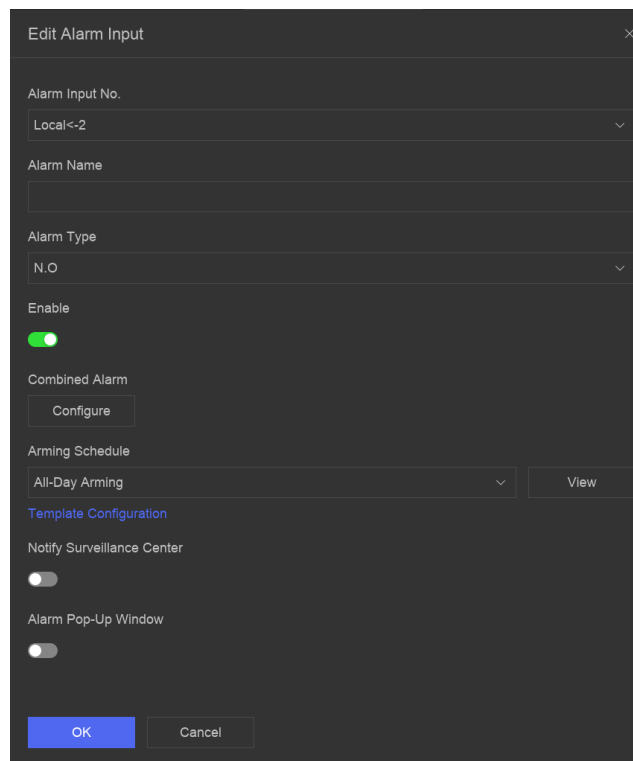


Figure 13-5 Configure Alarm Input



Note

For example, **Local<-1** represents the alarm input number at the device rear panel is 1.

3. Edit **Alarm Name**.

4. Set **Alarm Type**.

N.O

When contacts are in natural and off-power state, if two contacts are off, then they can be called normal open.

N.C

When contacts are in natural and off-power state, if two contacts are conducted, then they can be called normal closed.

5. Turn on **Enable**.

6. **Optional:** If you select **Local<-1** in Step 2, select the processing method.

- Select **Process Alarm Input**, and then you can set the corresponding arming schedule, linkage methods, etc.



Note

The operations below are all available when you select this processing method.

- Select **Quick Disarming**, and then linkage methods of all events will be disabled.

7. Click **Configure** to configure combined alarm.

- 1) Select a channel.
- 2) Select combined alarm events such as motion detection and video tampering detection.
- 3) Click **OK**.

The combined alarm will be triggered when it receives alarms from both alarm input and events.

8. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00** to set specified time schedule.

9. Click **Linkage Method** to set linkage methods.

Table 13-12 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos. Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

10. Click **Save**.

13.1.7 Audio Analysis Event

Steps

1. Go to **Event Center** → → **Event Configuration** → **Audio Analysis** .

2. Select a channel.
3. Select an event type.
4. Turn on **Enable**.
5. Click **Rule Settings** to set the rule.

Table 13-13 Audio Analysis Event

Event Name	Event Description	Rule Configuration
Audio Exception Detection	Audio exception detection detects abnormal sounds in the scene, such as a sudden increase/decrease in sound intensity.	Sudden Increase of Sound Intensity Detection Detects a steep sound increase in the scene. Sudden Decrease of Sound Intensity Detection Detects a steep sound drop in the scene. Sensitivity The higher the value is, the easier the detection alarm can be triggered. Sound Intensity Threshold It can filter the sound in the environment. The louder the environment sound is, the higher the value should be. Adjust it according to the environment.

6. Click **Arming Schedule** to select an arming schedule type.



Note

If you set **Arming Schedule** as **Custom**, you can drag the cursor on time bar to set customized arming schedule, or move the cursor on time bar and click **00:00-24:00**  to set specified time schedule.

7. Click **Linkage Method** to set linkage methods.

Table 13-14 Linkage Method Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Alarm Pop-Up Window	When an alarm is triggered, the local monitor displays the alarm pop-up window.
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.

Linkage Method	Description
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.
Record	When an alarm is detected, the selected channel would record videos.  Note Video recording schedule shall be enabled for the channel, otherwise this linkage would be invalid. You can go to System → Storage Management → Storage Schedule → Video Recording to configure video recording schedule.

8. Click **Save**.

13.2 Linkage Configuration

Configure parameters for event linkages.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Linkage Configuration** or **System** → **Event Configuration** →  → **Event Configuration** → **Linkage Configuration**.
2. Click **Email** to configure email parameters.

Table 13-15 Email Linkage

Item	Description
Server Authentication	Enable it if the SMTP server requires user authentication and enter the user name and password accordingly.
SMTP Server	The IP address of SMTP Server or host name (e.g., smtp.263xmail.com).
SMTP Port	The SMTP port. The default TCP/IP port used for SMTP is 25.
Enable SSL/TLS	Enable SSL/TLS if the SMTP server has the requirement.
Sender	The sender name.
Sender's Address	The sender's address.
Select Receivers	Select the receiver. Up to 3 receivers can be configured.
Attached Image	Send email with attached alarm images.

Item	Description
Enable 3 Attached Images for Perimeter Protection	When a perimeter protection event is triggered, the device would send an email with 3 attached alarm images.
Interval	The time interval for capturing the attached images.

Note

If you are using an Outlook email account, please set **Email Type** as **Outlook**, and click **Help** at the right side to read the configuration instructions, then follow the steps on the interface to complete the configuration.

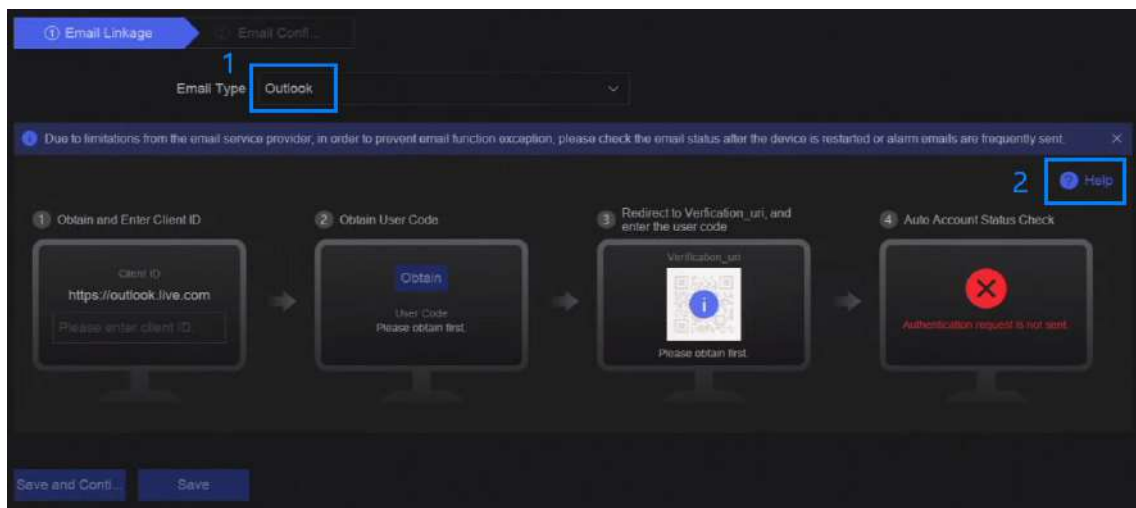


Figure 13-6 Outlook Email Configuration

3. Click **Audio Management** to manage audio files for alarm linkage.

Note

There are 3 default audio files in the list which cannot be deleted. You can import audio files from USB flash drive. The files shall in AAC or MP3 format, and each file size should be within 1 MB.

4. If you have connected IP speakers, click **IP Speaker** to import audio files in to the selected IP speaker(s) for alarm linkage.

Note

- This linkage action is only available for few event types.
- The uploaded audio file should be in MP3, WAV, or ACC format, and the file size should be less than 1 MB.

5. Click **Alarm Output** to set alarm output parameters.



Note

- Click the name of each alarm output to edit it.
 - The alarm output No. is the same as the one at the device rear panel. For example, **Local->1** means the alarm out No. 1 at the device rear panel.
-

Delay

The alarm signal duration.

Alarm Status

Click **Trigger** to switch the status.

6. If you have connected audio and light cameras, click **Camera Audio and Light Configuration** to configure the camera flashing light and camera speaker parameters for alarm linkage.
-



Note

This linkage action is only available for few event types.

7. If you have connected security control panels, click **Security Control Panel** to configure parameters including IP address and port number.
-

13.3 Disarming Configuration

After a disarming template is configured, you can use the template to disarm channels in a batch. The channels that have enabled **Allow Disarming** would not trigger the alarm linkage items according the disarming template.

Steps

1. Go to **Event Center** →  → **Event Configuration** → **Linkage Configuration** or **System** → **Event Configuration** →  → **Event Configuration** → **Linkage Configuration**.

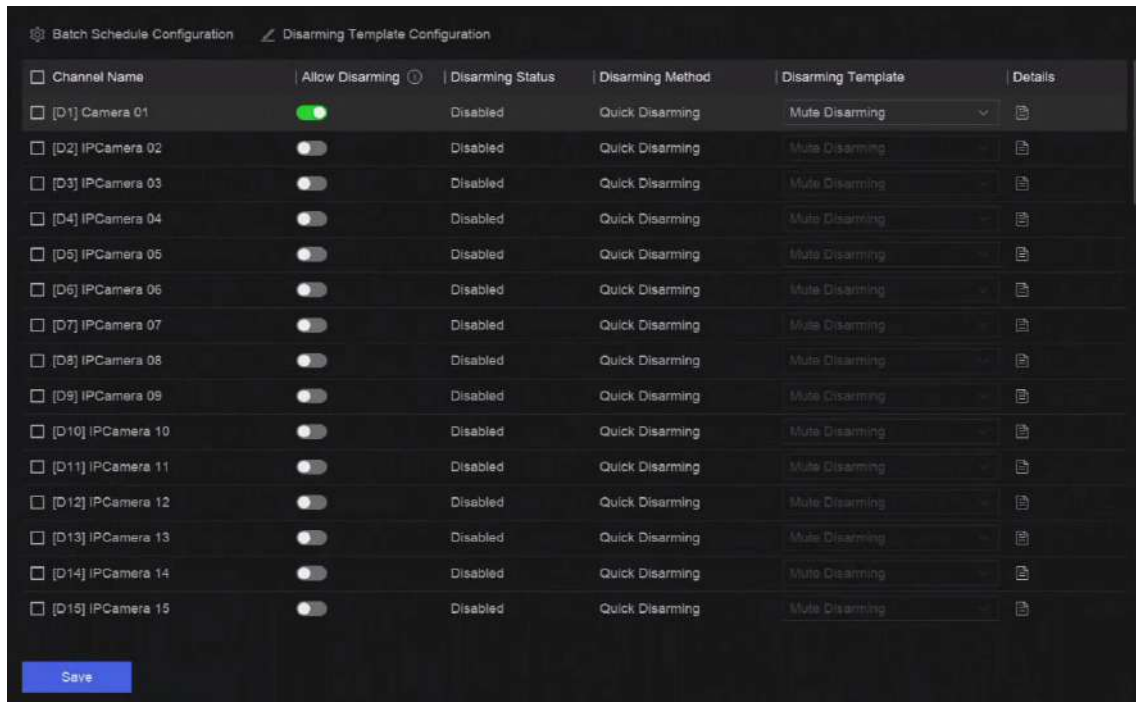


Figure 13-7 Disarming Configuration

2. Select channel(s) that are allowed for disarming.
3. Click **Batch Schedule Configuration**.
4. Turn on **Enable**.
5. Select **Disarming Template**. Only two types are available



Note

Currently, only two template types are available and each template parameters cannot configured.

6. Click **OK**.

13.4 Batch Configuration

The listed events and the corresponding linkage action of **Notify Surveillance Center** can be enabled or disabled in batches through **Event Center** → → **Event Configuration** → **Batch Configuration** or **System** → **Event Configuration** → → **Event Configuration** → **Batch Configuration**. After an event is enabled, please click **Go to Event Configuration** to set rules.

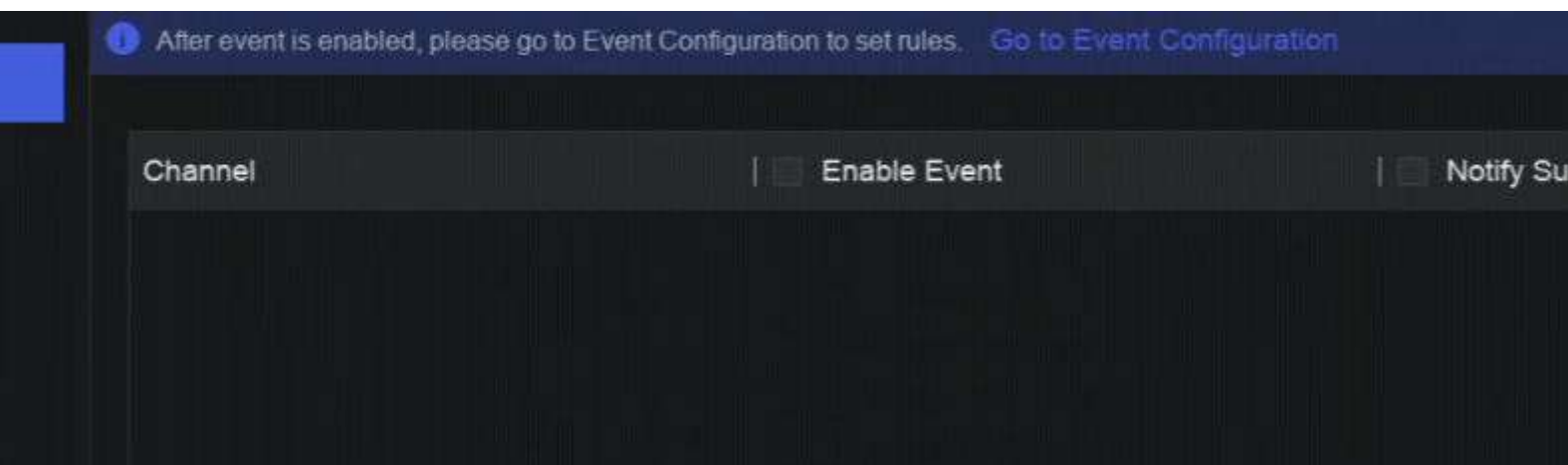


Figure 13-8 Batch Configuration

13.5 Event Search

You can search event files like videos and pictures according to the searching condition.

Steps

1. Go to **Event Center** → .

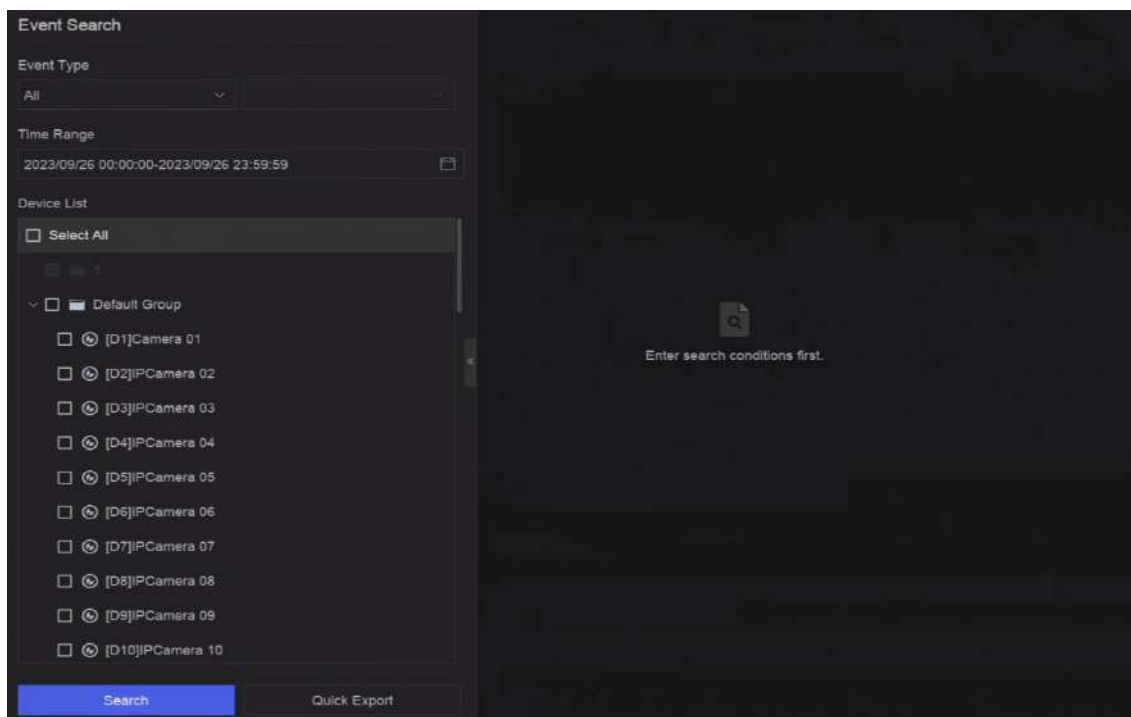


Figure 13-9 Event Search

2. Specify detailed conditions, including event type, time, channel, etc.
3. Click **Search**.

The device will display the searching results of the selected channel(s).

What to do next

Select the items from the result list and export them for backup.

13.6 View Alarms

You can view real-time alarm videos and pictures, and play them back.

Steps

1. Go to **Event Center** → .
2. Click **Real-Time Alarm**.
3. Select the alarm from the list.
If there are too many alarms, click **Filter** to search and find the alarm.
4. Click **Playback**, and the alarm recording video would be played back.
5. View the alarm picture(s) at the right side. The number of available pictures would be listed.

Chapter 14 Search and Backup

You can search files according to different searching conditions, including file type, event type, time, tag, etc. The searching results can be exported to another device, such as a USB flash drive.

Before You Start

Ensure HDD is correctly installed and recording parameters are properly configured.

Steps

1. Go to **Backup**.

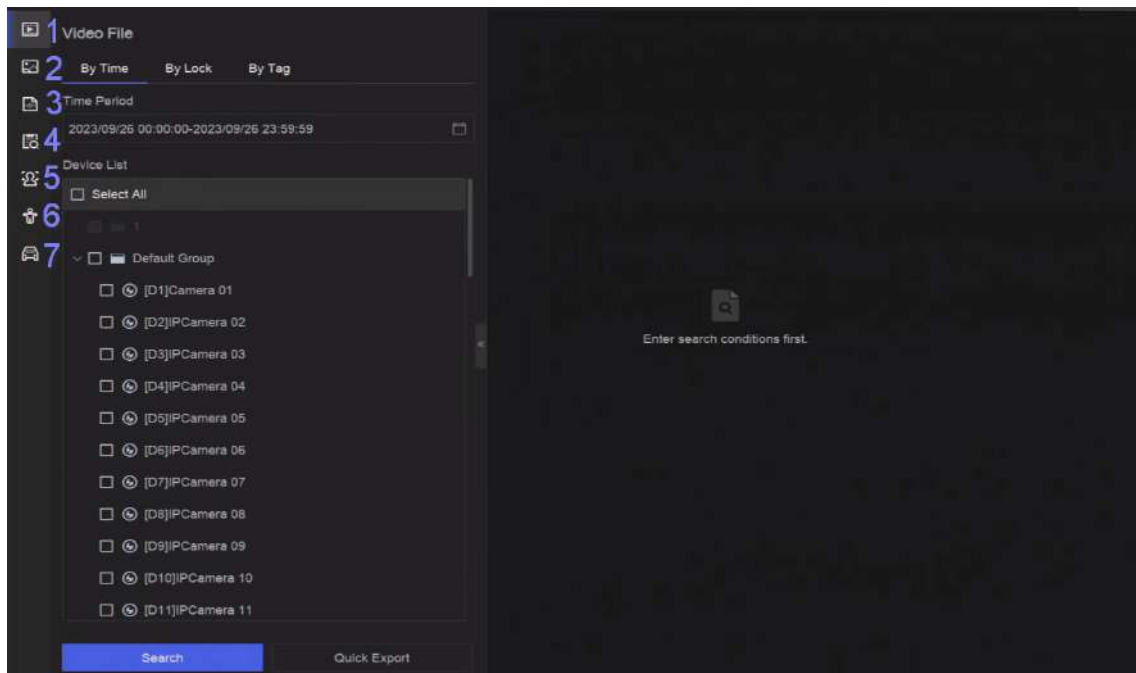


Figure 14-1 Search and Backup

2. Choose a searching method from at the left side as your desire, 7 types are supported.



Note

The searching conditions would vary according to the selected searching method.

3. Set the searching conditions.
4. Click **Search**.

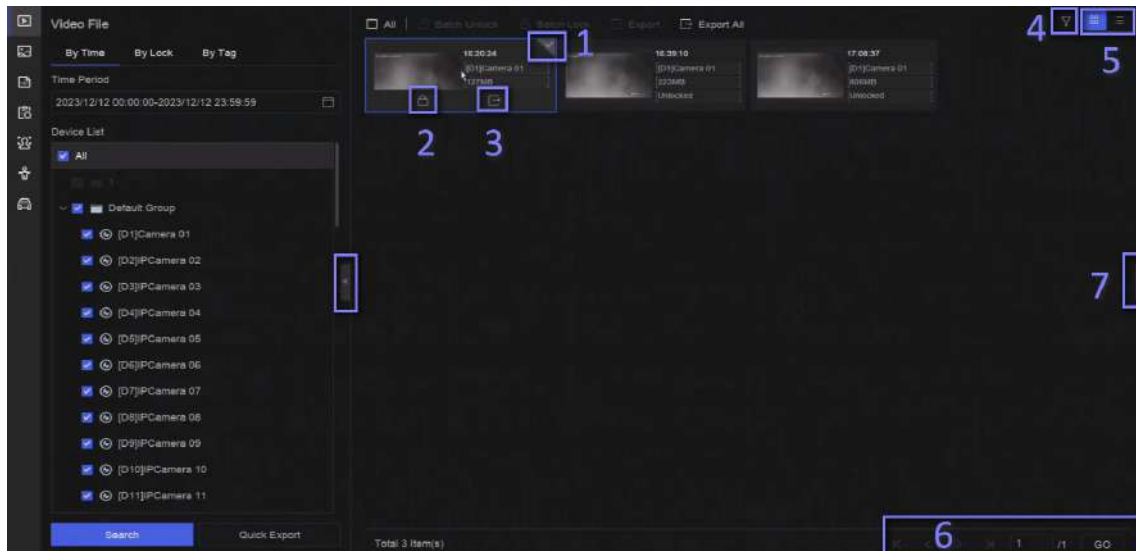


Figure 14-2 Searching Result

5. Optional: Perform the following operations.

- 1 Click to select a file.
 - 2 Click to lock a file. After a file is locked, it will not be overwritten.
 - 3 Click to export a file.
 - 4 Use the tool bar at the top to filter results by channel.
 - 5 Use the tool bar at the top to switch display effect.
 - 6 Go to different result pages.
 - 7 Expand or collapse the interface. After selecting a video from the result list, you would be able to quickly play it back.
- 6.** Insert a USB flash drive to the device for backup.
- 7.** Export files to the USB flash drive.
- Select file(s) in the result list and click **Export**.
 - Click **Export All** to export all the files.

Chapter 15 AcuSearch

AcuSearch function firstly extracts pictures of human face or body from a video scene during live view or playback, then compares the extracted picture with recorded videos, and eventually finds out videos that contains the target.

Before You Start

Ensure your device or camera supports this function.

Steps

1. Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** to enable AcuSearch algorithm.
 - **AI by Camera:** The camera will perform the AcuSearch analysis.
 - **AI by NVR:** The device will perform the AcuSearch analysis, and engine resource is required for analysis.
2. Go to Live View or Playback, and click  at the lower-left corner during video playing.



Note

- If targets are hard to find during playback, it is recommended to use **Smart Search** () to find scenes that contain targets.
- Human face and body would be framed with different colors.
- After clicking  , you can also drag the cursor on the image to manually frame a target, or manually adjust the frame area.

-
3. Click  of the selected target.



Figure 15-1 AcuSearch

If compared videos are found, the device will redirect to AcuSearch interface.

4. View searching results.

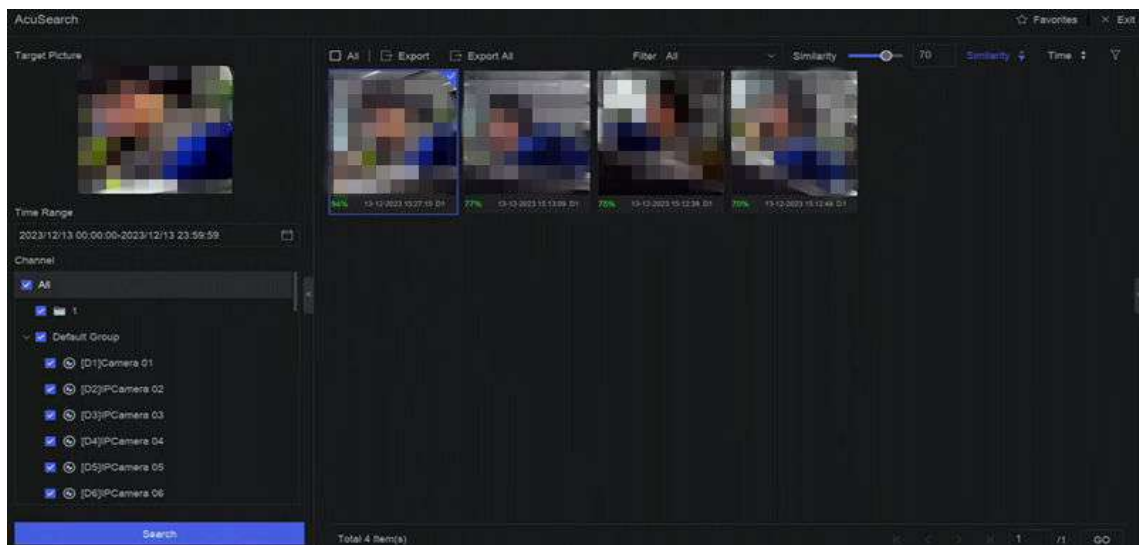


Figure 15-2 AcuSearch Result

5. **Optional:** If the results are not desired, you can adjust parameters like **Time Range**, **Channel**, or **Similarity** to search again.
6. **Optional:** Select an item from the result list, and its corresponding video would be played back at the right side and be marked with red color. You can click the icons at the tool bar to perform functions.

Chapter 16 Smart Settings

16.1 Algorithm Management

Algorithms are used for device engines to analyze different smart functions. Smart function would be usable after allocating the corresponding algorithm to an engine.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Algorithm Management** or **Event Center → Event Configuration → Smart Settings → Algorithm Management**. The available algorithms would be listed, and you can click the required algorithm to link engine(s).

For certain models that support AcuSearch algorithm, you can choose the camera (**AI by Camera**) or NVR (**AI by NVR**) to run AcuSearch algorithm.

16.2 Engine Status

You can view the engine status, including running status, temperature and algorithm name.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Engine Status** or **Event Center → Event Configuration → Smart Settings → Engine Status**. If you need to switch the algorithm, refer to [Algorithm Management](#).

16.3 Task Plan Management

You can view the task status in task configuration. Smart analysis results are used for filtering the pictures when searching interested human body and vehicle pictures.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Task Plan Management** or **Event Center → Event Configuration → Smart Settings → Task Plan Management**. For **Non-Real-Time Target Comparison**, you can view the progress of each day. Task status mainly includes 3 conditions: **Disabled**, **Waiting**, and **Enabled**.

Disabled

No analysis task is enabled on the camera.

Waiting

The analysis task of the camera is enabled. Device is waiting to analyze data.

Enabled

The analysis task of the camera is enabled and device is analyzing data of the camera.

16.4 List library Management

List library is mainly used for target picture storage and target comparison. **Strangers** library is used to store pictures for strangers, and it cannot be deleted.

16.4.1 Add a List Library

Steps

1. Go to **System** → **Event Configuration** → **Event Configuration** → **Data Archive** → **List Library** or **Event Center** → **Event Configuration** → **Data Archive** → **List Library**.
2. Click **Add**.
3. Enter the library name.
4. Click **Confirm**.



Note

- After a list library, you can move the cursor on the library to edit or delete it.
 - You can click **Delete in Batch** to delete selected libraries, or clear all pictures in the selected libraries.
-

16.4.2 Upload Face Pictures to the Library

Target picture comparison is based on target pictures in the library. You can upload a single target picture or import multiple target pictures to the library.

Before You Start

- Ensure the picture format is JPEG or JPG.
- Import all pictures to a backup device in advance.

Steps

1. Double click a list library.
2. **Optional:** Click **Custom Tag** to add tags to pictures. The tag can be edit as your desire, for example, personal information, organization, position, etc.
3. Click **Add** or **Import**.
4. Import picture(s).
 - **Add:** Click  to upload a picture at a time. If the picture has multiple targets, you have to pick one from them.
 - **Import:** Multiple pictures can be imported at a time. The device will use the file name as its picture name and leave other attributes empty, or import picture files by specified rules. If a picture has multiple targets in the image, the device will choose the target at the center by default.
5. **Optional:** Perform the following operations.

Delete Pictures from the Library

- Select a picture and delete it.
- Select pictures and click **Delete in Batch** to delete the select ones.

Search Pictures in the Library

Click  at the tool bar to search pictures.

Copy Pictures to Another Library

Select pictures and click **Copy to** to copy the uploaded pictures of the current library to another library.

Edit Pictures

Click the picture name, and edit its attributes.

Export Pictures

Select pictures, and click **Export** to export them to a USB flash drive.

16.5 Self-Learning Settings

Self-learning technology optimizes algorithm accuracy and requires minimum manual intervention from users. When self-learning function is enabled, the device would automatically collect false alarm materials, and use the collected materials to constantly train and optimize the corresponding algorithm.

Go to **System → Event Configuration → Event Configuration → Smart Settings → Algorithm Management** or **Event Center → Event Configuration → Smart Settings → Algorithm Management** to enable **Self-Learning** algorithm.



Note

- Only certain models support this function.
 - Currently, self-learning function can only be adopted for perimeter protection events.
 - If your device only has one engine, **AI by NVR** has to be disabled and the camera should perform the analysis of detection targets. If your device only has two or more engines, you can enable **AI by NVR** and use one engine for the analysis of detection targets, then use another engine to run the self-learning algorithm.
-

16.5.1 Self-Learning Task Management

After self-learning algorithm is running, the self-learning task should be enabled as well.

Go to **System → Event Configuration → Event Configuration → Self-Learning → Task Management** or **Event Center → Event Configuration → Self-Learning → Task Management** to enable the task.

The available task would be listed, and you can view task status and progress bar. It would take a long time for the material collection.

When the task is completed, self-learning algorithm would be updated automatically. You can click **Auto Update Config** to set **Update Time**.



Note

- When the self-learning algorithm would be unavailable for perimeter protection events when the algorithm is updating.
 - **Force Training** is only used for the technical support.
-

16.5.2 Model Management

You can set the self-learning algorithm model version according to your requirement.

Go to **System → Event Configuration → Event Configuration → Self-Learning → Model Management** or **Event Center → Event Configuration → Self-Learning → Model Management** to set the model version.

Restore to Previous Version

Restore the model to the version before this one.

Restore to Default Version

Restore the model to the factory default version.

16.5.3 Smart Status

You can view the self-learning algorithm performance status of each channel in **System → Event Configuration → Event Configuration → Self-Learning → Smart Status** or **Event Center → Event Configuration → Self-Learning → Smart Status**.

Chapter 17 Application Center

17.1 Human and Vehicle Detection

The human and vehicle information will be displayed for the selected channel at real-time.

Human and vehicle detection should be configured in advance. Go to **Event Center** →  to configure.



Figure 17-1 Human and Vehicle Detection

Table 17-1 Human and Vehicle Detection Description

No.	Description
1	Right-click shortcut menu.
2	Human and vehicle detection settings. You can set the layout, comparison succeeded prompt, and resource channels.
3	Enter/exit full screen.

17.2 Person Check-In

After check-in tasks are added, you can view the live check-in information and search check-in results.

17.2.1 Add Check-In Task

Before starting person check-in, the corresponding task should be properly configured.

Before You Start

- A camera for person check-in is properly connected.
- Go to **System → Smart Settings → Algorithm Configuration → Algorithm Management** .
Allocate **Target Recognition** to at least one engine.
- The list library for check-in comparison is properly configured. Refer to [Add a List Library](#) for details.

Steps

1. Click **Person Check-In** .
2. Right click to display the menu at left side.
3. Click  .
4. Click **Add**.

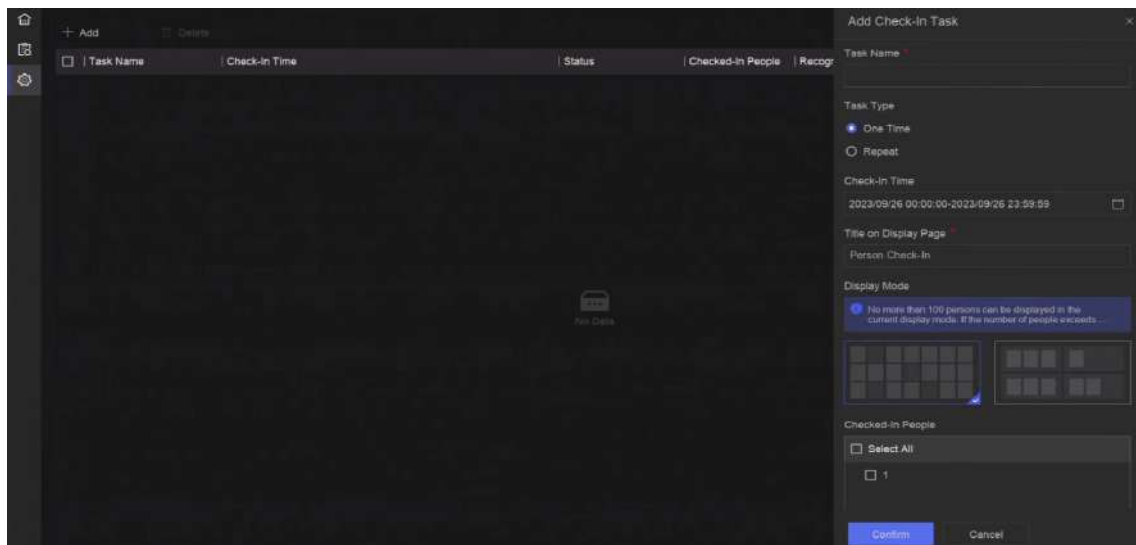


Figure 17-2 Add Check-In Task

5. Set **Task**.

One-Time

The task will be used for one time.

Repeat

The task will be used and repeated for several times.

6. Configure other parameters, including **Task Name**, **Check-In Time**, **Recognition Channel**, etc.
7. Click **Confirm**.

17.2.2 Search Check-In Records

After check-in tasks are configured, you can search the records by day or month.

Before You Start

Ensure check-in tasks are configured.

Steps

1. Go to **Person Check-In** .
2. Right click to display the menu at the left side.
3. Click  .

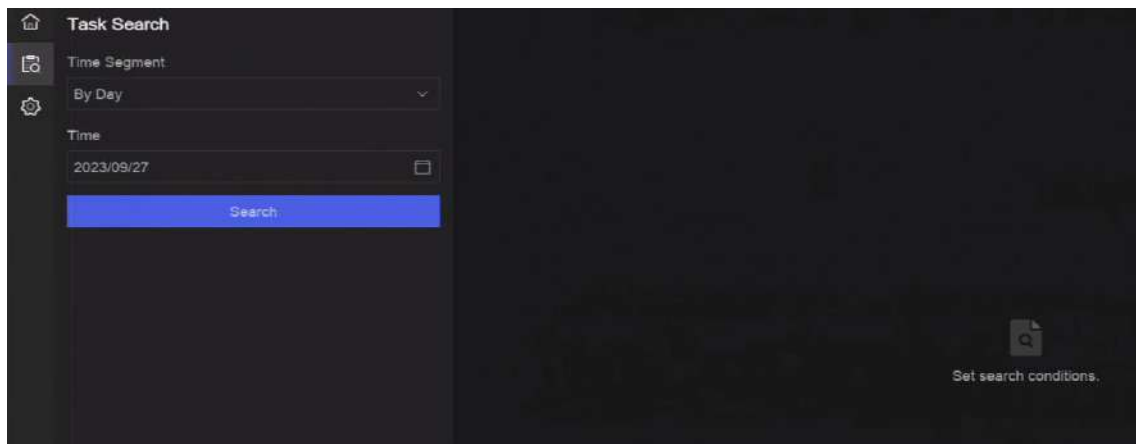


Figure 17-3 Search Check-In Records

4. Set time.
5. Click **Search**.

17.3 Statistic Report

You can view reports of people counting and heat map.

Table 17-2 Statistic Report Introduction

Function Name	Icon	Condition	Description
People Counting		The function must be supported by the connected IP camera. For example, a people counting	People counting calculates the number of people entering or leaving a certain configured area and creates daily/weekly/monthly/annual reports for analysis.

Function Name	Icon	Condition	Description
		camera is connected to your device. • Camera statistic data can be stored to the device HDD.	
Heat Map		• The function must be supported by the connected IP camera. • Camera statistic data can be stored to the device HDD.	Heat map is a graphical representation of data. The heat map function is used to analyze how many people visited and stayed in a specific area.

Chapter 18 System Parameter Settings

System parameters include device name, region, time, lock screen time, language, etc.

Go to **System** → **System Settings** → **System Configuration** to configure parameter.

Table 18-1 Parameter Description

Type	Parameter Name	Description
Basic Info	Lock Screen Time	The screen would be locked when the cursor is not moving for the specified time.
	Live View Permission on Lock Screen	After the screen is locked, the device would play the live image of cameras that have this permission.
Region & Time Configuration	Time Zone Lock	The admin password is required for this operation. After Time Zone is locked, the device time zone information cannot be remotely changed from other platforms or interfaces, such as the web interface via web browser. You can only lock or unlock Time Zone through local GUI interface.
	Time Sync Mode	• NTP Time Sync: You can select NTP Time Sync and configure NTP Server, NTP Server Port, NTP Client Port, and Interval. Interval is the time interval between two synchronizing actions within the NTP server. If the device is connected to a public network, you should use a NTP server that has a time synchronization function, such as the listed server addresses for selection. If the device is set in a customized network, NTP software can be used to establish a NTP server for time synchronization. • Manual Time Sync: Manually set the system time. • Hik-Connect Server Time Sync: The device will sync time with Hik-Connect instead of NTP server. • Guarding Vision Server Time Sync: The device will sync time with Guarding Vision instead of NTP server.
	DST	DST (daylight saving time) refers to the period of the year when clocks are moved one period ahead. In some areas worldwide, this has the effect of creating more sunlit hours in the evening during months when the weather is the warmest.

Type	Parameter Name	Description
		We advance our clocks ahead a certain period (depends on the DST bias you set) at the beginning of DST, and move them back the same period when we return to standard time (ST).
Menu Output	Auxiliary Port Auto-Switch	When two or more monitors are connected to rear panel, one of the them may become the auxiliary output that cannot enter main menu. Images at the auxiliary output windows will be automatically switched to next ones according to the interval.
Channel-Zero	-	Channel-zero, known as virtual channel, can show live images of all channels of the device, which saves bandwidth for transmission.
RS-232	Usage	Console After connecting it to PC with a convertor, PC can set the device parameters. Transparent Channel It is directly connected to a serial device. PC can remotely access the serial device through network.

Chapter 19 Hot Spare Device Backup

Video recorders can form an N+M hot spare system. The system consists of several working video recorders and at least one hot spare video recorder. When a working video recorder fails, the hot spare video recorder would switch into operation, which increases the reliability of the system. A bidirectional connection shown in the figure below is required to be built between hot spare video recorder(s) and working video recorders.



Figure 19-1 Build a Hot Spare System



Note

- Up to 32 working devices and 32 hot spare devices are allowed.
 - It is recommended to use all devices in a same model for compatibility. Contact your dealer for details of models that support the hot spare function.
 - Only certain models support this function.
-

19.1 Set Working Device

Steps

1. Go to **System** → **System Management** → **N+M Hot Spare** .
2. Set **Working Mode** as **Normal Mode**.
3. Turn on **Enable**.
4. Click **Save**.
5. **Optional:** View **Hot Spare Device IP Address** and **Hot Spare Device Working Status**.

19.2 Set Hot Spare Device

Hot spare device will take over working device tasks when working device fails.

Steps

1. Go to **System** → **System Management** → **N+M Hot Spare** .
2. Set **Working Mode** as **Hot Spare Mode**.
3. Click **Save**. Your device will restart automatically.



Note

- The camera connection will be disabled when the device works in hot spare mode.
- It is highly recommended to restore the device defaults after switching the work mode of hot spare devices to normal mode to ensure the normal operation afterwards.

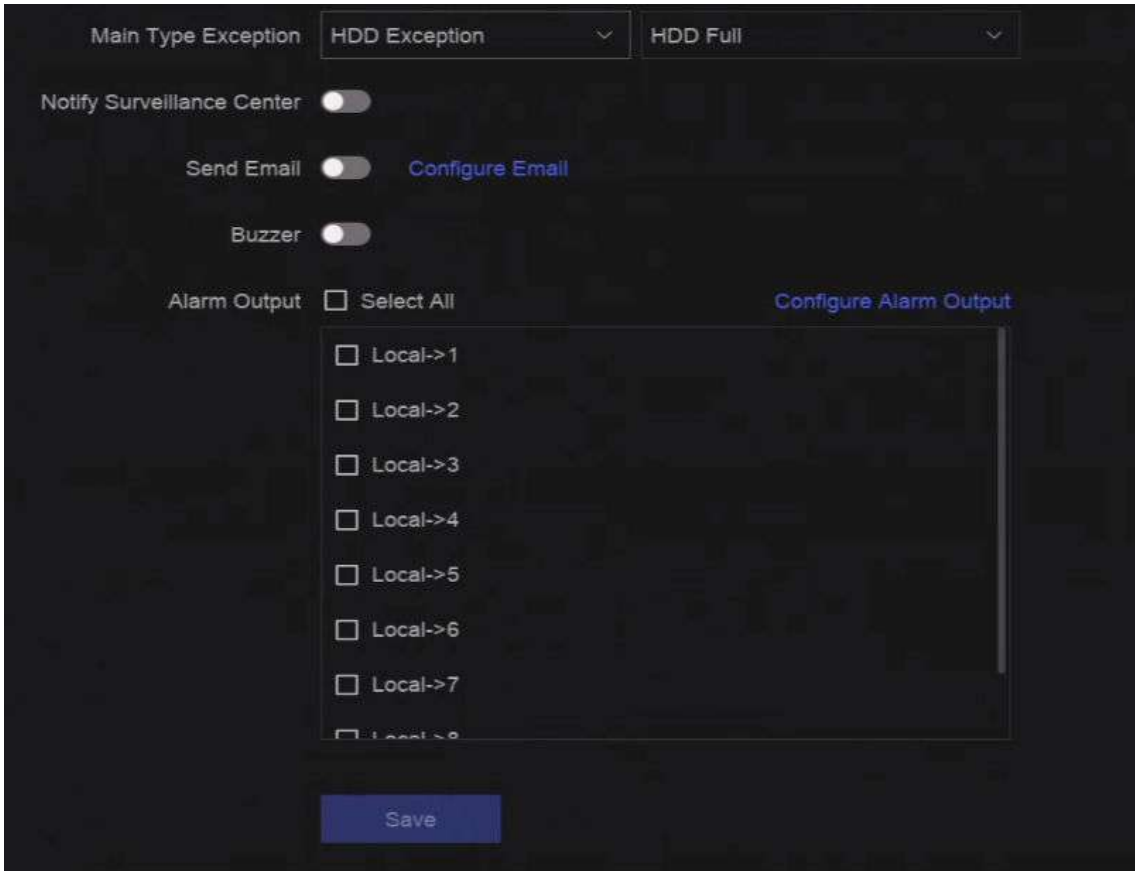
-
4. Go to **System → System Management → N+M Hot Spare** again.
 5. Add working devices to the hot spare system.
 6. Add hot spare devices to the hot spare system.
 7. Click **Save**.

Chapter 20 Configure Exception Event

Exception events can be configured to take the event hint in the live view interface and trigger alarm output and linkage actions.

Steps

1. Go to **System → System Settings → Exception** .



The screenshot shows the 'Exception Event Configuration' interface. At the top, there are two dropdown menus: 'Main Type Exception' set to 'HDD Exception' and 'HDD Full'. Below these are three toggle switches: 'Notify Surveillance Center' (off), 'Send Email' (off), and 'Buzzer' (on). To the right of the 'Send Email' toggle is a blue link 'Configure Email'. Below the 'Buzzer' toggle is another blue link 'Configure Alarm Output'. Under the 'Alarm Output' section, there is a checkbox 'Select All' and a list of checkboxes labeled 'Local->1' through 'Local->8'. At the bottom center is a blue 'Save' button.

Figure 20-1 Exception Event Configuration

2. Select exception type.
3. Configure the linkage methods.

Table 20-1 Linkage Description

Linkage Method	Description
Notify Surveillance Center	The device can send an exception or alarm signal to the remote alarm host when an event occurs. The alarm host refers to the PC installed with client software (e.g., iVMS-4200, iVMS-5200).
Buzzer	When an alarm is detected, the buzzer will make an audible beep.
Send Email	The system can send an email with alarm information to a user or users when an alarm is detected.
Alarm Output	The alarm output can be triggered by the alarm input, motion detection, video tampering detection, face detection, line crossing detection, and any all other events.



Note

When exception events occur,  at the upper-right corner would notify, and you can click  to view.

4. Click **Save.**

Chapter 21 View System Info

Go to **System** → **System Maintenance** → **Running Info** → **System Info** to view the system information, including video recording information, HDD information, network information, stream information of live view or video playback, time sync diagnosis information, etc.

If device exception occurs, for example, when time sync exception occurs and the RTC (coin/button cell) battery is out of power, it may affect the video recording or playback, please resolve the exception as soon as possible.

Chapter 22 System Maintenance

System maintenance functions include log search, schedule reboot, upgrade, etc.

22.1 Schedule Reboot

The device will automatically restart according to the schedule.

Go to **System** → **System Maintenance** → **Maintenance** → **Schedule Reboot** to enable the function, and set the reboot schedule.

22.2 Upgrade Device

The device system can be upgraded with a local USB flash drive, remote FTP server, etc.

Go to **System** → **System Maintenance** → **Maintenance** → **Upgrade** to upgrade your device.

22.3 Backup and Restore

Go to **System** → **System Maintenance** → **Maintenance** → **Backup and Restore** to restore or back up system parameters.

Import/Export Configuration File

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

Simple Restore

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, and leave all settings unchanged except restoring user accounts.

22.4 Log Info

Go to **System → System Maintenance → Maintenance → Log** to search and export log information.

Expired Time Settings

When the log disk is full, logs that exceed the period will be overwritten.

22.5 Configure Log Server

You can upload system logs to the server for backup.

Steps

1. Go to **System → CX → System Settings → Network → Network → Log Server**.
2. Turn on **Enable**.
3. Set **Upload Time**, **Server IP Address**, and **Port**.
4. **Optional**: Click **Test** to test if parameters are valid.
5. Click **Save**.

22.6 Maintenance Tools

Multiple tools are provided for system maintenance, such as S. M. A. R. T. detection and bad sector detection.

Before You Start

Ensure HDD is properly installed.

Steps

1. Go to **System → System Maintenance → Maintenance → Maintenance Tools**.
2. Select tools according to your requirement.

Table 22-1 Tool Description

Tool Name	Description
Network Data Monitoring	Network data monitoring is the process of reviewing, analyzing and managing network data for any abnormality or process that can affect network performance, availability, or security.
Network Packet Capture	Ping The ping test is used to detect whether the destination IP address is reachable. NIC Packet Capture

Tool Name	Description
	After the recorder accessing network, you can use USB flash drive to capture and export network packet.
HDD Status Detection	You can view the health status of a 4 TB to 8 TB Seagate HDD that generated after October 1, 2017. Use this function to help troubleshoot HDD problems. Health Detection shows a more detailed HDD status than the S.M.A.R.T. function.
S.M.A.R.T. Detection	S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) are HDD monitoring systems to detect various reliability indicators in the hopes of anticipating failures.
Bad Sector Detection	When an HDD contains too many bad sectors, it is recommended to replaced the HDD, otherwise files in the HDD may be lost.
HDD Clone	Cope the data in HDD to another one through eSATA interface.



Note

It is recommended to use maintenance tools with the help of technical support.

22.7 Soft Power Off Configuration

Soft power off function is only available for devices with POWER-AC (AC power exception), POWER-UPS (UPS exception), and POWER-UPSL (UPS low power) alarm outputs (at the real panel). The device can receive and record these alarms. When both POWER-AC and POWER-UPSL alarms are triggered, the device will automatically be powered off according to the preset time. When either POWER-AC or POWER-UPSL alarm is not triggered, the device will automatically be powered on.

Steps

1. Go to **System → System Maintenance → Maintenance → Soft Power Off Configuration**.

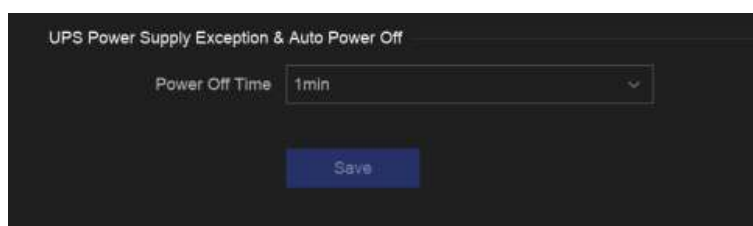


Figure 22-1 Soft Power Off Configuration

2. Set **Power Off Time**. The device would automatically power off after the preset time when corresponding alarms are triggered.
3. Click **Save**.

Example

For example, if **Power Off Time** is set as **1min**, when both POWER-AC (AC power exception) and POWER-UPSL (UPS low power) alarms are triggered, the device would automatically power off after 1 minute.

Chapter 23 Security Management

23.1 Address Filter

The address filter decides whether to allow or forbid specific IP/MAC address to get access to your device.

Before You Start

Log in with the admin account.

Steps

1. Go to **System → System Maintenance → Security Management → Address Filter**.
2. Turn on **Enable**.
3. Set **Filtering Type**. Choose to filter by IP address or MAC Address.
4. Set **Restriction Type**. The device mechanism will allow or forbid specific IP/MAC address to get access to your device.
5. **Optional**: Set **Restriction List**. You can add, edit or delete address.
6. Click **Save**.

23.2 Stream Encryption

After enabling stream encryption, encryption key would be required for remote live view, remote playback, and the downloaded videos.

Steps

1. Go to **System → System Maintenance → Security Management → Stream Encryption**.
2. Turn on **Enable**.
3. Set **Encryption Key**.



Note

The stream encryption key is synchronized with the Hik-Connect service verification code. After enabling the encryption code, the Hik-Connect stream will be forcedly encrypted.

4. Click **Save**.

23.3 Select TLS Version

TLS settings will be effective for HTTP(s) and enhanced SDK service. It provides more secure stream transmission service. Go to **System → System Maintenance → Security Management → TLS** to select TLS version.

Chapter 24 Appendix

24.1 List of Applicable Power Adapter

Only use power adapters listed below.

Power Adapter Model	Specifications	Manufacturer
ADS-26FSG-12 12024EPG	12 V, 2 A	Shenzhen Honor Electronic Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	Moso Power Supply Technology Co., Ltd.
MSA-C1500IC12.0-18P-DE	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
ADS-25FSG-12 12018GPG	CE, 100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C1500IC12.0-18P-US	12 V, 1.5 A	0000201935 MOSO Technology Co., Ltd.
TS-A018-120015AD	100 to 240 VAC, 12 V, 1.5 A, 18 W, $\Phi 5.5 \times 2.1 \times 10$	0000200878 Shenzhen Transin Technologies Co., Ltd.
MSA-C2000IC12.0-24P-DE	12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-24S-12 1224GPG	CE, 100 to 240 VAC, 12 V, 2 A, 24 W, $\Phi 2.1$	0000200174 Shenzhen Honor Electronic Co., Ltd.
MSA-C2000IC12.0-24P-US	US, 12 V, 2 A	0000201935 MOSO Technology Co., Ltd.
ADS-26FSG-12 12024EPCU	US, 12 V, 2 A	0000200174 Shenzhen Honor Electronic Co., Ltd.
KPL-040F-VI	12 V, 3.33 A, 40 W	0000203078 Channel Well Technology Co., Ltd.
MSA-Z3330IC12.0-48W-Q	12 V, 3.33 A	0000201935 MOSO Technology Co., Ltd.
MSP-Z1360IC48.0-65W	48 V, 1.36 A	0000201935 MOSO Technology Co., Ltd.
KPL-050S-II	48 V, 1.04 A	0000203078 Channel Well Technology Co., Ltd.

24.2 Glossary

Dual-Stream

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 1080P and the sub-stream having a maximum resolution of CIF.

DVR

Acronym for Digital Video Recorder. A DVR is device that is able to accept video signals from analog cameras, compress the signal and store it on its hard drives.

HDD

Acronym for Hard Disk Drive. A storage medium which stores digitally encoded data on platters with magnetic surfaces.

DHCP

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.

HTTP

Acronym for Hypertext Transfer Protocol. A protocol to transfer hypertext request and information between servers and browsers over a network.

PPPoE

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.

DDNS

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 hostnames, addresses or other information stored in DNS.

Hybrid DVR

A hybrid DVR is a combination of a DVR and NVR.

NTP

Acronym for Network Time Protocol. A protocol designed to synchronize the clocks of computers over a network.

NTSC

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.

NVR

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.

PAL

Acronym for Phase Alternating Line. PAL is also another video standard used in broadcast televisions systems in large parts of the world. PAL signal contains 625 scan lines at 50Hz.

PTZ

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.

USB

Acronym for Universal Serial Bus. USB is a plug-and-play serial bus standard to interface devices to a host computer.

24.3 Frequently Asked Questions

24.3.1 Why is there a part of channels displaying “No Resource” or turning black screen in multi-screen live view?

Reason

1. Sub-stream resolution or bitrate settings is inappropriate.
2. Connecting sub-stream failed.

Solution

1. Go to **Camera → Video Parameters → Sub-Stream** . Select the channel, and turn down the resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps).



Note

If your video recorder notifies not support this function, you can log in to the camera, and adjust video parameters via web browser.

2. Properly set the sub-stream resolution and max. bitrate (resolution shall be less than 720p, max. bitrate shall be less than 2048 Kbps), then delete the channel and add it back again.

24.3.2 Why is the video recorder notifying risky password after a network camera is added?

Reason

The camera password is too weak.

Solution

Change the camera password.



Warning

We highly recommend you create a strong password of your own choosing (Using a minimum of 8 characters, including at least three of the following categories: 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.

24.3.3 Why is the video recorder notifying the stream type is not supported?

Reason

The camera encoding format mismatches with the video recorder.

Solution

If the camera is using H.265/MJPEG for encoding, but video recorder does not support H.265/MJPEG, change the camera encoding format to the same as video recorder.

24.3.4 How to confirm the video recorder is using H.265 to record video?

Solution

Check if the encoding type at live view toolbar is H.265.

24.3.5 Why is the video recorder notifying IP conflict?

Reason

The video recorder uses the same IP address as other devices.

Solution

Change the IP address of video recorder. Ensure it is not the same as other devices.

24.3.6 Why is image getting stuck when playing back by single or multi-channel cameras?

Reason

HDD read/write exception.

Solution

Export the video, and play it with other devices. If it plays normally on other device, change your HDD, and try again.

24.3.7 Why is the device not able to control PTZ camera via coaxitron?

Reason

1. The camera does not support coaxitron.
2. The coaxitron protocol is incorrect.
3. The signal is affected by video optical transceiver.

Solution

1. Ensure the video input signal is HDTVI, and the camera supports coaxitron.
2. Ensure coaxitron protocol parameters are correct, such as baud rate and address.
3. Remove the video optical transceiver, and try again.

24.3.8 Why does the PTZ seem unresponsive via RS-485?

Reason

1. The RS-485 cable is not properly connected.
2. The RS-485 interface is broken.
3. The control protocol is not correct.

Solution

1. Check if RS-485 cable is properly connected.
2. Change RS-485 interface, and try again.
3. Ensure control protocol is Pelco.

24.3.9 Why is the video sound quality not good?

Reason

1. The audio input device does not have a good effect in sound collection.
2. Interference in transmission.
3. The audio parameter is not properly set.

Solution

1. Check if the audio input device is working properly. You can change another audio input device, and try again.
2. Check the audio transmission line. Ensure all lines are well connected or welded, and there is no electromagnetic interference.
3. Adjust the audio volume according to the environment and audio input device.

24.4 Notification for Corrosive Gas

In non-data center room, the corrosive gas concentration limit is recommended to meet the requirements of the chemical active substance 3C2 level in IEC 60721-3-3:2002.

Table 24-1 Corrosive Gas Concentration Limit

Corrosive Gas Category	Average Value (mg/m ³)	Max. Value (mg/m ³)
SO ₂ (Sulfur Dioxide)	0.3	1.0
H ₂ S (Hydrogen Sulfide)	0.1	0.5
Cl ₂ (Chlorine)	0.1	0.3
HCl (Hydrogen Chloride)	0.1	0.5
HF (Hydrogen Fluoride)	0.01	0.03
NH ₃ (Ammonia)	1.0	3.0
O ₃ (Ozone)	0.05	0.1
NO _x (Nitrogen Oxides)	0.5	1.0

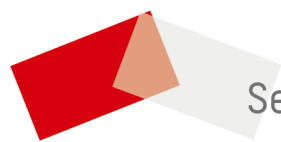


Note

- The average values in the table above are typical control limits for corrosive gases in the machine room environment. In general, it is not recommended that the concentration of corrosive gases exceed the average value.
- The maximum value refers to the limit or peak value. The duration for the corrosive gas concentration to reach the maximum value should not exceed 30 minutes per day.

Table 24-2 Common Categories and Sources of Corrosive Gases

Category	Primary Sources
H ₂ S (Hydrogen Sulfide)	Geothermal emissions, microbial activity, oil manufacturing, wood corrosion, wastewater treatment, etc.
SO ₂ (Sulfur Dioxide), SO ₃ (Sulfur Trioxide)	Coal combustion, petroleum products, automobile exhaust, smelting ore, sulfuric acid manufacturing, tobacco combustion, etc.
S (Sulfur)	Foundry shops, sulfur manufacturing, etc.
HF (Hydrogen Fluoride)	Fertilizer manufacturing, aluminum manufacturing, ceramic manufacturing, steel manufacturing, electronic equipment manufacturing, mineral combustion, etc.
NO _x (Nitrogen Oxides)	Automobile exhaust, oil combustion, microbial activity, chemical industry, etc.
NH ₃ (Ammonia)	Microbial activity, sewage, fertilizer manufacturing, geothermal emissions, etc.
CO (Carbon Monoxide)	Combustion, automobile exhaust, microbial activity, tree decay, etc.
Cl ₂ (Chlorine), ClO ₂ (Chlorine Dioxide)	Chlorine manufacturing, aluminum manufacturing, zinc manufacturing, waste decomposition, etc.
HCl (Hydrogen Chloride)	Automobile exhaust, combustion, forest fires, marine process polymer combustion, etc.
HBr (Hydrobromic Acid), HI (Hydroiodic Acid)	Automobile exhaust, etc.
O ₃ (Ozone)	Atmospheric optical processes (mostly including nitric oxide and hydrogen peroxide), etc.
C _n H _n (Alkane)	Automobile exhaust, tobacco burning, animal waste, sewage, tree decay, etc.



See Far, Go Further

DS-9616NI-M8 M Series 8K NVR

Key Feature

- Up to 16-ch IP camera inputs
- Up to 2-ch@32 MP + 2-ch@8 MP/10-ch@8 MP/20-ch@4 MP/40-ch@1080p decoding capacity
- Up to 320 Mbps incoming bandwidth and 400 Mbps outgoing bandwidth
- 2 HDMI (different source) and 2 VGA (different source) interfaces, 8K or dual 4K video outputs
- Supports special cameras, including people counting camera, ANPR (automatic number plate recognition) camera, and fisheye camera
- Advanced streaming technology enables smooth live view in poor network conditions
- Supports RAID 0, 1, 5, 6, 10 and N+M hot spare for even more reliable data storage, effectively avoids data loss risks



Professional and Reliability

- H.265+ compression effectively reduces the storage space by up to 75%
- Dual-stream recording saves bandwidth
- Adopt stream over TLS encryption technology which provides more secure stream transmission service
- Support double verification for playback and downloading
- Solar-powered camera is connectable through OTAP protocol. NVR would get stream when user requests, and camera would send back videos according to the schedule

HD Video Output

- Provide independent HDMI and VGA outputs
- HDMI video output at up to 8K or dual 4K resolution

Storage and Playback

- 8 SATA interfaces for HDD connection (up to 16 TB capacity per HDD)
- 1 eSATA interface for HDD connection
- 16-ch synchronous playback

Smart & POS Function

- Support multiple VCA (Video Content Analytics) events
- Configurable special camera smart functions, such as VCA detection (motion, line crossing, intrusion, etc.), heat map, ANPR, and people counting
- POS information overlay on live view and playback, and POS triggered recording and alarm

Network & Ethernet Access

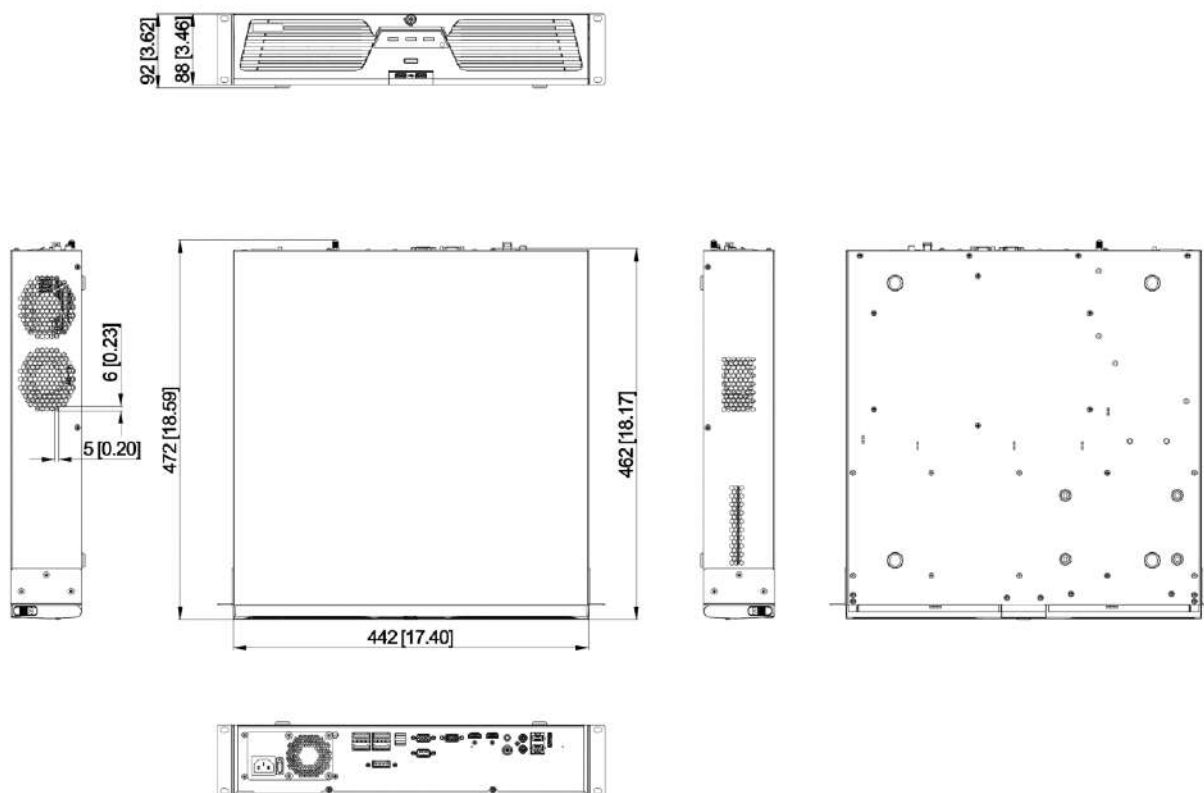
- 2 self-adaptive 10/100/1000 Mbps Ethernet interfaces
- Hik-Connect & DDNS (Dynamic Domain Name System) for easy network management
- Smooth streaming technology
- Support web access without plug-in

▪ Specification

Video and Audio	
IP Video Input	16-ch
Incoming Bandwidth	320 Mbps
Outgoing Bandwidth	400 Mbps
HDMI 1 Output	8K (7680 × 4320)/30Hz, 4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
HDMI 2 Output	4K (3840 × 2160)/60Hz, 4K (3840 × 2160)/30Hz, 2K (2560 × 1440)/60Hz, 1920 × 1080/60Hz, 1600 × 1200/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz *: When HDMI 1 output resolution is 8K, the maximum HDMI 2 output resolution is 1080p.
VGA 1 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
VGA 2 Output	1920 × 1080/60Hz, 1280 × 1024/60Hz, 1280 × 720/60Hz, 1024 × 768/60Hz
Video Output Mode	HDMI 1 and VGA 1 provide simultaneous video output, and work as the main output; HDMI 2 and VGA 2 provide simultaneous video output, and work as the auxiliary output
CVBS Output	1-ch, BNC (1.0 Vp-p, 75 Ω), resolution: PAL: 704 × 576, NTSC: 704 × 480
Audio Output	2-ch, RCA (Linear, 1 KΩ)
Two-Way Audio	1-ch, RCA (2.0 Vp-p, 1 KΩ, using the audio input)
Decoding	
Decoding Format	H.265+/H.265/H.264+/H.264
Recording Resolution	32 MP/24 MP/12 MP/8 MP/7 MP/6 MP/5 MP/4 MP/3 MP/1080p/UXGA/720p/VGA/4CIF/DCIF/2CIF/CIF/QCIF
Synchronous playback	16-ch
Decoding Capability	2-ch@32 MP (30 fps) + 2-ch@8 MP (30 fps)/10-ch@8 MP (30 fps)/20-ch@4 MP (30 fps)/40-ch@1080p (30 fps)
Audio Compression	G.711ulaw/G.711alaw/G.722/G.726/AAC/MP2L2/PCM

Network	
Network Protocol	TCP/IP, DHCP, IPv4, IPv6, DNS, DDNS, NTP, RTSP, SADP, SMTP, SNMP, NFS, iSCSI, ISUP, UPnP™, HTTP, HTTPS
Network Interface	2, RJ-45 10/100/1000 Mbps self-adaptive Ethernet interface
RAID	
RAID Type	RAID0, RAID1, RAID5, RAID6, RAID10
Auxiliary Interface	
Serial Interface	1 RS-485 (full-duplex), 1 RS-232
SATA	8 SATA interfaces supporting hot-plug
eSATA	1 eSATA interface
Capacity	Up to 16 TB capacity for each disk
Alarm In/Out	16/9
USB Interface	Front panel: 2 × USB 2.0; Rear panel: 2 × USB 3.0
Ctrl 12V	Controllable 12 VDC, 1 A power output for external alarm device; The power will be turned on when the alarm output is triggered. *: The Ctrl 12V power is controlled by alarm output 9.
DC 12V	12 VDC, 1 A power output
General	
Power Supply	100 to 240 VAC, 50 to 60 Hz
Consumption	≤ 50 W (without HDD)
Working Temperature	-10 °C to 55 °C (14 °F to 131 °F)
Working Humidity	10% to 90%
Chassis	2U chassis
Dimension (W × D × H)	442 × 462 × 88 mm (17.4"× 18.2" × 3.5")
Weight	≤ 10 kg (without HDD, 22 lb.)
Certification	
Obtained Certification	CE, FCC
FCC	Part 15 Subpart B, ANSI C63.4-2014
CE	EN 55032:2015, EN 61000-3-2, EN 61000-3-3, EN 50130-4

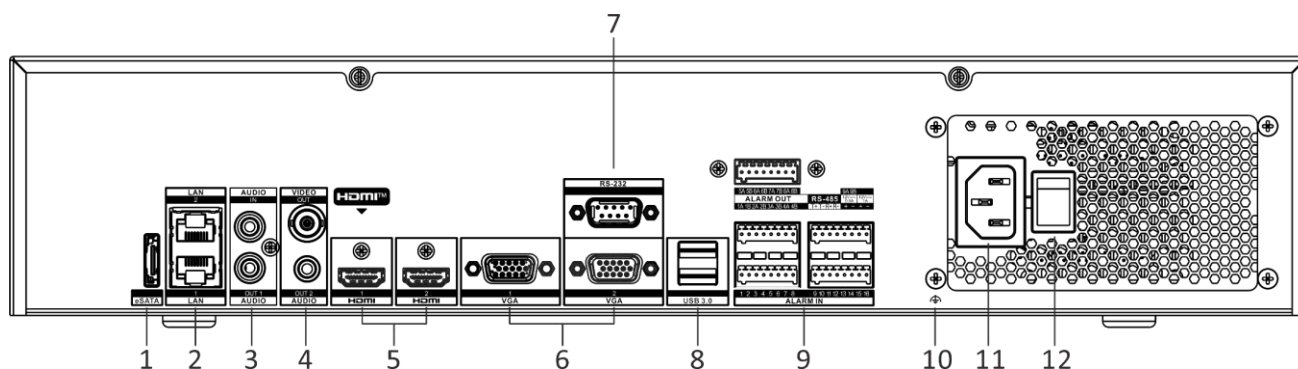
Dimension



Unit:mm [inch]

SCALE 1:1

Physical Interface



No.	Description	No.	Description
1	eSATA interface	7	RS-232 Serial interface
2	LAN interfaces	8	USB 3.0 interfaces
3	Audio in and out	9	Alarm in, alarm out, RS-485 serial interface, Ctrl 12V and DC 12V
4	Audio out and video out	10	GND
5	HDMI 1 and HDMI 2 interfaces	11	100 to 240 VAC power supply
6	VGA 1 and VGA 2 interfaces		

Available Model

DS-9616NI-M8

Headquarters

No.555 Qianmo Road, Binjiang District,
Hangzhou 310051, China
T +86-571-8807-5938
www.hikvision.com

Follow us on social media to get the latest product and solution information.



Hikvision



HikvisionHQ



HikvisionHQ



Hikvision_Global



Hikvision
Corporate Channel



hikvisionhq





Highlights

- Up-to 26TB¹ capacity
- Enterprise-class reliability and performance
- 5-year limited warranty⁸
- 550TB¹ per year workload rating⁶
- Up-to 2.5 million hours Mean Time Between Failure (MTBF)⁷
- Innovative AllFrame™ AI technology helps reduce dropped frames
- Western Digital Device Analytics™ (WDDA) proactive health management

Ideal For:

- Advanced AI-Enabled Recorders
- Video Storage Servers
- Video Management Systems (VMS)

WD Purple® Pro Smart Video Hard Drive

Professional Grade Storage for Smart Video Recording and AI Video Analytics

WD Purple® Pro delivers ultimate reliability and performance for the most demanding video recording and analytics environments.

Higher Capacity Drives for More Demanding Smart Video Solutions

WD Purple® Pro delivers big capacities (up to 26TB¹) for larger scale deployments and longer-term video retention requirements.

Enterprise Class Reliability

True enterprise class drives designed with the highest level of reliability. With up to 2.5 million hours MTBF⁷ and backed with a 5-year limited warranty⁸, WD Purple® Pro is built for high-end video recorders and analytics servers.

High Performance for Simultaneous Video Recording and Real-Time AI Analysis

Modern cameras and AI-enabled recording systems send multiple streams of high-definition video, picture files and metadata to storage. WD Purple Pro drives deliver our highest level of performance for video storage and analysis.

Built for Advanced Smart Video Workloads

WD Purple Pro delivers higher workload capability up-to 550TB/year⁶. Keep up with heavy video data capture and AI analysis found in advanced video management systems.

Innovative AllFrame™ AI Technology

AllFrame™ AI technology intelligently guides video, picture and metadata streams to disk while helping to reduce dropped video frames.

Proactive Drive Health Insights with WDDA™

Western Digital Device Analytics™ (WDDA) monitors drive health and recommends action to improve drive operation. Requires compatible video recorder or system.

WD Purple® Pro Smart Video Hard Drive

Specifications

Model number	WD260PURP	WD241PURP	WD221PURP	WD181PURP
Formatted capacity ¹	26TB	24TB	22TB	18TB
Form factor	3.5-inch	3.5-inch	3.5-inch	3.5-inch
Advanced Format (AF)	Yes	Yes	Yes	Yes
Interface	SATA	SATA	SATA	SATA
Recording Technology	CMR	CMR	CMR	CMR
Drive Technology	Helium	Helium	Helium	Helium
RV Sensors	Yes	Yes	Yes	Yes
RoHS compliant ²	Yes	Yes	Yes	Yes
Product Features				
Maximum drive bays supported	No Limit	No Limit	No Limit	No Limit
Camera Support ³	Up to 64 HD	Up to 64 HD	Up to 64 HD	Up to 64 HD
AI Streams	32	32	32	32
Firmware Feature Name	AllFrame AI	AllFrame AI	AllFrame AI	AllFrame AI
Tarnish resistant components	Yes	Yes	Yes	Yes
Performance				
Interface transfer rate (max) Buffer to host	6 Gb/s	6 Gb/s	6 Gb/s	6 Gb/s
Internal transfer rate (max) ⁴	287 MB/s	287 MB/s	265 MB/s	272 MB/s
Cache (MB) ¹	512 MB	512 MB	512 MB	512 MB
RPM	7200	7200	7200	7200
Reliability/Data Integrity				
Load/unload cycles ⁵	600,000	600,000	600,000	600,000
Annualized Workload Rate ⁶ (TB/year)	Up to 550 TB/year	Up to 550 TB/year	Up to 550 TB/year	Up to 550 TB/year
Non-recoverable read errors per bits read	<1 in 10 ¹⁵	<1 in 10 ¹⁵	<1 in 10 ¹⁵	<1 in 10 ¹⁵
MTBF ⁷ (hours)	2,500,000	2,500,000	2,500,000	2,500,000
Limited warranty (years) ⁸	5 years	5 years	5 years	5 years
Power Management				
Average Power (W) ⁹				
Read/Write	6.2 W	6.2 W	6.9 W	6.3 W
Idle	5.7 W	5.7 W	5.6 W	5.9 W
Standby/Sleep	1.1 W	1.1 W	1.2 W	0.9 W
Environmental Specifications				
Temperature				
Operating	5°C to 65°C	5°C to 65°C	0°C to 65°C	0°C to 65°C
Non-operating	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C
Shock				
Operating (2 ms, read/write)	40Gs	40Gs	40Gs	50Gs
Operating (2 ms, read)	40Gs	40Gs	40Gs	50Gs
Non-operating (2 ms)	200Gs	200Gs	200Gs	250Gs
Acoustics (dBA)				
Idle dBA	25	25	20	20
Seek (average) dBA	32	32	32	36
Physical Dimensions				
Height (max) (in / mm)	1.028 / 26.1	1.028 / 26.1	1.028 / 26.1	1.028 / 26.1
Length (max) (in / mm)	5.787 / 147	5.787 / 147	5.787 / 147	5.787 / 147
Width (± .01 in.) (in / mm)	4 / 101.6	4 / 101.6	4 / 101.6	4 / 101.6
Weight (± 3%) (lb / kg)	1.47 / 0.67	1.47 / 0.67	1.48 / 0.67	1.52 / 0.69

WD Purple® Pro Smart Video Hard Drive

Specifications

Model number	WD142PURP	WD122PURP	WD102PURP	WD8002PURP
Formatted capacity ¹	14TB	12TB	10TB	8TB
Form factor	3.5-inch	3.5-inch	3.5-inch	3.5-inch
Advanced Format (AF)	Yes	Yes	Yes	Yes
Interface	SATA	SATA	SATA	SATA
Recording Technology	CMR	CMR	CMR	CMR
Drive Technology	Helium	Air	Air	Air
RV Sensors	Yes	Yes	Yes	Yes
RoHS compliant ²	Yes	Yes	Yes	Yes
Product Features				
Maximum drive bays supported	No Limit	No Limit	No Limit	No Limit
Camera Support ³	Up to 64 HD	Up to 64 HD	Up to 64 HD	Up to 64 HD
AI Streams	32	32	32	32
Firmware Feature Name	AllFrame AI	AllFrame AI	AllFrame AI	AllFrame AI
Tarnish resistant components	Yes	Yes	Yes	Yes
Performance				
Interface transfer rate (max)	6 Gb/s	6 Gb/s	6 Gb/s	6 Gb/s
Buffer to host				
Internal transfer rate (max) ⁴	265 MB/s	267 MB/s	267 MB/s	267 MB/s
Cache (MB) ¹	512 MB	512 MB	512 MB	256 MB
RPM	7200	7200	7200	7200
Reliability/Data Integrity				
Load/unload cycles ⁵	600,000	600,000	600,000	600,000
Annualized Workload Rate ⁶ (TB/year)	Up to 550 TB/year	Up to 550 TB/year	Up to 550 TB/year	Up to 550 TB/year
Non-recoverable read errors per bits read	<1 in 10 ¹⁵	<1 in 10 ¹⁵	<1 in 10 ¹⁵	<1 in 10 ¹⁵
MTBF ⁷ (hours)	2,500,000	2,000,000	2,000,000	2,000,000
Limited warranty (years) ⁸	5 years	5 years	5 years	5 years
Power Management				
Average Power (W) ⁹				
Read/Write	6.6 W	9.1 W	9.1 W	7.3W
Idle	5.7 W	8.2 W	8.2 W	6.5 W
Standby/Sleep	0.9 W	0.3 W	0.3 W	0.3 W
Environmental Specifications				
Temperature				
Operating	5°C to 65°C	5°C to 65°C	0°C to 65°C	0°C to 65°C
Non-operating	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C	-40°C to 70°C
Shock				
Operating (2 ms, read/write)	50Gs	70Gs	70Gs	70Gs
Operating (2 ms, read)	50Gs	70Gs	70Gs	70Gs
Non-operating (2 ms)	250Gs	250Gs	250Gs	300Gs
Acoustics (dBA)				
Idle dBA	20	34	34	29
Seek (average) dBA	36	39	39	36
Physical Dimensions				
Height (max) (in / mm)	1.028 / 26.1	1.028 / 26.1	1.028 / 26.1	1.028 / 26.1
Length (max) (in / mm)	5.787 / 147	5.787 / 147	5.787 / 147	5.787 / 147
Width (± .01 in.) (in / mm)	4 / 101.6	4 / 101.6	4 / 101.6	4 / 101.6
Weight (± 3%) (lb / kg)	1.52 / 0.69	1.65 / 0.75	1.65 / 0.75	1.58 / 0.715

¹ 1MB = one million bytes, 1GB = one billion bytes, and 1TB = one trillion bytes. Actual user capacity may be less, depending on operating environment.

² This drive is in compliance with the European Union Directive 2011/65/EU and Directive (EU) 2015/863 on the restriction of the use of certain hazardous substances in electrical and electronic equipment.

³ Single stream per camera @ 3.2Mbps (1080p, H.265, 25 fps). Results may vary depending on camera resolution, file format, frames per second, software, system settings, video quality, and other factors.

⁴ Based on read speed, unless otherwise stated. 1MB/s = 1 million bytes per second. Based on internal testing; performance may vary depending upon host device, usage conditions, drive capacity, and other factors.

⁵ Controlled unload at ambient condition.

⁶ Workload Rate is defined as the amount of user data transferred to or from the hard drive. Workload Rate is annualized (TB transferred X (8760 / recorded power-on hours)). Workload Rate will vary depending on your hardware and software components and configurations.

⁷ Projected values. When final, MTBF specifications will be based on a sample population and are estimated by statistical measurements and acceleration algorithms under typical operating conditions, workload of 220TB/year, and drive temperature of 40°C. Derating of MTBF will occur above these parameters, up to 550TB writes per year, and 65°C drive temperature. MTBF ratings do not predict an individual drive's reliability and do not constitute a warranty.

⁸ See <http://support.wdc.com/warranty> for regional specific warranty details.

⁹ Power measurements at room-ambient temperature.



5601 Great Oaks Parkway
San Jose, CA 95119, USA
www.westerndigital.com

© 2025 Western Digital Corporation or its affiliates. All rights reserved. Western Digital, the Western Digital design, the Western Digital logo, AllFrame, OptiNAND, WD Purple, WDDA, and Western Digital Device Analytics are registered trademarks or trademarks of Western Digital Corporation or its affiliates in the US and/or other countries. All other marks are the property of their respective owners. Product specifications subject to change without notice. Pictures shown may vary from actual products.

ESPECIFICAÇÃO TÉCNICA – SUPORTES PRO REV01_2024



• COLUNAS PARA FIXAÇÃO NAS MESAS E CONSOLES ELLAN

Alturas e capacidade de carga das colunas (SLATWALL E SLATRAIL):

- 300mm / 2 telas até 24" ou 40kg
- 700mm / 4 telas até 24" ou 75kg
- 1000mm / 6 telas até 24" ou 115kg
- Perfil base em alumínio extrudado, com canais de apoio e encaixe tipo "tromba de elefante", mantendo a estabilidade e possibilitando o deslocamento do sistema de maneira uniforme pelo trilho (slatwall ou slatrail); fixação s/ ferramenta, com manípulos e parafuso tipo martelo, com bordas arredondadas
- Perfil vertical em alumínio extrudado, soldado no perfil base, com 2 canais espelhados (Esq / Dir) possibilitando a montagem e ajuste de altura de diversos braços p/ tela de acordo com a altura da coluna selecionada; tampa superior de acabamento em plástico injetado
- Acabamento em pintura eletrostática a pó, na cor prata

• BRAÇOS ELLAN

Modelos disponíveis:

- Braço p/ 1 tela (6kg)
- Braço p/ 1 tela c/ suporte p/ mini CPU (9kg)
- Braço p/ 1 tela c/ inclinação de 45 graus (6kg)
- Braço p/ 1 tela Heavy Duty (18kg)
- Braço p/ 1 Notebook (6kg)
- Para uso de telas acima de 24" ou 6kg, consultar nossa engenharia para dimensionamento

ELLAN S A

Rod. Est. SP 115/ 280 – Acesso José Sartorelli Km 3,2 – Parque das Árvores – 18555-225 - Boituva – SP

Tel: (0xx15) 3363-8233

CNPJ: 04.345.304/0001-41 - IE: 219.079.801.110

- Base de encaixe do braço na coluna com trilho em alumínio extrudado com bordas em 45 graus, c/ 5,5mm de espessura, fixado e com possibilidade de ajuste por manípulos (sem uso de ferramentas)
- Eixos de articulação construídos em aço usinado, com buchas em plástico injetado
- Segmentos de braço construídos em aço trefilado, c/ 2mm de espessura, com tampas em plástico injetado encaixadas em todas as extremidades
- Esfera de aço para articulação das telas, possibilitando o giro em 360 graus, e inclinação de 30 a 45 graus, a depender do modelo escolhido
- Placa para telas com fixação modelo VESA 100x100mm e 75x75mm

• GARANTIA

Assegura-se ao produto Ellan a garantia contra qualquer defeito de material ou de fabricação que nele se apresente no período de 05 (cinco) anos, exceto para os casos de mau uso do produto, contando a partir da data de sua aquisição pelo usuário, conforme NF Ellan emitida com seu número sequencial e data.

Os serviços em garantia a serem prestados são restritos unicamente à substituição ou conserto gratuitos das peças defeituosas, desde que, a critério de um técnico credenciado, se constate falha em condições normais de uso, durante a vigência desta garantia.

A garantia torna-se nula e sem efeito se o produto sofrer qualquer dano provocado por acidentes, agentes da natureza, vandalismo de qualquer natureza, desgaste natural das peças e componentes, uso abusivo ou em desacordo, descuido do usuário no manuseio, transporte ou remoção dos mesmos, ou ainda, no caso de apresentar sinais de violação, ajuste ou conserto por pessoas não autorizadas. Os serviços acima referidos, tanto os gratuitos como os remunerados, somente serão prestados nos locais autorizados e indicados pela Ellan S/A.

• Normas, certificados e laudos aplicáveis:

1- Normas regulamentadoras e demais normas aplicáveis:

- Acabamento: DIN 68761; ISO 4211, 9241, 11469; VDE 1000.
- Laminados melamínicos de alta pressão: EN 438.
- Especificações de normas (desenhos) mobiliários e estações de trabalho: EN 527, 614, 717, ZH1/428 – 1988, 31001, 60950, PP52024(1990, 1996) e EM 60335 1:1994.
- Norma de Ergonomia: NR 17.
- Norma anticorrosão para o banho e pintura: ASTM B 117 /1997 ou ABNT NBR 8094/1983 ou ISO 9227/2006.
- Norma NBR ISO 9001: 2008 (edição e versão 2008).
- Réguas de tomada norma ABNT NBR 5410 – item 7.3.3 – Tabela 55. Norma baseada na IEC 60.364 – Electrical Installations of Buildings.
- Aderência das tintas conforme norma ABNT NBR 11003/2009 grau GRO
- Camada de tinta conforme norma interna ITTES007 – Determinação de camada com QUANIX 1500.

2- Certificados e Laudos:

- **Certificado de Ergonomia** em conformidade com a Lei n. 6.514 e Portaria n. 3.214/NR 17, emitido por profissional qualificado em ergonomia (médico do trabalho, ergonomista ou fisioterapeuta do trabalho capacitados para tal).
- **Laudo de Resistência à Corrosão em névoa salina (Salt Spray)**, conforme norma ASTM B 117 /1997 ou ABNT NBR 8094/1983 ou ISO 9227/2006, mediante corpos de prova expostos em teste de névoa salina. A

ELLAN S A

Rod. Est. SP 115/ 280 – Acesso José Sartorelli Km 3,2 – Parque das Árvores – 18555-225 - Boituva – SP

Tel: (0xx15) 3363-8233

CNPJ: 04.345.304/0001-41 - IE: 219.079.801.110

duração do teste de névoa salina para aço laminado e perfis de alumínio é de no mínimo 500 horas e máximo de 1000hs de exposição, respectivamente.

- **Atestado de fornecimento, experiência e de capacidade técnica** de linhas similares e já fornecidas para ambientes similares e com todos os dados do contato no cliente, com assinatura e firma reconhecida.
- **Declaração do responsável pelo CREA da empresa**, declarando atendimento a especificação técnica de tratamento superficial e de pintura com tinta pó eletrostática poliéster ou híbrida, com no mínimo 80 micrometros de camada protetiva e aderência grau GR0, através do cumprimento do item 7.5.2. da norma ABNT NBR 9001/2008 – validação de processos – pela qual a empresa é certificada.
- **Apresentação de desenho** do produto ofertado, realizado em software de modelagem 2D/3D, junto da proposta técnica / comercial, conforme a layout e informações fornecidas.
- **Declaração de cumprimento em 100% às diretivas RoHs** através do responsável pelo CREA da empresa, contra a utilização de substâncias perigosas.
- **Apresentação de teste comprobatório de validação termográfica** (tempo x temperatura), realizado semestralmente na estufa de secagem da pintura eletrostática, garantindo qualidade do acabamento e cura com tinta a pó poliéster eletrostática.
- **Apresentação de certificado conforme Norma NBR ISO 9001: 2015 (edição e versão 2015)**. Esta nova versão é necessária, pois foi elaborada para apresentar maior compatibilidade com a família da ISO 14000, cujas alterações trouxeram maior compatibilidade para as traduções e consequentemente um melhor entendimento e interpretação de seu texto.
- **Declaração com comprovação em fábrica do processo de pintura eletrostática com tinta a pó** para substratos não ferrosos quanto à determinação da camada de tinta conforme norma ABNT NBR 11003 – 2000, utilizando-se de equipamento calibrado anualmente, modelo: Quanix 1500, assegurando uma deposição de camada de no mínimo 80 micrometros.

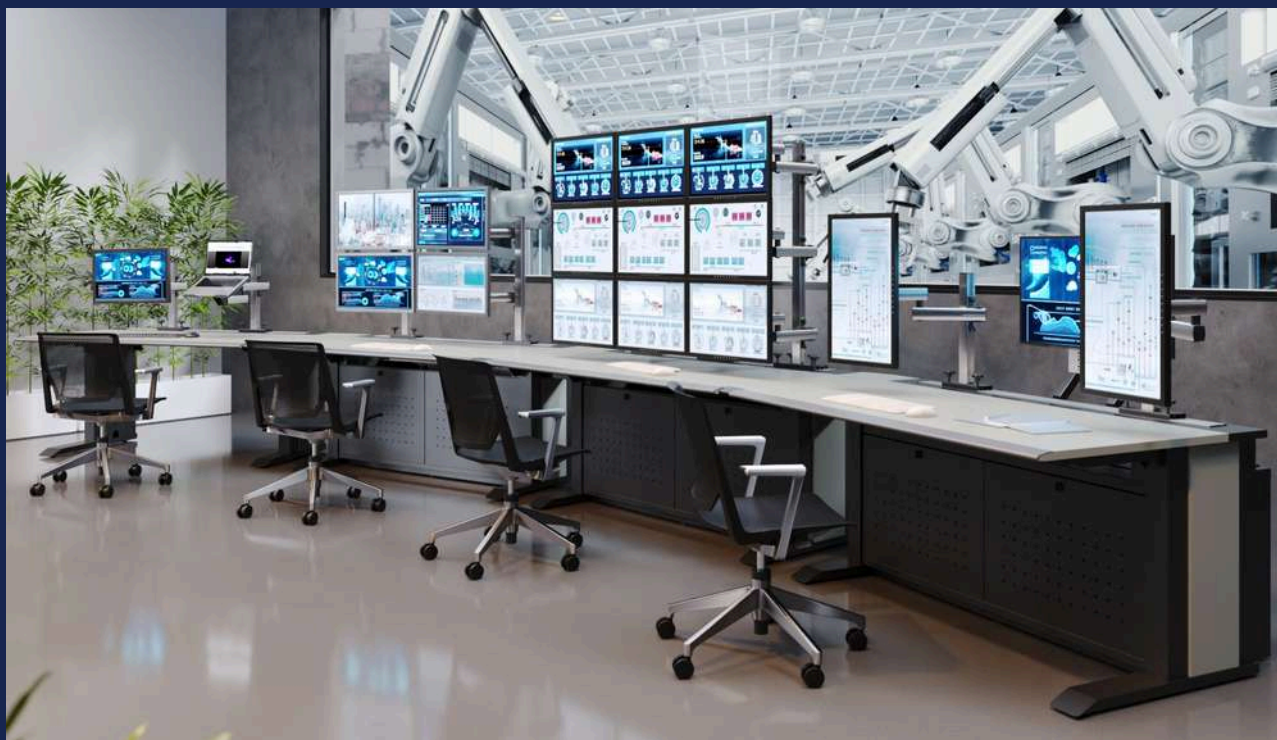
ellan.

SUORTES PARA MONITORES



1. LAYOUT monitores

Os suportes Ellan são compatíveis com diferentes modelos e tamanhos de monitores, permitindo que eles permaneçam alinhados e regulados.



7 Monitores



3 Monitores



1 monitor e 1 Notebook



2. MODELOS **Braços**

A Ellan oferece uma variedade de braços para suportes de monitores, cada um projetado para situações específicas e diferentes tipos de equipamentos, garantindo a melhor solução para cada necessidade.

BRAÇO PADRÃO



ATÉ 6Kg

BRAÇO PARA MONITORES ULTRAWIDE(PESADOS)



ATÉ 18Kg | 25 Á 39 POLEGAS

BRAÇO INCLINADO



ATÉ 6Kg

SUPORTE PARA TELEVISORES



ATÉ 18Kg | 40 Á 70 POLEGAS

BRAÇO PARA NOTEBOOK



ATÉ 6Kg

BRAÇO PARA 01 MONITOR E THIN CLIENT



ATÉ 6Kg

3. SUPORTES ergonômicos

Veja neste video a importância da Ergonomia quando se trabalha com monitores



Ajuste ideal para cada operador



Escaneie o QR code para assistir ao vídeo.



Conforto e segurança .

ellan.

4. PAINÉIS para fixação



SUPORTES PARA SLATWALL

A estrutura de Slatwall é composta por painéis verticais com ranhuras horizontais. É ideal para trabalhos em que não é necessária a interação com o ambiente ao redor da estação de trabalho. Além disso, a estrutura de Slatwall contribui para um ambiente mais limpo e organizado, pois permite a passagem de cabos de forma discreta, reduzindo a desordem visual.

SUPORTES PARA SLATRAIL

Composta por trilhos horizontais fixados na frente do tampo, a estrutura Slatrail permite a passagem de cabos de forma discreta, proporcionando organização visual. Essa estrutura é ideal para estações de trabalho que precisam de interação ao redor, como, por exemplo, quando há um videowall à frente da estação.



A MELHOR SOLUÇÃO

para sua operação

A Ellan está presente no mercado brasileiro a mais de 35 anos com suas linhas de produtos sempre com foco em oferecer o melhor aos nossos clientes. Estamos localizados em Boituva, interior de São Paulo, em uma área própria de 25.000 m² de terreno e 5.000m² de área fabril. Nossa fábrica está estruturada com máquinas precisas e de qualidade para conseguirmos entregar o melhor produto dentro do melhor prazo possível para nossos clientes. Oferecemos uma linha completa de produtos distintos para atender a diversas necessidades. Se Você necessita de customização a Ellan é especialista em

desenvolver soluções para os projetos dos clientes que não se encaixam em nossos produtos padrão. Após levantar toda a sua necessidade realizamos um projeto ainda em fase de cotação.



WWW.ELLAN.COM.BR

ELLAN S/A - Rod. SP 115/280, km 3,2 Acesso Jardim Sartorelli - Pq. das Árvores

Boituva - SP - Brasil - CEP 18555-225

Telefone para contato: (15) 3363-8233

Whatsapp: (15) 98145-0788

ellan.

PRODUTOS

MOBILIÁRIO

Para operação,
controle e
monitoramento

INDUSTRIAL

Bancadas, armários
e carrinhos

LOGÍSTICA

Carrinhos, bancadas
e prateleiras



1. CONSOLES

para operação, controle e monitoramento



Eleve o padrão da sua Sala de Controle com nossa linha de mobiliário especializado. Projetados para suportar operações 24/7, nosso mobiliário oferece ergonomia necessária, promovendo o conforto dos operadores e aumentando a eficiência. A escolha do mobiliário adequado é crucial para a operação ininterrupta. Transforme seu espaço de controle em um ambiente de excelência.

1. CONSOLES

design
personalizado



1. LINHA MF

eficiência técnica



1. LINHA EB

organização simples
e eficaz



ellan.

2. INDUSTRIAL bancadas, armários e carrinhos



Traga excelência para sua produção industrial com nossa linha Industrial: bancadas, armários e carrinhos projetados especificamente para atender às demandas do ambiente fabril. Nossa solução oferece organização, durabilidade e ergonomia inigualáveis, otimizando o espaço de trabalho e melhorando a segurança. Reduza o tempo de processo e impulsione a sua produção. O mobiliário certo faz toda a diferença!

Bancadas SAM

Linha modular

Bancadas básicas

ellan.

3. LOGÍSTICA

carrinhos, bancadas e prateleiras



Maximize a eficiência da sua operação logística com nossa linha de bancadas, carrinhos de movimentação e prateleiras de alta qualidade. Com designs ergonômicos e durabilidade excepcional, nossos produtos otimizam o espaço de armazenamento e agilizam o fluxo de trabalho. Aumente a produtividade e reduza custos operacionais. Invista na infraestrutura certa para o sucesso logístico.

Bancadas



Prateleiras



Carrinhos



ellan.

SUPORTES

para monitores
e acessórios



Aprimore a eficiência da sua operação com nossos suportes de monitor e teclado preparados para a Indústria 4.0. Com sua articulação inteligente, liberam todo o espaço do tampo para tarefas produtivas. Além disso, oferecem ajustes ergonômicos para o conforto e produtividade de seus operadores. Potencialize sua produção com nossas soluções exclusivas de suportes para monitores.



Ajustes sem necessidade de
ferramentas

ellan.

A MELHOR SOLUÇÃO

para sua operação

A Ellan está presente no mercado brasileiro a mais de 35 anos com suas linhas de produtos sempre com foco em oferecer o melhor aos nossos clientes. Estamos localizados em Boituva, interior de São Paulo, em uma área própria de 25.000 m² de terreno e 5.000m² de área fabril. Nossa fábrica está estruturada com máquinas precisas e de qualidade para conseguirmos entregar o melhor produto dentro do melhor prazo possível para nossos clientes. Oferecemos uma linha completa de produtos distintos para atender a diversas necessidades. Se Você necessita de customização a Ellan é especialista em desenvolver soluções para os projetos dos clientes que não se encaixam em nossos produtos padrão. Após levantar toda a sua necessidade realizamos um projeto ainda em fase de cotação.



ellan.

WWW.ELLAN.COM.BR

ELLAN S/A - Rod. SP 115/280, km 3,2 Acesso Jardim Sartorelli - Pq. das Árvores

Boituva - SP - Brasil - CEP 18555-225

Telefone para contato: (15) 3363 8233

Whatsapp: (15) 3363 8236



Ultra High Definition (UHD) Decoder

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND

HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Preface

Applicable Models

This manual is applicable to the DS-69XXUDI (C) series UHD decoders, including DS-6901UDI(C), DS-6904UDI(C), DS-6908UDI(C), DS-6910UDI(C), DS-6912UDI(C), and DS-6916UDI(C).

Default Parameters

Type	Default Parameter
Device	• Login user name: admin • IP address: 192.0.0.64
SSH connection	



To improve system security, it is highly recommended to change password regularly. In order to protect your privacy and corporate data and avoid network security issues, it is recommended to set strong password that meets security requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions



In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.



- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- + identifies the positive terminals of the device which is used with, or generates direct current, and - identifies the negative terminals of the device which is used with, or generates direct current.
- The serial port of the device is used for debugging only.
- The interface varies with the models. Please refer to the product datasheet for details.
- The USB port of the device is used for connecting to a mouse, a keyboard, or a USB flash drive only. The current for the connected device shall be not more than 0.1 A.

TABLE OF CONTENTS

Chapter 1 Introduction	1
1.1 Overview	1
1.2 First-Time Configuration Process	1
Chapter 2 Device Basic Settings	2
2.1 Activate and Log In to Device	2
2.2 Configure the Network Address	5
2.2.1 Configure TCP/IP	5
Chapter 3 Video Wall Management	7
3.1 Configure the Video Wall	7
3.1.1 Configure the Video Wall Scale	7
3.1.2 Configure the Output	8
3.1.3 Manage Signal Sources	11
3.1.4 Bind Signal Sources with the Video Wall	14
3.2 Operate the Video Wall	16
3.2.1 Edit Signal Source Window Parameters	16
3.2.2 Manage Scenes	18
3.2.3 Maintain Screens	20
3.3 Configure Image Effect on Screen	22
3.3.1 Edit a Signal Source	22
3.3.2 Configure Encoding Parameters	25
3.3.3 Set Other Parameters	26
Chapter 4 Device Maintenance	28
4.1 View Device Status	28
4.2 Configure System Parameters	28
4.3 Configure HTTP(S) Parameters	32
4.4 Configure Event	33
4.5 Maintain the System	33
4.6 Maintain the Device Security	35

Chapter 1 Introduction

1.1 Overview

The DS-69XXUDI (C) ultra high definition (UHD) decoder (hereinafter referred as the device), is the latest generation decoder designed specifically for high-definition network cameras, making it suitable for various video security system projects. The device offers exceptional video processing capabilities and a seamless video decoding experience.

The device has the following core advantages:

- **Format Flexibility:** Supports various video encoding formats including H.265, H.264, MJPEG, Smart264, and Smart265 to meet diverse video source requirements.
- **Resolution Handling:** Decodes H.265 or H.264 video streams of up to 32 MP and lower resolution, ensuring real-time processing and output for high-definition video streams.
- **Output Compatibility:** Provides HDMI 1.4 and BNC ports for connection to various display devices.
- **Stunning UHD:** Supports 4K UHD decoding output, delivering enhanced image detail and improving the visual quality for both video security and video playback scenarios.

1.2 First-Time Configuration Process

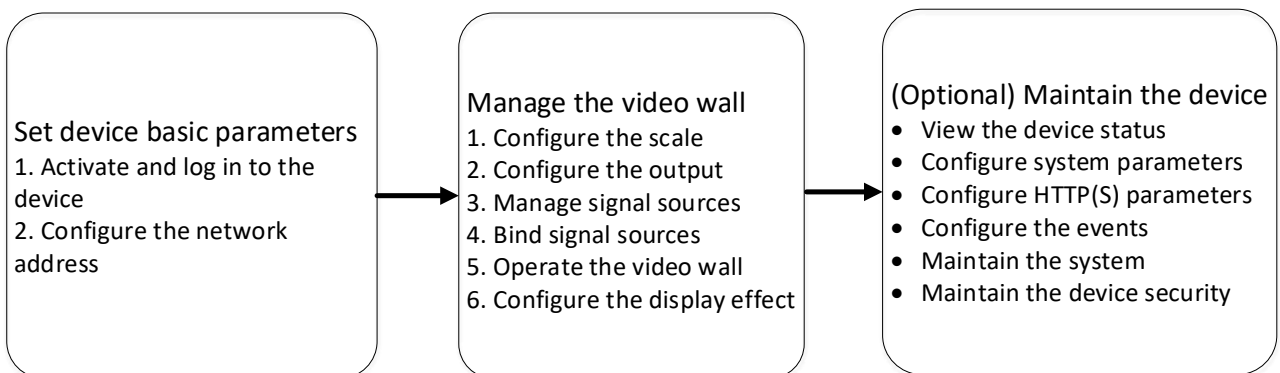


Figure 1-1 First-Time Configuration Process

Chapter 2 Device Basic Settings

2.1 Activate and Log In to Device

You should activate the device before using the device for the first time. You can use the SADP client or the device web page to activate the device. When activating the device, obey the following requirements to set the password:

- To improve system security, it is highly recommended to change password regularly. In order to protect your privacy and corporate data and avoid network security issues, it is recommended to set strong password that meets security requirements.
- Password should contain 8 to 16 characters and at least 2 of the following types: digits, lowercase letters, uppercase letters, and special characters.
- Password cannot contain user name, 123, admin (case insensitive), 4 or more continuously ascending or descending digits, or 4 or more consecutive repeated characters.

Use SADP Client and Web Page

Step 1 Connect the device and computer to the same LAN. Make sure that the device and computer are in the same network segment.

Step 2 Download the [SADP client](#) from the Hikvision website and install it on the computer.

Step 3 Open the SADP client.

Step 4 Select the device that is not activated, enter the activation password and confirm it, and click **Activate**.

If the device cannot be found, you can restart the SADP client.

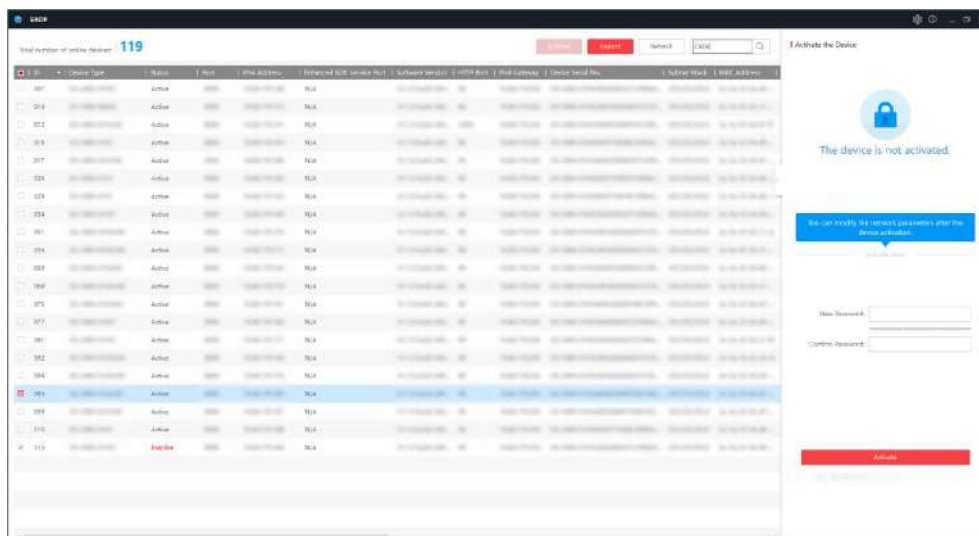


Figure 2-1 Activate the Device via SADP Client

Step 5 View the device IP address in the SADP client and enter the device IP address in the computer browser.

Step 6 Enter the user name and the set activation password, and then click **Log In**.

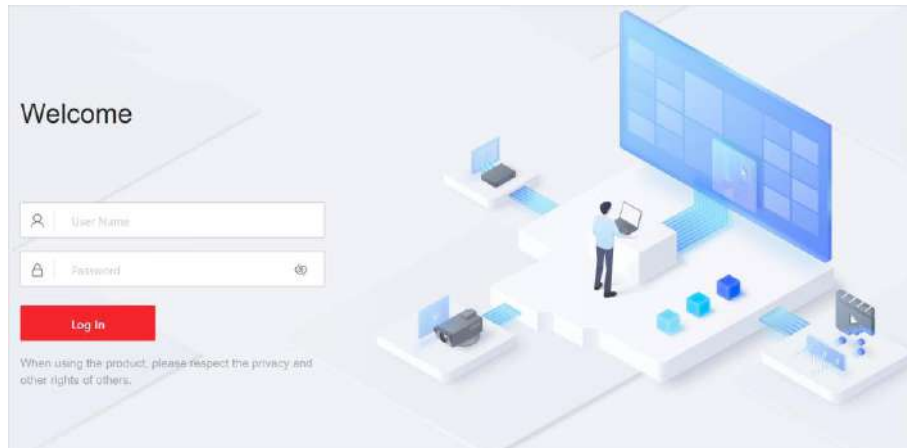


Figure 2-2 Login Page

Step 7 (Optional) To edit the password, you can click the user name in the upper right corner of the web page and then click **Change Password**.

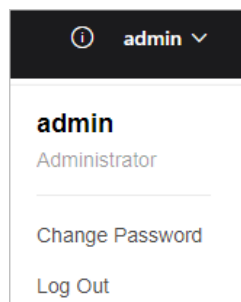


Figure 2-3 Change Password

Use Web Page

Step 1 Use a network cable to connect a computer to the device.

Step 2 Set the computer IP address to any IP address in the range of 192.0.0.2 to 192.0.0.253 (excluding 192.0.0.64) and set the computer gateway address to 192.0.0.1.

By default, the device IP address is 192.0.0.64 and the gateway address is 192.0.0.1.

Step 3 Enter 192.0.0.64 in the computer browser to enter the device activation page.

Step 4 Set the activation password, and then click **Activate**.

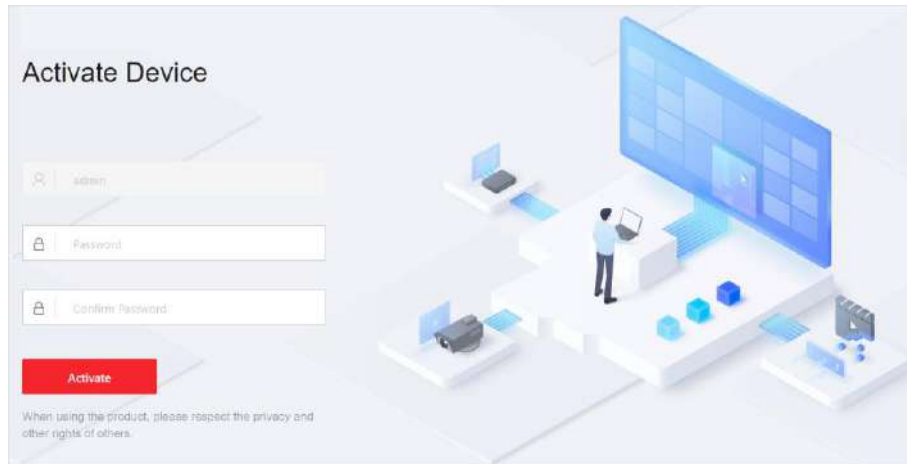


Figure 2-4 Activate the Device via Browser

Step 5 Enter the user name and the set activation password on the login page, and then click **Log In**.

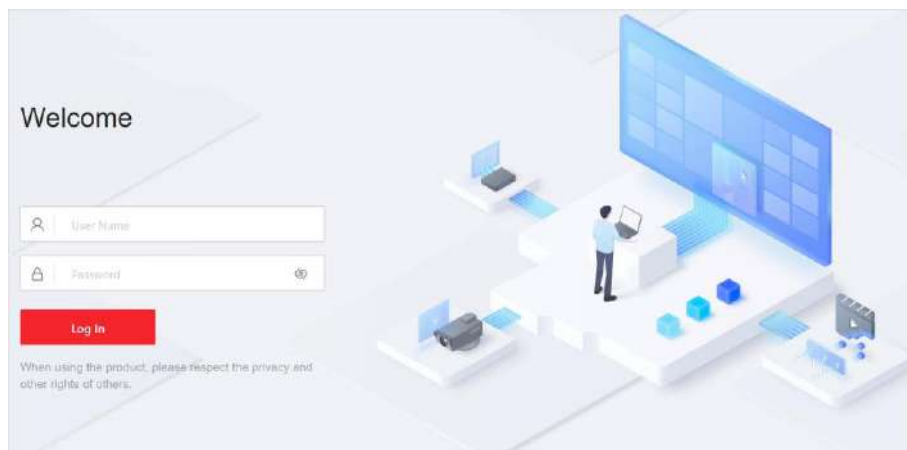


Figure 2-5 Login Page

Step 6 (Optional) To edit the password, you can click the user name in the upper right corner of the web page and then click **Change Password**.

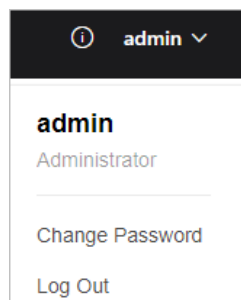


Figure 2-6 Change Password

2.2 Configure the Network Address

2.2.1 Configure TCP/IP

Before You Start

Make sure the device and the computer are in the same segment after the device connects to the on-site network.

Steps

Step 1 Go to **Configuration** → **Network** → **Network Configuration** → **TCP/IP**.

The screenshot shows the TCP/IP configuration page. At the top, there's a red header 'TCP/IP'. Below it, the 'NIC Type/NIC' is set to '10/100/1000 Mbps Self-Adaption'. The IPv4 section has three required fields: *IPv4 Address, *IPv4 Subnet Mask, and *IPv4 Default Gateway. The IPv6 section has a radio button for 'Manual' selected, with three required fields: *IPv6 Address, *IPv6 Subnet Prefix Length, and *IPv6 Default Gateway. The DNS Server Settings section has two required fields: *Preferred DNS Server and *Alternative DNS Server. A red 'Save' button is at the bottom.

Figure 2-7 Configure TCP/IP Parameters

Step 2 Set the IPv4 address, subnet mask, and gateway.

Step 3 Set the IPv6 parameters:

- Select **Manual**, and then enter the IPv6 address, subnet prefix length, and gateway.
- Select **Auto Obtain**.

Step 4 Set the preferred and alternative DNS server.

Step 5 Click **Save**.

Step 6 Remove the network cable that connects the device and computer, and use the network cable to connect the device to the on-site network.

Step 7 Enter the configured device IP address in the web browser of the computer to log in to the web page of the device.

Chapter 3 Video Wall Management

3.1 Configure the Video Wall

3.1.1 Configure the Video Wall Scale

Step 1 Go to **Video Wall Configuration**, and then click **Edit Video Wall Scale**.

You can click **Edit Name** to change the video wall name.

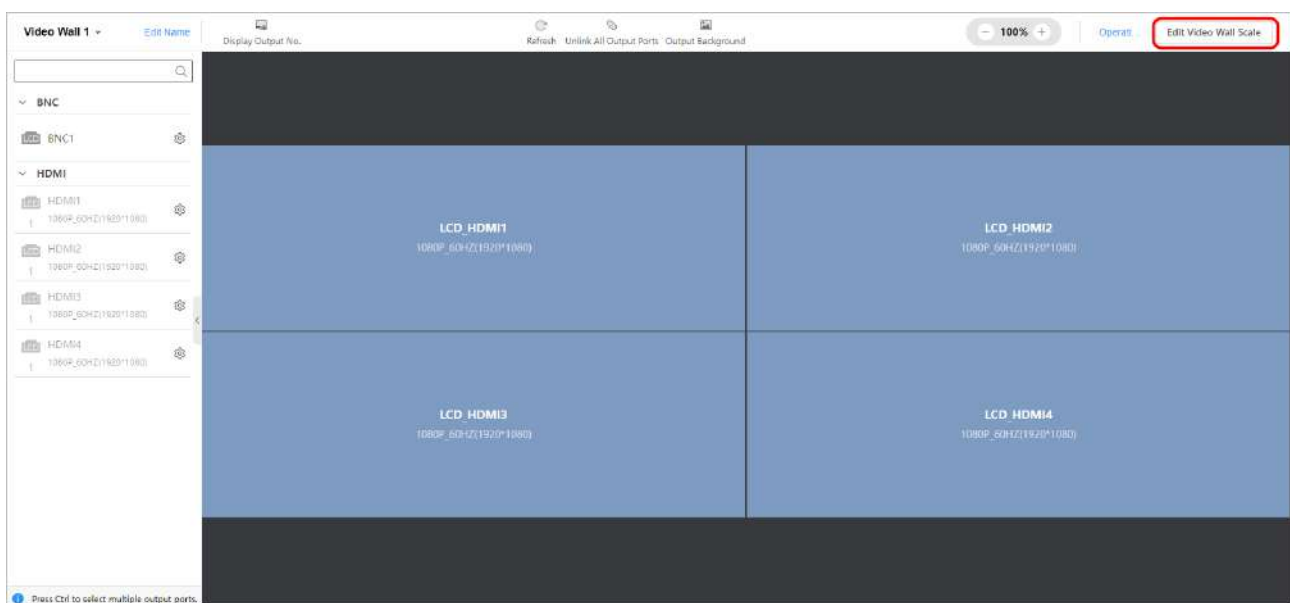


Figure 3-1 Video Wall Configuration Page

Step 2 According to the actual screen quantity, directly enter the number of rows and columns, or select the area with the mouse, and click **Save**.

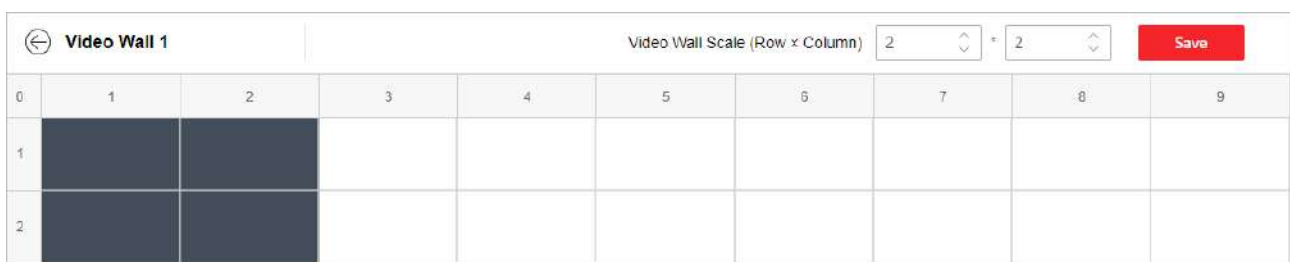


Figure 3-2 Set the Video Wall Scale

3.1.2 Configure the Output

Configure Output Port

On the **Video Wall Configuration** page, click  of an output port. According to the screen type, configure the output port and then click **Save**.

- Click  of a BNC port to select the video standard for the LCD screen.

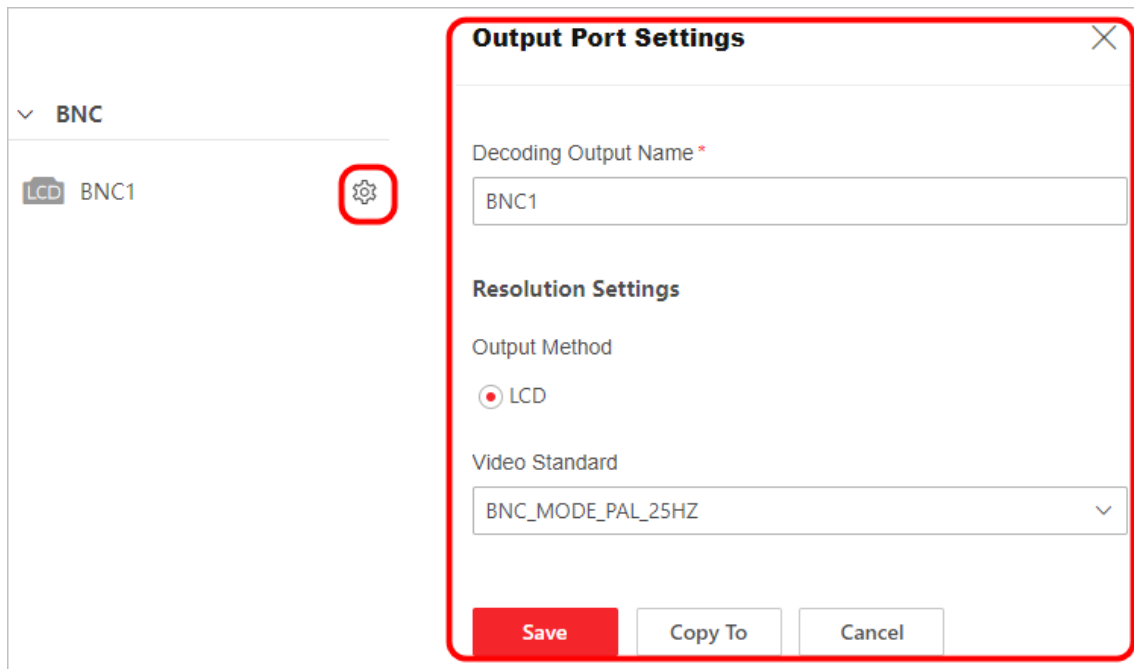


Figure 3-3 Configure a BNC port

- Click  of an HDMI port to configure its parameters:
 - The DVI mode has better compatibility and the HDMI mode supports embedded audio output. If you select AUTO, the output mode of the device output port will automatically adapt to the output mode supported by the screen.
 - If you select LCD output method, select the LCD screen resolution as required.
 - If you select LED output method, enter the width and height of the LED screen.
 - If you select the loading mode, make sure that the configured resolution (width × height) is smaller than 2.6 MP.
 - If you select the clipping mode, make sure that the configured resolution is smaller than the reference resolution that is shown when you select the LCD output method.

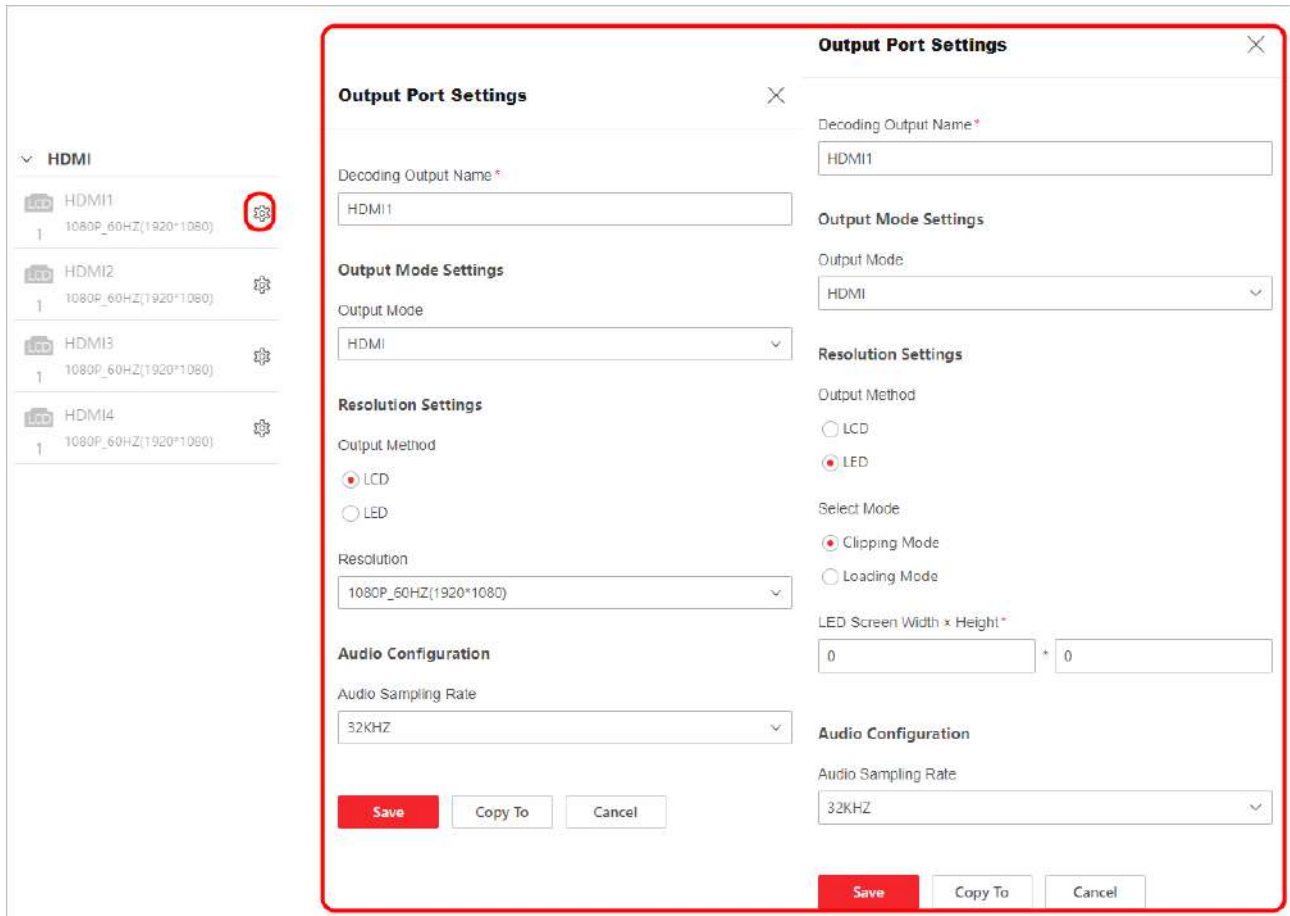


Figure 3-4 Configure an HDMI Port

- Click **Copy To** to copy the current output configuration to other output ports.

Bind Output Ports with Video Wall

Step 1 Click **Display Output No..**

Step 2 According to the output number shown on the actual screen, drag the corresponding output ports to the screens of the video wall.

- To batch bind output ports with the video wall, press Ctrl to select multiple output ports and drag the output ports to the screens of the video wall.
- To cancel the linkage between a screen and an output port, click  in the upper right corner of the screen.
- To cancel the linkage between all screens and output ports, click **Unlink All Output Ports**.

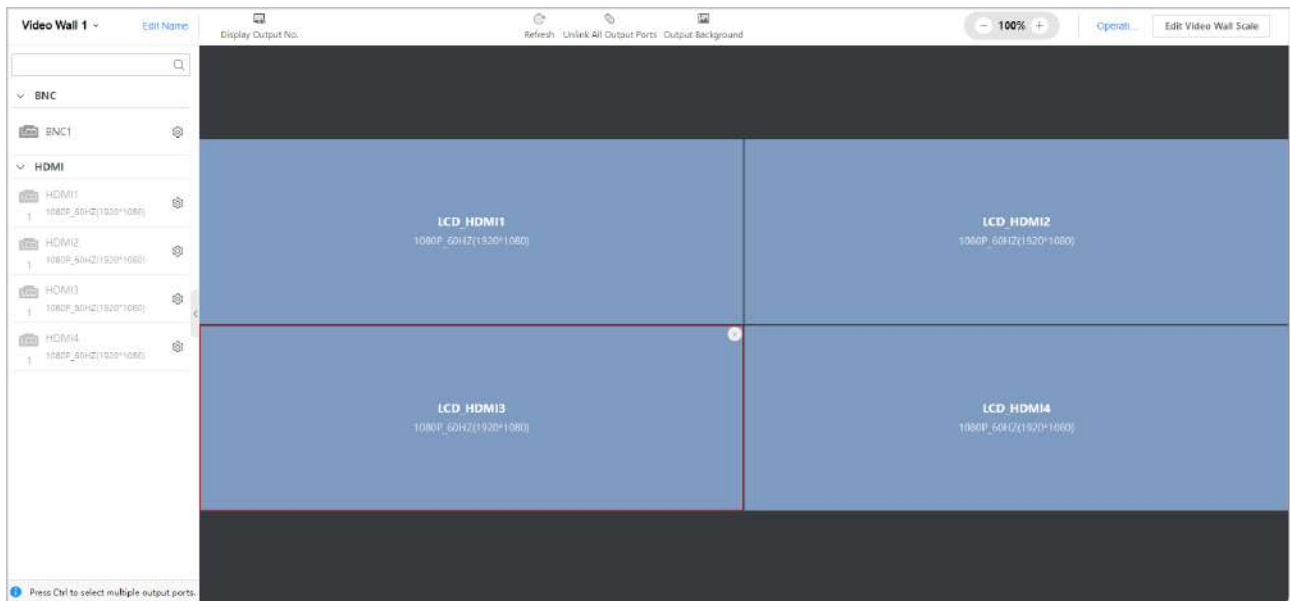


Figure 3-5 Bind Output Ports with Video Wall

Step 3 (Optional) If the screens that are used to configure the video wall support control linkage function, you can perform the following operations to automatically bind output ports to the screens of the video wall.

- 1) Make sure all screens are enabled with the control linkage function.
- 2) Use the remote control to set the location information for all actual screens.
- 3) Click **Edit Wall Scale** and select **Auto Configure**.

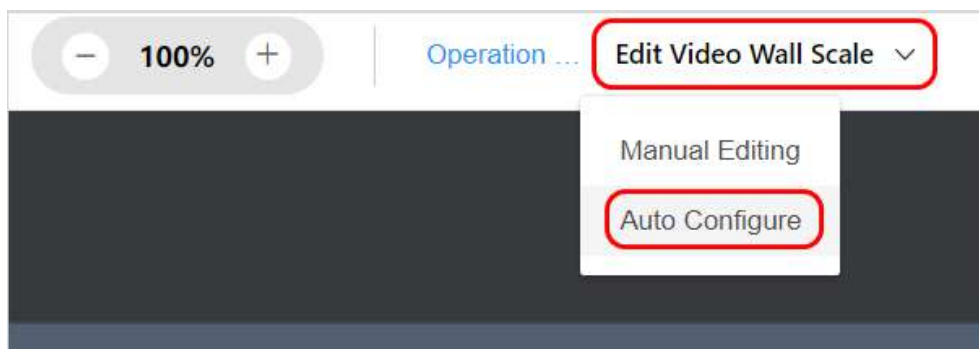


Figure 3-6 Auto Bind Output Ports with Screens

Configure Output Background

At the top of the **Video Wall Configuration** page, click **Output Background** to edit the background color or import images.

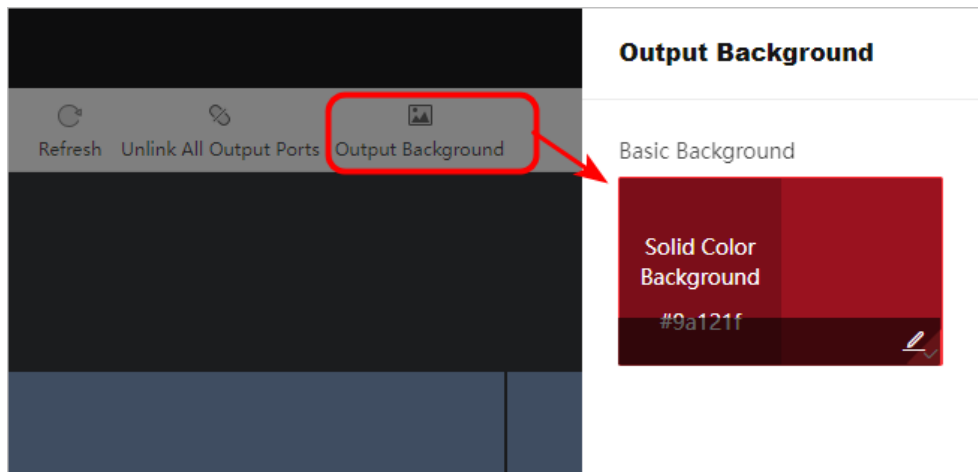


Figure 3-7 Edit Output Background

3.1.3 Manage Signal Sources

Add a Network Signal Source via IP Address

Step 1 Go to **Video Wall Operation** → **Source**, click , and select **IP Address**.

Step 2 Enter the signal source information and stream media information.

- (Optional) Enable **Encrypted Stream** and enter the secret key.
- Select an added group or click **Add Group** to create a new group.
- Click **More** to select the transmission protocol, stream type, encrypted stream, device manufacturer, and streaming media information.

After enabling **Get Stream via Streaming Server**, you can perform live view data forwarding through the streaming server to reduce network stress.

Step 3 Click **Save**.

Add Signal Source

Transmission Protocol: TCP

Stream Type: Main Stream

Encrypted Stream: ☐

Device Manufacturer: HIKVISION

Get Stream via Streaming Server: ☐

Stream Media IP Address:

Port No.:

Save Cancel

Figure 3-8 Add a Network Signal Source via IP Address

Add a Network Signal Source via DDNS

Before you start

Before adding network signal sources via DDNS, you should configure DNS servers on the **TCP/IP** page.

Steps

Step 1 Go to **Video Wall Operation** → **Signal Source**, click , and select **DDNS**.

Step 2 Enter the signal source information and stream media information.

- (Optional) Enable **Encrypted Stream** and enter the secret key.
- Select an added group or click **Add Group** to create a new group.
- Click **More** to select the transmission protocol, stream type, device manufacturer, and streaming media information.

After enabling **Get Stream via Streaming Server**, you can perform live view data forwarding through the streaming server to reduce network stress.

Step 3 Click **Save**.

The screenshot shows the 'Add Signal Source' dialog box with the 'DDNS' tab selected. The dialog is divided into two main sections. The left section contains fields for 'Device Name *', 'Host IP Address *', 'Port No. *', 'User Name *', 'Password *' (with a copy icon), and a 'Group *' section with an '+ Add Group' button and two input fields containing '0' and '1'. Below these are two buttons labeled 'onvif' and 'test'. The right section, titled 'More', contains a 'Transmission Protocol' dropdown set to 'TCP', a 'Stream Type' dropdown set to 'Main Stream', an 'Encrypted Stream' toggle switch, a 'Device Manufacturer' dropdown set to 'HIKVISION', a 'Get Stream via Streaming Server' toggle switch, a 'Stream Media IP Address' field, a 'Port No.' field, and another 'Transmission Protocol' dropdown set to 'TCP'. At the bottom right are 'Save' and 'Cancel' buttons.

Figure 3-9 Add a Network Signal Source via DDNS

Add a Network Signal Source via URL

Step 1 Go to **Video Wall Operation** → **Source**, click , and select **URL**.

Step 2 Enter the device name and the URL.

Step 3 (Optional) Enable **Encrypted Stream** and enter the secret key.

Step 4 Select an added group or click **Add Group** to create a new group.

Step 5 Click **Save**.

Add Signal Source [X]

IP Address DDNS **URL**

Device Name *

URL *

Encrypted Stream ☐

Group *

+ Add Group 0 1

onvif test

Save Cancel

Figure 3-10 Add a Network Signal Source via URL

Batch Delete Network Signal Sources

To batch delete invalid network signal sources, you can select multiple network signal sources with Ctrl or Shift pressed and then click .

3.1.4 Bind Signal Sources with the Video Wall

Note

You can bind a maximum of 1-channel 4K local signal source to the video wall.

Go to **Video Wall Operation**, take either of the following methods to bind signal sources with the video wall:

- Select a signal source and then drag it rightward to the video wall.
 - If you bind a signal source to an LCD video wall, the signal source window fully covers a single screen by default.
 - If you bind a signal source to an LED video wall, the signal source window fully covers the LED video wall by default.

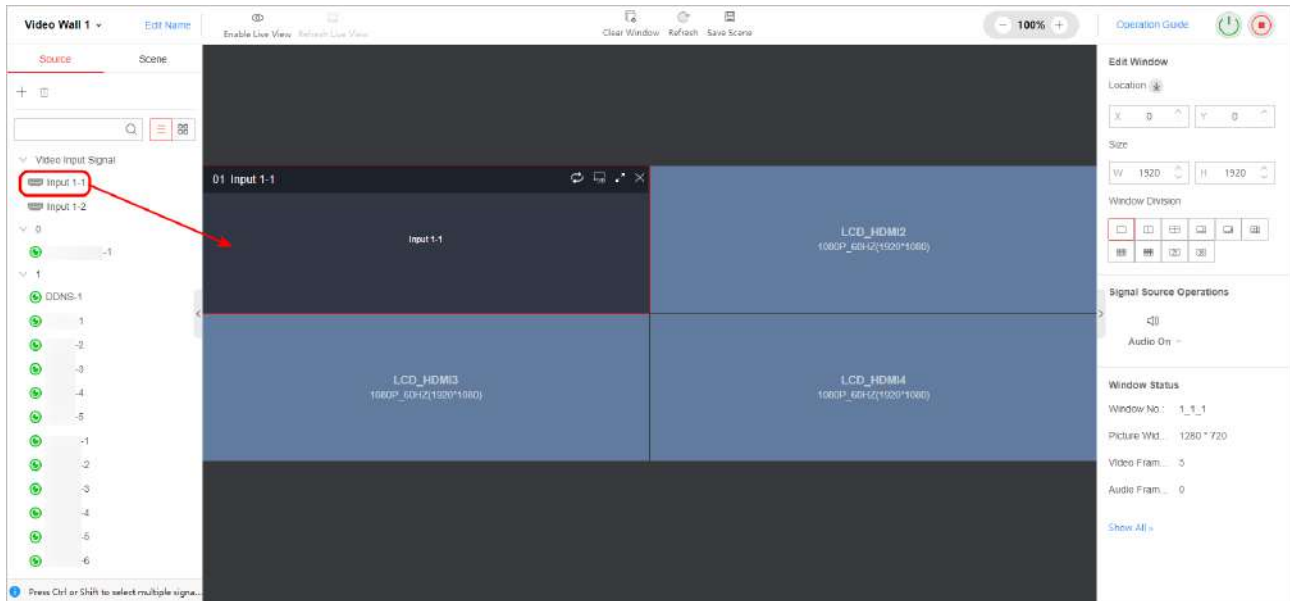


Figure 3-11 Bind a Signal Source to LCD Video Wall

- Choose either of the following methods to batch bind signal sources to the video wall:
 - Drag the video input signal group or a newly created network signal source group rightward to the video wall. The local signal sources join the video input signal group by default.
 - Press Ctrl to select multiple signal sources of the same group, and drag signal sources rightward to the video wall.

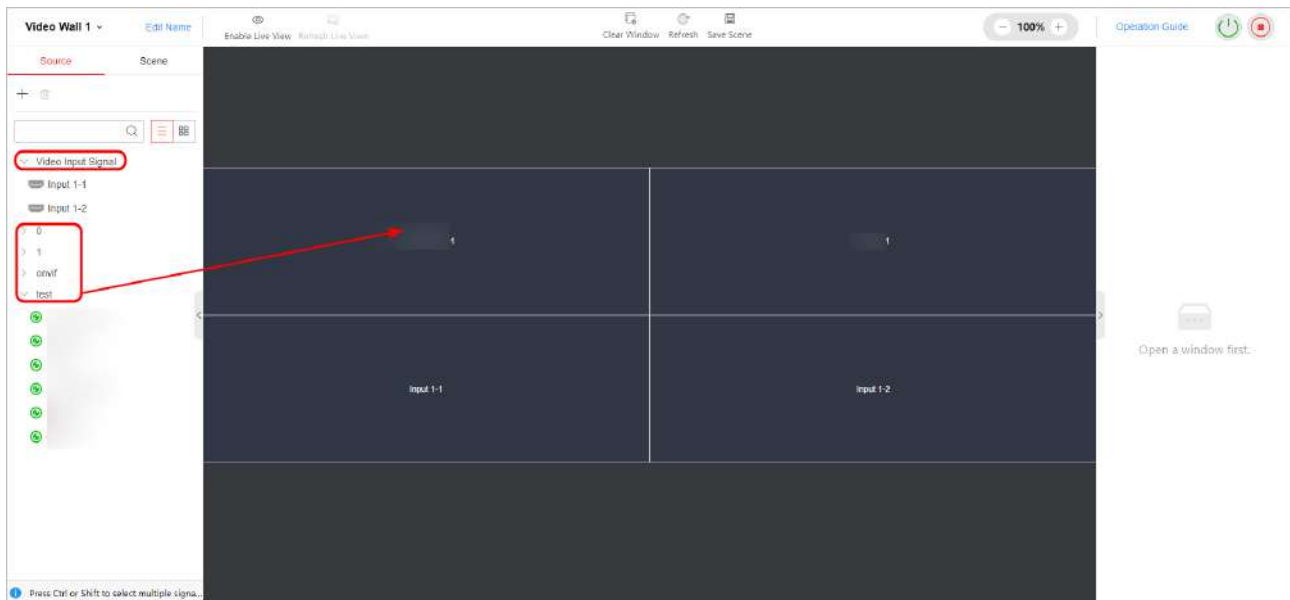


Figure 3-12 Batch Bind Signal Sources to Video Wall

3.2 Operate the Video Wall

3.2.1 Edit Signal Source Window Parameters

Edit a Signal Source Window

On the **Video Wall Operation** page, select a signal source window and perform the following operations as required:

- Adjust the window position: Move the window directly or enter the specific X and Y values.
- Divide the window: Click a window division icon.
- Adjust the window size:
 - Drag the window edge to adjust its size.
 - Enter W and H values.
 - Click  in the upper right corner of the window to make it fully cover the occupied output ports and click  to restore the original size.
- Set the window to the bottom: Click .

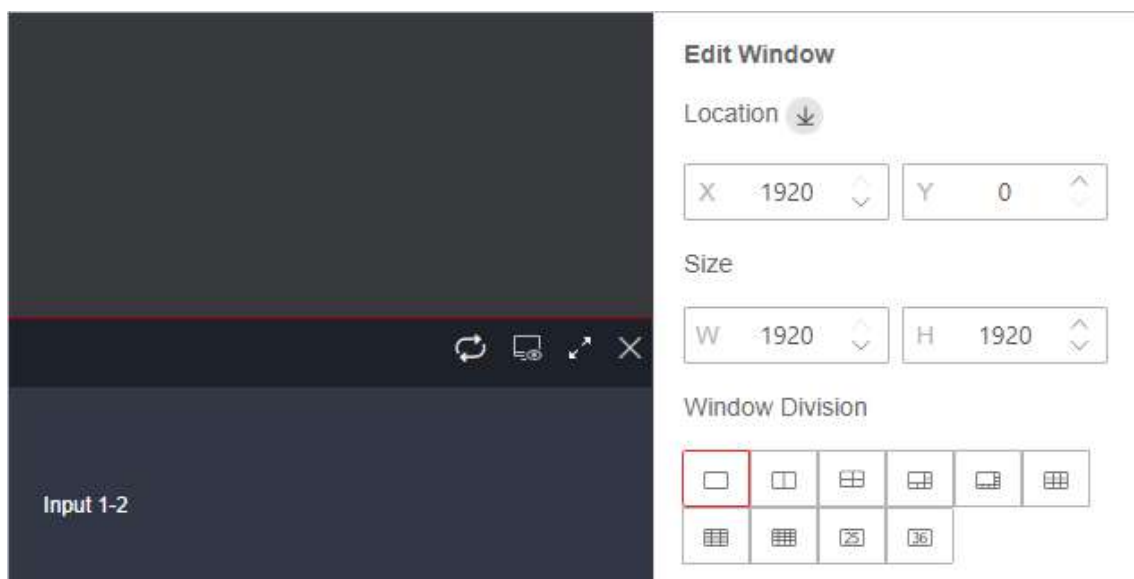


Figure 3-13 Adjust Position of a Signal Source Window

- Enable audio for a signal source window.
 - Select a local signal source, click **Audio On** and select an audio output port to enable the audio for the local signal source.

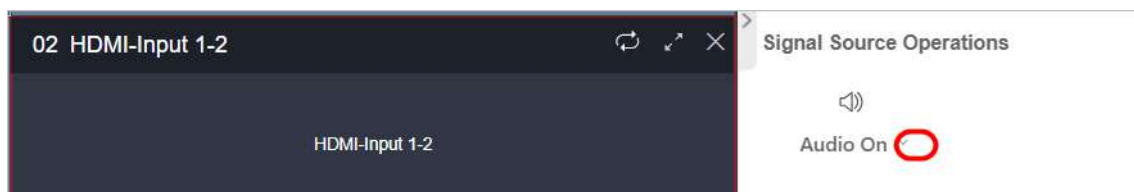


Figure 3-14 Configure Audio for Local Signal Source

- Select a network signal source to configure its decoding status, audio status, decoding delay, smart decoding, and stream exporting.
 - After you enable Websocket, you can export stream.
 - After you enable smart decoding, the device can decode the smart alarm events from the network cameras.

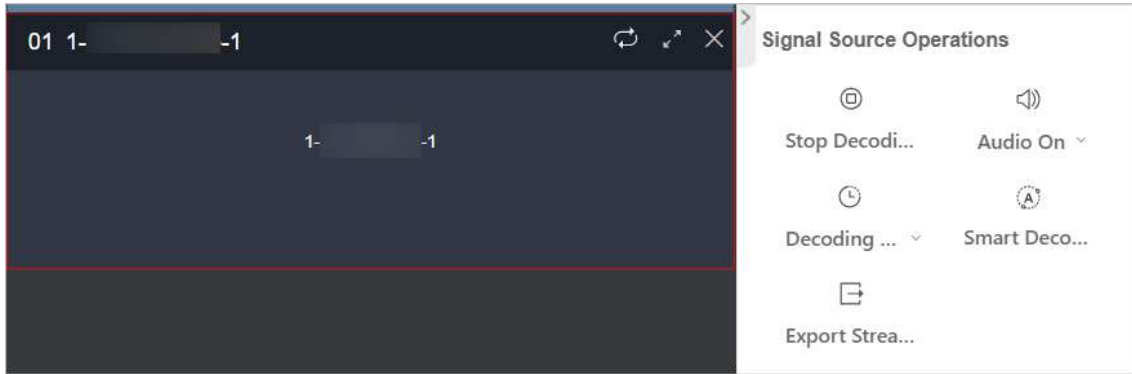


Figure 3-15 Configure Audio for Network Signal Source

- Set the signal source group auto-switching: Click  in the upper right corner of the signal source window, select a signal source group, set the image interval, and then click **Start Auto-Switch**.

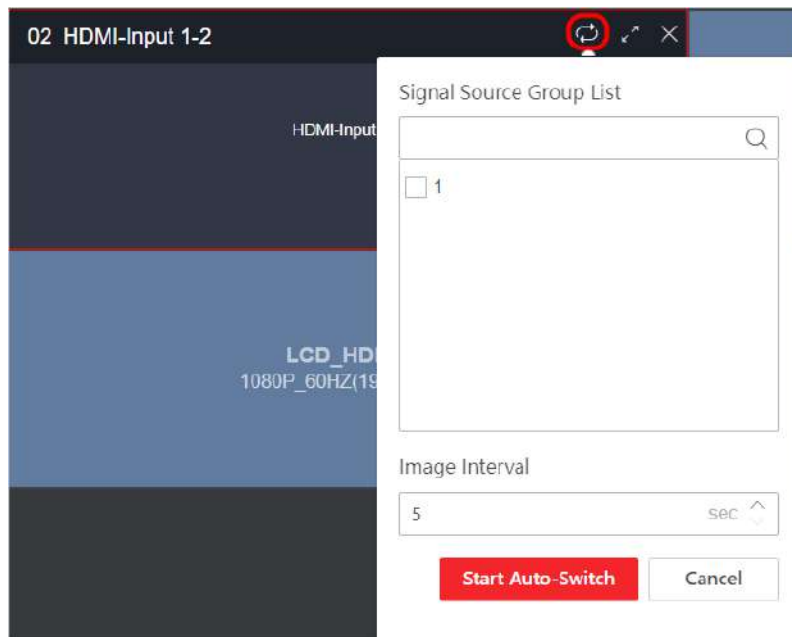


Figure 3-16 Set Signal Source Group Auto-Switching

- View the window status: You can click **Show All** to view the decoding status list.

Edit Multiple Signal Source Windows

On the **Video Wall Operation** page, perform the following operations as required:

- Preview the signal sources:

- Click  in the upper right corner of a signal source window to preview the signal source. Click  to cancel the live view.
- Click **Enable Live View** at the top of the **Video Wall Operation** page to preview all signal sources on the video wall. Click **Close Live View** to stop previewing all signal sources on the video wall.
- Click **Refresh Live View** at the top of the **Video Wall Operation** page to refresh the live view of all signal sources.

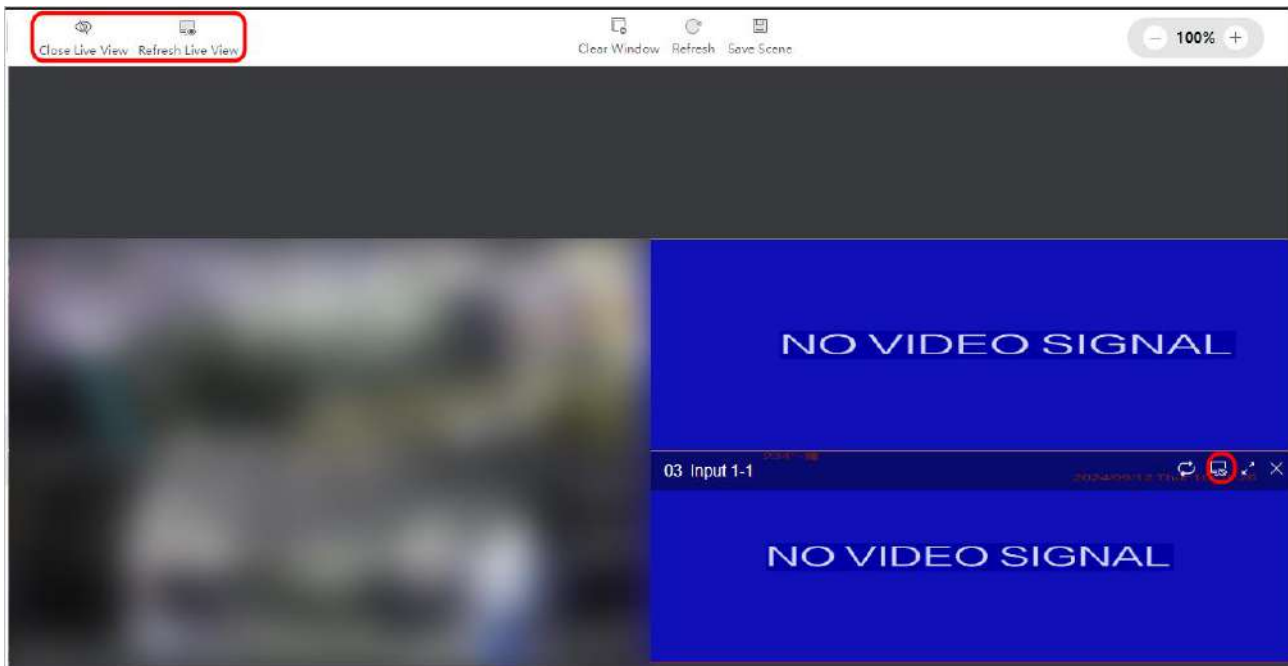


Figure 3-17 Preview Signal Source

- Power on or off all screens: Click  or .
- Clear all bound signal source windows: Click **Clear Window**.

3.2.2 Manage Scenes

Up to 64 scenes are supported. Go to **Video Wall Operation** to manage scenes.

- Click **Save Scene** to save the configuration as a new scene or overwrite the existing scene.

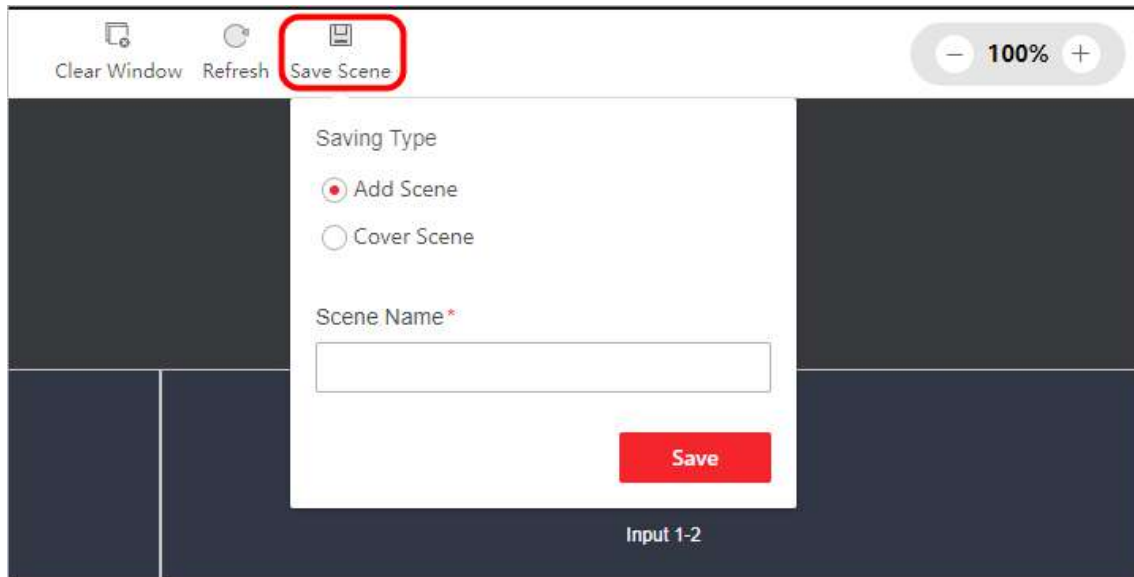


Figure 3-18 Save Scene

- Click **Scene** and hover over a scene name. Click  to call the scene.
- Click **Scene** and hover over a scene name. Click  to edit the scene name.
- Click **Scene** and hover over a scene name. Click  to delete the scene.

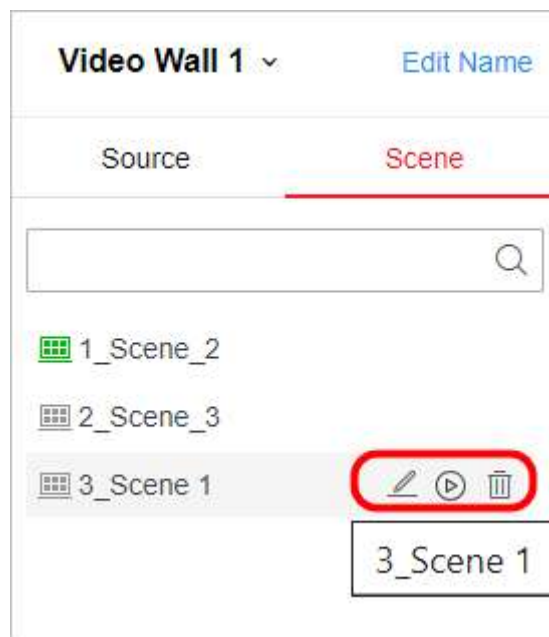
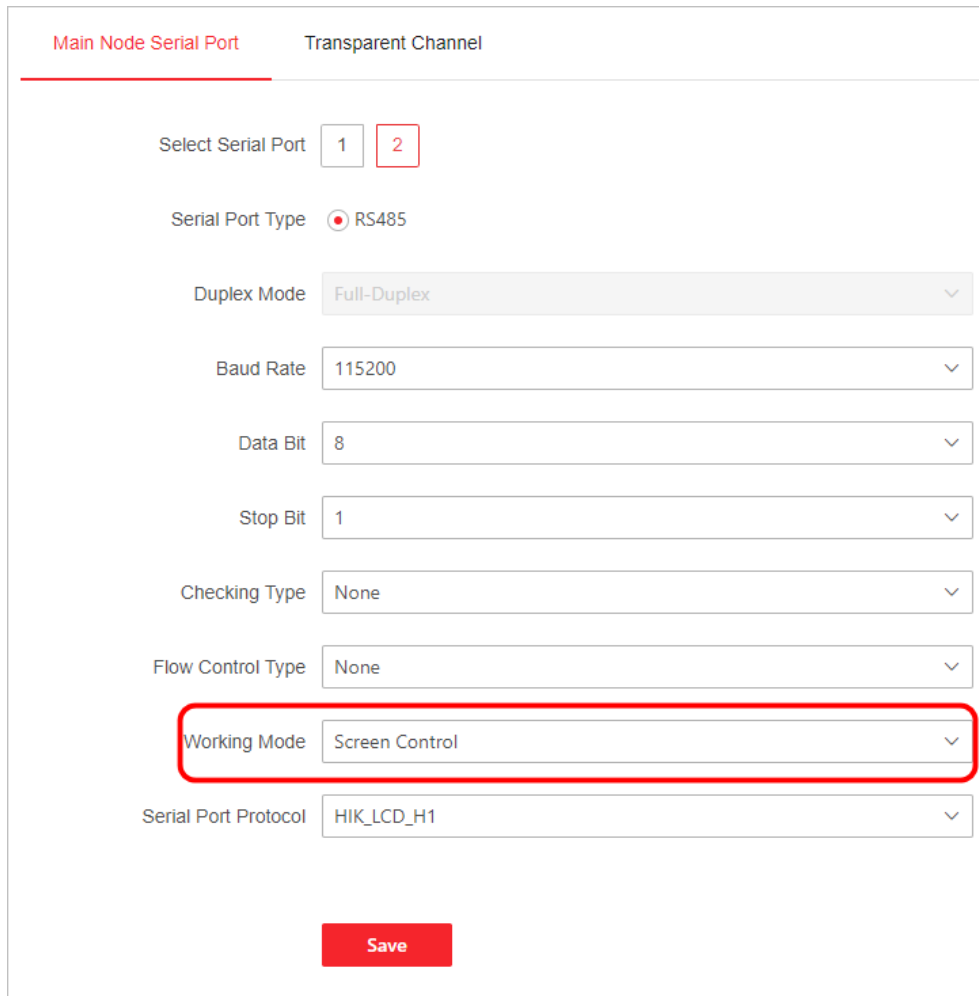


Figure 3-19 Manage Scene

3.2.3 Maintain Screens

Control Screen via Serial Port

Step 1 Go to **Configuration** → **System** → **Serial Port Settings** → **Main Node Serial Port**, select serial port 2, select **Screen Control** as the working mode, set the baud rate of the device same as the baud rate of the screen, and set other serial port parameters.



The screenshot displays the 'Main Node Serial Port' configuration window. At the top, there are two tabs: 'Main Node Serial Port' (selected) and 'Transparent Channel'. Below the tabs, the following settings are visible:

- Select Serial Port:** Two buttons, '1' and '2'. Button '2' is highlighted with a red border.
- Serial Port Type:** A radio button selection with 'RS485' selected.
- Duplex Mode:** A dropdown menu set to 'Full-Duplex'.
- Baud Rate:** A dropdown menu set to '115200'.
- Data Bit:** A dropdown menu set to '8'.
- Stop Bit:** A dropdown menu set to '1'.
- Checking Type:** A dropdown menu set to 'None'.
- Flow Control Type:** A dropdown menu set to 'None'.
- Working Mode:** A dropdown menu set to 'Screen Control', which is highlighted with a red rectangular box.
- Serial Port Protocol:** A dropdown menu set to 'HIK_LCD_H1'.

At the bottom center of the form is a red 'Save' button.

Figure 3-20 Configure Serial Port

Step 2 Use a serial port cable to connect a screen and the device RS-485 port.

Step 3 Go to **Screen Maintenance** and select the screen that is connected with the serial port cable.

Step 4 Select an image mode and adjust the backlight.

Step 5 (Optional) Click  to power on the screen or click  to power off the screen.

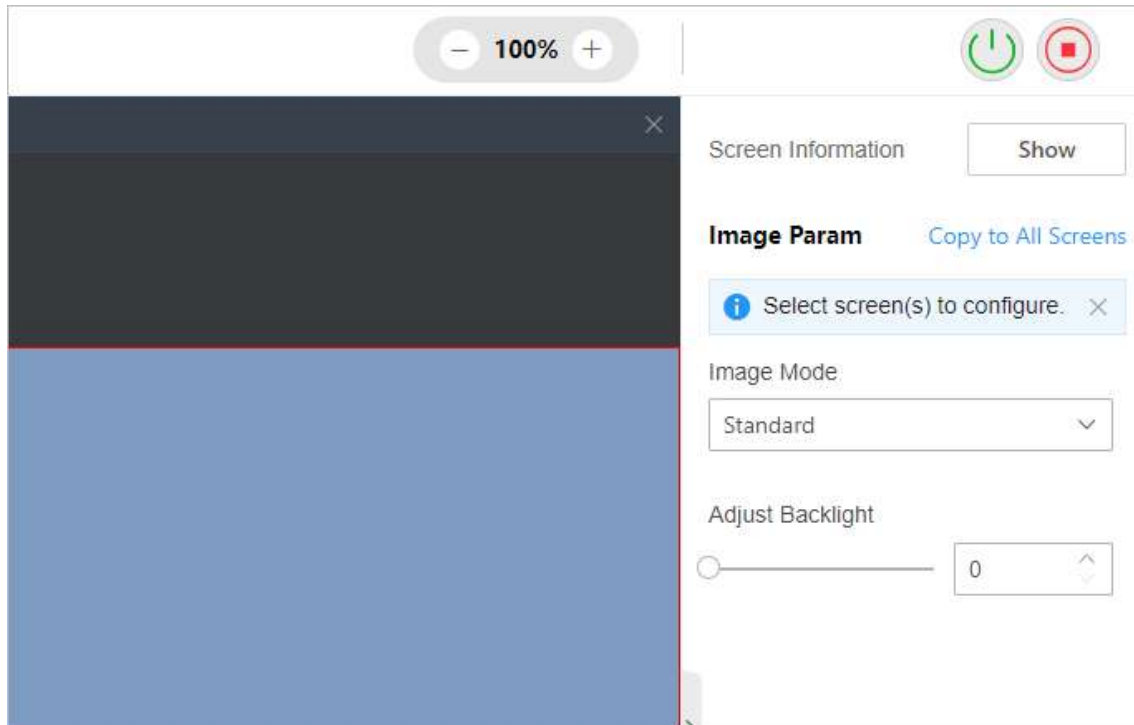


Figure 3-21 Control Screen via Serial Port

Control Screens via HDMI Ports

Step 1 Use multiple HDMI cables to connect the multiple screens to the device. Make sure all connected screens support and are enabled with the control linkage function.

Step 2 Go to **Screen Maintenance** and select a screen.

Step 3 Select an image mode and adjust the backlight.

Step 4 (Optional) You can perform the following operations as required:

- Click **Show** to show the serial number, software version, work duration, and device temperature on all screens.
- Click  or  to power on or off all screens that are connected with the HDMI cables.
- Click **Copy to All Screens** to copy the image parameters of the current screen to all screens.

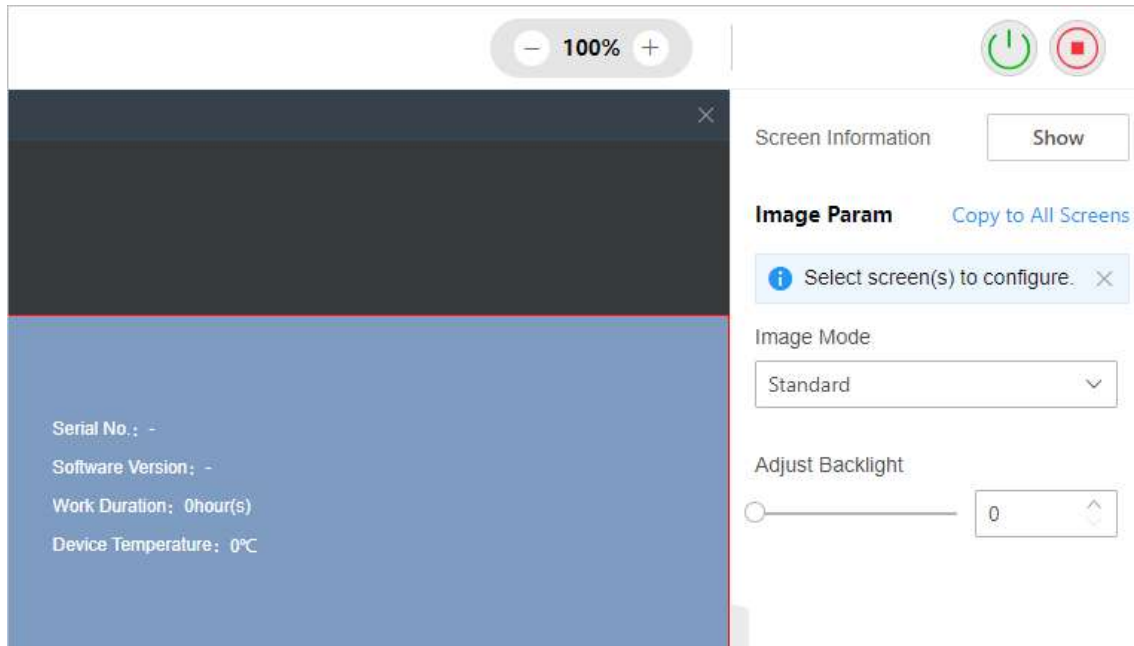


Figure 3-22 Show Screen Information

3.3 Configure Image Effect on Screen

3.3.1 Edit a Signal Source

Edit a Local Signal Source

Go to **Video Wall Operation**, hover over a local signal source and then click  to edit its parameters:

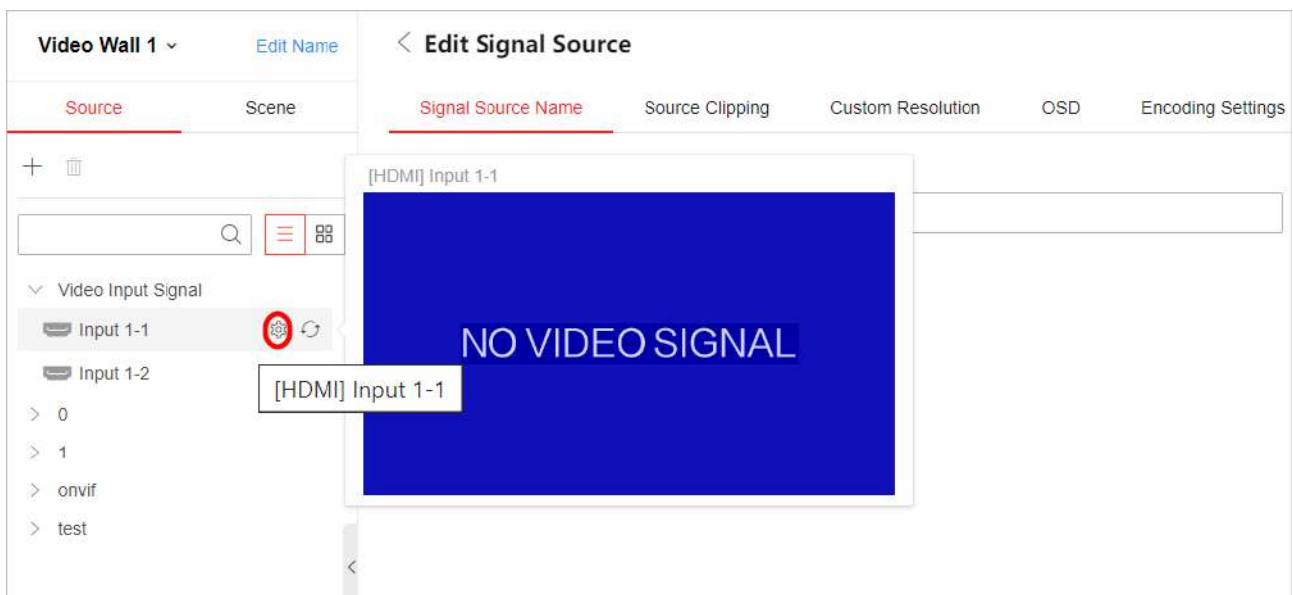


Figure 3-23 Edit a Local Signal Source

- Edit the signal source name.
- Click **Source Clipping**, and set the clipping value at top, bottom, left, and right edges.
The clipping value ranges from 0 to 200. The clipping value at the top and bottom edges should be a multiple of 2, and the clipping value at the left and right edges should be a multiple of 4.



Signal Source Name Input 1-1

Top Edge Clipping 0 Pixel  

Lower Edge Clipping 0 Pixel  

Left Edge Clipping 0 Pixel  

Right Edge Clipping 0 Pixel  

Save

NO VIDEO SIGNAL

Figure 3-24 Clip a Signal Source

- If the resolution of a signal source does not match the resolution of the screen, you can customize the signal source resolution.
 - 1) Click **Custom Resolution**.
 - 2) Enable custom resolution and set the refresh rate and resolution. The width should be a multiple of 4 and the height should be a multiple of 2.
 - 3) (Optional) Click **Copy To** to copy the resolution configuration of the current signal source to other signal sources.
 - 4) Click **Save**.



Signal Source Name Input 1-1

Enable 

*Refresh Rate 30 

*Resolution 1920 * 1080

Save Copy To

NO VIDEO SIGNAL

Figure 3-25 Customize Resolution

- Click **OSD**, and then you can add channel name, date, time, character 1, or character 2 to the input signal image.
 - Set the font size, font color, and font direction.
 - Enter the position values or directly drag the character to adjust the position.
 - Customize the channel name and character content.

- Click **Copy To** to copy the OSD configuration of the current signal source to other signal sources.

Signal Source Name: Input 1-1

Basic Configuration

Font Size: 64

Font Color: #f4a00d

Font Direction: Custom

Channel Name

Enable: ☒

*Name: Input 1-1

*Character Position: 333 + 0

Date and Time

Date: ☒

Date Display Format: YYYY/MM/DD

Time: ☒

Time Format: ☐ 12 Hours ☒ 24 Hours

*Character Position: 1272 + 199

Text Overlay

Character: Character 1 Character 2

Enable: ☒

*Character Content: Welcome

*Font Size: 64

Font Color: #000000

*Character Position: 1409 + 1400

Save **Copy To**

Figure 3-26 Add OSDs

Edit a Network Signal Source

Go to **Video Wall Operation**, hover over a network signal source and then click  to edit its parameters.

Edit Signal Source ✕

Device Name*
-1

IP Address*

Port No.*
8000

User Name*
user

Password*

Group*

+ Add Group	0	1
onvif	test	

More ⬆

Transmission Protocol
TCP

Stream Type
Main Stream

Encrypted Stream
☐

Device Manufacturer
HIKVISION

Channel No.
1

Get Stream via Streaming Server
☐

Stream Media IP Address

Port No.

Transmission Protocol
TCP

Save Copy To Cancel

Figure 3-27 Edit a Network Signal Source

3.3.2 Configure Encoding Parameters

Step 1 Go to **Video Wall Operation**, hover over a local signal source and then click .

Step 2 Click **Encoding Settings**.

Step 3 Set the video encoding parameters.

- Set the bit rate type and maximum bit rate.
 - If you select **Constant Bit Rate**, the device uses the average bit rate for transmission and uses fast compression speed. The video mosaic might occur.
 - If you select **Variable Bit Rate**, the device automatically adjusts the bit rate for transmission as long as the bit rate is within the limit and uses slow compression speed to ensure the image definition in complex scenarios.

- If you select **Variable Bit Rate**, you should select a video quality. The higher video quality, the higher the bandwidth requirement.
- Enter an I-frame interval. The larger the I-frame interval, the smaller the stream fluctuation, and the lower the image quality.
- Select a resolution. The higher resolution, the higher the bandwidth requirement.
- Select an encoding type and video type.

Step 4 Select an audio encoding type.

Step 5 Click **Save**.

The screenshot displays the configuration interface for the UHD Decoder. At the top, the 'Signal Source Name' is set to 'Input 1-1'. The 'Video Encoding' section includes the following settings: 'Stream Type' is set to 'Sub-stream' (radio button selected); 'Bit Rate Type' is set to 'Constant Bit Rate' (radio button selected); 'Video Quality' is set to 'Medium' (dropdown menu); '*I-Frame Interval' is set to '60' (text input); '*Custom Max. Bit Rate' is set to '512' (dropdown menu) with the unit 'kbps'; 'Resolution' is set to '704*576' (dropdown menu); 'Frame Rate' is set to '20' (dropdown menu) with the unit 'fps'; 'Encoding Type' is set to 'H.265' (radio button selected); and 'Video Type' is set to 'Video and Audio Stream' (radio button selected). The 'Audio Encoding' section shows 'Encoding Type' set to 'G.722.1' (dropdown menu). A red 'Save' button is located at the bottom of the form.

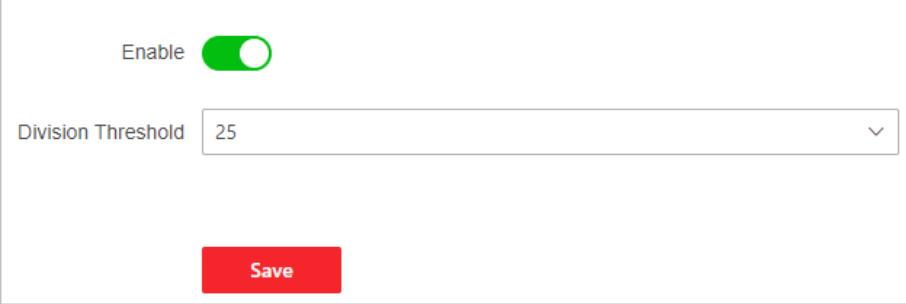
Figure 3-28 Configure Encoding Parameters

3.3.3 Set Other Parameters

Go to **Configuration** → **Other Settings** to set the following parameters:

- Enable **Sub-Stream Auto-Switch** and set the window division threshold.

If the window division reaches the window division threshold, the device will automatically use sub-stream to get the images. In low bandwidth networks, you can use sub-stream to get relatively smooth images with a small bandwidth footprint.

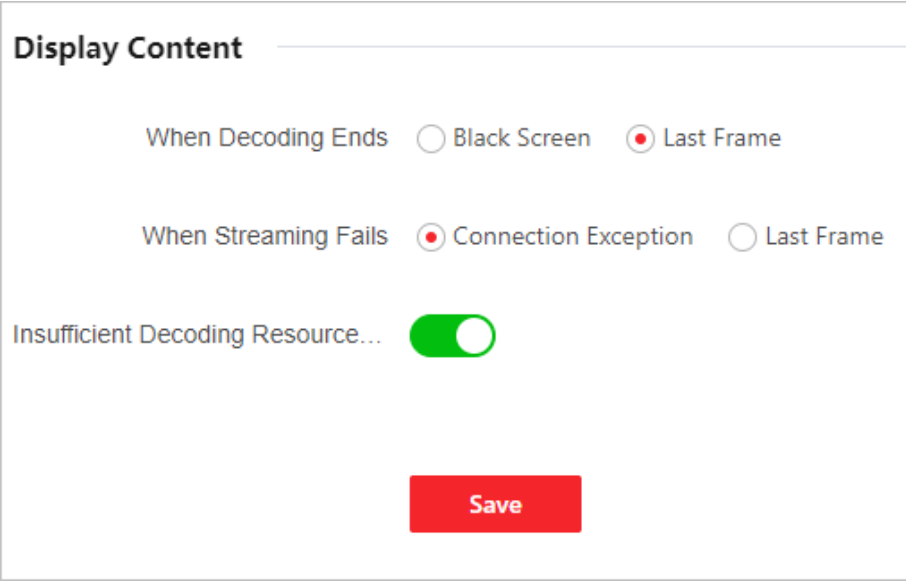


The screenshot shows a settings panel for 'Sub-Stream Auto-Switch'. At the top, there is a toggle switch labeled 'Enable' which is turned on (green). Below it, a 'Division Threshold' is set to '25' in a dropdown menu. At the bottom of the panel is a red 'Save' button.

Figure 3-29 Set Sub-Stream Auto-Switch

- Click **Display Settings** to configure the content displayed when decoding ends, when streaming fails, and when the decoding resource is insufficient.

If you select **Connection Exception**, the specific streaming failure reason will be displayed on the screen.



The screenshot shows a settings panel titled 'Display Content'. It contains three sections: 'When Decoding Ends' with radio buttons for 'Black Screen' and 'Last Frame' (selected); 'When Streaming Fails' with radio buttons for 'Connection Exception' (selected) and 'Last Frame'; and 'Insufficient Decoding Resource...' with a toggle switch that is turned on (green). A red 'Save' button is at the bottom.

Figure 3-30 Set Display Content

- Click **Decoding Delay** and select a default decoding delay level of the device.

Chapter 4 Device Maintenance

4.1 View Device Status

Click **Overview** to view the decoding resource status, network status, device status, and subsystem status.



Figure 4-1 View Device Status

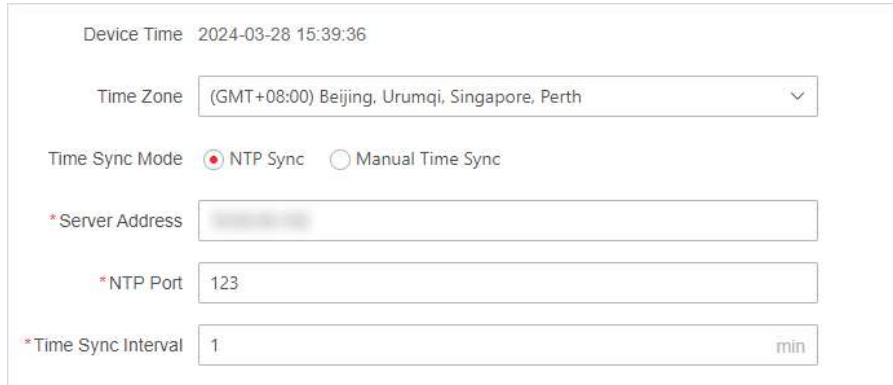
4.2 Configure System Parameters

Go to **Configuration** → **System** to configure the following parameters:

- Go to **System Settings** → **Basic Information** to view the device information and edit the device name as required. You can click **Upgrade** to go to the upgrade page for device upgrade.

Figure 4-2 View Basic Information

- Go to **System Settings** → **Time Settings**, if you select **NTP Sync**, the device clock synchronizes with the clock of the NTP server at the specified interval.
 - Set the address and port number of the NTP server.
 - Set the synchronization interval.



Device Time 2024-03-28 15:39:36

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync Mode ☒ NTP Sync ☐ Manual Time Sync

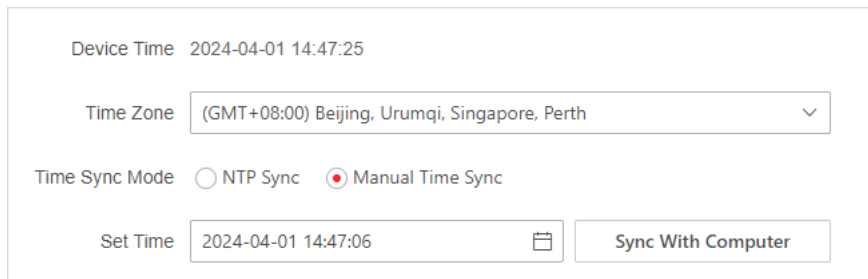
* Server Address

* NTP Port 123

* Time Sync Interval 1 min

Figure 4-3 Select NTP Sync

- On the **Time Settings** page, if you select **Manual Time Sync**, you can click **Sync with Computer** to make the device time same as the computer time.



Device Time 2024-04-01 14:47:25

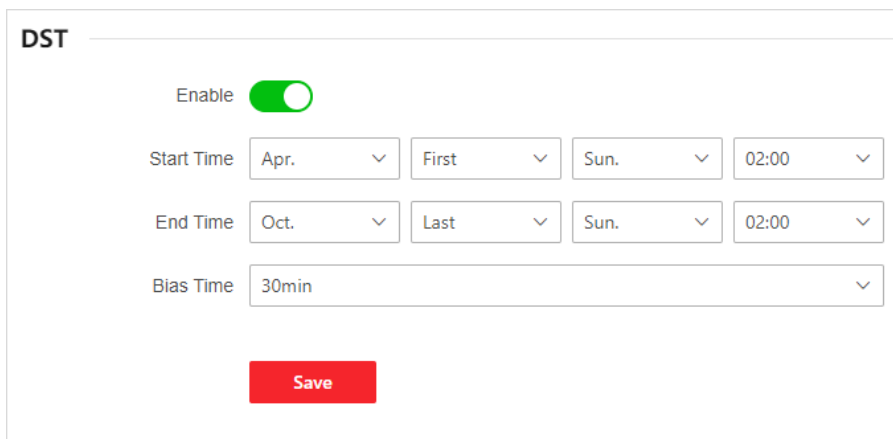
Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync Mode ☐ NTP Sync ☒ Manual Time Sync

Set Time 2024-04-01 14:47:06 Sync With Computer

Figure 4-4 Select Manual Time Sync

- On the **Time Settings** page, if you enable DST (Daylight Saving Time), the device clock is set forward a specified time during the summer months.
 - Set the start time and end time.
 - Set the bias time.



DST

Enable ☒

Start Time Apr. First Sun. 02:00

End Time Oct. Last Sun. 02:00

Bias Time 30min

Save

Figure 4-5 Enable DST

- Go to **User Management** → **User Management** to add users, edit the user name or password, or delete the users. When the user type is administrator, you cannot edit or delete it.

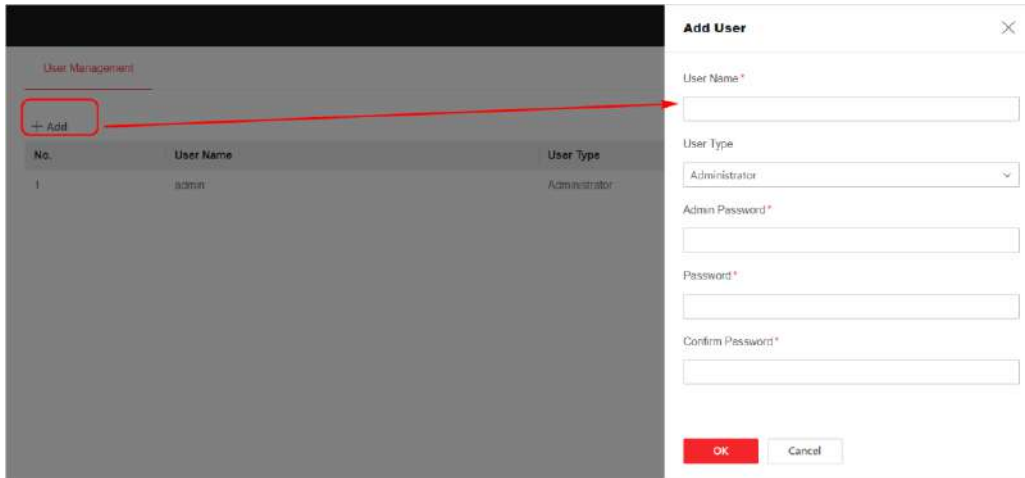


Figure 4-6 Manage Users

Control the Device via Keyboard

- Step 1 Go to **Configuration** → **System** → **Serial Port Settings** → **Main Node Serial Port**, select serial port 2, select **Keyboard Control** as the working mode, set the baud rate of the device same as the baud rate of the keyboard, and set other serial port parameters.

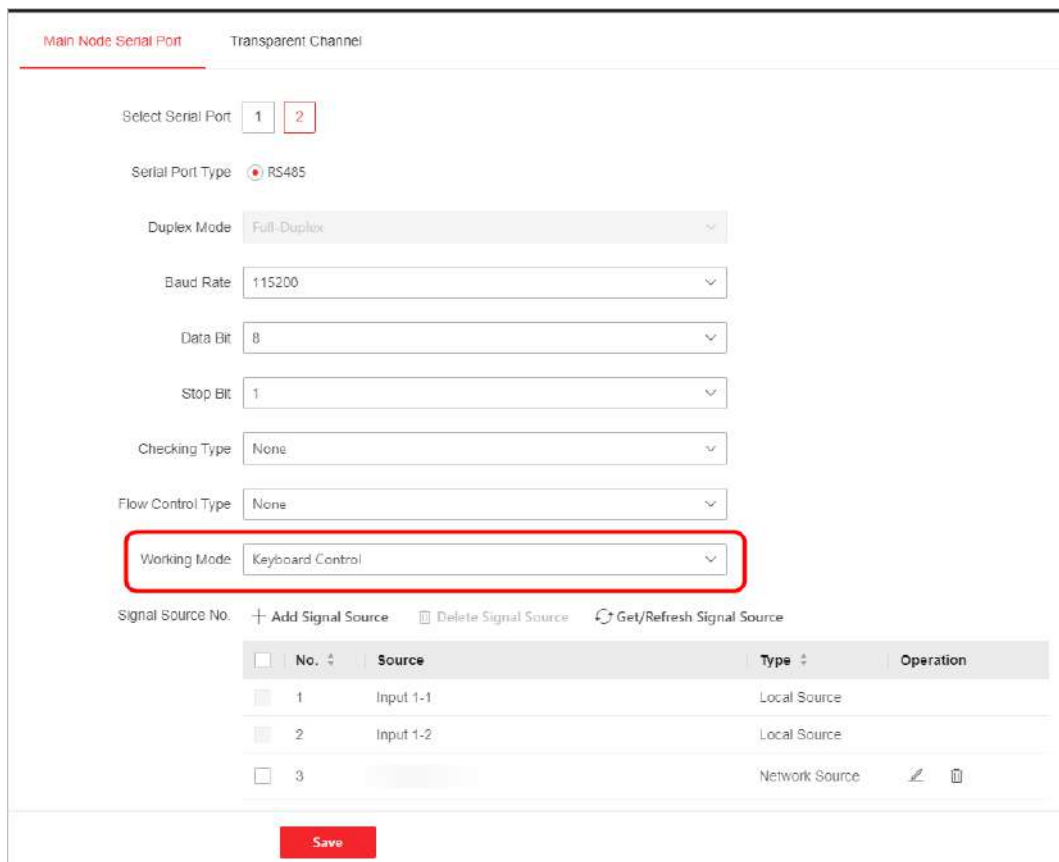


Figure 4-7 Control the Device via Keyboard

Step 2 (Optional) For a serial keyboard, click **Get/Refresh Signal Source** to obtain the local signal sources and click **Add Signal Source** to add the network signal source.

Step 3 Use a serial port cable to connect the keyboard and device.

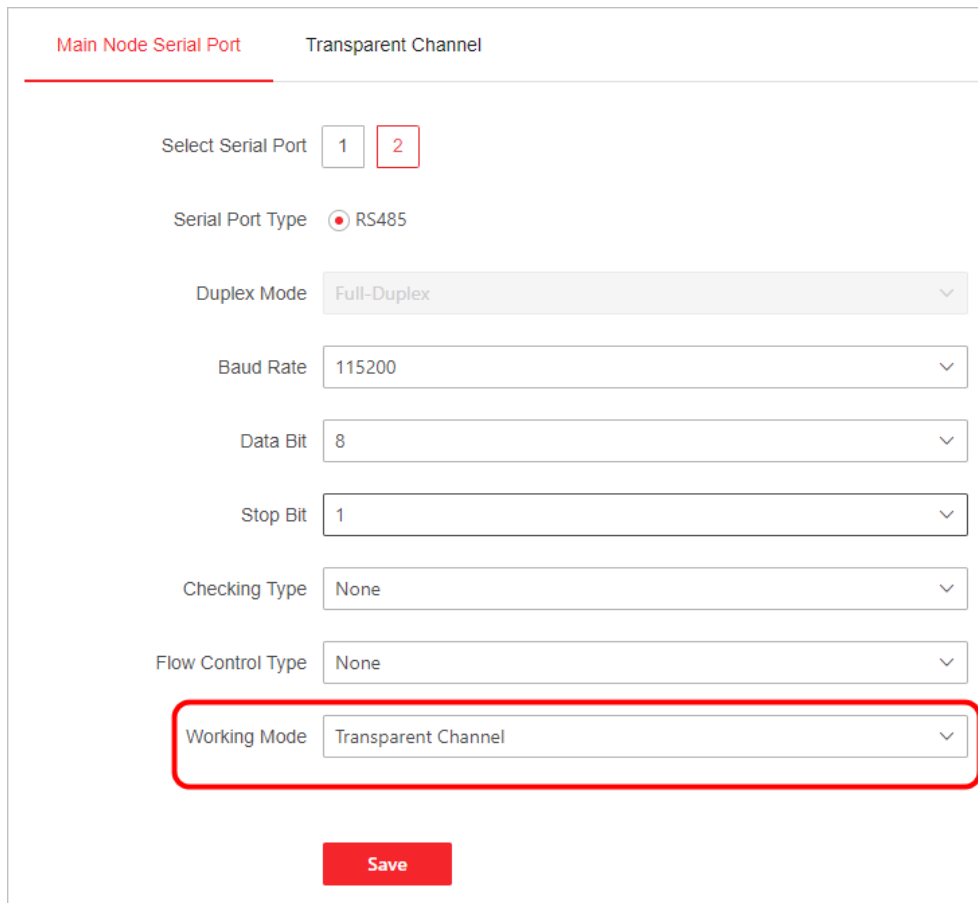
Step 4 Use the serial keyboard to control the device.

Configure Transparent Channel

To directly transmit the signals obtained by the decoder without any compression or modification to the receiving device, configure a transparent channel.

Step 1 Go to **Configuration** → **System** → **Serial Port Settings** → **Main Node Serial Port**, select serial port 2, and select **Transparent Control** as the working mode.

Step 2 Set the baud rate of the device same as the baud rate of the receiving device, set other serial port parameters, and click **Save**.

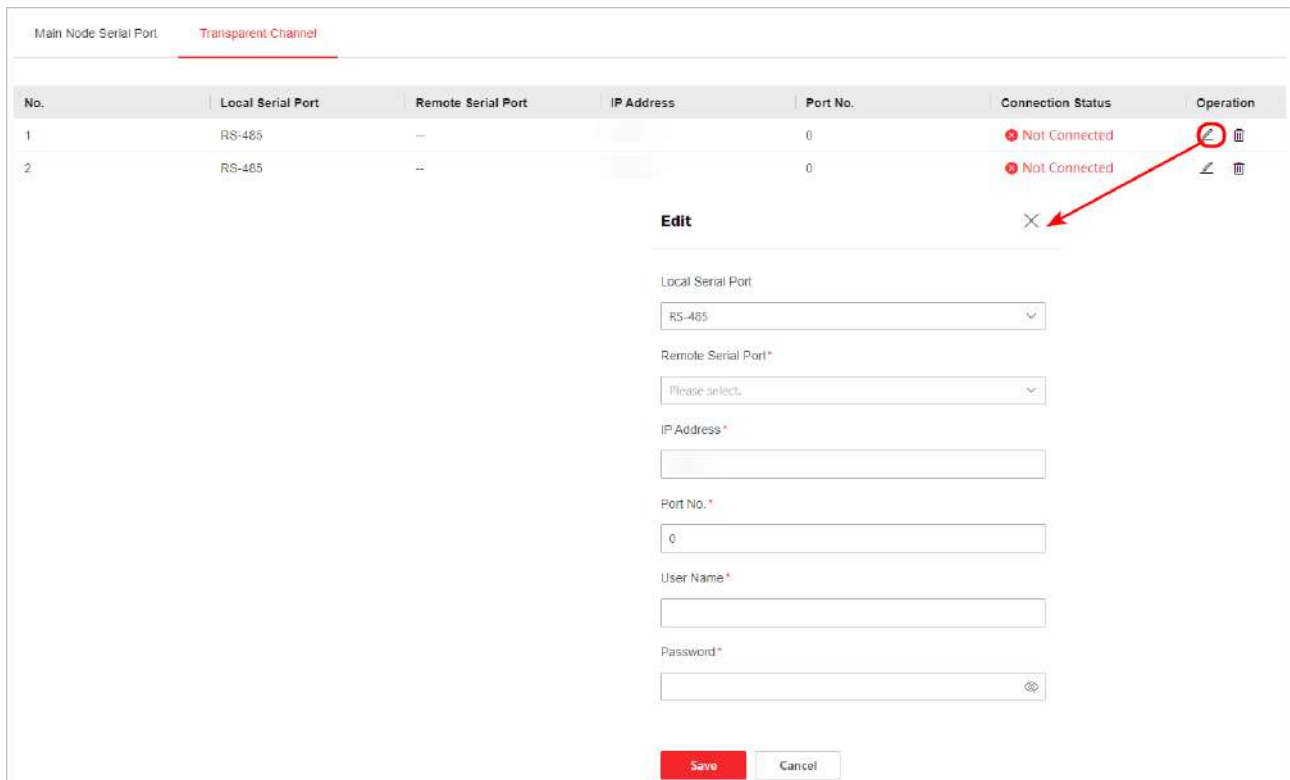


The screenshot shows the 'Main Node Serial Port' configuration window. The 'Transparent Channel' tab is selected. The 'Select Serial Port' dropdown is set to '2'. The 'Serial Port Type' is 'RS485'. The 'Duplex Mode' is 'Full-Duplex'. The 'Baud Rate' is '115200'. The 'Data Bit' is '8'. The 'Stop Bit' is '1'. The 'Checking Type' is 'None'. The 'Flow Control Type' is 'None'. The 'Working Mode' is 'Transparent Channel'. A red box highlights the 'Working Mode' dropdown. A red 'Save' button is at the bottom.

Figure 4-8 Select Transparent Channel

Step 3 Click **Transparent Channel**.

Step 4 Click  of a transparent channel to edit its remote serial port, IP address, port number, user name and password of the receiving device, and click **Save**.



The screenshot shows the 'Transparent Channel' configuration interface. At the top, there are two tabs: 'Main Node Serial Port' and 'Transparent Channel'. Below the tabs is a table with the following columns: No., Local Serial Port, Remote Serial Port, IP Address, Port No., Connection Status, and Operation. There are two rows in the table, both with 'Not Connected' status. A red arrow points to the 'Edit' icon (a pencil) in the 'Operation' column of the first row. Below the table is an 'Edit' form with the following fields: Local Serial Port (dropdown menu showing 'RS-485'), Remote Serial Port* (dropdown menu showing 'Please select...'), IP Address* (text input field), Port No.* (text input field showing '0'), User Name* (text input field), and Password* (password input field with a toggle icon). At the bottom of the form are 'Save' and 'Cancel' buttons.

No.	Local Serial Port	Remote Serial Port	IP Address	Port No.	Connection Status	Operation
1	RS-485	—		0	Not Connected	 
2	RS-485	—		0	Not Connected	 

Edit

Local Serial Port
 RS-485

Remote Serial Port*
 Please select...

IP Address*

Port No.*

User Name*

Password*

Save **Cancel**

Figure 4-9 Edit a Transparent Channel

4.3 Configure HTTP(S) Parameters

Step 1 Go to **Configuration** → **Network** → **Network Service** → **HTTP(S)**.

Step 2 Set the HTTP port number.

The port number can be either 80 or any value from 2000 to 65535. After editing the HTTP port, you need to enter HTTP://Device IP Address: Port in the browser to access the device.

Step 3 Enable HTTPS and then set the HTTPS port.

The default port number is 443. After editing the HTTPS port, you need to enter HTTPS://Device IP Address: Port in the browser to access the device.

Step 4 (Optional) Enable **Redirect to HTTPS Automatically**. Thus, accessing the device via HTTPS is used by default.

Step 5 Click **Save**.

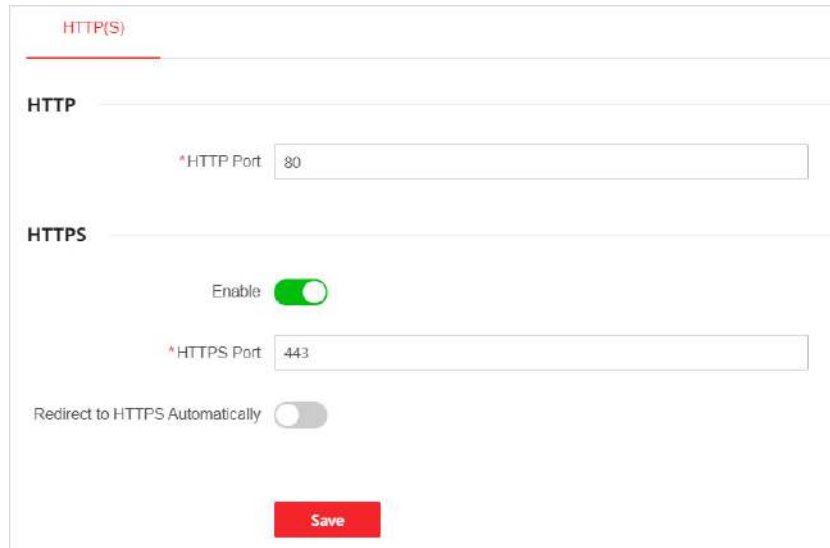


Figure 4-10 Configure HTTP (S) Parameters

4.4 Configure Event

Go to **Configuration** → **Event**, set the highest and lowest temperature thresholds for the device, and set the audible warning and alarm reporting to the platform when the exceptional events occur.

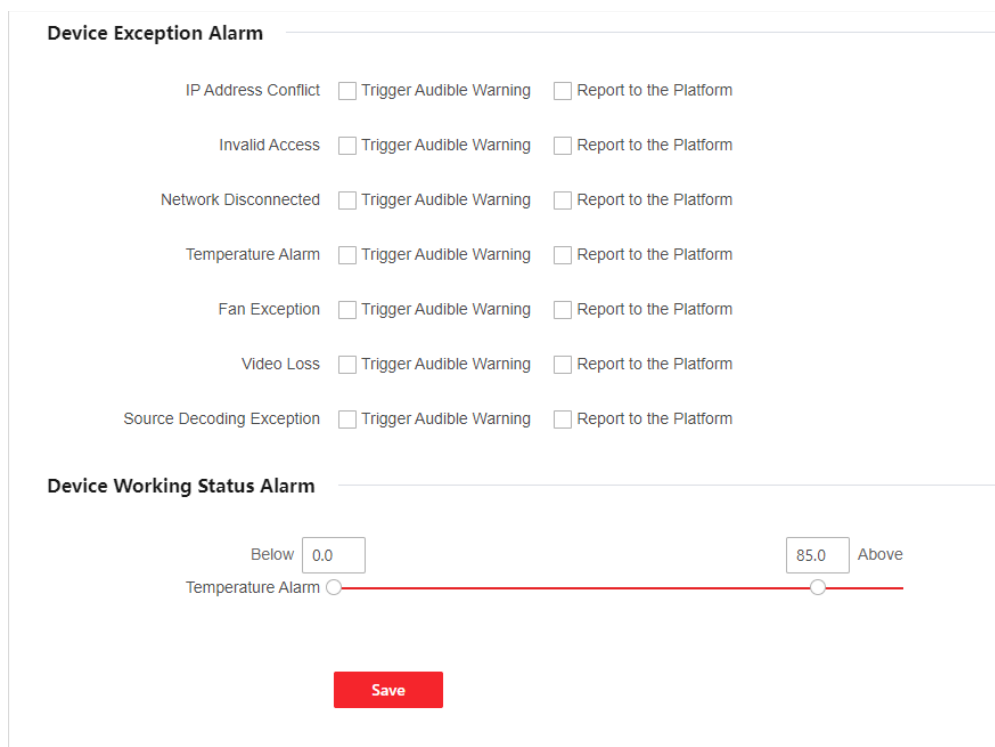


Figure 4-11 Set Device Exception Alarm

4.5 Maintain the System

Go to **Maintenance and Security** → **System Maintenance** to configure the following parameters:

- On the **Restart** page, click **Restart** to restart the device.
- On the **Upgrade** page, click  to select an upgrade file, and click **Upgrade**. You need to get the upgrade file in advance and save it locally.

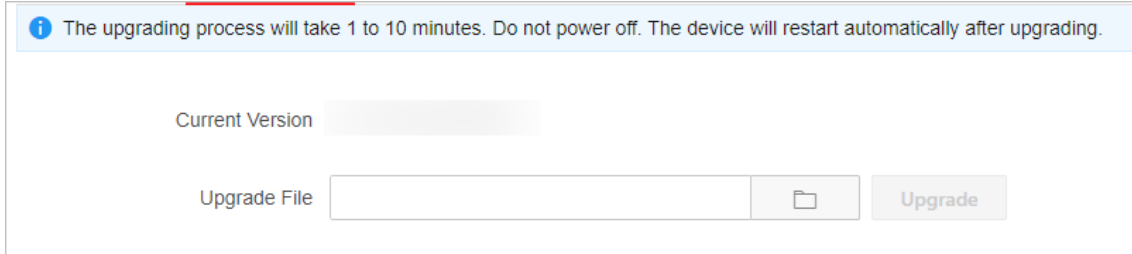


Figure 4-12 Upgrade the System

- On the **Backup and Reset** page, back up the device parameters and scene parameters.
- On the **Backup and Reset** page, reset the device:
 - Click **Restore Default** to restore the parameters except for user information and network parameters, and scene parameters to the default settings. Please use this function with caution.
 - Click **Restore Factory** to restore all functions and parameters of the device to the factory settings. Please use this function with caution.
 - Click  to select a parameter file saved locally, and click **Import** to import device parameters.
 - Click  to select a parameter file saved locally, and click **Import** to import scene parameters.

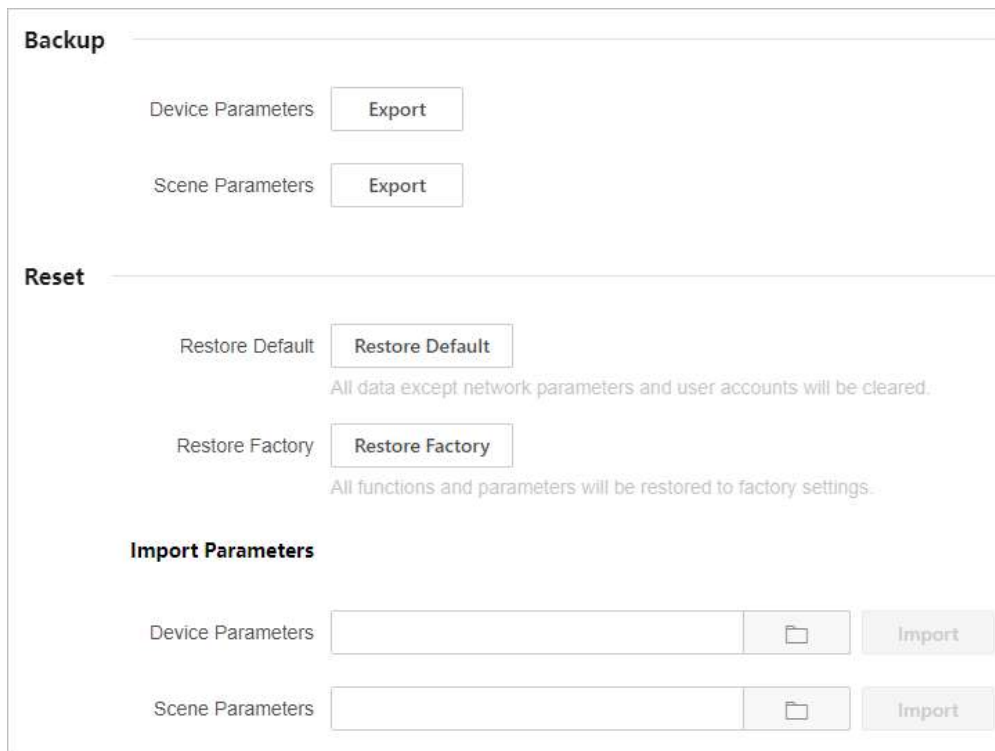


Figure 4-13 Backup and Reset Device Parameters

- On the **Log** page, set the search condition and click **Search**. You can view the searched logs in the list below. You can click **Export CSV File** to export the found logs.

Figure 4-14 Search Logs

- On the **Device Debugging** page, configure the following parameters:
 - Enable SSH (Secure Shell) as required. After enable SSH, you need to set the port number. With SSH enabled, you can use a computer installed with the SSH client to access the device.
 - Format the USB flash drive before inserting into the device. Only the USB flash drives in FAT32 format are supported. Insert a USB flash drive into the device, and click **Start Exporting** to export the logs to the USB flash drive.
 - Select a subsystem, click **Start Capturing** and then you can download the obtained packet capture file.
 - Send a shell command and then check the response message.

Figure 4-15 Debug the Device

4.6 Maintain the Device Security

Go to **Maintenance and Security** → **Security Management** to configure the following parameters:

- Enable IP filtering control and configure the IP addresses that are allowed to or forbidden to access the device.

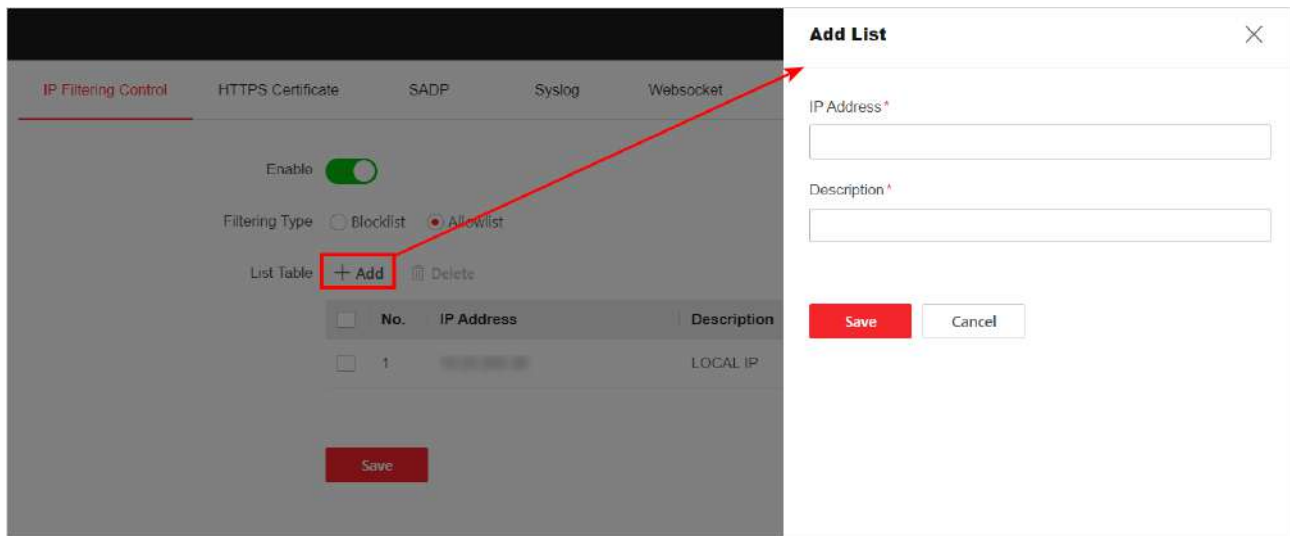


Figure 4-16 Configure IP Address Filter

- Import the locally saved HTTPS certificate and secret key.

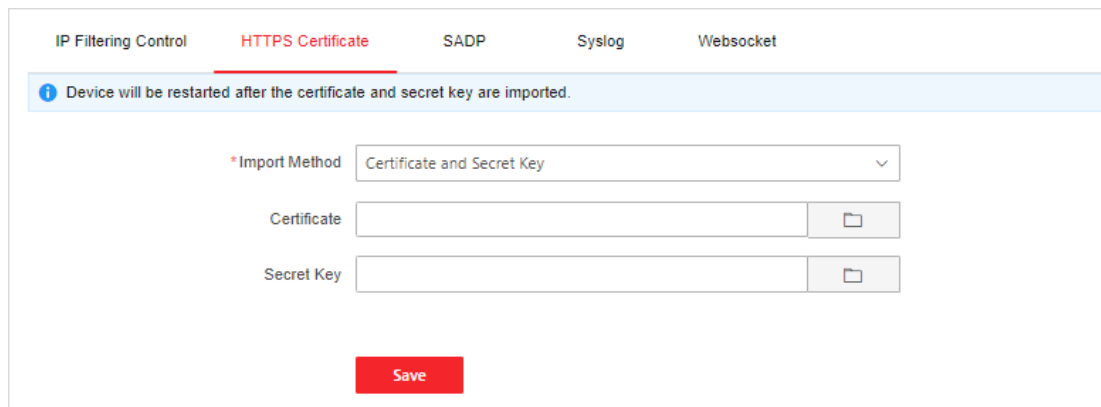
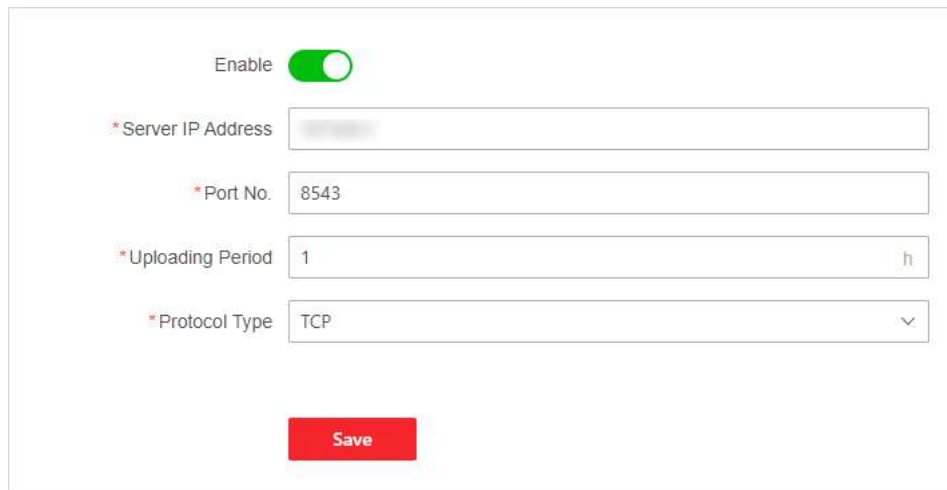


Figure 4-17 Import HTTPS Certificate and Secret Key

- Enable SADP as required. With SADP enabled, you can use the SADP software to search the device when it is in the same network segment with the computer.
- Enable Syslog as required. With Syslog enabled, the device logs can be uploaded to the Syslog server.



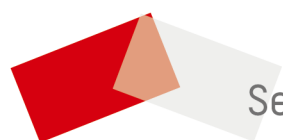
The screenshot shows a configuration interface for enabling Syslog. At the top, there is a toggle switch labeled 'Enable' which is currently turned on (green). Below this, there are four input fields, each preceded by a red asterisk indicating a required field:

- * Server IP Address:** An empty text input field.
- * Port No.:** A text input field containing the value '8543'.
- * Uploading Period:** A text input field containing the value '1', followed by a unit selector dropdown menu showing 'h' (hours).
- * Protocol Type:** A dropdown menu currently set to 'TCP'.

At the bottom of the form is a red button labeled 'Save'.

Figure 4-18 Enable Syslog

- Enable Websocket as required. With Websocket enabled, you can export the stream of network signal sources.



See Far, Go Further

DS-6908UDI(C) Ultra High Definition Decoder



Developed on the basis of embedded hardware platform, the DS-69XXUDI(C) ultra high definition (UHD) decoder is a new generation decoder for HD network cameras and can be widely used in various video security system projects. It uses the HDMI 1.4 port and BNC port for decoded data output, supports various decoding formats including H.265, H.264, MJPEG, Smart264, and Smart265, supports decoding the H.265 or H.264 video of no more than 32 MP, and supports 4K video output.

Video Input

- Supports the video input from the computers and video conference terminals, and 4K HDMI signal input.
- Supports using network cameras, NVRs, and other devices as network signal sources.
- Supports embedded HDMI audio input. The audio input supports 16 bit, 48 KHz or 32 KHz sampling rate, dual audio channel, and stereo.
- Supports signal input via the HDMI 1.4 port, 2 channels of 1080p@50/60 Hz input, or 1 channel of 4K@30 Hz input.

Video Output

- Supports signal output via the HDMI 1.4 port, and 4K (3840 × 2160@30 Hz) UHD video output.
- Supports embedded HDMI audio output and external audio output.
- Adopts frame synchronization technology to ensure that the images of all HDMI output ports are completely synchronized, with complete picture and smooth playback, and without lag, frame loss, tearing, or splicing.
- Supports the maximum LED loading capacity of 2.6 MP per port.

Video Encoding and Decoding

- Supports H.264 encoding format (the default), H.265 encoding formats, sub-stream encoding, and main stream encoding.
- Supports decoding the network cameras, NVRs and other network sources, decoding sub-stream and main stream, and auto-switching to sub-stream when the window division reaches the threshold.
- Provides 128 video decoding channels and supports simultaneously decoding 64 channels of 2 MP video or 128 channels of 720p video to the video wall.
- Supports decoding streams of no more than 32 MP resolution.
- Supports the mainstream decoding formats such as H.264, H.265, Smart264, Smart265, MJPEG, and HIK264, and mainstream encapsulation formats such as PS, TS, ES, and RTP.
- Supports audio decoding of G.722, G.711A, G.726, G.711U, MPEG2-L2, AAC, MP3, and PCM.
- Supports rotate mode decoding of front-end camera videos that are of no more than 2560 × 1440 resolution.
- Supports active decoding and passive decoding.
- Supports decoding the encrypted stream, multi-channel stream, and smart stream, editing and switching stream, and prompting for decoding exceptions.
- Supports decoding the recorded video files to the video wall.

Video Wall Function

- Supports splicing signal sources on the video wall, opening the signal source window, and performing signal source window roaming, scene switching, and window switching. Each screen supports four 1080p signal source windows or two 4K signal source windows.
- Each signal source window can be divided into 1, 2, 4, 6, 8, 9, 12, 16, 25, and 36 windows.
- Supports up to 64 scenes. You can customize the video wall layout and save it as a scene.
- Supports the auto-switching of up to 100 view groups on the HCP client. You can customize the camera location, scenes and time for each view group.
- Supports double clicking the divided sub-window to zoom in and double clicking again to zoom out.
- Supports displaying output channel number.
- Supports PTZ control of network signal sources, including 8-direction control, auto-scanning, aperture adjustment, focal length change, focusing, and preset calling.
- Supports setting the live view status, decoding status, switching status, audio status, and location of the signal source window.
- Supports video recording playback. You can set the playback status and select time to play back.
- Supports using the HCP client to capture images on the screen and display the captured images on the video wall.
- Supports the live view of network signal sources over RTP or RTSP.

Device Access

- Supports docking with 32 MP PanoVu series cameras, fisheye cameras, conventional front-end network cameras, DVRs, NVRs, XVRs, and mainstream third-party security devices.
- Supports integrating multiple decoding devices into one decoding device on the platform by using the software development kit (SDK).
- Supports using the ONVIF protocol to access the decoder.
- Supports interaction with LCD screen, including the screen information acquisition, image mode configuration, serial port control, time synchronization, backlight parameters configuration and acquisition, output port auto-binding, and error code reporting.
- Supports IPv4 and IPv6 protocols and the simultaneous access of IPv4 network sources and IPv6 network sources.
- Supports using the network keyboard or serial port keyboard to control the device, and to realize sub-window changing, group operation and auto-switching, scene changing, PTZ control, and video wall playback.

Maintenance

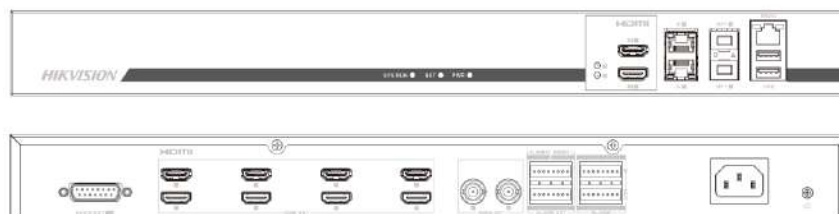
- Supports using the PC client and web browser of Chrome 45 and higher version to access and control the device.
- Provides built-in Gigabit switching network, and supports auto-adaption between the optical port and electrical port, and supports NAT.
- Supports obtaining and configuring parameters remotely, importing and exporting parameters remotely, and obtaining system running status and system logs remotely.
- Supports restarting the device remotely, restoring the default settings, and upgrading the device.
- Supports auto detection and alarm for failures, including network disconnection, IP conflict, illegal access, temperature threshold exceeding, decoding signal source exception and device exception.
- Supports user permission management, allowing users with different permissions to use designated resources and operate designated video wall modules.
- Supports visualization maintenance. The maintenance interface displays the network topology structure and keynote network status of main control system and subsystems.
- Supports manual time synchronization and NTP time synchronization.

▪ Specification

Product Model	
Product Model	DS-6908UDI(C)
Interface	
USB Interface	2 × USB 2.0 port
Serial Interface	1 × RS-232 serial port (RJ-45) + 1 × RS-485 serial port
Network Interface	2 × 10/100/1000 Mbps self-adaptive Ethernet interface (RJ-45) 2 × 100 BASE-FX/1000 BASE-X port Supports the self-adaption between the optical port and electrical port.
Alarm In Interface No.	8 channels of alarm input
Alarm Out Interface No.	8 channels of alarm output
Power	
Power Interface	Embedded 220 VAC
Device Consumption	< 70 W
Video Wall	
Video Walls	1
Video Wall Scale	≤8
Split Window	Supported
Window Division per Output Port	1, 2, 4, 6, 8, 9, 12, 16, 25, 36
Input Source Copy Capability	Not supported
Layers Per Screen	4 × 1080p or 2 × 4K
Layers per Device	Layers Per Screen × Output Interface(s)
Scenes	64
Plans	100 view groups on the HCP client
General	
Working Temperature	-10 °C to 55 °C (14 °F to 131 °F)
Working Humidity	0% RH to 90% RH
Net Weight	≤ 5.2 kg (11.46 lb)
Gross Weight	≤ 6.3 kg (13.89 lb)
Dimensions (W × H × D)	440 mm × 44.5 mm × 320.8 mm (17.32 inch × 1.75 inch × 12.63 inch)
Packing List	1 × decoder, 1 × regulatory compliance and safety information manual, 1 × mounting bracket, 1 × power cord, 4 × pads, 1 × grounding cable
Audio Input	
Audio Input Interfaces	2
Audio Input Interface Type	Embedded HDMI
Video Input	
Video Input Interface Type	2
Video Input Interfaces	HDMI 1.4
Max. Video Input Resolution	4K (only in odd-numbered port)

Video Input Resolution	3840 × 2160@30 Hz, 1920 × 1200@60 Hz, 1920 × 1080@60 Hz, 1920 × 1080@50 Hz, 1280 × 720@60 Hz, 1280 × 720@50 Hz, 1600 × 1200@60 Hz, 1280 × 960@60 Hz, 1680 × 1050@60 Hz, 1440 × 900@60 Hz, 1366 × 768@60 Hz, 1280 × 1024@60 Hz, 1024 × 768@60 Hz Supports custom resolution. For 60 Hz input, width ranges from 800 to 1920, and height ranges from 600 to 1200. For 30 Hz input, width ranges from 800 to 3840, and height ranges from 600 to 2160. Width must be a multiple of 4. Height must be a multiple of 2.
Video Encoding	
Video Encoding Format	H.264 (default), H.265
Video Encoding Channels	2
Video Encoding Capability	1 channel of 4K@30 Hz or 2 channels of 1080p@60 Hz
Audio Encoding	
Audio Encoding Format	G722.1, G711_U, G711_A, AAC
Video Output	
Video Output Interface Type	HDMI 1.4
Video Output Interfaces	8
Max. Video Output Resolution	4K
Video Output Resolution	3840 × 2160@30 Hz, 2560 × 1440@30 Hz, 1920 × 1200@60 Hz, 1920 × 1080@60 Hz, 1920 × 1080@50 Hz, 1680 × 1050@60 Hz, 1600 × 1200@60 Hz, 1280 × 1024@60 Hz, 1280 × 720@60 Hz, 1280 × 720@50 Hz, 1024 × 768@60 Hz
Loading Capacity for Video Output to LED	Single port load: 2600000, Width: 144 - 4096, Height: 144 - 2160, Width must be a multiple of 2 and height must be a multiple of 2
Video Output Interface (BNC)	2 channels of CVBS output (BNC port)
Video Output Resolution (BNC)	PAL: 704 × 576@25 Hz NTSC: 704 × 480@30 Hz
Video Decoding	
Video Decoding Format	H.264, H.265, Smart264, Smart265, MJPEG
Video Decoding Channels	128
Video Decoding Capability	1) H.264/H.265 format: Supports decoding 4-channel 32 MP/24 MP, 8-channel 12 MP, 16-channel 8 MP, 20-channel 6 MP, 32-channel 4 MP, 64-channel 1080p, 128-channel 720p and lower resolution in real time. Every four output ports (HDMI output ports 1 to 4 and 5 to 8) forms a group and 2 groups share the decoding capabilities. Each group supports up to 4-channel smart decoding or 4-channel encrypted stream decoding. The smart decoding allows the device to decode the smart alarm events from the network cameras. 2) MJPEG format: 8-channel of 1080p and lower resolution 3) HIK264 format: 4-channel of 720p and lower resolution
Video Decoding Resolution	Up to 32 MP
Audio Output	
Audio Output Interface Type	Embedded HDMI audio output port or independent DB15-to-BNC audio output port
Audio Output Interfaces	8
Audio Decoding	
Audio Decoding Format	G711A, G711U, G722.1, G726-16/U/A, MPEG, AAC-LC, PCM

▪ Physical Interface

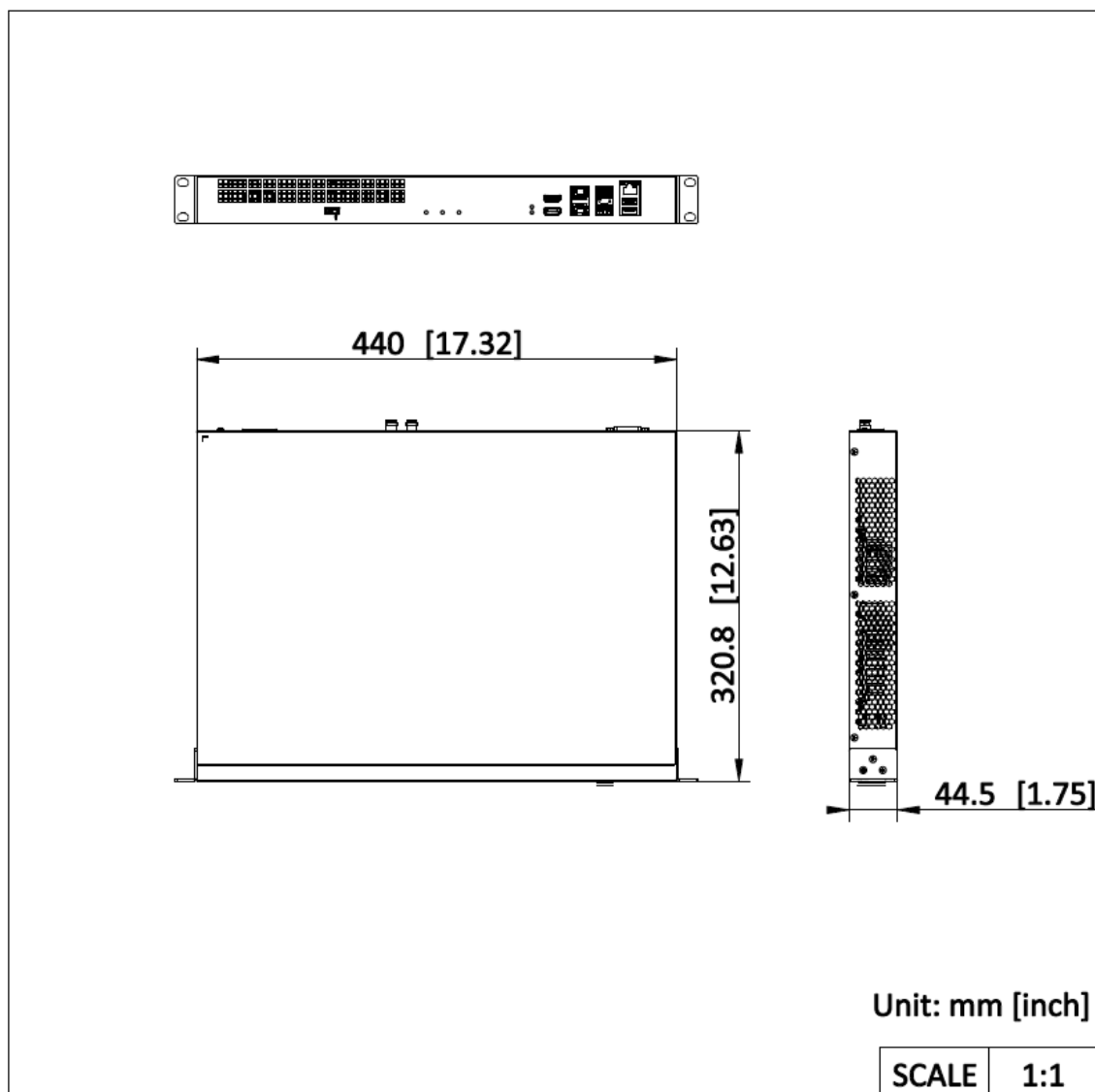


Front Panel	Description	Rear Panel	Description
SYS RUN	System running LED. It is steady green when the system runs normally.	AUDIO OUT	Audio output port
NET	Internal network LED. It is steady green when the internal network of the device is normal.	HDMI OUT	HDMI output port
PWR	Power status LED. It is steady green when the device is powered on.	VIDEO OUT	Video output port
HDMI IN 1	HDMI input port 1. Its LED is steady green when the signal is connected.	RS485	RS-485 port
HDMI IN 2	HDMI input port 2. Its LED is steady green when the signal is connected.	ALARM IN	Alarm input port
G 1	1000 Mbps electrical port 1	ALARM OUT	Alarm output port
G 2	1000 Mbps electrical port 2		
OPT 1	1000 Mbps optical port 1		
OPT 2	1000 Mbps optical port 2		
RS232	Device debug serial port		
USB	USB 2.0 port		

▪ Available Model

DS-6908UDI(C)

▪ Dimension



See Far, Go Further



www.hikvision.com
support@hikvision.com





CH 2005

- » Suporte a resolução 4k / 60Hz
- » Largura de banda de 18 Gbps
- » Compatível com TVs LCD, LED, OLED, QLED, Plasma, videogames, notebooks e projetores.
- » Permite o uso de funções inerentes a tecnologia HDMI, tais como CEC e ARC.
- » Conectores banhados a ouro
- » Suporte a Ethernet
- » Cabo com comprimento de **5m**
- » Blindagem tripla para maior proteção contra interferências externas
- » Versão 2.0



CONECTORES
BANHADOS
A OURO

4K

60 HZ

18
Gbps

VELOCIDADE
DE TRANSMISSÃO

HDR

SUPOORTE HDR

3D

COMPATÍVEL

HDMI™
HIGH SPEED
WITH ETHERNET

O CH 2005 é um cabo com a tecnologia HDMI® (*High Definition Multimedia Interface*) versão 2.0 que permite a transmissão de vídeo e áudio de alta resolução entre aparelhos compatíveis com esta tecnologia, assim o cabo HDMI CH 2005 é ideal para interligar de forma simples e fácil os seus dispositivos, como TVs, DRV's, NVR's, projetores, notebooks, home theaters, sound bars, etc.

Especificações técnicas

Comprimento	5 metros
Versão	2.0

Construção do cabo	30 AWG / CCS (<i>copper clad steel</i>)
Material do cabo	PVC
Conector HDMI	Tipo A – Banhado a ouro
Quantidade de vias	19 vias + 1 Terra
sRGB	✓
YCbCr 4:2:2/4:4:4	✓
8 canais LPCM, 192 kHz, 24-bit áudio	✓
Imagem Blu-ray Full HD e DVD HD	✓
CEC (<i>Consumer Electronic Control</i>)	✓
Largura de Banda	18 Gbps
Áudio DVD	✓
Super Áudio CD (DSD - <i>Direct Stream Digital</i>)	✓
Deep Color	✓
xvYCC	✓
Auto lip-sync	✓
Áudio Dolby TrueHD / DTS-HD	✓
Lista atualizada de comandos CEC	✓
Suporte 3D	✓
Suporte Ethernet (100 Mbit/s)	✓
ARC (<i>Áudio Return Channel</i>)	✓
Máxima resolução de vídeo	4k (3840 x 2160 pixels) / 60 Hz
Máxima resolução de áudio	1536 kHz
Suporte de canais de áudio	32 canais
4 streams de áudio	✓
2 streams de vídeo	✓
HLG (<i>Hybrid Log-Gamma</i>)	✓
HDR (<i>High Dynamic Range</i>) Estático	✓
HDCP (<i>High-bandwidth Digital Content Protection</i>)	✓

Soluções Integradas

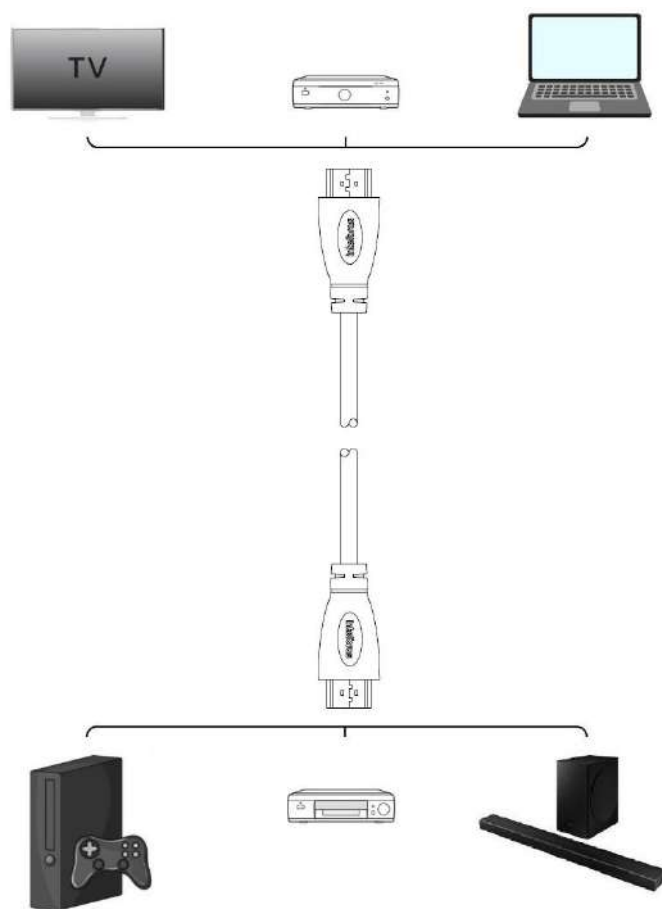
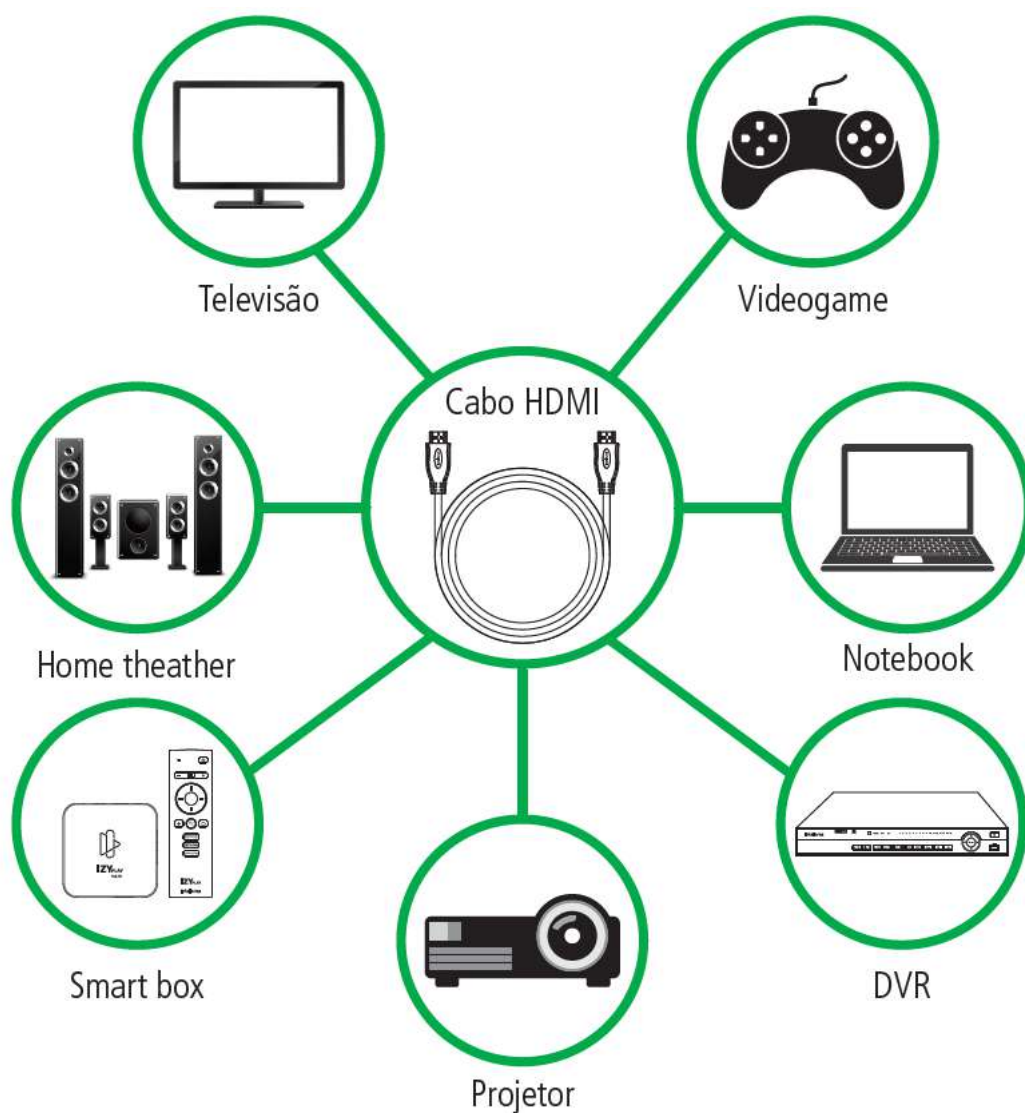
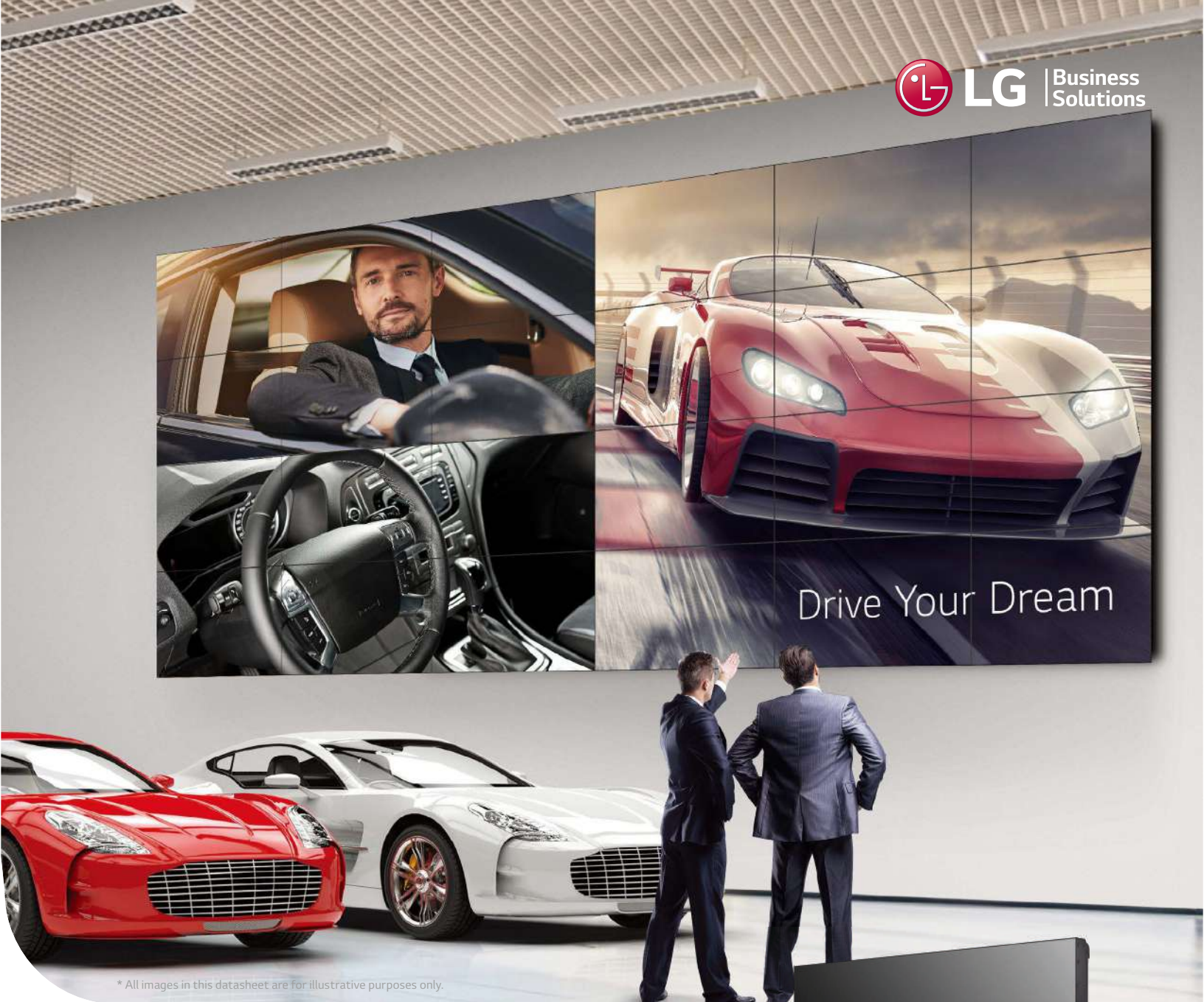


Figura 1 – Cenários de uso





* All images in this datasheet are for illustrative purposes only.

Video Wall 55VM5J-H

55" Narrow Bezel Video Wall with 1.74 mm BtB



Extreme-Narrow
Bezel



Wider
Viewing Angle



Easy Color
Adjustment



Efficient
Operation

55VM5J-H

Screen Size	55"
Aspect Ratio	16 : 9
Native Resolution	FHD (1,920 × 1,080)
Brightness	500 nits (Typ.)
Contrast Ratio	1,000:1



Large Screens with Narrow Bezel

The slim bezel, with its 1.74mm BtB (Bezel-to-Bezel) seams and delivers immersive content on assembled video wall screens.

* The 1.74mm BtB seams have been verified by Nemko, a global institution that tests and certifies electrical equipment.



Image Gap Reduction

The 55VM5J-H includes an image improvement algorithm that can reduce perception of image gaps among tiled displays when playing back videos. Objects located on the bezel boundaries are adjusted for a smoother viewing experience.

* The "LG Conventional" refers to displays which do not include an image improvement algorithm.

** The image shown above are for illustration purposes only.



High Viewing Angle

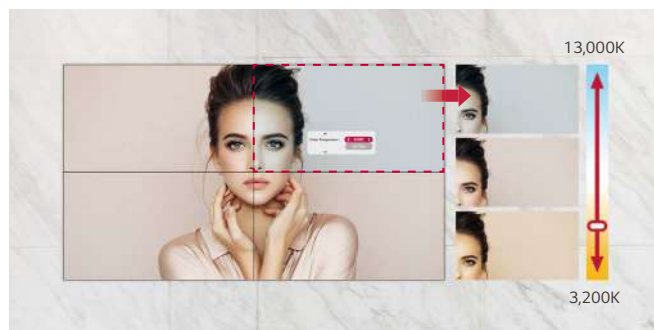
Large screens are usually positioned higher than human-eye level. Wide half luminance angle (40°) enables effective picture quality for video walls. The viewing angle of the 55VM5J-H is high enough to display vivid colors throughout even up to 40 degrees of viewing angle difference.

* Results based on in-house testing. Actual test results may differ depending on environment and measuring equipment.



Wide Viewing Angle

LG IPS panel technology enables stable and smooth control of liquid crystals, and allows the screen to be viewed from virtually any angle. Therefore, the 55VM5J-H captivates the attention of more viewers with lifelike colors, regardless of their horizontal viewing position.



Easy Color Adjustment

Depending on the content, the color temperature of the display can be easily adjusted in increments of 100K using a remote control.



Simple White Balance Adjustment

In conventional video walls, white balance was adjustable only in "full-white" mode, but the 55VM5J-H allows you to modify each value of grey scale to achieve more detailed and precise white balance adjustment.



High Performance and Great Scalability

Thanks to its built-in System-on-Chip and webOS smart signage platform, the 55VM5J-H can execute several tasks at once while providing smooth content playback without the need for a media player. As webOS supports HTML5 as a web-based platform and offers an SDK (Software Development Kit), it is even easier for system integrators to build and optimize their web apps.

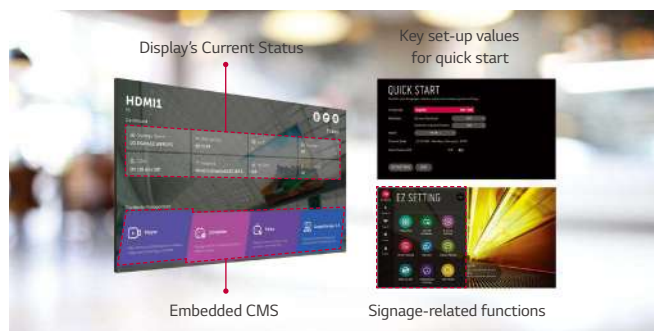
* SDK can be downloaded at
<https://webossignage.developer.lge.com>.



Flexible Content Creation

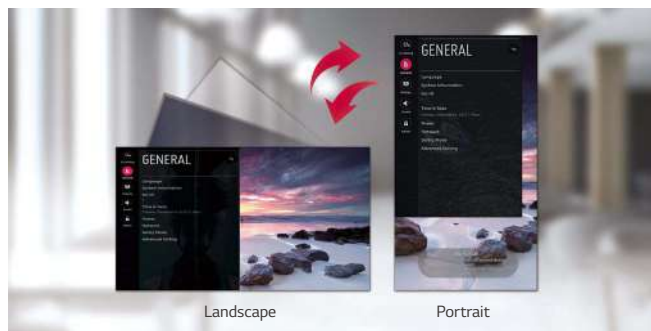
Four different videos can be played simultaneously via web apps, and various animation effects, such as scaling or rotating, are added to content using CSS (Cascading Style Sheets) transition effects. Real-time streaming is also available, providing the flexibility to organize and diversify content free from capacity limits.

* Supported protocols: RTSP, RTP, HLS, UDP Multicast



Intuitive Menu Structure

The menu structure has been optimized for commercial use. It simplifies approach flows and groups similar functions together, adopting a more intuitive GUI for ease of use. This way, users can avoid having to do trial-and-error when exploring desired functions and managing displays.



Dedicated User Interface for Portrait Orientation

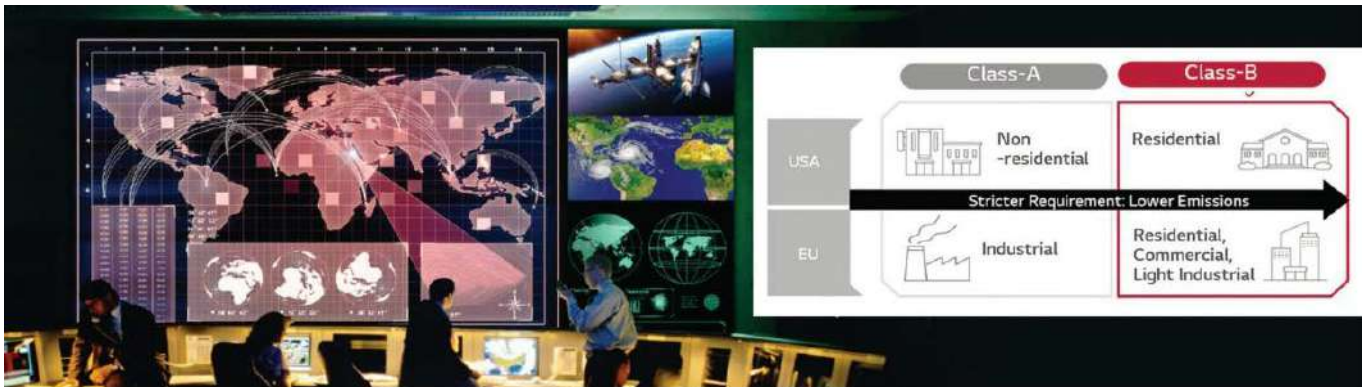
The user interface was designed based on landscape-oriented consumer TV usage, so on-screen display menu wasn't well-suited for screens in portrait mode. The OSD of the VM5J-H, however, consists of a long range menu with bigger font sizes and a 9:16 ratio, creating a comfortable and efficient business environment.



Conformal Coating

Video wall in various places can't avoid exposure to environments with dust, and humidity, which may lead to hampered performance over time. Conformal coating on the major circuit board (power board) offers protection from such environments by protecting video wall from salt, dust, iron powder, humidity, etc.

* Actual images available may differ from the example images shown.



EMC Class B Certified

The VM5J-H is certified as EMC Class B, which requires electronic equipment made for use in residential environments as well as commercial, industrial, or business environments. Therefore, it is suitable for up-close uses such as corporate meeting rooms, board rooms, etc.



Real-Time LG ConnectedCare

Maintenance is easy and fast with the optional LG ConnectedCare* service, a cloud service solution provided by LG. It remotely manages the status of displays in client workplaces for fault diagnosis and remote-control services, enabling the stable operation of clients' businesses.

* LG ConnectedCare is the brand name of LG Signage365Care Service. The availability differs by region.



Daisy Chain Capability

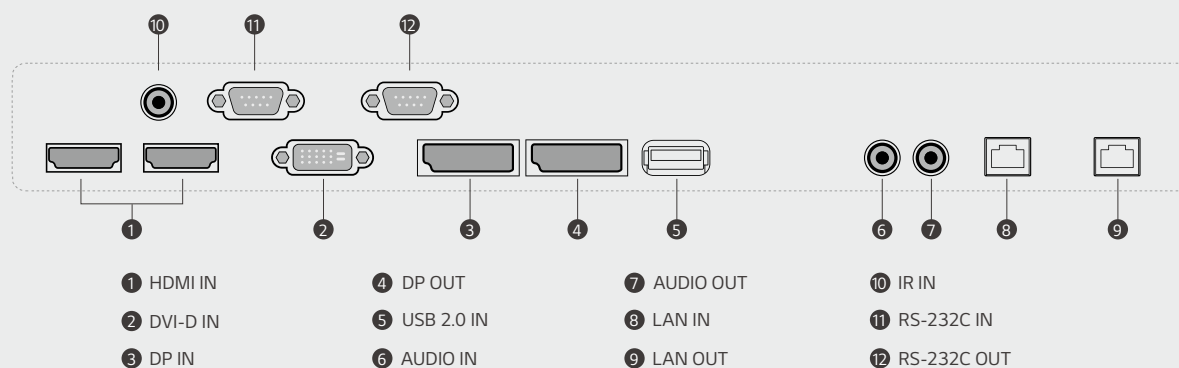
A LAN daisy chain allows you to control and monitor video walls and even update their firmwares at once. Also, through UHD daisy chain using HDMI and DisplayPort, you can set up a UHD video wall without the need of DisplayPort MST hub.



IP5x Certified Design

The IP5x Certification demonstrates protection of the internal parts of the product against dust particles.

CONNECTIVITY



* Jack Panels may differ from the above image, so please contact LG sales team to verify before ordering.



MODEL	55VM5J-H	
PANEL	Screen Size	55"
	Panel Technology	IPS
	Back Light Type	Direct
	Aspect Ratio	16:9
	Native Resolution	1920 X 1080 (FHD)
	Refresh Rate	60 Hz
	Brightness	500 nits
	Contrast Ratio	1,000:1
	Dynamic CR	500,000:1
	Color gamut	NTSC 72%
	Viewing Angle (H x V)	178° X 178°
	Color Depth	10 bit, 1.07 Billion colors
	Response Time	8ms (G to G)
	Surface Treatment (Haze)	28%
	Lifetime (Typ)	60,000 Hrs
	Operation Hours (Hours/Day)	24/7
	Portrait / Landscape	Yes / Yes
CONNECTIVITY IN	HDMI	Yes (x2), HDCP2.2
	DP	Yes (x1), HDCP2.2
	DVI-D	Yes (x1), HDCP1.4
	Audio In	Yes
	RS232C IN	Yes
	RJ45(LAN)	Yes
	IR IN	Yes
CONNECTIVITY OUT	USB	USB2.0 Type A
	DP Out	Yes (Input: HDMI / DVI / DP)
	Audio Out	Yes
	RS232C OUT	Yes
MECHANICAL	RJ45(LAN)	Yes
	Bezel Color	Black
	Bezel Width (Bezel-to-Bezel)	1.74mm BtB (1.3mm (T/L), 0.44 mm(B/R))
	Bezel Width (Active area to Active area)	2.49mm AtA (1.75mm (T/L), 0.74mm (B/R))
	Weight	41.4 lbs / 18.8 kg
	Shipping Weight	61.7 lbs / 28.0 kg
	Monitor Dimension (W x H x D)	47.7 x 26.9 x 3.4 in 1212.2 x 683.0 x 86.9 mm
	Carton Dimensions (W x H x D) (Box outer size)	54.8 x 37.6 x 11.9 in 1393 x 955 x 303 mm
	Handle	Yes
	VESA™ Standard Mount Interface	600 x 400
	Operation Temperature	32°F to 104°F 0°C to 40°C
	Operation Humidity	10% to 80%
	IP Rating	IP5X
HARDWARE FEATURES	Internal Memory	8GB
	Temperature Sensor	Yes
	BLU Sensor	Yes
	Acceleration (Gyro) Sensor	Yes
	Local Key Operation	Yes
	Fanless Design	Yes
	OPS type compatible	Yes (Piggyback)

MODEL	55VM5J-H	
SOFTWARE FEATURES	webOS ver.	webOS 4.1
	Local Contents Scheduling	Yes
	Group Manager	Yes
	USB Plug & Play	Yes
	Fail over	Yes
	No Signal Image	Yes
	RS-232C Sync	Yes
	Local Network Sync	Yes
	Video Tag	Yes (x4)
	Play via URL	Yes
	Screen Rotation	Yes
	External Input Rotation	Yes
	Gapless Playback	Yes
	Tile Mode Setting	Yes (Max. 15x15)
	Setting Data Cloning	Yes
	SNMP	Yes
	ISM Method	Yes
	Auto Set ID	Yes
	Status Mailing	Yes
	Control Manager	Yes
	Crestron Inside	Yes
	Smart Energy Saving	Yes
	PM mode	Yes
	Wake on LAN	Yes
	Network Ready	Yes
	HDMI-CEC	Yes
	SI Server Setting	Yes
	webRTC	Yes
	Pro:Idiom	Yes
	W/B Setting by Grey scale	Yes
	Scan Inversion	Yes
POWER	Power Supply	100-240 Vac, 50/60Hz
	Power Type	Built-In Power
	Typ. Power Consumption	160 W 546 BTU/hr
	Max. Power Consumption	190 W 648 BTU/hr
	Smart Energy Saving	90 W
	DPM	0.5 W
	Power off	0.5W
	FCC	Class "B"
CERTIFICATION	CE	Yes
	ErP / Energy Star	Yes / Energy Star 8.0
	SuperSign CMS	Yes
SOFTWARE COMPATIBILITY	SuperSign Control / Control+	Yes / Yes
	SuperSign WB	Yes
	SuperSign Media Editor	Yes
	LG Connected Care	Yes
ACCESSORIES & OTHER	Basic Accessories	Remote Controller(includes battery 2ea), Power Cord, RS232C cable, Lan cable, DP cable, IR Receiver, Guide Bracket, Screws, Manual
	Optional Accessories	OPS Kit (KT-OPSF)



EMPRESA

PRODUTOS

DISTRIBUIDORES

BRACKETS STANDARD

Home > Produtos > Brackets > Brackets Standard

> RACKS FECHADOS

> Triunfo Standard

> Triunfo Server

> Triunfo Left

> Triunfo Left Server

> Rack Triunfo Plus

> Triunfo Industrial

> Rack Triunfo Flex

> RACKS ABERTOS

> Triunfo Plus

> Triunfo HD

> Rack Aberto Evo

> Rack Triunfo Open HD



Brackets Standard

Categoria: **Brackets**

Descrição

- Porta frontal em vidro temperado e fecho cilindro com chave.
- Estrutura em chapa de aço 0,75mm. e 1,2mm.
- Monobloco.
- Planos de montagem com marcação em meio "U" e regulagem na profundidade em chapa de aço 1,5mm.
- Teto com predisposição para instalação de 2 micro ventiladores
- Laterais removíveis em chapa de aço 0,75mm. com aletas de ventilação.
- Abertura superior e inferior para passagem de cabos.
- Acabamento: Toda a estrutura em aço é revestida com pintura eletrostática a pó na cor preta.

> Rack Open



CÓDIGO	UNIDADE	ALTURA	LARGURA	PROFUNDIDADE
BKS2-9350P	03U	171mm	530mm	350mm
BKS2-9450P	03U	171mm	530mm	450mm
BKS2-9550P	05U	260mm	530mm	350mm
BKS2-5450P	05U	349mm	530mm	350mm
BKS2-5550P	05U	349mm	530mm	450mm
BKS2-7350P	07U	349mm	530mm	350mm
BKS2-7450P	07U	349mm	530mm	450mm
BKS2-7550P	07U	349mm	530mm	550mm
BKS2-9350P	09U	438mm	530mm	350mm
BKS2-9450P	09U	438mm	530mm	450mm
BKS2-9550P	09U	438mm	530mm	550mm
BKS2-12350P	12U	572mm	530mm	350mm
BKS2-12450P	12U	572mm	530mm	450mm
BKS2-12550P	12U	572mm	530mm	550mm



EMPRESA

PRODUTOS

DISTRIBUIDORES

> Bracket
Standard Flex

> ACESSÓRIOS

> Guia de
Cabos
Fechado

> Guia de
Cabos Aberto

> Guia de
Cabos Anel

> Frente Falsa

> Bandeja Fixa
Light

> Bandeja Fixa
Estendida

> Bandeja Fixa
4 Pontos

> Bandeja
Telescópica

> Calhas de
tomadas

> DIO Rack
19"

> Mini Dio

> Caixa de
Emenda

> Unidade de
Ventilação

> Gaveta de
Ventilação

> Suporte para
servidor

> Base no-

Produtos relacionados



Bracket Standard Flex

break



EMPRESA

PRODUTOS

DISTRIBUIDORES



MENU

- Home
- Empresa
- Produtos
- Distribuidores
- Vídeos
- News
- Contato

CONTATO

📍 R. Antônio Lacerda Braga,
455
CIC - Curitiba - PR

✉️
racks@triunfometalurgica.co
m.br

☎️ (41) 3347.1850

UNIDADE DE VENTILAÇÃO

Home > Produtos > Acessórios > Unidade de Ventilação

> RACKS FECHADOS

- > Triunfo Standard
- > Triunfo Server
- > Triunfo Left
- > Triunfo Left Server
- > Rack Triunfo Plus
- > Triunfo Industrial
- > Rack Triunfo Flex

> RACKS ABERTOS

- > Triunfo Plus
- > Triunfo HD
- > Rack Aberto Evo
- > Rack Triunfo Open HD
- > Rack Open Plus

> BRACKETS

- > Brackets Standard
- > Bracket Standard Flex

> ACESSÓRIOS

- > Guia de Cabos Fechado
- > Guia de Cabos Aberto
- > Guia de Cabos Anel
- > Frente Falsa
- > Bandeja Fixa Light



Unidade de Ventilação

Categoria: **Acessórios**

Descrição

Utilizado para forçar a saída de ar quente e causar circulação de ar interna ao rack, auxiliando o funcionamento dos equipamentos. Possui chave liga/desliga, fusível e chave comutadora 110/220v.

Código	Ventiladores
UV02	2
UV04	4

Produtos relacionados





CALHA DE TOMADAS 19"



Calhas com 4, 6, 8, 10 e 12 tomadas com fixação para 19" Tomadas padrão brasileiro (NBR 14136) 2P +T (10A e 20A) 250V Cabo constituído de 3 via PP 2,5 m de Comprimento (10A e 20A) com plug; Montadas com barramento de latão

Estrutura em aço com pintura eletrostática poliéster, RAL 9011 preto texturizado; Cantoneira giratória para quatro posições de fixação.

Dados Técnicos			
Código	largura	Qtd de Tomadas	Amper
CALHA 0019	483(19")	4	10A
CALHA 0015	483(19")	4	20A
CALHA 0020	483(19")	6	10A
CALHA 0030	483(19")	6	20A
CALHA 0021	483(19")	8	10A
CALHA 0009	483(19")	8	20A
CALHA 0037	483(19")	10	10A
CALHA 0014	483(19")	10	20A
CALHA 0024	483(19")	12	10A
CALHA 0028	483(19")	12	20A

CALHA DE TOMADAS ESPECIAL 10 E 12

ESPECIFICAÇÃO TÉCNICA – SUPORTES PRO REV01_2024



• COLUNAS PARA FIXAÇÃO NAS MESAS E CONSOLES ELLAN

Alturas e capacidade de carga das colunas (SLATWALL E SLATRAIL):

- 300mm / 2 telas até 24" ou 40kg
- 700mm / 4 telas até 24" ou 75kg
- 1000mm / 6 telas até 24" ou 115kg
- Perfil base em alumínio extrudado, com canais de apoio e encaixe tipo "tromba de elefante", mantendo a estabilidade e possibilitando o deslocamento do sistema de maneira uniforme pelo trilho (slatwall ou slatrail); fixação s/ ferramenta, com manípulos e parafuso tipo martelo, com bordas arredondadas
- Perfil vertical em alumínio extrudado, soldado no perfil base, com 2 canais espelhados (Esq / Dir) possibilitando a montagem e ajuste de altura de diversos braços p/ tela de acordo com a altura da coluna selecionada; tampa superior de acabamento em plástico injetado
- Acabamento em pintura eletrostática a pó, na cor prata

• BRAÇOS ELLAN

Modelos disponíveis:

- Braço p/ 1 tela (6kg)
- Braço p/ 1 tela c/ suporte p/ mini CPU (9kg)
- Braço p/ 1 tela c/ inclinação de 45 graus (6kg)
- Braço p/ 1 tela Heavy Duty (18kg)
- Braço p/ 1 Notebook (6kg)
- Para uso de telas acima de 24" ou 6kg, consultar nossa engenharia para dimensionamento

ELLAN S A

Rod. Est. SP 115/ 280 – Acesso José Sartorelli Km 3,2 – Parque das Árvores – 18555-225 - Boituva – SP
Tel: (0xx15) 3363-8233
CNPJ: 04.345.304/0001-41 - IE: 219.079.801.110

- Base de encaixe do braço na coluna com trilho em alumínio extrudado com bordas em 45 graus, c/ 5,5mm de espessura, fixado e com possibilidade de ajuste por manípulos (sem uso de ferramentas)
 - Eixos de articulação construídos em aço usinado, com buchas em plástico injetado
 - Segmentos de braço construídos em aço trefilado, c/ 2mm de espessura, com tampas em plástico injetado encaixadas em todas as extremidades
 - Esfera de aço para articulação das telas, possibilitando o giro em 360 graus, e inclinação de 30 a 45 graus, a depender do modelo escolhido
 - Placa para telas com fixação modelo VESA 100x100mm e 75x75mm
- **GARANTIA**

Assegura-se ao produto Ellan a garantia contra qualquer defeito de material ou de fabricação que nele se apresente no período de 05 (cinco) anos, exceto para os casos de mau uso do produto, contando a partir da data de sua aquisição pelo usuário, conforme NF Ellan emitida com seu número sequencial e data.

Os serviços em garantia a serem prestados são restritos unicamente à substituição ou conserto gratuitos das peças defeituosas, desde que, a critério de um técnico credenciado, se constata falha em condições normais de uso, durante a vigência desta garantia.

A garantia torna-se nula e sem efeito se o produto sofrer qualquer dano provocado por acidentes, agentes da natureza, vandalismo de qualquer natureza, desgaste natural das peças e componentes, uso abusivo ou em desacordo, descuido do usuário no manuseio, transporte ou remoção dos mesmos, ou ainda, no caso de apresentar sinais de violação, ajuste ou conserto por pessoas não autorizadas. Os serviços acima referidos, tanto os gratuitos como os remunerados, somente serão prestados nos locais autorizados e indicados pela Ellan S/A.

- **Normas, certificados e laudos aplicáveis:**

1- Normas regulamentadoras e demais normas aplicáveis:

- Acabamento: DIN 68761; ISO 4211, 9241, 11469; VDE 1000.
- Laminados melamínicos de alta pressão: EN 438.
- Especificações de normas (desenhos) mobiliários e estações de trabalho: EN 527, 614, 717, ZH1/428 – 1988, 31001, 60950, PP52024(1990, 1996) e EM 60335 1:1994.
- Norma de Ergonomia: NR 17.
- Norma anticorrosão para o banho e pintura: ASTM B 117 /1997 ou ABNT NBR 8094/1983 ou ISO 9227/2006.
- Norma NBR ISO 9001: 2008 (edição e versão 2008).
- Réguas de tomada norma ABNT NBR 5410 – item 7.3.3 – Tabela 55. Norma baseada na IEC 60.364 – Electrical Installations of Buildings.
- Aderência das tintas conforme norma ABNT NBR 11003/2009 grau GRO
- Camada de tinta conforme norma interna ITTES007 – Determinação de camada com QUANIX 1500.

2- Certificados e Laudos:

- **Certificado de Ergonomia** em conformidade com a Lei n. 6.514 e Portaria n. 3.214/NR 17, emitido por profissional qualificado em ergonomia (médico do trabalho, ergonomista ou fisioterapeuta do trabalho capacitados para tal).
- **Laudo de Resistência à Corrosão em névoa salina (Salt Spray)**, conforme norma ASTM B 117 /1997 ou ABNT NBR 8094/1983 ou ISO 9227/2006, mediante corpos de prova expostos em teste de névoa salina. A

ELLAN S A

Rod. Est. SP 115/ 280 – Acesso José Sartorelli Km 3,2 – Parque das Árvores – 18555-225 - Boituva – SP

Tel: (0xx15) 3363-8233

CNPJ: 04.345.304/0001-41 - IE: 219.079.801.110

duração do teste de névoa salina para aço laminado e perfis de alumínio é de no mínimo 500 horas e máximo de 1000hs de exposição, respectivamente.

- **Atestado de fornecimento, experiência e de capacidade técnica** de linhas similares e já fornecidas para ambientes similares e com todos os dados do contato no cliente, com assinatura e firma reconhecida.
- **Declaração do responsável pelo CREA da empresa**, declarando atendimento a especificação técnica de tratamento superficial e de pintura com tinta pó eletrostática poliéster ou híbrida, com no mínimo 80 micrometros de camada protetiva e aderência grau GR0, através do cumprimento do item 7.5.2. da norma ABNT NBR 9001/2008 – validação de processos – pela qual a empresa é certificada.
- **Apresentação de desenho** do produto ofertado, realizado em software de modelagem 2D/3D, junto da proposta técnica / comercial, conforme a layout e informações fornecidas.
- **Declaração de cumprimento em 100% às diretivas RoHs** através do responsável pelo CREA da empresa, contra a utilização de substâncias perigosas.
- **Apresentação de teste comprobatório de validação termográfica** (tempo x temperatura), realizado semestralmente na estufa de secagem da pintura eletrostática, garantindo qualidade do acabamento e cura com tinta a pó poliéster eletrostática.
- **Apresentação de certificado conforme Norma NBR ISO 9001: 2015 (edição e versão 2015)**. Esta nova versão é necessária, pois foi elaborada para apresentar maior compatibilidade com a família da ISO 14000, cujas alterações trouxeram maior compatibilidade para as traduções e consequentemente um melhor entendimento e interpretação de seu texto.
- **Declaração com comprovação em fábrica do processo de pintura eletrostática com tinta a pó** para substratos não ferrosos quanto à determinação da camada de tinta conforme norma ABNT NBR 11003 – 2000, utilizando-se de equipamento calibrado anualmente, modelo: Quanix 1500, assegurando uma deposição de camada de no mínimo 80 micrometros.

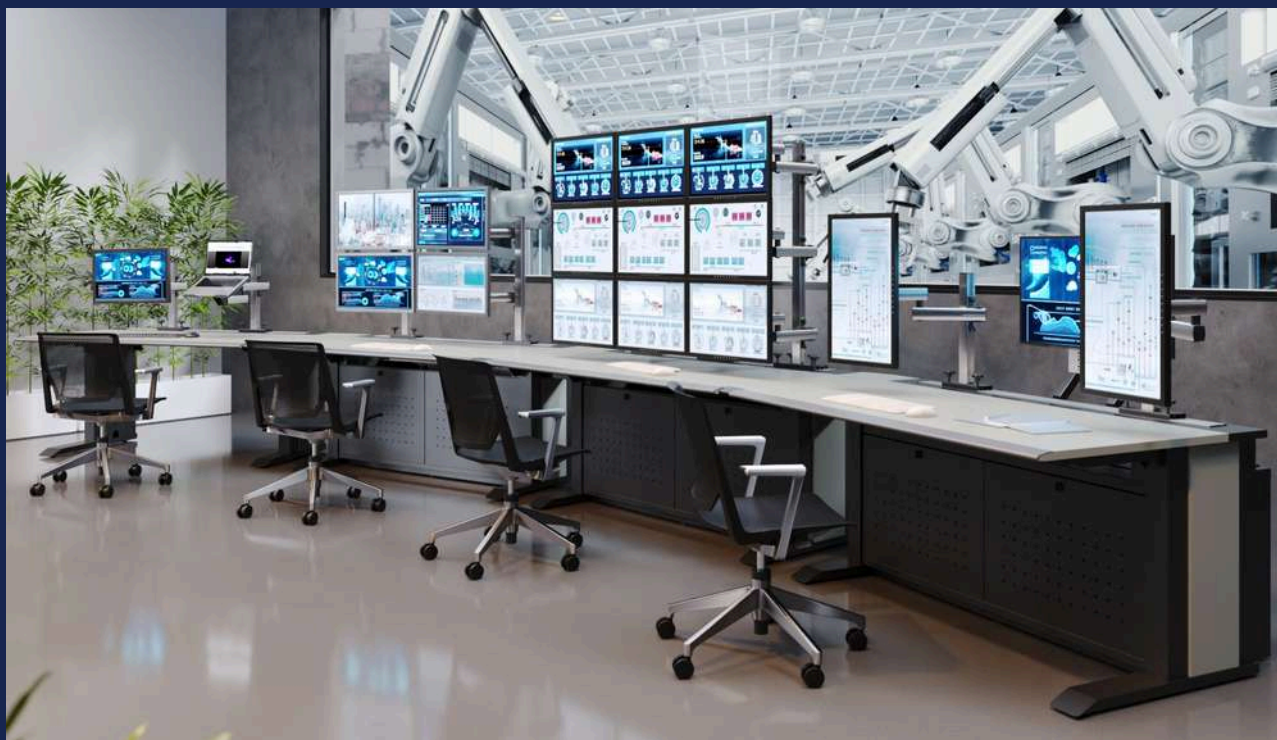
ellan.

SUORTES PARA MONITORES



1. LAYOUT monitores

Os suportes Ellan são compatíveis com diferentes modelos e tamanhos de monitores, permitindo que eles permaneçam alinhados e regulados.



7 Monitores



3 Monitores



1 monitor e 1 Notebook



2. MODELOS **Braços**

A Ellan oferece uma variedade de braços para suportes de monitores, cada um projetado para situações específicas e diferentes tipos de equipamentos, garantindo a melhor solução para cada necessidade.

BRAÇO PADRÃO



ATÉ 6Kg

BRAÇO PARA MONITORES ULTRAWIDE(PESADOS)



ATÉ 18Kg | 25 Á 39 POLEGAS

BRAÇO INCLINADO



ATÉ 6Kg

SUPORTE PARA TELEVISORES



ATÉ 18Kg | 40 Á 70 POLEGAS

BRAÇO PARA NOTEBOOK



ATÉ 6Kg

BRAÇO PARA 01 MONITOR E THIN CLIENT



ATÉ 6Kg

3. SUPORTES ergonômicos

Veja neste video a importância da Ergonomia quando se trabalha com monitores



Ajuste ideal para cada operador



Conforto e segurança .



Escaneie o QR code para assistir ao vídeo.

ellan.

4. PAINÉIS para fixação



SUPORTES PARA SLATWALL

A estrutura de Slatwall é composta por painéis verticais com ranhuras horizontais. É ideal para trabalhos em que não é necessária a interação com o ambiente ao redor da estação de trabalho. Além disso, a estrutura de Slatwall contribui para um ambiente mais limpo e organizado, pois permite a passagem de cabos de forma discreta, reduzindo a desordem visual.

SUPORTES PARA SLATRAIL

Composta por trilhos horizontais fixados na frente do tampo, a estrutura Slatrail permite a passagem de cabos de forma discreta, proporcionando organização visual. Essa estrutura é ideal para estações de trabalho que precisam de interação ao redor, como, por exemplo, quando há um videowall à frente da estação.



A MELHOR SOLUÇÃO

para sua operação

A Ellan está presente no mercado brasileiro a mais de 35 anos com suas linhas de produtos sempre com foco em oferecer o melhor aos nossos clientes. Estamos localizados em Boituva, interior de São Paulo, em uma área própria de 25.000 m² de terreno e 5.000m² de área fabril. Nossa fábrica está estruturada com máquinas precisas e de qualidade para conseguirmos entregar o melhor produto dentro do melhor prazo possível para nossos clientes. Oferecemos uma linha completa de produtos distintos para atender a diversas necessidades. Se Você necessita de customização a Ellan é especialista em

desenvolver soluções para os projetos dos clientes que não se encaixam em nossos produtos padrão. Após levantar toda a sua necessidade realizamos um projeto ainda em fase de cotação.



WWW.ELLAN.COM.BR

ELLAN S/A - Rod. SP 115/280, km 3,2 Acesso Jardim Sartorelli - Pq. das Árvores

Boituva - SP - Brasil - CEP 18555-225

Telefone para contato: (15) 3363-8233

Whatsapp: (15) 98145-0788

ellan.

PRODUTOS

MOBILIÁRIO

Para operação,
controle e
monitoramento



INDUSTRIAL

Bancadas, armários
e carrinhos



LOGÍSTICA

Carrinhos, bancadas
e prateleiras



1. CONSOLES

para operação, controle e monitoramento



Eleve o padrão da sua Sala de Controle com nossa linha de mobiliário especializado. Projetados para suportar operações 24/7, nosso mobiliário oferece ergonomia necessária, promovendo o conforto dos operadores e aumentando a eficiência. A escolha do mobiliário adequado é crucial para a operação ininterrupta. Transforme seu espaço de controle em um ambiente de excelência.

1. CONSOLES

design
personalizado



1. LINHA MF

eficiência técnica



1. LINHA EB

organização simples
e eficaz



ellan.

2. INDUSTRIAL bancadas, armários e carrinhos



Traga excelência para sua produção industrial com nossa linha Industrial: bancadas, armários e carrinhos projetados especificamente para atender às demandas do ambiente fabril. Nossa solução oferece organização, durabilidade e ergonomia inigualáveis, otimizando o espaço de trabalho e melhorando a segurança. Reduza o tempo de processo e impulsione a sua produção. O mobiliário certo faz toda a diferença!

Bancadas SAM



Linha modular



Bancadas básicas



ellan.

3. LOGÍSTICA

carrinhos, bancadas e prateleiras



Maximize a eficiência da sua operação logística com nossa linha de bancadas, carrinhos de movimentação e prateleiras de alta qualidade. Com designs ergonômicos e durabilidade excepcional, nossos produtos otimizam o espaço de armazenamento e agilizam o fluxo de trabalho. Aumente a produtividade e reduza custos operacionais. Invista na infraestrutura certa para o sucesso logístico.

Bancadas



Prateleiras



Carrinhos



ellan.

SUPORTES

para monitores
e acessórios



Aprimore a eficiência da sua operação com nossos suportes de monitor e teclado preparados para a Indústria 4.0. Com sua articulação inteligente, liberam todo o espaço do tampo para tarefas produtivas. Além disso, oferecem ajustes ergonômicos para o conforto e produtividade de seus operadores. Potencialize sua produção com nossas soluções exclusivas de suportes para monitores.



Ajustes sem necessidade de
ferramentas

ellan.

A MELHOR SOLUÇÃO

para sua operação

A Ellan está presente no mercado brasileiro a mais de 35 anos com suas linhas de produtos sempre com foco em oferecer o melhor aos nossos clientes. Estamos localizados em Boituva, interior de São Paulo, em uma área própria de 25.000 m² de terreno e 5.000m² de área fabril. Nossa fábrica está estruturada com máquinas precisas e de qualidade para conseguirmos entregar o melhor produto dentro do melhor prazo possível para nossos clientes. Oferecemos uma linha completa de produtos distintos para atender a diversas necessidades. Se Você necessita de customização a Ellan é especialista em desenvolver soluções para os projetos dos clientes que não se encaixam em nossos produtos padrão. Após levantar toda a sua necessidade realizamos um projeto ainda em fase de cotação.



ellan.

WWW.ELLAN.COM.BR

ELLAN S/A - Rod. SP 115/280, km 3,2 Acesso Jardim Sartorelli - Pq. das Árvores

Boituva - SP - Brasil - CEP 18555-225

Telefone para contato: (15) 3363 8233

Whatsapp: (15) 3363 8236



Ultra High Definition (UHD) Decoder

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (<https://www.hikvision.com>). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

This product can only enjoy the after-sales service support in the country or region where the purchase is made.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- **HIKVISION** and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.
- **HDMI**™ The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.
- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND

HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

© Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

Preface

Applicable Models

This manual is applicable to the DS-69XXUDI (C) series UHD decoders, including DS-6901UDI(C), DS-6904UDI(C), DS-6908UDI(C), DS-6910UDI(C), DS-6912UDI(C), and DS-6916UDI(C).

Default Parameters

Type	Default Parameter
Device	• Login user name: admin • IP address: 192.0.0.64
SSH connection	



To improve system security, it is highly recommended to change password regularly. In order to protect your privacy and corporate data and avoid network security issues, it is recommended to set strong password that meets security requirements.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Note	Provides additional information to emphasize or supplement important points of the main text.
 Caution	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Danger	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

Safety Instructions



In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.



- Provide a surge suppressor at the inlet opening of the device under special conditions such as the mountain top, iron tower, and forest.
- + identifies the positive terminals of the device which is used with, or generates direct current, and - identifies the negative terminals of the device which is used with, or generates direct current.
- The serial port of the device is used for debugging only.
- The interface varies with the models. Please refer to the product datasheet for details.
- The USB port of the device is used for connecting to a mouse, a keyboard, or a USB flash drive only. The current for the connected device shall be not more than 0.1 A.

TABLE OF CONTENTS

Chapter 1 Introduction	1
1.1 Overview	1
1.2 First-Time Configuration Process	1
Chapter 2 Device Basic Settings	2
2.1 Activate and Log In to Device	2
2.2 Configure the Network Address	5
2.2.1 Configure TCP/IP	5
Chapter 3 Video Wall Management	7
3.1 Configure the Video Wall	7
3.1.1 Configure the Video Wall Scale	7
3.1.2 Configure the Output	8
3.1.3 Manage Signal Sources	11
3.1.4 Bind Signal Sources with the Video Wall	14
3.2 Operate the Video Wall	16
3.2.1 Edit Signal Source Window Parameters	16
3.2.2 Manage Scenes	18
3.2.3 Maintain Screens	20
3.3 Configure Image Effect on Screen	22
3.3.1 Edit a Signal Source	22
3.3.2 Configure Encoding Parameters	25
3.3.3 Set Other Parameters	26
Chapter 4 Device Maintenance	28
4.1 View Device Status	28
4.2 Configure System Parameters	28
4.3 Configure HTTP(S) Parameters	32
4.4 Configure Event	33
4.5 Maintain the System	33
4.6 Maintain the Device Security	35

Chapter 1 Introduction

1.1 Overview

The DS-69XXUDI (C) ultra high definition (UHD) decoder (hereinafter referred as the device), is the latest generation decoder designed specifically for high-definition network cameras, making it suitable for various video security system projects. The device offers exceptional video processing capabilities and a seamless video decoding experience.

The device has the following core advantages:

- **Format Flexibility:** Supports various video encoding formats including H.265, H.264, MJPEG, Smart264, and Smart265 to meet diverse video source requirements.
- **Resolution Handling:** Decodes H.265 or H.264 video streams of up to 32 MP and lower resolution, ensuring real-time processing and output for high-definition video streams.
- **Output Compatibility:** Provides HDMI 1.4 and BNC ports for connection to various display devices.
- **Stunning UHD:** Supports 4K UHD decoding output, delivering enhanced image detail and improving the visual quality for both video security and video playback scenarios.

1.2 First-Time Configuration Process

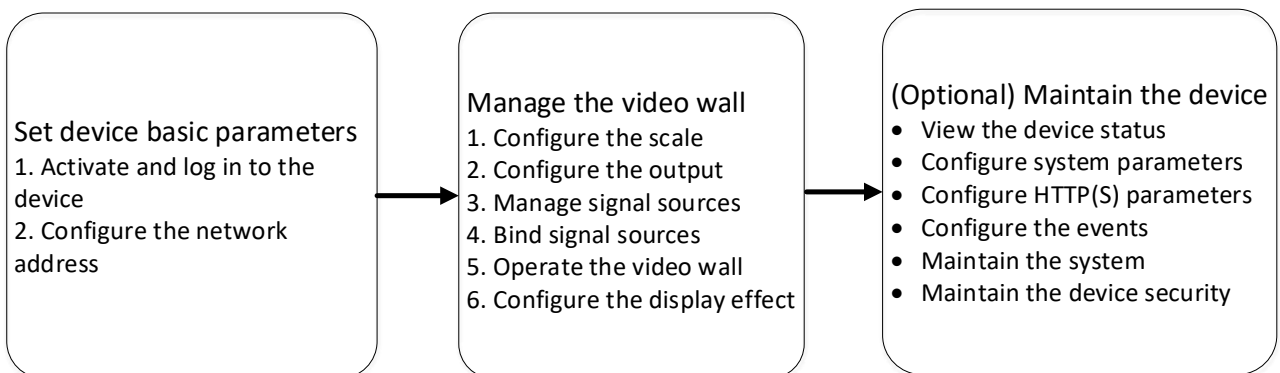


Figure 1-1 First-Time Configuration Process

Chapter 2 Device Basic Settings

2.1 Activate and Log In to Device

You should activate the device before using the device for the first time. You can use the SADP client or the device web page to activate the device. When activating the device, obey the following requirements to set the password:

- To improve system security, it is highly recommended to change password regularly. In order to protect your privacy and corporate data and avoid network security issues, it is recommended to set strong password that meets security requirements.
- Password should contain 8 to 16 characters and at least 2 of the following types: digits, lowercase letters, uppercase letters, and special characters.
- Password cannot contain user name, 123, admin (case insensitive), 4 or more continuously ascending or descending digits, or 4 or more consecutive repeated characters.

Use SADP Client and Web Page

Step 1 Connect the device and computer to the same LAN. Make sure that the device and computer are in the same network segment.

Step 2 Download the [SADP client](#) from the Hikvision website and install it on the computer.

Step 3 Open the SADP client.

Step 4 Select the device that is not activated, enter the activation password and confirm it, and click **Activate**.

If the device cannot be found, you can restart the SADP client.

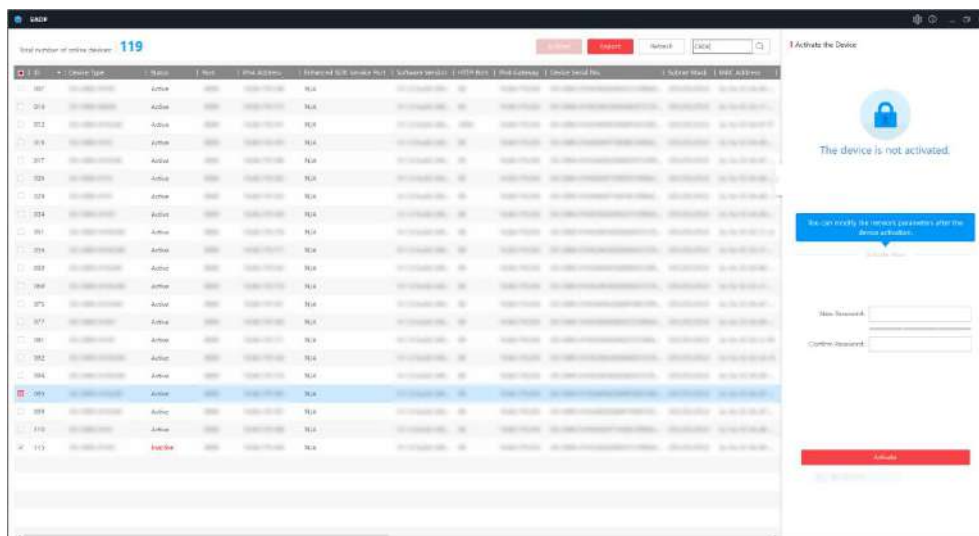


Figure 2-1 Activate the Device via SADP Client

Step 5 View the device IP address in the SADP client and enter the device IP address in the computer browser.

Step 6 Enter the user name and the set activation password, and then click **Log In**.

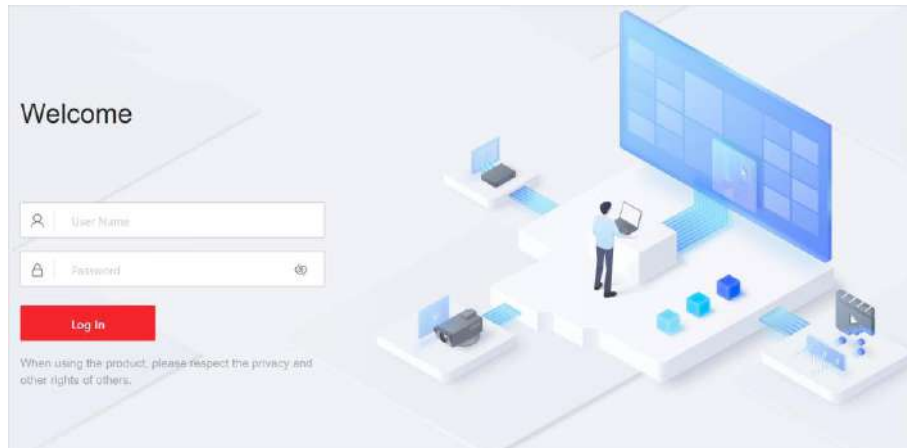


Figure 2-2 Login Page

Step 7 (Optional) To edit the password, you can click the user name in the upper right corner of the web page and then click **Change Password**.

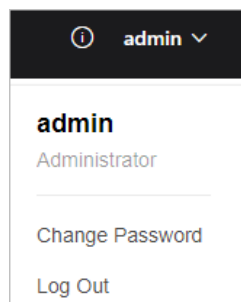


Figure 2-3 Change Password

Use Web Page

Step 1 Use a network cable to connect a computer to the device.

Step 2 Set the computer IP address to any IP address in the range of 192.0.0.2 to 192.0.0.253 (excluding 192.0.0.64) and set the computer gateway address to 192.0.0.1.

By default, the device IP address is 192.0.0.64 and the gateway address is 192.0.0.1.

Step 3 Enter 192.0.0.64 in the computer browser to enter the device activation page.

Step 4 Set the activation password, and then click **Activate**.

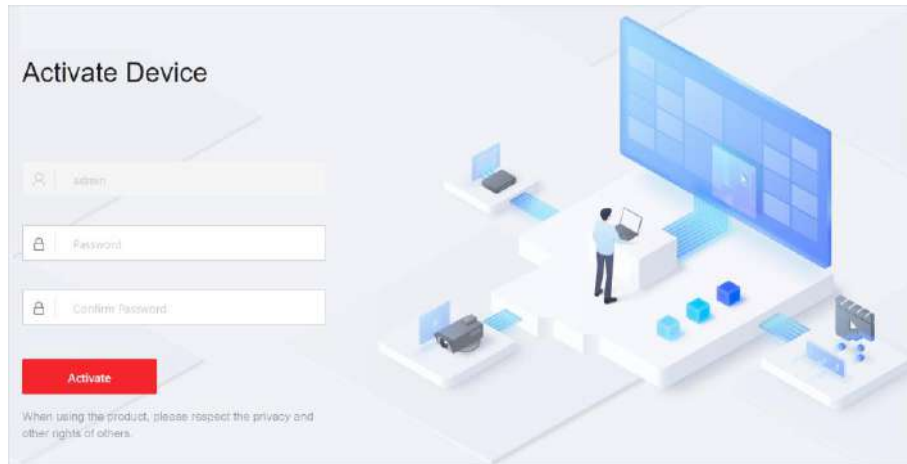


Figure 2-4 Activate the Device via Browser

Step 5 Enter the user name and the set activation password on the login page, and then click **Log In**.

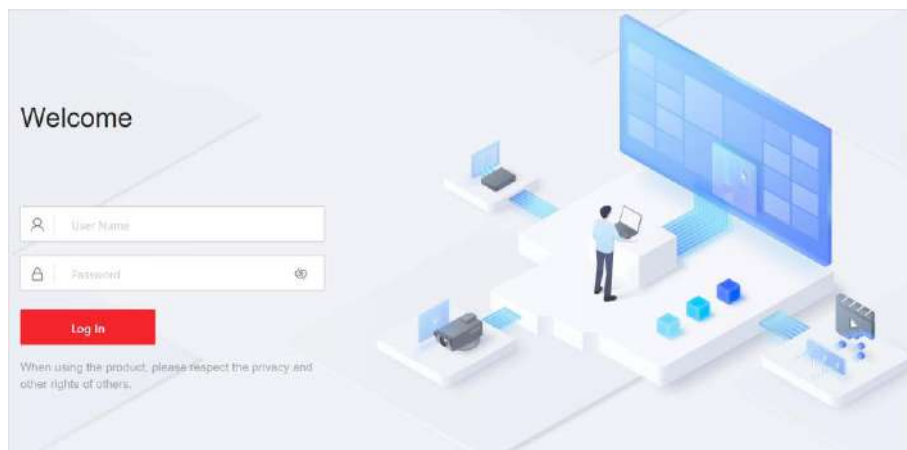


Figure 2-5 Login Page

Step 6 (Optional) To edit the password, you can click the user name in the upper right corner of the web page and then click **Change Password**.

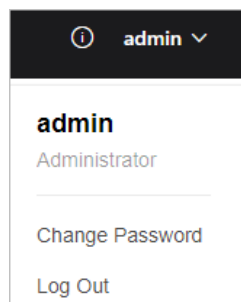


Figure 2-6 Change Password

2.2 Configure the Network Address

2.2.1 Configure TCP/IP

Before You Start

Make sure the device and the computer are in the same segment after the device connects to the on-site network.

Steps

Step 1 Go to **Configuration** → **Network** → **Network Configuration** → **TCP/IP**.

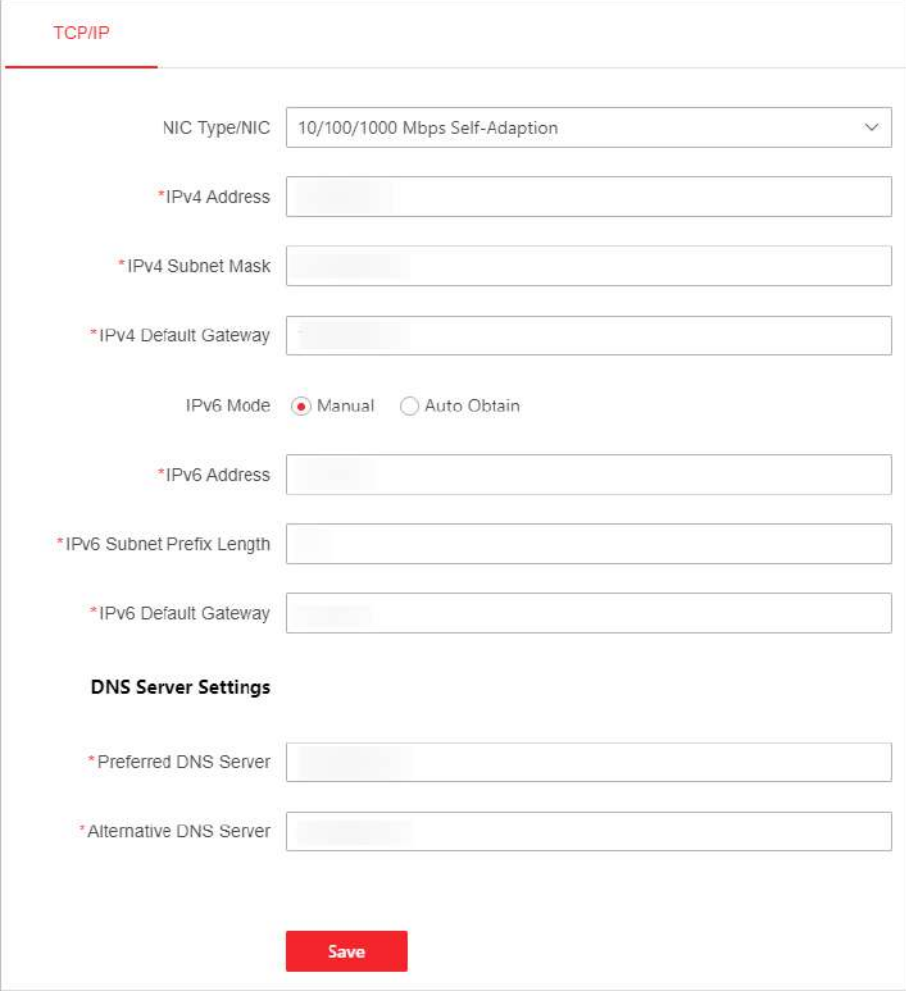
The screenshot shows a web-based configuration interface for TCP/IP settings. At the top, there is a red header bar with the text "TCP/IP". Below this, the "NIC Type/NIC" is set to "10/100/1000 Mbps Self-Adaption". The IPv4 section includes fields for "IPv4 Address", "IPv4 Subnet Mask", and "IPv4 Default Gateway", each preceded by a red asterisk. The IPv6 section has a "Mode" selector with "Manual" (selected) and "Auto Obtain" options, followed by fields for "IPv6 Address", "IPv6 Subnet Prefix Length", and "IPv6 Default Gateway", each preceded by a red asterisk. A "DNS Server Settings" section contains fields for "Preferred DNS Server" and "Alternative DNS Server", each preceded by a red asterisk. A red "Save" button is located at the bottom center of the form.

Figure 2-7 Configure TCP/IP Parameters

Step 2 Set the IPv4 address, subnet mask, and gateway.

Step 3 Set the IPv6 parameters:

- Select **Manual**, and then enter the IPv6 address, subnet prefix length, and gateway.
- Select **Auto Obtain**.

Step 4 Set the preferred and alternative DNS server.

Step 5 Click **Save**.

Step 6 Remove the network cable that connects the device and computer, and use the network cable to connect the device to the on-site network.

Step 7 Enter the configured device IP address in the web browser of the computer to log in to the web page of the device.

Chapter 3 Video Wall Management

3.1 Configure the Video Wall

3.1.1 Configure the Video Wall Scale

Step 1 Go to **Video Wall Configuration**, and then click **Edit Video Wall Scale**.

You can click **Edit Name** to change the video wall name.

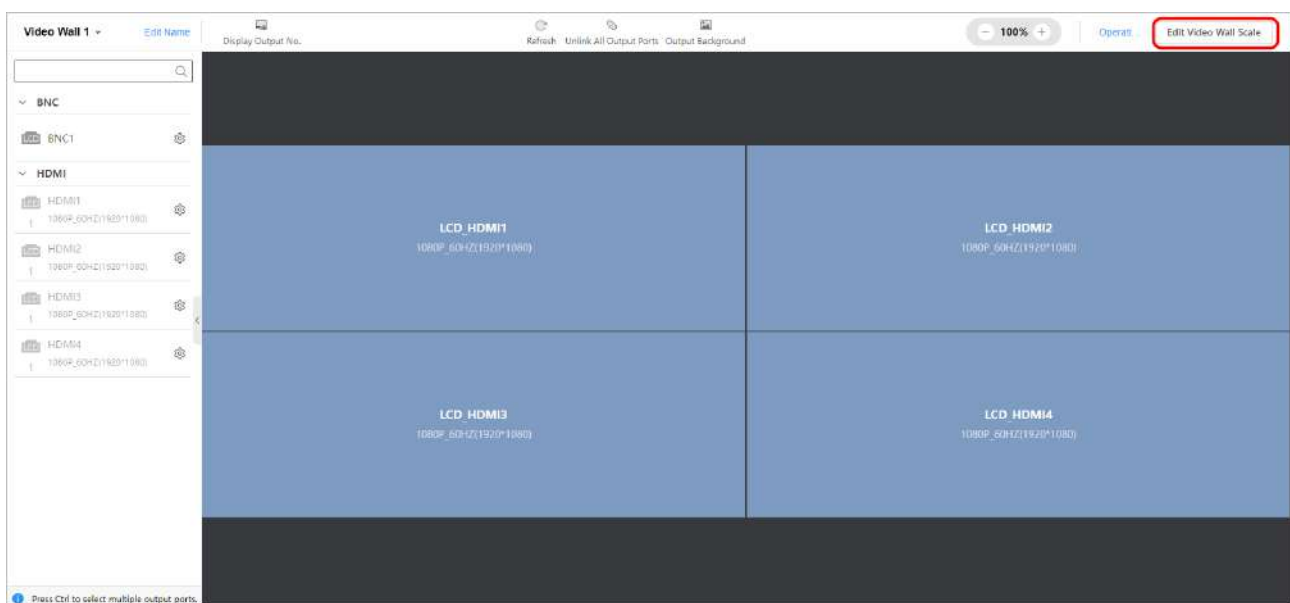


Figure 3-1 Video Wall Configuration Page

Step 2 According to the actual screen quantity, directly enter the number of rows and columns, or select the area with the mouse, and click **Save**.

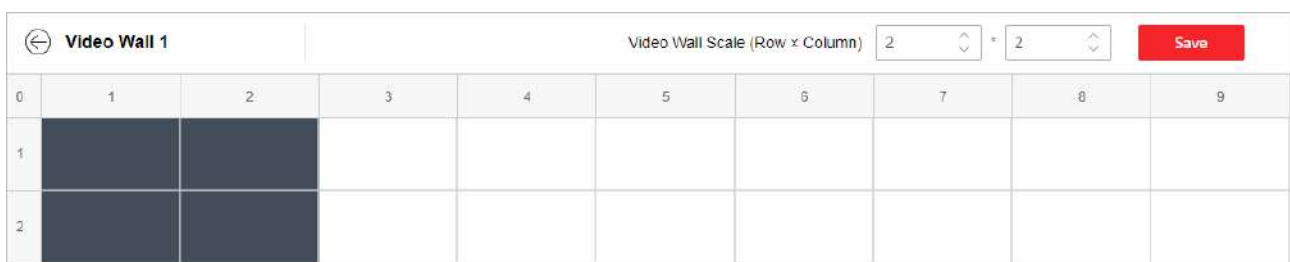


Figure 3-2 Set the Video Wall Scale

3.1.2 Configure the Output

Configure Output Port

On the **Video Wall Configuration** page, click  of an output port. According to the screen type, configure the output port and then click **Save**.

- Click  of a BNC port to select the video standard for the LCD screen.

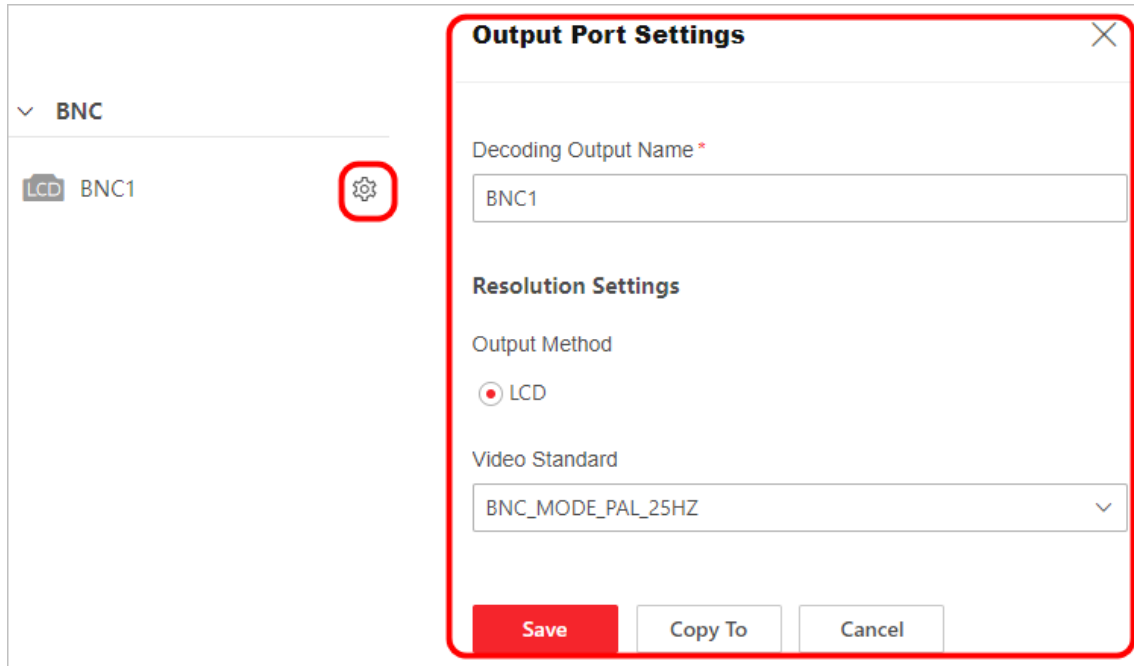


Figure 3-3 Configure a BNC port

- Click  of an HDMI port to configure its parameters:
 - The DVI mode has better compatibility and the HDMI mode supports embedded audio output. If you select AUTO, the output mode of the device output port will automatically adapt to the output mode supported by the screen.
 - If you select LCD output method, select the LCD screen resolution as required.
 - If you select LED output method, enter the width and height of the LED screen.
 - If you select the loading mode, make sure that the configured resolution (width × height) is smaller than 2.6 MP.
 - If you select the clipping mode, make sure that the configured resolution is smaller than the reference resolution that is shown when you select the LCD output method.

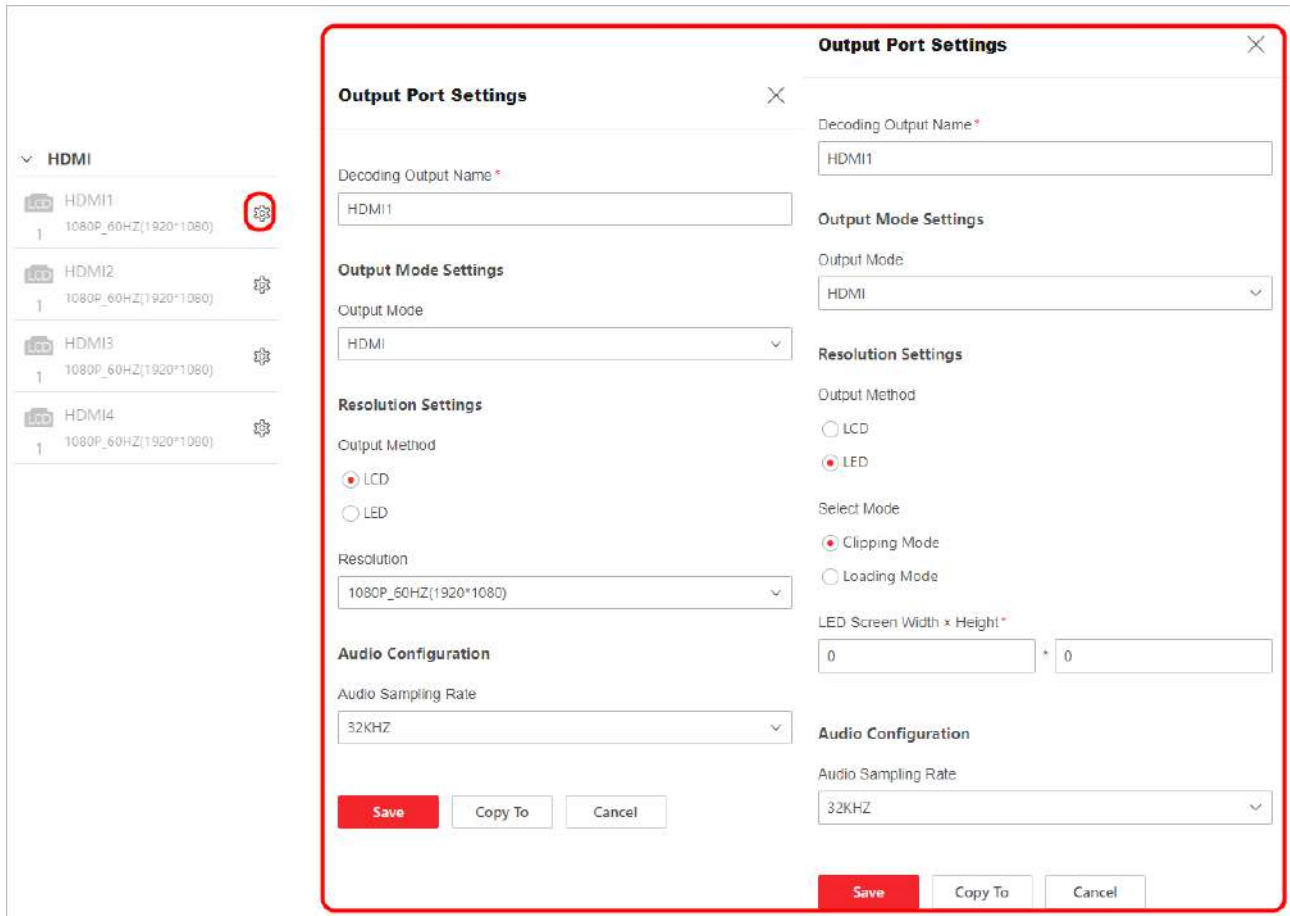


Figure 3-4 Configure an HDMI Port

- Click **Copy To** to copy the current output configuration to other output ports.

Bind Output Ports with Video Wall

Step 1 Click **Display Output No..**

Step 2 According to the output number shown on the actual screen, drag the corresponding output ports to the screens of the video wall.

- To batch bind output ports with the video wall, press Ctrl to select multiple output ports and drag the output ports to the screens of the video wall.
- To cancel the linkage between a screen and an output port, click  in the upper right corner of the screen.
- To cancel the linkage between all screens and output ports, click **Unlink All Output Ports**.

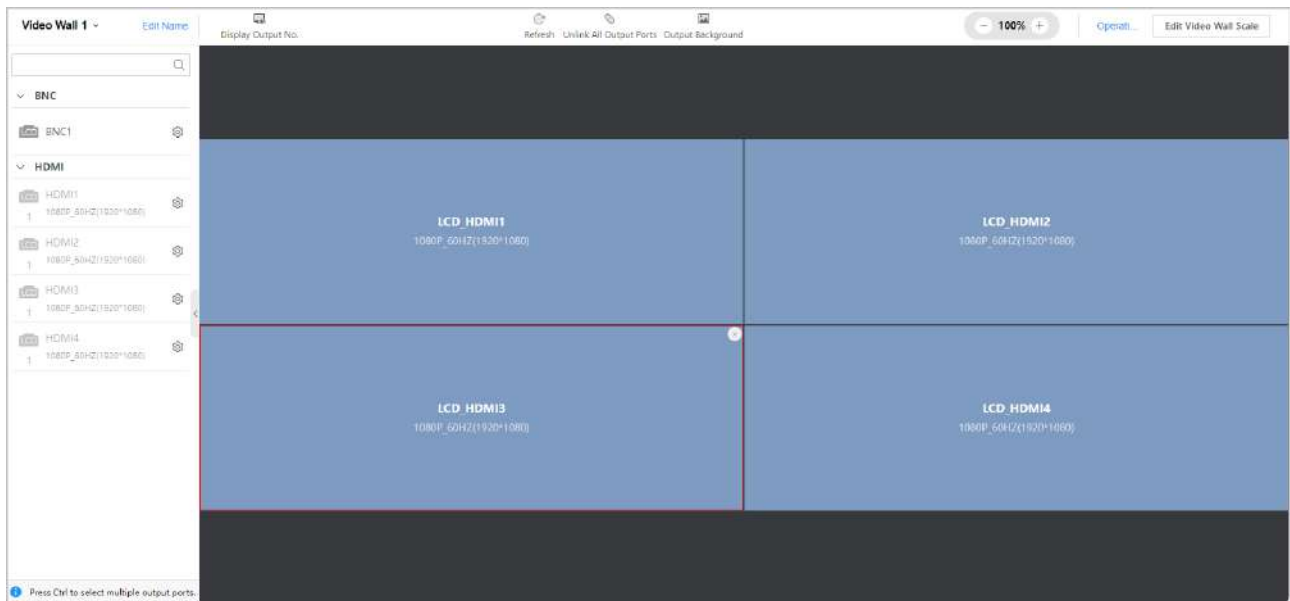


Figure 3-5 Bind Output Ports with Video Wall

Step 3 (Optional) If the screens that are used to configure the video wall support control linkage function, you can perform the following operations to automatically bind output ports to the screens of the video wall.

- 1) Make sure all screens are enabled with the control linkage function.
- 2) Use the remote control to set the location information for all actual screens.
- 3) Click **Edit Wall Scale** and select **Auto Configure**.

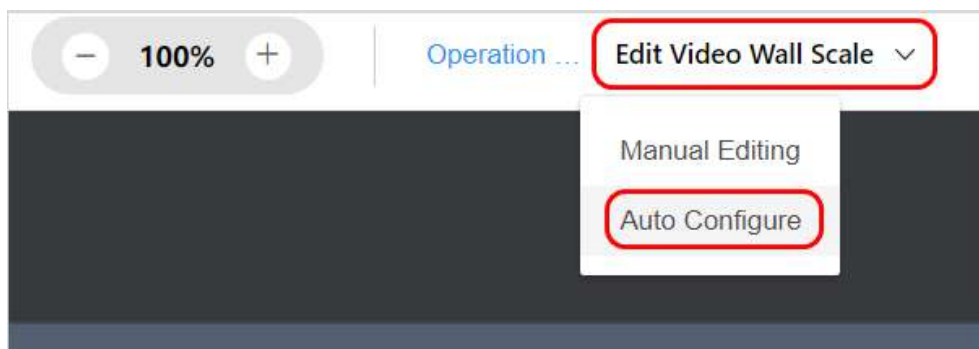


Figure 3-6 Auto Bind Output Ports with Screens

Configure Output Background

At the top of the **Video Wall Configuration** page, click **Output Background** to edit the background color or import images.

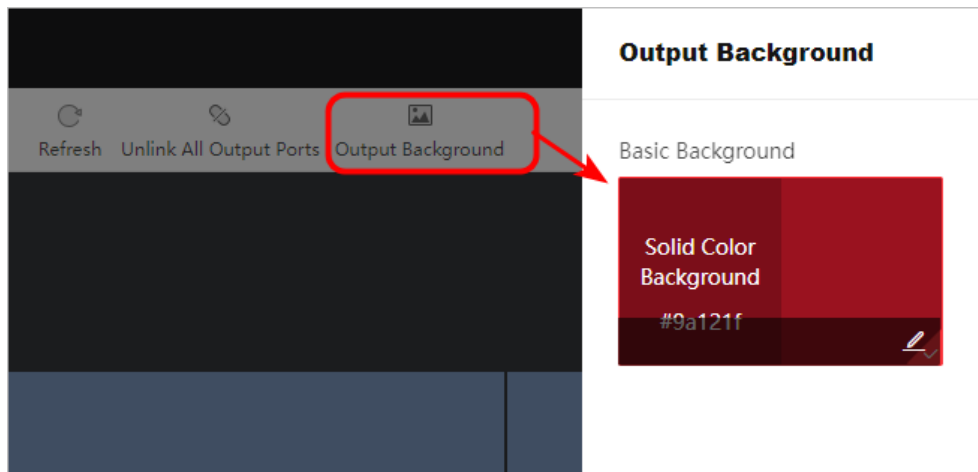


Figure 3-7 Edit Output Background

3.1.3 Manage Signal Sources

Add a Network Signal Source via IP Address

Step 1 Go to **Video Wall Operation** → **Source**, click , and select **IP Address**.

Step 2 Enter the signal source information and stream media information.

- (Optional) Enable **Encrypted Stream** and enter the secret key.
- Select an added group or click **Add Group** to create a new group.
- Click **More** to select the transmission protocol, stream type, encrypted stream, device manufacturer, and streaming media information.

After enabling **Get Stream via Streaming Server**, you can perform live view data forwarding through the streaming server to reduce network stress.

Step 3 Click **Save**.

Figure 3-8 Add a Network Signal Source via IP Address

Add a Network Signal Source via DDNS

Before you start

Before adding network signal sources via DDNS, you should configure DNS servers on the **TCP/IP** page.

Steps

Step 1 Go to **Video Wall Operation** → **Signal Source**, click , and select **DDNS**.

Step 2 Enter the signal source information and stream media information.

- (Optional) Enable **Encrypted Stream** and enter the secret key.
- Select an added group or click **Add Group** to create a new group.
- Click **More** to select the transmission protocol, stream type, device manufacturer, and streaming media information.

After enabling **Get Stream via Streaming Server**, you can perform live view data forwarding through the streaming server to reduce network stress.

Step 3 Click **Save**.

The screenshot shows the 'Add Signal Source' dialog box with the 'DDNS' tab selected. The dialog is divided into two main sections. The left section contains fields for 'Device Name *', 'Host IP Address *', 'Port No. *', 'User Name *', 'Password *', and 'Group *'. The 'Group *' section includes a '+ Add Group' button and two input fields with values '0' and '1'. Below these are two buttons labeled 'onvif' and 'test'. The right section, titled 'More', contains a 'Transmission Protocol' dropdown set to 'TCP', a 'Stream Type' dropdown set to 'Main Stream', an 'Encrypted Stream' toggle switch, a 'Device Manufacturer' dropdown set to 'HIKVISION', a 'Get Stream via Streaming Server' toggle switch, a 'Stream Media IP Address' field, a 'Port No.' field, and another 'Transmission Protocol' dropdown set to 'TCP'. At the bottom right are 'Save' and 'Cancel' buttons.

Figure 3-9 Add a Network Signal Source via DDNS

Add a Network Signal Source via URL

Step 1 Go to **Video Wall Operation** → **Source**, click , and select **URL**.

Step 2 Enter the device name and the URL.

Step 3 (Optional) Enable **Encrypted Stream** and enter the secret key.

Step 4 Select an added group or click **Add Group** to create a new group.

Step 5 Click **Save**.

Add Signal Source

IP Address DDNS **URL**

Device Name *

URL *

Encrypted Stream

Group *

+ Add Group 0 1

onvif test

Save Cancel

Figure 3-10 Add a Network Signal Source via URL

Batch Delete Network Signal Sources

To batch delete invalid network signal sources, you can select multiple network signal sources with Ctrl or Shift pressed and then click .

3.1.4 Bind Signal Sources with the Video Wall

Note

You can bind a maximum of 1-channel 4K local signal source to the video wall.

Go to **Video Wall Operation**, take either of the following methods to bind signal sources with the video wall:

- Select a signal source and then drag it rightward to the video wall.
 - If you bind a signal source to an LCD video wall, the signal source window fully covers a single screen by default.
 - If you bind a signal source to an LED video wall, the signal source window fully covers the LED video wall by default.

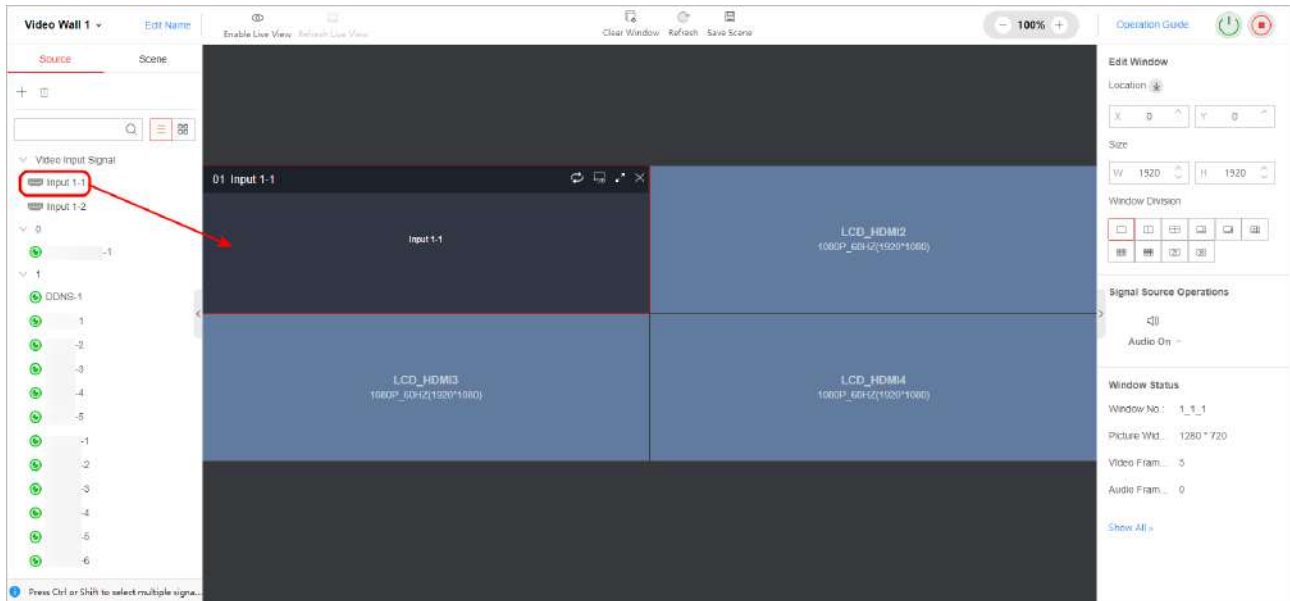


Figure 3-11 Bind a Signal Source to LCD Video Wall

- Choose either of the following methods to batch bind signal sources to the video wall:
 - Drag the video input signal group or a newly created network signal source group rightward to the video wall. The local signal sources join the video input signal group by default.
 - Press Ctrl to select multiple signal sources of the same group, and drag signal sources rightward to the video wall.

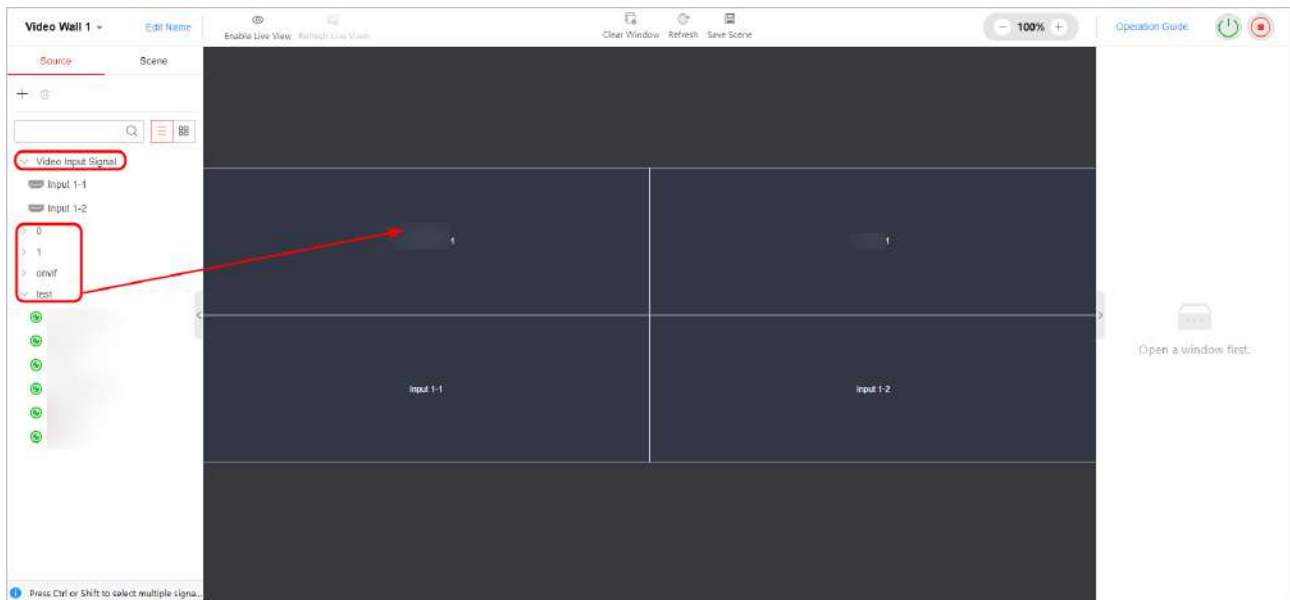


Figure 3-12 Batch Bind Signal Sources to Video Wall

3.2 Operate the Video Wall

3.2.1 Edit Signal Source Window Parameters

Edit a Signal Source Window

On the **Video Wall Operation** page, select a signal source window and perform the following operations as required:

- Adjust the window position: Move the window directly or enter the specific X and Y values.
- Divide the window: Click a window division icon.
- Adjust the window size:
 - Drag the window edge to adjust its size.
 - Enter W and H values.
 - Click  in the upper right corner of the window to make it fully cover the occupied output ports and click  to restore the original size.
- Set the window to the bottom: Click .

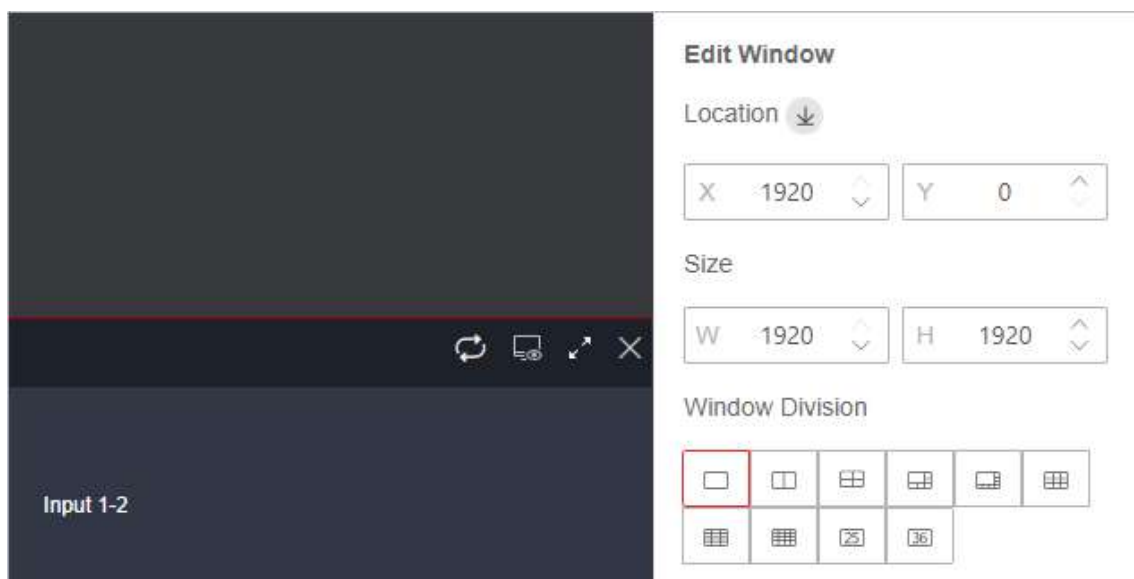


Figure 3-13 Adjust Position of a Signal Source Window

- Enable audio for a signal source window.
 - Select a local signal source, click **Audio On** and select an audio output port to enable the audio for the local signal source.

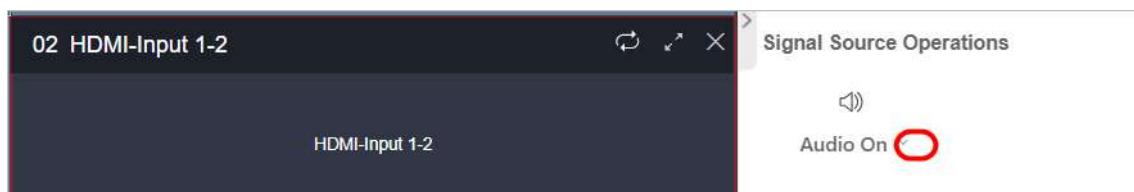


Figure 3-14 Configure Audio for Local Signal Source

- Select a network signal source to configure its decoding status, audio status, decoding delay, smart decoding, and stream exporting.
 - After you enable Websocket, you can export stream.
 - After you enable smart decoding, the device can decode the smart alarm events from the network cameras.

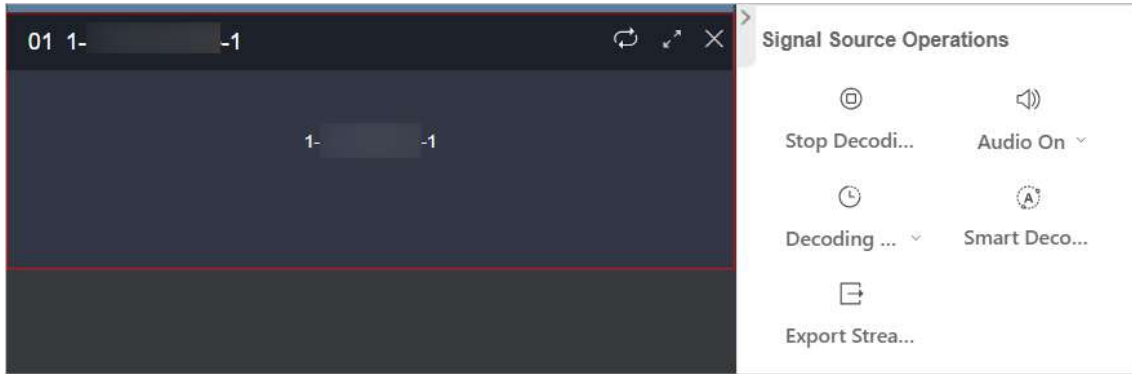


Figure 3-15 Configure Audio for Network Signal Source

- Set the signal source group auto-switching: Click  in the upper right corner of the signal source window, select a signal source group, set the image interval, and then click **Start Auto-Switch**.

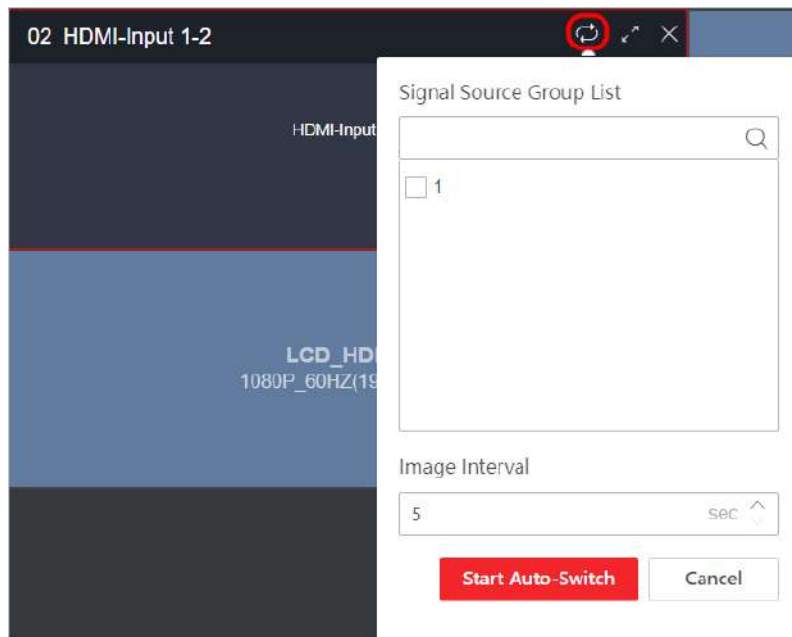


Figure 3-16 Set Signal Source Group Auto-Switching

- View the window status: You can click **Show All** to view the decoding status list.

Edit Multiple Signal Source Windows

On the **Video Wall Operation** page, perform the following operations as required:

- Preview the signal sources:

- Click  in the upper right corner of a signal source window to preview the signal source. Click  to cancel the live view.
- Click **Enable Live View** at the top of the **Video Wall Operation** page to preview all signal sources on the video wall. Click **Close Live View** to stop previewing all signal sources on the video wall.
- Click **Refresh Live View** at the top of the **Video Wall Operation** page to refresh the live view of all signal sources.

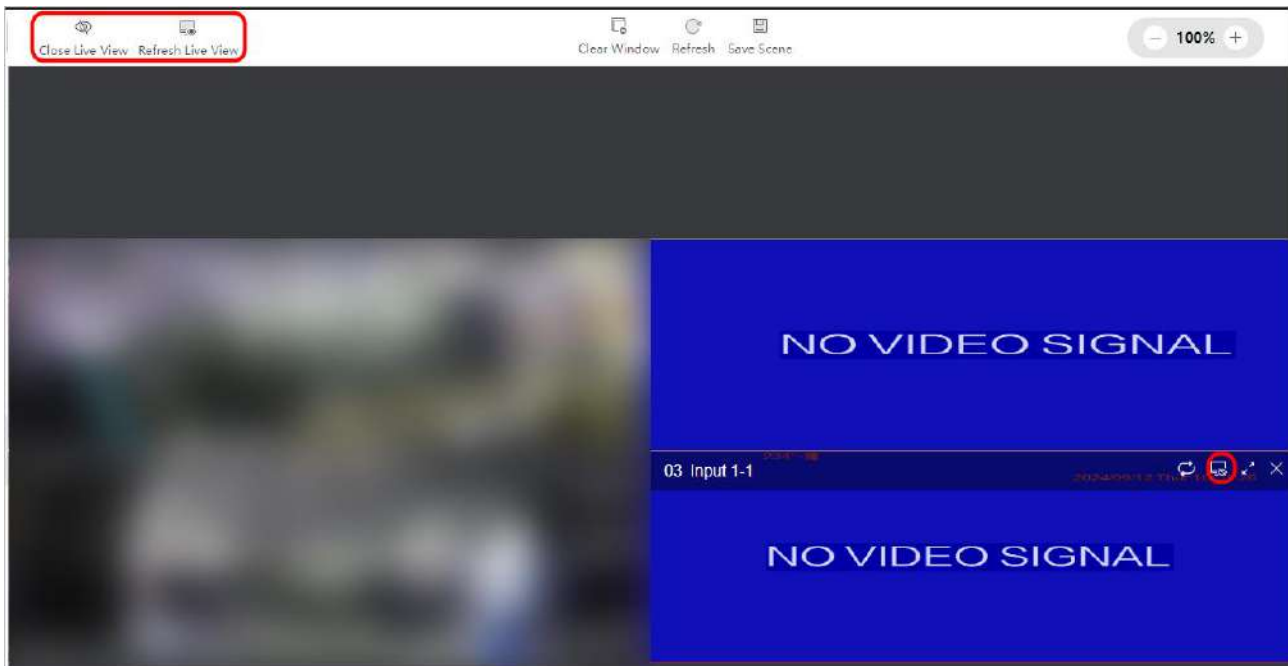


Figure 3-17 Preview Signal Source

- Power on or off all screens: Click  or .
- Clear all bound signal source windows: Click **Clear Window**.

3.2.2 Manage Scenes

Up to 64 scenes are supported. Go to **Video Wall Operation** to manage scenes.

- Click **Save Scene** to save the configuration as a new scene or overwrite the existing scene.

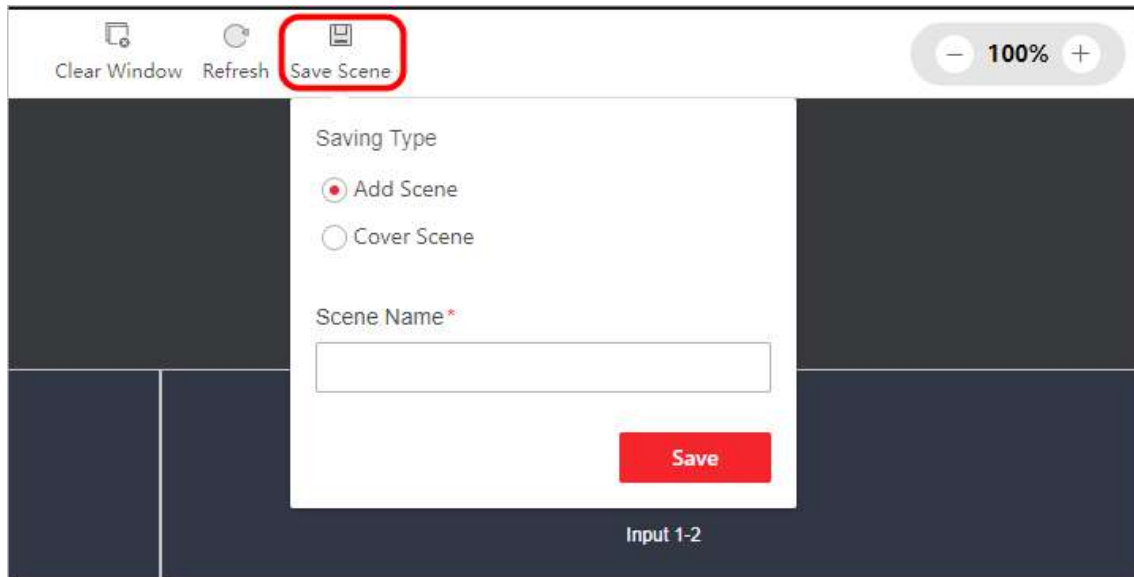


Figure 3-18 Save Scene

- Click **Scene** and hover over a scene name. Click  to call the scene.
- Click **Scene** and hover over a scene name. Click  to edit the scene name.
- Click **Scene** and hover over a scene name. Click  to delete the scene.

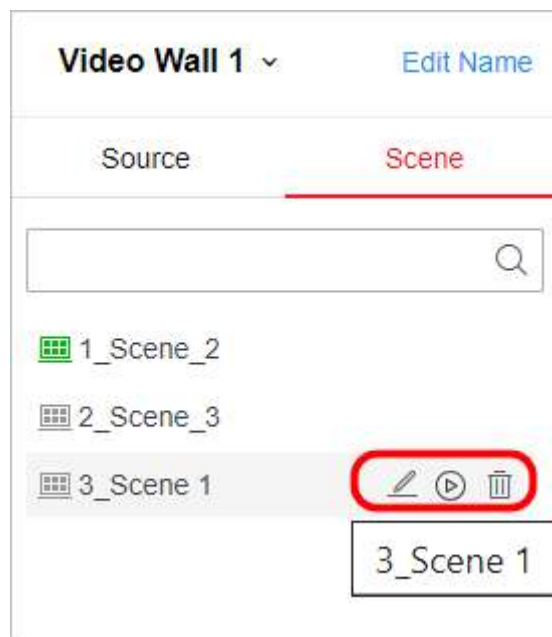
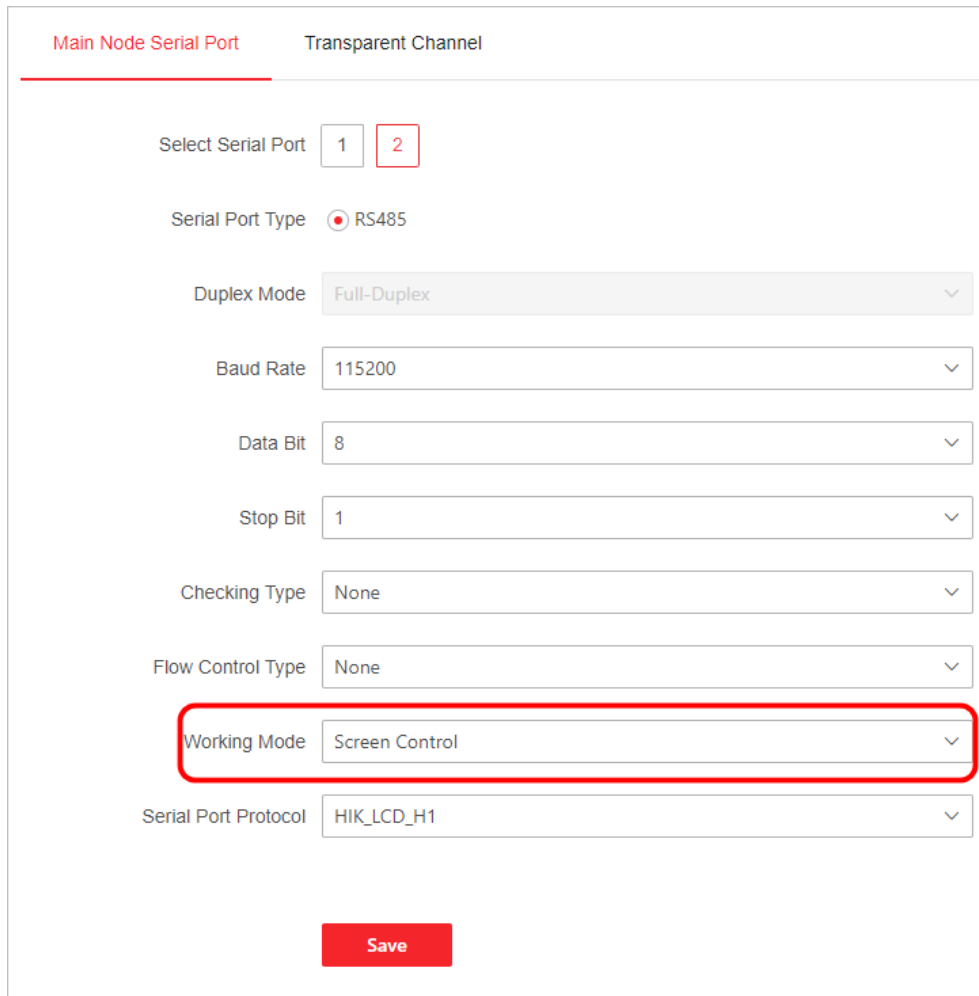


Figure 3-19 Manage Scene

3.2.3 Maintain Screens

Control Screen via Serial Port

Step 1 Go to **Configuration** → **System** → **Serial Port Settings** → **Main Node Serial Port**, select serial port 2, select **Screen Control** as the working mode, set the baud rate of the device same as the baud rate of the screen, and set other serial port parameters.



The screenshot displays the 'Main Node Serial Port' configuration window. At the top, there are two tabs: 'Main Node Serial Port' (selected) and 'Transparent Channel'. Below the tabs, the following settings are visible:

- Select Serial Port:** Two buttons labeled '1' and '2'. Button '2' is highlighted with a red border.
- Serial Port Type:** A radio button selection with 'RS485' selected.
- Duplex Mode:** A dropdown menu set to 'Full-Duplex'.
- Baud Rate:** A dropdown menu set to '115200'.
- Data Bit:** A dropdown menu set to '8'.
- Stop Bit:** A dropdown menu set to '1'.
- Checking Type:** A dropdown menu set to 'None'.
- Flow Control Type:** A dropdown menu set to 'None'.
- Working Mode:** A dropdown menu set to 'Screen Control', which is highlighted with a red rectangular box.
- Serial Port Protocol:** A dropdown menu set to 'HIK_LCD_H1'.

At the bottom center of the window is a red 'Save' button.

Figure 3-20 Configure Serial Port

Step 2 Use a serial port cable to connect a screen and the device RS-485 port.

Step 3 Go to **Screen Maintenance** and select the screen that is connected with the serial port cable.

Step 4 Select an image mode and adjust the backlight.

Step 5 (Optional) Click  to power on the screen or click  to power off the screen.

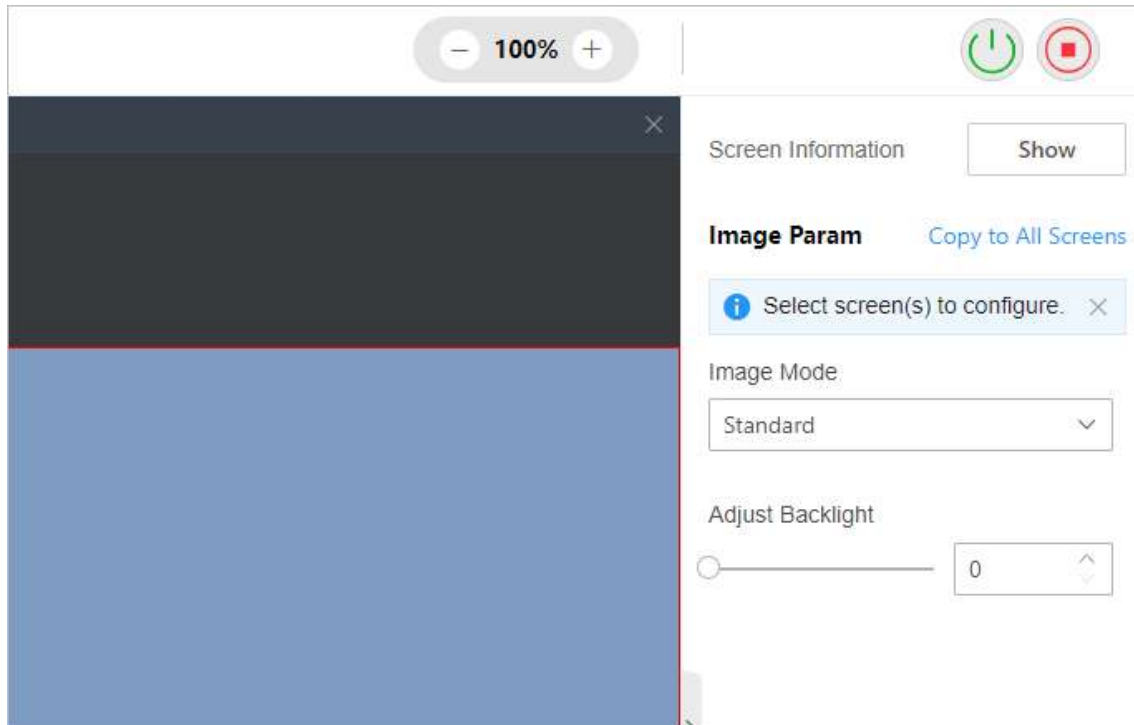


Figure 3-21 Control Screen via Serial Port

Control Screens via HDMI Ports

Step 1 Use multiple HDMI cables to connect the multiple screens to the device. Make sure all connected screens support and are enabled with the control linkage function.

Step 2 Go to **Screen Maintenance** and select a screen.

Step 3 Select an image mode and adjust the backlight.

Step 4 (Optional) You can perform the following operations as required:

- Click **Show** to show the serial number, software version, work duration, and device temperature on all screens.
- Click  or  to power on or off all screens that are connected with the HDMI cables.
- Click **Copy to All Screens** to copy the image parameters of the current screen to all screens.

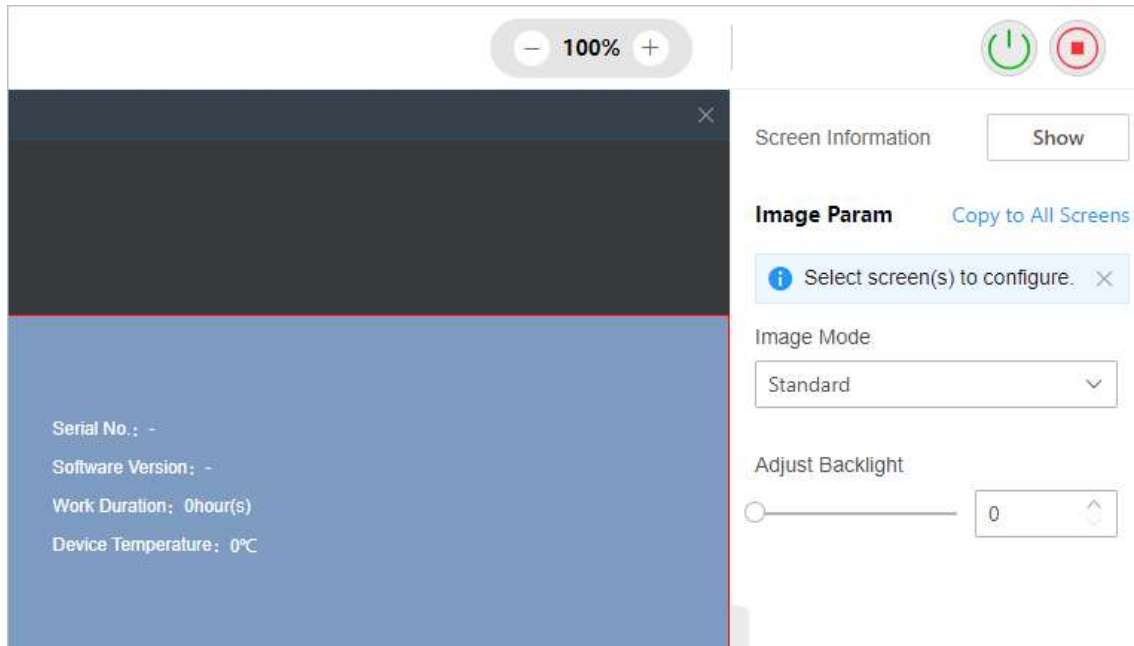


Figure 3-22 Show Screen Information

3.3 Configure Image Effect on Screen

3.3.1 Edit a Signal Source

Edit a Local Signal Source

Go to **Video Wall Operation**, hover over a local signal source and then click  to edit its parameters:

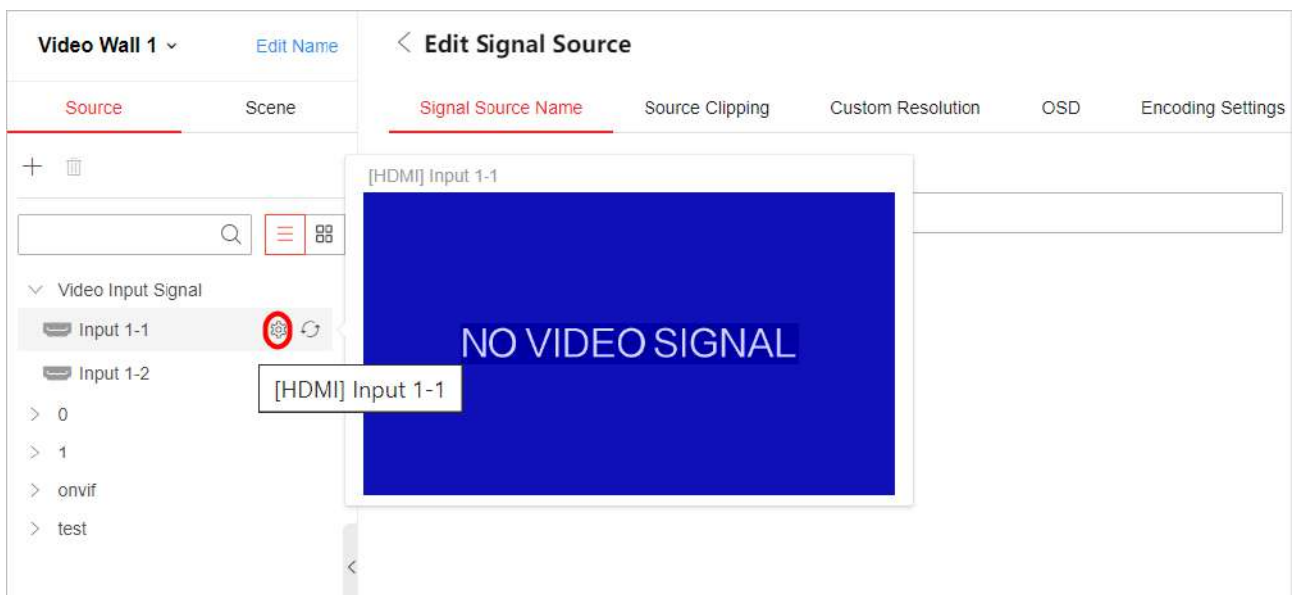


Figure 3-23 Edit a Local Signal Source

- Edit the signal source name.
- Click **Source Clipping**, and set the clipping value at top, bottom, left, and right edges.
The clipping value ranges from 0 to 200. The clipping value at the top and bottom edges should be a multiple of 2, and the clipping value at the left and right edges should be a multiple of 4.



Signal Source Name Input 1-1

Top Edge Clipping 0 Pixel  

Lower Edge Clipping 0 Pixel  

Left Edge Clipping 0 Pixel  

Right Edge Clipping 0 Pixel  

Save

NO VIDEO SIGNAL

Figure 3-24 Clip a Signal Source

- If the resolution of a signal source does not match the resolution of the screen, you can customize the signal source resolution.
 - 1) Click **Custom Resolution**.
 - 2) Enable custom resolution and set the refresh rate and resolution. The width should be a multiple of 4 and the height should be a multiple of 2.
 - 3) (Optional) Click **Copy To** to copy the resolution configuration of the current signal source to other signal sources.
 - 4) Click **Save**.



Signal Source Name Input 1-1

Enable 

*Refresh Rate 30 

*Resolution 1920 * 1080

Save Copy To

NO VIDEO SIGNAL

Figure 3-25 Customize Resolution

- Click **OSD**, and then you can add channel name, date, time, character 1, or character 2 to the input signal image.
 - Set the font size, font color, and font direction.
 - Enter the position values or directly drag the character to adjust the position.
 - Customize the channel name and character content.

- Click **Copy To** to copy the OSD configuration of the current signal source to other signal sources.

Signal Source Name: Input 1-1

Basic Configuration

Font Size: 64

Font Color: #f4a00d

Font Direction: Custom

Channel Name

Enable: ☒

*Name: Input 1-1

*Character Position: 333 + 0

Date and Time

Date: ☒

Date Display Format: YYYY/MM/DD

Time: ☒

Time Format: ☐ 12 Hours ☒ 24 Hours

*Character Position: 1272 + 199

Text Overlay

Character: Character 1 Character 2

Enable: ☒

*Character Content: Welcome

*Font Size: 64

Font Color: #000000

*Character Position: 1409 + 1400

Save **Copy To**

Figure 3-26 Add OSDs

Edit a Network Signal Source

Go to **Video Wall Operation**, hover over a network signal source and then click  to edit its parameters.

Edit Signal Source ✕

Device Name*
-1

IP Address*

Port No.*
8000

User Name*
user

Password*

Group*

+ Add Group	0	1
onvif	test	

More ⬆

Transmission Protocol
TCP

Stream Type
Main Stream

Encrypted Stream
☐

Device Manufacturer
HIKVISION

Channel No.
1

Get Stream via Streaming Server
☐

Stream Media IP Address

Port No.

Transmission Protocol
TCP

Save Copy To Cancel

Figure 3-27 Edit a Network Signal Source

3.3.2 Configure Encoding Parameters

Step 1 Go to **Video Wall Operation**, hover over a local signal source and then click .

Step 2 Click **Encoding Settings**.

Step 3 Set the video encoding parameters.

- Set the bit rate type and maximum bit rate.
 - If you select **Constant Bit Rate**, the device uses the average bit rate for transmission and uses fast compression speed. The video mosaic might occur.
 - If you select **Variable Bit Rate**, the device automatically adjusts the bit rate for transmission as long as the bit rate is within the limit and uses slow compression speed to ensure the image definition in complex scenarios.

- If you select **Variable Bit Rate**, you should select a video quality. The higher video quality, the higher the bandwidth requirement.
- Enter an I-frame interval. The larger the I-frame interval, the smaller the stream fluctuation, and the lower the image quality.
- Select a resolution. The higher resolution, the higher the bandwidth requirement.
- Select an encoding type and video type.

Step 4 Select an audio encoding type.

Step 5 Click **Save**.

The screenshot displays the 'Signal Source Name' as 'Input 1-1'. The 'Video Encoding' section includes the following settings:

- Stream Type:** Radio buttons for 'Main Stream (Scheduled)' and 'Sub-stream' (selected).
- Bit Rate Type:** Radio buttons for 'Variable Bit Rate' and 'Constant Bit Rate' (selected).
- Video Quality:** A dropdown menu set to 'Medium'.
- *I-Frame Interval:** A text input field containing '60'.
- *Custom Max. Bit Rate:** A dropdown menu set to '512' kbps.
- Resolution:** A dropdown menu set to '704*576'.
- Frame Rate:** A dropdown menu set to '20' fps.
- Encoding Type:** Radio buttons for 'H.264' and 'H.265' (selected).
- Video Type:** Radio buttons for 'Video Stream' and 'Video and Audio Stream' (selected).

The 'Audio Encoding' section includes:

- Encoding Type:** A dropdown menu set to 'G.722.1'.

A red 'Save' button is located at the bottom of the configuration panel.

Figure 3-28 Configure Encoding Parameters

3.3.3 Set Other Parameters

Go to **Configuration** → **Other Settings** to set the following parameters:

- Enable **Sub-Stream Auto-Switch** and set the window division threshold.

If the window division reaches the window division threshold, the device will automatically use sub-stream to get the images. In low bandwidth networks, you can use sub-stream to get relatively smooth images with a small bandwidth footprint.

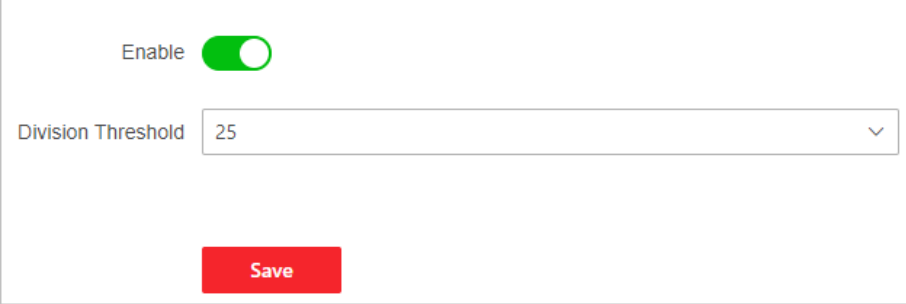
The screenshot shows a settings panel for 'Sub-Stream Auto-Switch'. At the top, there is a toggle switch labeled 'Enable' which is turned on (green). Below it, there is a dropdown menu labeled 'Division Threshold' with the value '25' selected. At the bottom of the panel is a red button labeled 'Save'.

Figure 3-29 Set Sub-Stream Auto-Switch

- Click **Display Settings** to configure the content displayed when decoding ends, when streaming fails, and when the decoding resource is insufficient.

If you select **Connection Exception**, the specific streaming failure reason will be displayed on the screen.

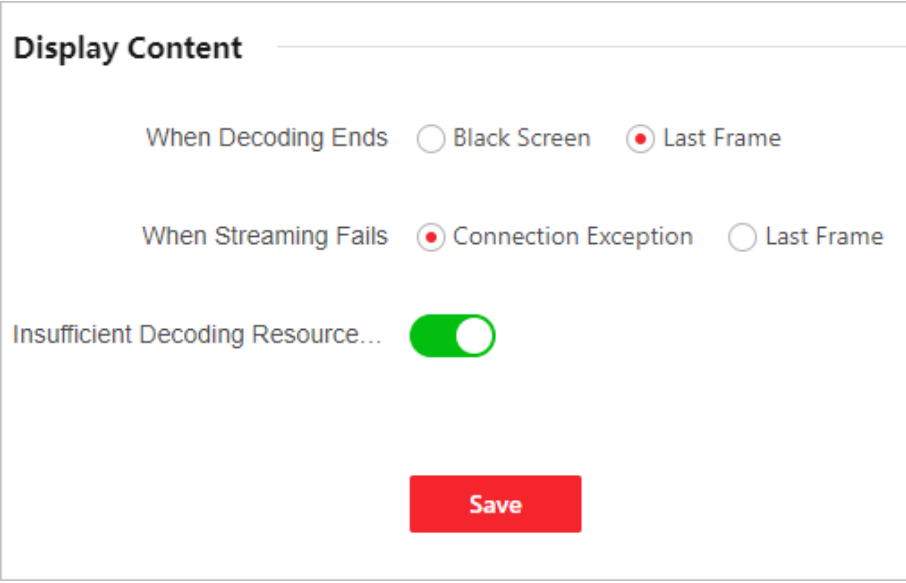
The screenshot shows a settings panel titled 'Display Content'. It contains three sections: 'When Decoding Ends' with radio buttons for 'Black Screen' and 'Last Frame' (selected); 'When Streaming Fails' with radio buttons for 'Connection Exception' (selected) and 'Last Frame'; and 'Insufficient Decoding Resource...' with a toggle switch that is turned on (green). A red 'Save' button is at the bottom.

Figure 3-30 Set Display Content

- Click **Decoding Delay** and select a default decoding delay level of the device.

Chapter 4 Device Maintenance

4.1 View Device Status

Click **Overview** to view the decoding resource status, network status, device status, and subsystem status.



Figure 4-1 View Device Status

4.2 Configure System Parameters

Go to **Configuration** → **System** to configure the following parameters:

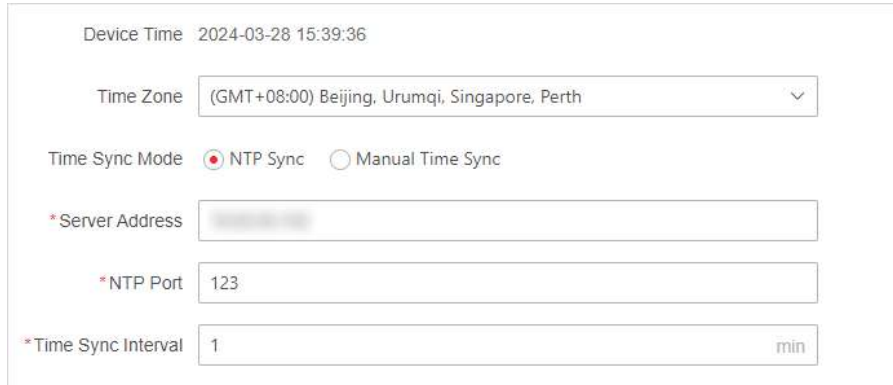
- Go to **System Settings** → **Basic Information** to view the device information and edit the device name as required. You can click **Upgrade** to go to the upgrade page for device upgrade.

The 'Basic Information' configuration page includes the following fields and controls:

- Device Name:** A text input field containing 'Decoder'.
- MAC Address:** A text input field.
- Model:** A text input field.
- Device Serial No.:** A text input field.
- Main Control:** A text input field with an **Upgrade** button next to it.
- Decoder Version:** A text input field.
- Web Version:** A text input field.
- Save:** A red button at the bottom of the form.

Figure 4-2 View Basic Information

- Go to **System Settings** → **Time Settings**, if you select **NTP Sync**, the device clock synchronizes with the clock of the NTP server at the specified interval.
 - Set the address and port number of the NTP server.
 - Set the synchronization interval.



Device Time 2024-03-28 15:39:36

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync Mode ☒ NTP Sync ☐ Manual Time Sync

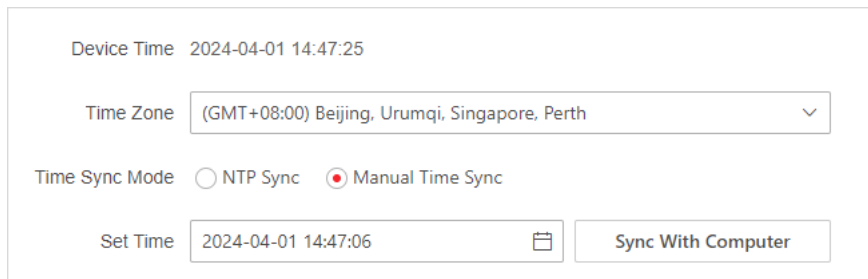
* Server Address

* NTP Port 123

* Time Sync Interval 1 min

Figure 4-3 Select NTP Sync

- On the **Time Settings** page, if you select **Manual Time Sync**, you can click **Sync with Computer** to make the device time same as the computer time.



Device Time 2024-04-01 14:47:25

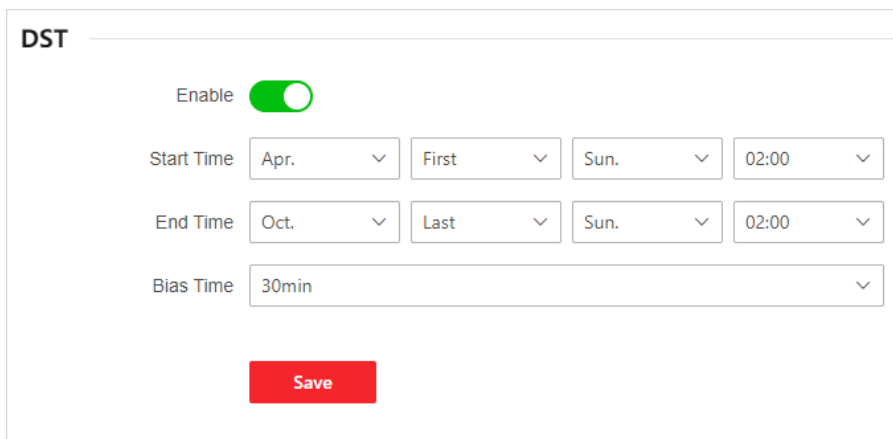
Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Sync Mode ☐ NTP Sync ☒ Manual Time Sync

Set Time 2024-04-01 14:47:06 Sync With Computer

Figure 4-4 Select Manual Time Sync

- On the **Time Settings** page, if you enable DST (Daylight Saving Time), the device clock is set forward a specified time during the summer months.
 - Set the start time and end time.
 - Set the bias time.



DST

Enable ☒

Start Time Apr. First Sun. 02:00

End Time Oct. Last Sun. 02:00

Bias Time 30min

Save

Figure 4-5 Enable DST

- Go to **User Management** → **User Management** to add users, edit the user name or password, or delete the users. When the user type is administrator, you cannot edit or delete it.

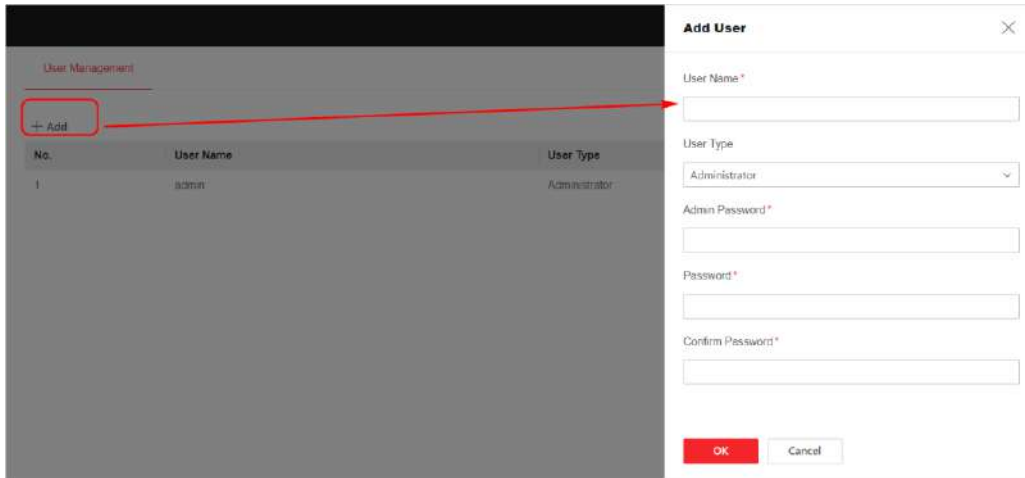


Figure 4-6 Manage Users

Control the Device via Keyboard

- Step 1 Go to **Configuration** → **System** → **Serial Port Settings** → **Main Node Serial Port**, select serial port 2, select **Keyboard Control** as the working mode, set the baud rate of the device same as the baud rate of the keyboard, and set other serial port parameters.

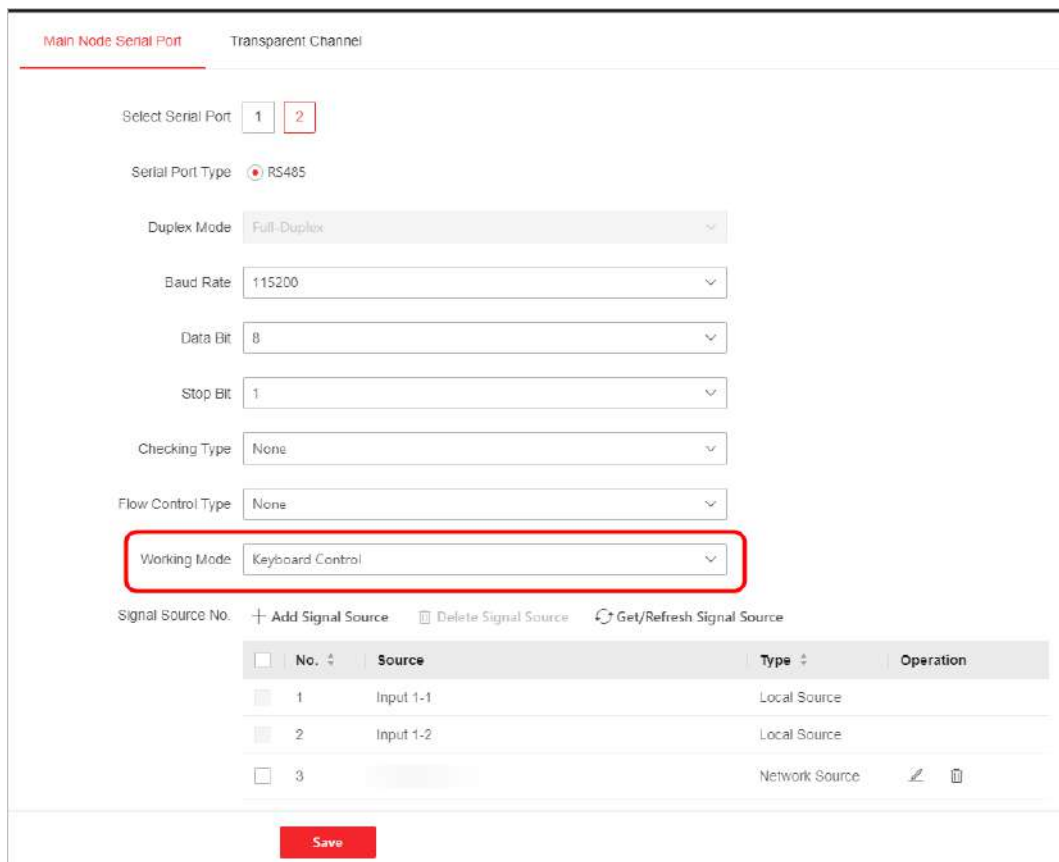


Figure 4-7 Control the Device via Keyboard

Step 2 (Optional) For a serial keyboard, click **Get/Refresh Signal Source** to obtain the local signal sources and click **Add Signal Source** to add the network signal source.

Step 3 Use a serial port cable to connect the keyboard and device.

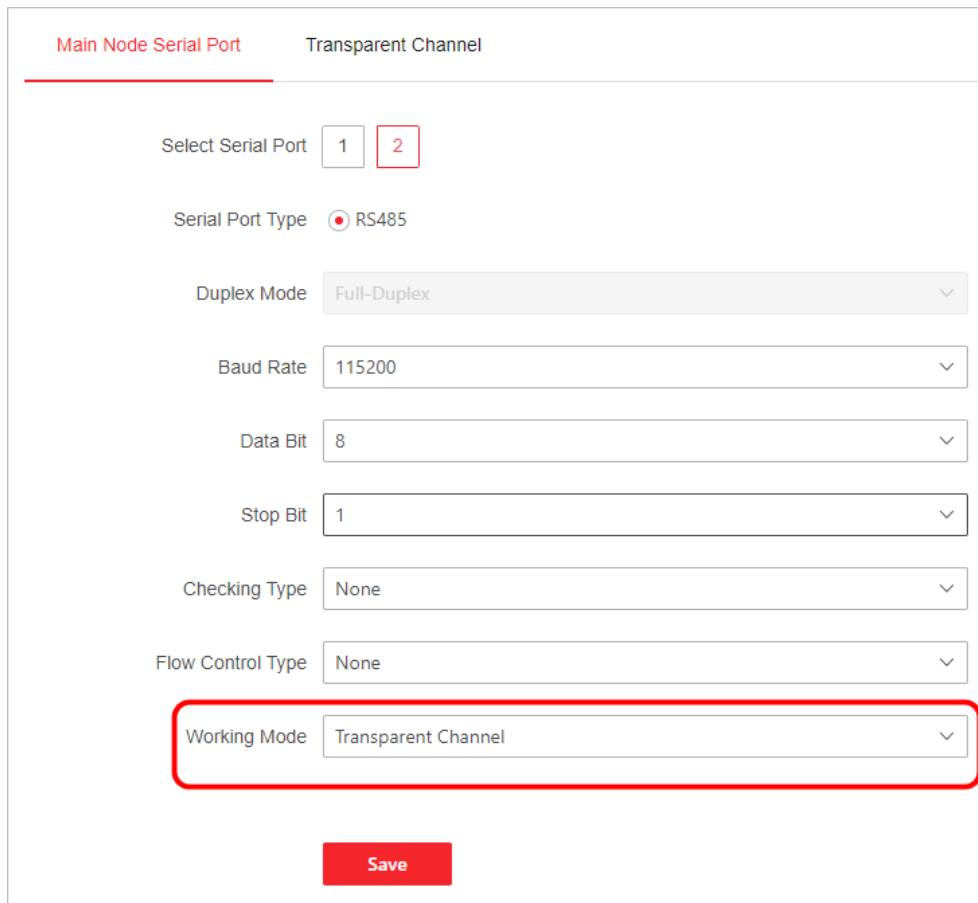
Step 4 Use the serial keyboard to control the device.

Configure Transparent Channel

To directly transmit the signals obtained by the decoder without any compression or modification to the receiving device, configure a transparent channel.

Step 1 Go to **Configuration** → **System** → **Serial Port Settings** → **Main Node Serial Port**, select serial port 2, and select **Transparent Control** as the working mode.

Step 2 Set the baud rate of the device same as the baud rate of the receiving device, set other serial port parameters, and click **Save**.

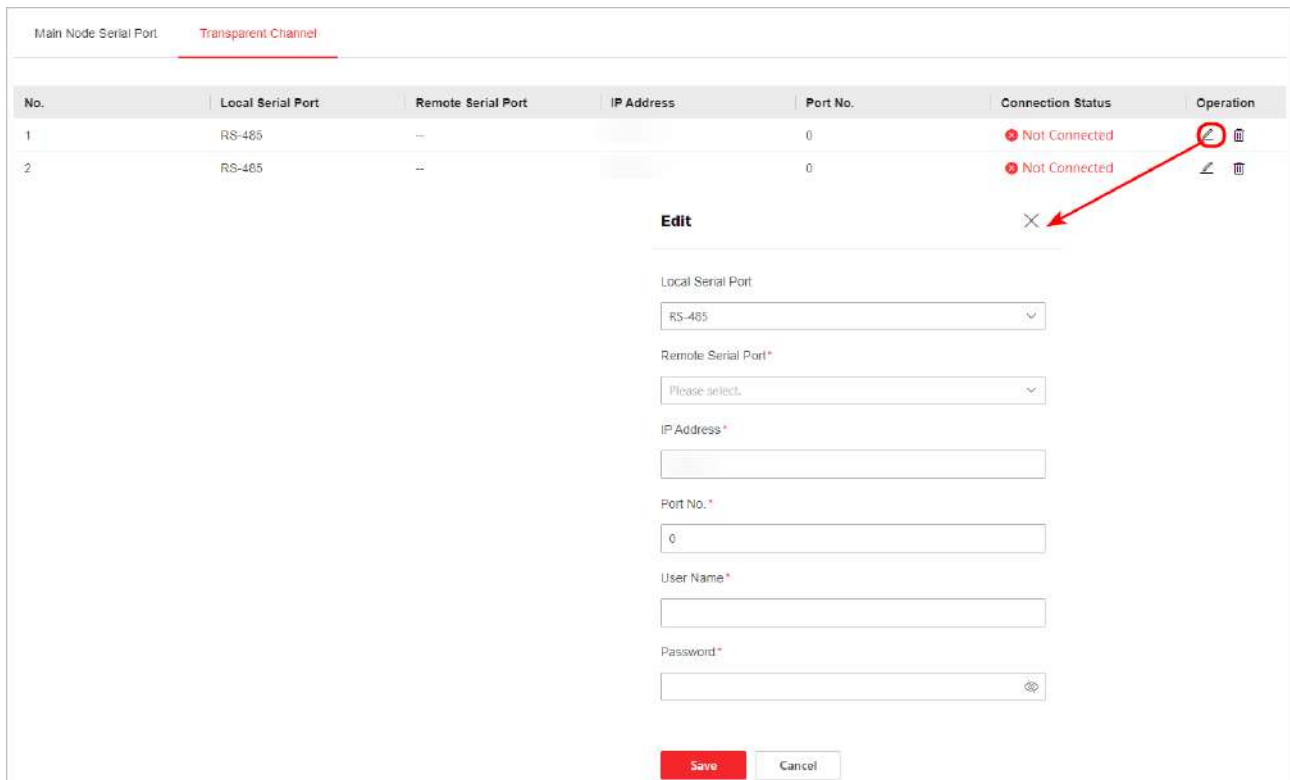


The screenshot shows the 'Main Node Serial Port' configuration window. The 'Transparent Channel' tab is selected. The 'Select Serial Port' dropdown is set to '2'. The 'Serial Port Type' is 'RS485'. The 'Duplex Mode' is 'Full-Duplex'. The 'Baud Rate' is '115200'. The 'Data Bit' is '8'. The 'Stop Bit' is '1'. The 'Checking Type' is 'None'. The 'Flow Control Type' is 'None'. The 'Working Mode' is 'Transparent Channel'. A red box highlights the 'Working Mode' dropdown. A red 'Save' button is at the bottom.

Figure 4-8 Select Transparent Channel

Step 3 Click **Transparent Channel**.

Step 4 Click  of a transparent channel to edit its remote serial port, IP address, port number, user name and password of the receiving device, and click **Save**.



The screenshot shows a web interface for configuring transparent channels. At the top, there are two tabs: 'Main Node Serial Port' and 'Transparent Channel'. Below the tabs is a table with the following columns: No., Local Serial Port, Remote Serial Port, IP Address, Port No., Connection Status, and Operation. There are two rows in the table, both with 'Not Connected' status. A red arrow points to the 'Edit' icon (a pencil) in the 'Operation' column of the first row. Below the table is an 'Edit' form with the following fields: Local Serial Port (dropdown menu showing 'RS-485'), Remote Serial Port* (dropdown menu showing 'Please select...'), IP Address* (text input field), Port No.* (text input field showing '0'), User Name* (text input field), and Password* (password input field with a toggle icon). At the bottom of the form are 'Save' and 'Cancel' buttons.

No.	Local Serial Port	Remote Serial Port	IP Address	Port No.	Connection Status	Operation
1	RS-485	—		0	Not Connected	 
2	RS-485	—		0	Not Connected	 

Edit

Local Serial Port
 RS-485

Remote Serial Port*
 Please select...

IP Address*

Port No.*

User Name*

Password*

Save **Cancel**

Figure 4-9 Edit a Transparent Channel

4.3 Configure HTTP(S) Parameters

Step 1 Go to **Configuration** → **Network** → **Network Service** → **HTTP(S)**.

Step 2 Set the HTTP port number.

The port number can be either 80 or any value from 2000 to 65535. After editing the HTTP port, you need to enter HTTP://Device IP Address: Port in the browser to access the device.

Step 3 Enable HTTPS and then set the HTTPS port.

The default port number is 443. After editing the HTTPS port, you need to enter HTTPS://Device IP Address: Port in the browser to access the device.

Step 4 (Optional) Enable **Redirect to HTTPS Automatically**. Thus, accessing the device via HTTPS is used by default.

Step 5 Click **Save**.

HTTP(S)

HTTP

*HTTP Port 80

HTTPS

Enable ☒

*HTTPS Port 443

Redirect to HTTPS Automatically ☐

Save

Figure 4-10 Configure HTTP (S) Parameters

4.4 Configure Event

Go to **Configuration** → **Event**, set the highest and lowest temperature thresholds for the device, and set the audible warning and alarm reporting to the platform when the exceptional events occur.

Device Exception Alarm

IP Address Conflict ☐ Trigger Audible Warning ☐ Report to the Platform

Invalid Access ☐ Trigger Audible Warning ☐ Report to the Platform

Network Disconnected ☐ Trigger Audible Warning ☐ Report to the Platform

Temperature Alarm ☐ Trigger Audible Warning ☐ Report to the Platform

Fan Exception ☐ Trigger Audible Warning ☐ Report to the Platform

Video Loss ☐ Trigger Audible Warning ☐ Report to the Platform

Source Decoding Exception ☐ Trigger Audible Warning ☐ Report to the Platform

Device Working Status Alarm

Below 0.0 85.0 Above

Temperature Alarm

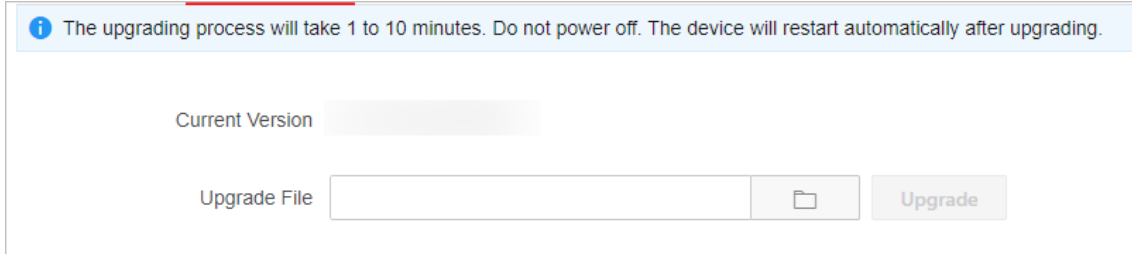
Save

Figure 4-11 Set Device Exception Alarm

4.5 Maintain the System

Go to **Maintenance and Security** → **System Maintenance** to configure the following parameters:

- On the **Restart** page, click **Restart** to restart the device.
- On the **Upgrade** page, click  to select an upgrade file, and click **Upgrade**. You need to get the upgrade file in advance and save it locally.



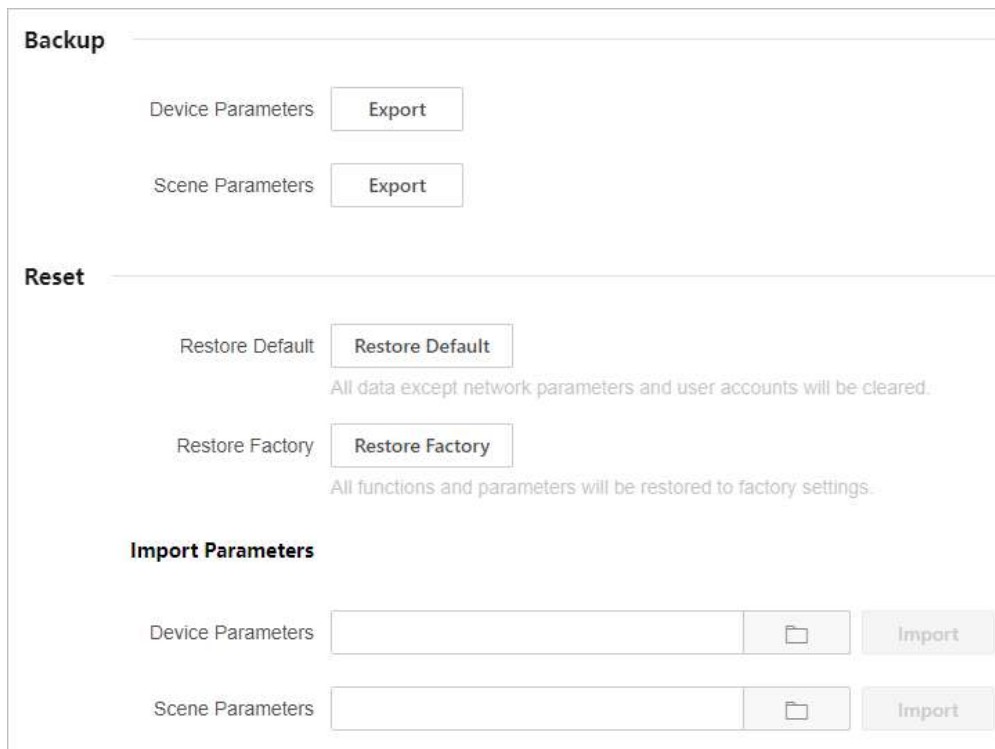
The upgrading process will take 1 to 10 minutes. Do not power off. The device will restart automatically after upgrading.

Current Version

Upgrade File  **Upgrade**

Figure 4-12 Upgrade the System

- On the **Backup and Reset** page, back up the device parameters and scene parameters.
- On the **Backup and Reset** page, reset the device:
 - Click **Restore Default** to restore the parameters except for user information and network parameters, and scene parameters to the default settings. Please use this function with caution.
 - Click **Restore Factory** to restore all functions and parameters of the device to the factory settings. Please use this function with caution.
 - Click  to select a parameter file saved locally, and click **Import** to import device parameters.
 - Click  to select a parameter file saved locally, and click **Import** to import scene parameters.



Backup

Device Parameters **Export**

Scene Parameters **Export**

Reset

Restore Default **Restore Default**
All data except network parameters and user accounts will be cleared.

Restore Factory **Restore Factory**
All functions and parameters will be restored to factory settings.

Import Parameters

Device Parameters  **Import**

Scene Parameters  **Import**

Figure 4-13 Backup and Reset Device Parameters

- On the **Log** page, set the search condition and click **Search**. You can view the searched logs in the list below. You can click **Export CSV File** to export the found logs.

Main Type: All Types | Sub Type: All Types | Time: 2024-06-24 00:00:00 - 2024-06-24 23:59:59

[Export CSV File](#)

No.	Time	Main Type	Sub Type	Remote Host IP	Description
No logs. Search first.					

Figure 4-14 Search Logs

- On the **Device Debugging** page, configure the following parameters:
 - Enable SSH (Secure Shell) as required. After enable SSH, you need to set the port number. With SSH enabled, you can use a computer installed with the SSH client to access the device.
 - Format the USB flash drive before inserting into the device. Only the USB flash drives in FAT32 format are supported. Insert a USB flash drive into the device, and click **Start Exporting** to export the logs to the USB flash drive.
 - Select a subsystem, click **Start Capturing** and then you can download the obtained packet capture file.
 - Send a shell command and then check the response message.

SSH

Enable: ☒ | Port No.: 22 | [Save](#)

Export Logs to USB

Start Exporting: ☐ | USB Drive Status: Default

Export Network Switching Packet

Subsystem: Board0_SubSys0 | [Start Capturing](#)

Packet Capture File: [Please click Start Capturing](#)

Shell Command Operation

Shell Command: | [Send](#)

Status:

Response Message:

Please send command first.

Figure 4-15 Debug the Device

4.6 Maintain the Device Security

Go to **Maintenance and Security** → **Security Management** to configure the following parameters:

- Enable IP filtering control and configure the IP addresses that are allowed to or forbidden to access the device.

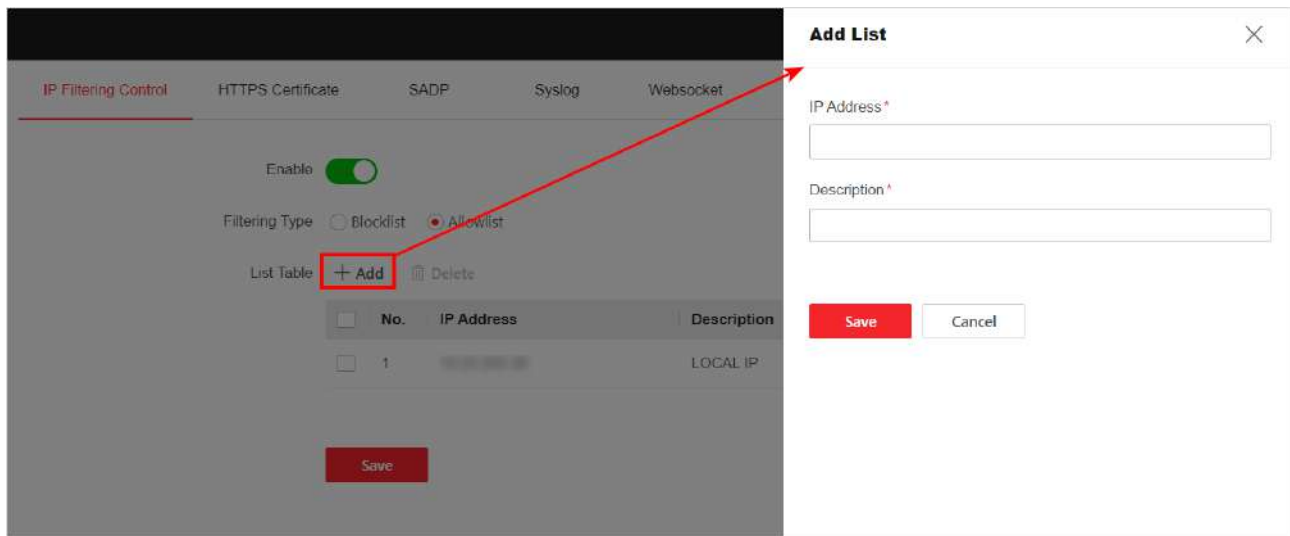


Figure 4-16 Configure IP Address Filter

- Import the locally saved HTTPS certificate and secret key.

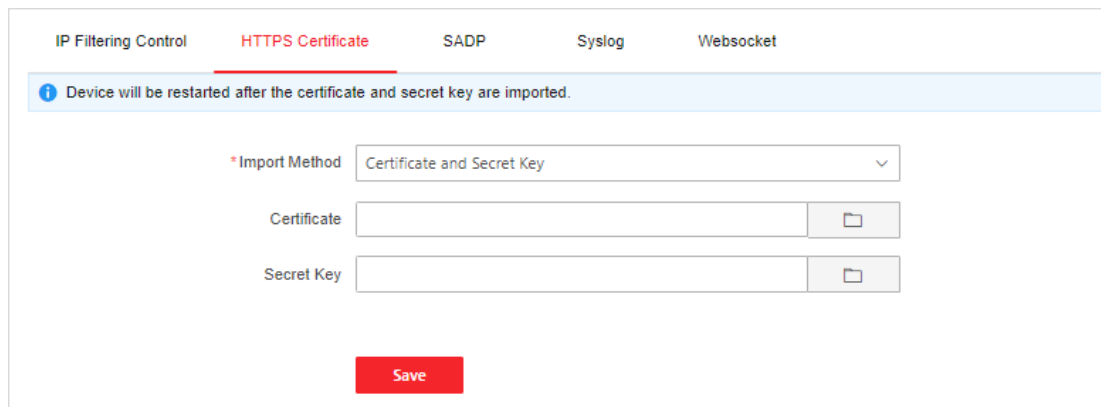
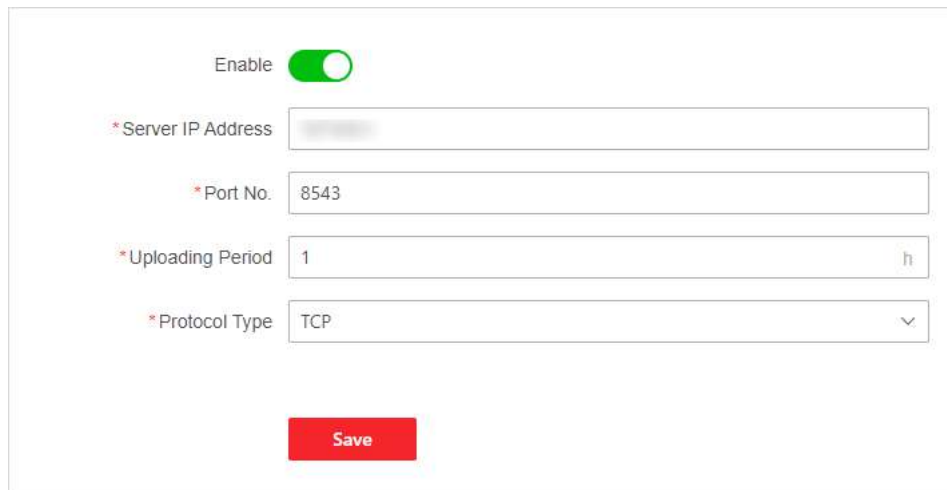


Figure 4-17 Import HTTPS Certificate and Secret Key

- Enable SADP as required. With SADP enabled, you can use the SADP software to search the device when it is in the same network segment with the computer.
- Enable Syslog as required. With Syslog enabled, the device logs can be uploaded to the Syslog server.



The screenshot shows a configuration interface for enabling Syslog. At the top, there is a toggle switch labeled 'Enable' which is currently turned on (green). Below this, there are four input fields, each preceded by a red asterisk indicating a required field:

- * Server IP Address:** An empty text input field.
- * Port No.:** A text input field containing the value '8543'.
- * Uploading Period:** A text input field containing the value '1', followed by a unit selector dropdown menu currently showing 'h' (hours).
- * Protocol Type:** A dropdown menu currently showing 'TCP'.

At the bottom of the form is a red button labeled 'Save'.

Figure 4-18 Enable Syslog

- Enable Websocket as required. With Websocket enabled, you can export the stream of network signal sources.



See Far, Go Further

DS-6904UDI(C) Ultra High Definition Decoder



Developed on the basis of embedded hardware platform, the DS-69XXUDI(C) ultra high definition (UHD) decoder is a new generation decoder for HD network cameras and can be widely used in various video security system projects. It uses the HDMI 1.4 port and DB15-to-BNC port for decoded data output, supports various decoding formats including H.265, H.264, MJPEG, Smart264, and Smart265, supports decoding the H.265 or H.264 video of no more than 32 MP, and supports 4K video output.

Video Input

- Supports the video input from the computers and video conference terminals, and 4K HDMI signal input.
- Supports using network cameras, NVRs, and other devices as network signal sources.
- Supports embedded HDMI audio input. The audio input supports 16 bit, 48 KHz or 32 KHz sampling rate, dual audio channel, and stereo.
- Supports signal input via the HDMI 1.4 port, 2 channels of 1080p@50/60 Hz input, or 1 channel of 4K@30 Hz input.

Video Output

- Supports signal output via the HDMI 1.4 port, and 4K (3840 × 2160@30 Hz) UHD video output.
- Supports embedded HDMI audio output and external audio output.
- Adopts frame synchronization technology to ensure that the images of all HDMI output ports are completely synchronized, with complete picture and smooth playback, and without lag, frame loss, tearing, or splicing.
- Supports the maximum LED loading capacity of 2.6 MP per port.

Video Encoding and Decoding

- Supports H.264 encoding format (the default), H.265 encoding formats, sub-stream encoding, and main stream encoding.
- Supports decoding the network cameras, NVRs and other network sources, decoding sub-stream and main stream, and auto-switching to sub-stream when the window division reaches the threshold.
- Provides 64 video decoding channels and supports simultaneously decoding 32 channels of 2 MP video or 64 channels of 720p video to the video wall.
- Supports decoding streams of no more than 32 MP resolution.
- Supports the mainstream decoding formats such as H.264, H.265, Smart264, Smart265, MJPEG, and HIK264, and mainstream encapsulation formats such as PS, TS, ES, and RTP.
- Supports audio decoding of G.722, G.711A, G.726, G.711U, MPEG2-L2, AAC, MP3, and PCM.
- Supports rotate mode decoding of front-end camera videos that are of no more than 2560 × 1440 resolution.
- Supports active decoding and passive decoding.
- Supports decoding the encrypted stream, multi-channel stream, and smart stream, editing and switching stream, and prompting for decoding exceptions.
- Supports decoding the recorded video files to the video wall.

Video Wall Function

- Supports splicing signal sources on the video wall, opening the signal source window, and performing signal source window roaming, scene switching, and window switching. Each screen supports four 1080p signal source windows or two 4K signal source windows.
- Each signal source window can be divided into 1, 2, 4, 6, 8, 9, 12, 16, 25, and 36 windows.
- Supports up to 64 scenes. You can customize the video wall layout and save it as a scene.
- Supports the auto-switching of up to 100 view groups on the HCP client. You can customize the camera location, scenes and time for each view group.
- Supports double clicking the divided sub-window to zoom in and double clicking again to zoom out.
- Supports displaying output channel number.
- Supports PTZ control of network signal sources, including 8-direction control, auto-scanning, aperture adjustment, focal length change, focusing, and preset calling.
- Supports setting the live view status, decoding status, switching status, audio status, and location of the signal source window.
- Supports video recording playback. You can set the playback status and select time to play back.
- Supports using the HCP client to capture images on the screen and display the captured images on the video wall.
- Supports the live view of network signal sources over RTP or RTSP.

Device Access

- Supports docking with 32 MP PanoVu series cameras, fisheye cameras, conventional front-end network cameras, DVRs, NVRs, XVRs, and mainstream third-party security devices.
- Supports integrating multiple decoding devices into one decoding device on the platform by using the software development kit (SDK).
- Supports using the ONVIF protocol to access the decoder.
- Supports interaction with LCD screen, including the screen information acquisition, image mode configuration, serial port control, time synchronization, backlight parameters configuration and acquisition, output port auto-binding, and error code reporting.
- Supports IPv4 and IPv6 protocols and the simultaneous access of IPv4 network sources and IPv6 network sources.
- Supports using the network keyboard or serial port keyboard to control the device, and to realize sub-window changing, group operation and auto-switching, scene changing, PTZ control, and video wall playback.

Maintenance

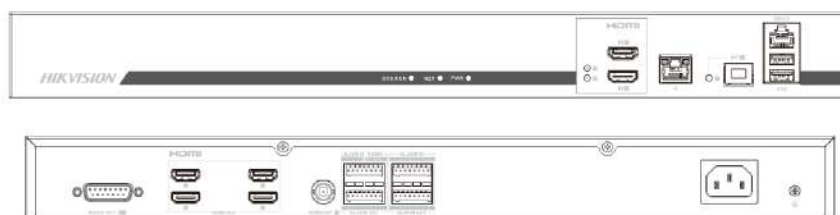
- Supports using the PC client and web browser of Chrome 45 and higher version to access and control the device.
- Provides built-in Gigabit switching network, and supports auto-adaption between the optical port and electrical port, and supports NAT.
- Supports obtaining and configuring parameters remotely, importing and exporting parameters remotely, and obtaining system running status and system logs remotely.
- Supports restarting the device remotely, restoring the default settings, and upgrading the device.
- Supports auto detection and alarm for failures, including network disconnection, IP conflict, illegal access, temperature threshold exceeding, decoding signal source exception and device exception.
- Supports user permission management, allowing users with different permissions to use designated resources and operate designated video wall modules.
- Supports visualization maintenance. The maintenance interface displays the network topology structure and keynote network status of main control system and subsystems.
- Supports manual time synchronization and NTP time synchronization.

▪ Specification

Product Model	
Product Model	DS-6904UDI(C)
Interface	
USB Interface	2 × USB 2.0 port
Serial Interface	1 × RS-232 serial port (RJ-45) + 1 × RS-485 serial port
Network Interface	1 × 10/100/1000 Mbps self-adaptive Ethernet interface (RJ-45) 1 × 100 BASE-FX/1000 BASE-X port Supports the self-adaption between the optical port and electrical port.
Alarm In Interface No.	8 channels of alarm input
Alarm Out Interface No.	8 channels of alarm output
Power	
Power Interface	Embedded 220 VAC
Device Consumption	< 50 W
Video Wall	
Video Walls	1
Video Wall Scale	≤ 4
Split Window	Supported
Window Division per Output Port	1, 2, 4, 6, 8, 9, 12, 16, 25, 36
Layers Per Screen	4 × 1080p or 2 × 4K
Layers per Device	Layers Per Screen × Output Interface(s)
Scenes	64
Plans	100 view groups on the HCP client
General	
Working Temperature	-10 °C to 55 °C (14 °F to 131 °F)
Working Humidity	0% RH to 90% RH
Net Weight	≤ 5.2 kg (11.46 lb)
Gross Weight	≤ 6.3 kg (13.89 lb)
Dimensions (W × H × D)	440 mm × 44.5 mm × 320.8 mm (17.32 inch × 1.75 inch × 12.63 inch)
Packing List	1 × decoder, 1 × regulatory compliance and safety information manual, 1 × mounting bracket, 1 × power cord, 4 × pads, 1 × grounding cable
Audio Input	
Audio Input Interfaces	2
Audio Input Interface Type	Embedded HDMI
Video Input	
Video Input Interface Type	2
Video Input Interfaces	HDMI 1.4
Max. Video Input Resolution	4K (only in odd-numbered port)

Video Input Resolution	3840 × 2160@30 Hz, 1920 × 1200@60 Hz, 1920 × 1080@60 Hz, 1920 × 1080@50 Hz, 1280 × 720@60 Hz, 1280 × 720@50 Hz, 1600 × 1200@60 Hz, 1280 × 960@60 Hz, 1680 × 1050@60 Hz, 1440 × 900@60 Hz, 1366 × 768@60 Hz, 1280 × 1024@60 Hz, 1024 × 768@60 Hz Supports custom resolution. For 60 Hz input, width ranges from 800 to 1920, and height ranges from 600 to 1200. For 30 Hz input, width ranges from 800 to 3840, and height ranges from 600 to 2160. Width: 4 alignment, height: 2 alignment.
Video Encoding	
Video Encoding Format	H.264 (default), H.265
Video Encoding Channels	2
Video Encoding Capability	1 channel of 4K@30 Hz or 2 channels of 1080p@60 Hz
Video Output	
Video Output Interface Type	HDMI 1.4
Video Output Interfaces	4
Max. Video Output Resolution	4K
Video Output Resolution	3840 × 2160@30 Hz, 2560 × 1440@30 Hz, 1920 × 1200@60 Hz, 1920 × 1080@60 Hz, 1920 × 1080@50 Hz, 1680 × 1050@60 Hz, 1600 × 1200@60 Hz, 1280 × 1024@60 Hz, 1280 × 720@60 Hz, 1280 × 720@50 Hz, 1024 × 768@60 Hz
Loading Capacity for Video Output to LED	Single port load: 26000000, Width: 144 - 4096, Height: 144 - 2160, Width must be a multiple of 2 and height must be a multiple of 2
Video Output Interface (BNC)	1 channels of CVBS output (BNC port)
Video Output Resolution (BNC)	PAL: 704 × 576@25 Hz NTSC: 704 × 480@30 Hz
Video Decoding	
Video Decoding Format	H.264, H.265, Smart264, Smart265, MJPEG
Video Decoding Channels	64
Video Decoding Capability	1) H.264/H.265 format: Supports decoding 2-channel 32 MP/24 MP, 4-channel 12 MP, 8-channel 8 MP, 10-channel 6 MP, 16-channel 4 MP, 32-channel 1080p, 64-channel 720p and lower resolution in real time. Four output ports (HDMI output ports 1 to 4) form a group and the group share the decoding capabilities. The group supports up to 4-channel smart decoding or 4-channel encrypted stream decoding. The smart decoding allows the device to decode the smart alarm events from the network cameras. 2) MJPEG format: 4-channel of 1080p and lower resolution 3) HIK264 format: 2-channel of 720p and lower resolution
Video Decoding Resolution	Up to 32 MP
Audio Output	
Audio Output Interface Type	Embedded HDMI audio output port or independent DB15-to-BNC audio output port
Audio Output Interfaces	4
Audio Decoding	
Audio Decoding Format	G711A, G711U, G722.1, G726-16/U/A, MPEG, AAC-LC, PCM

▪ Physical Interface

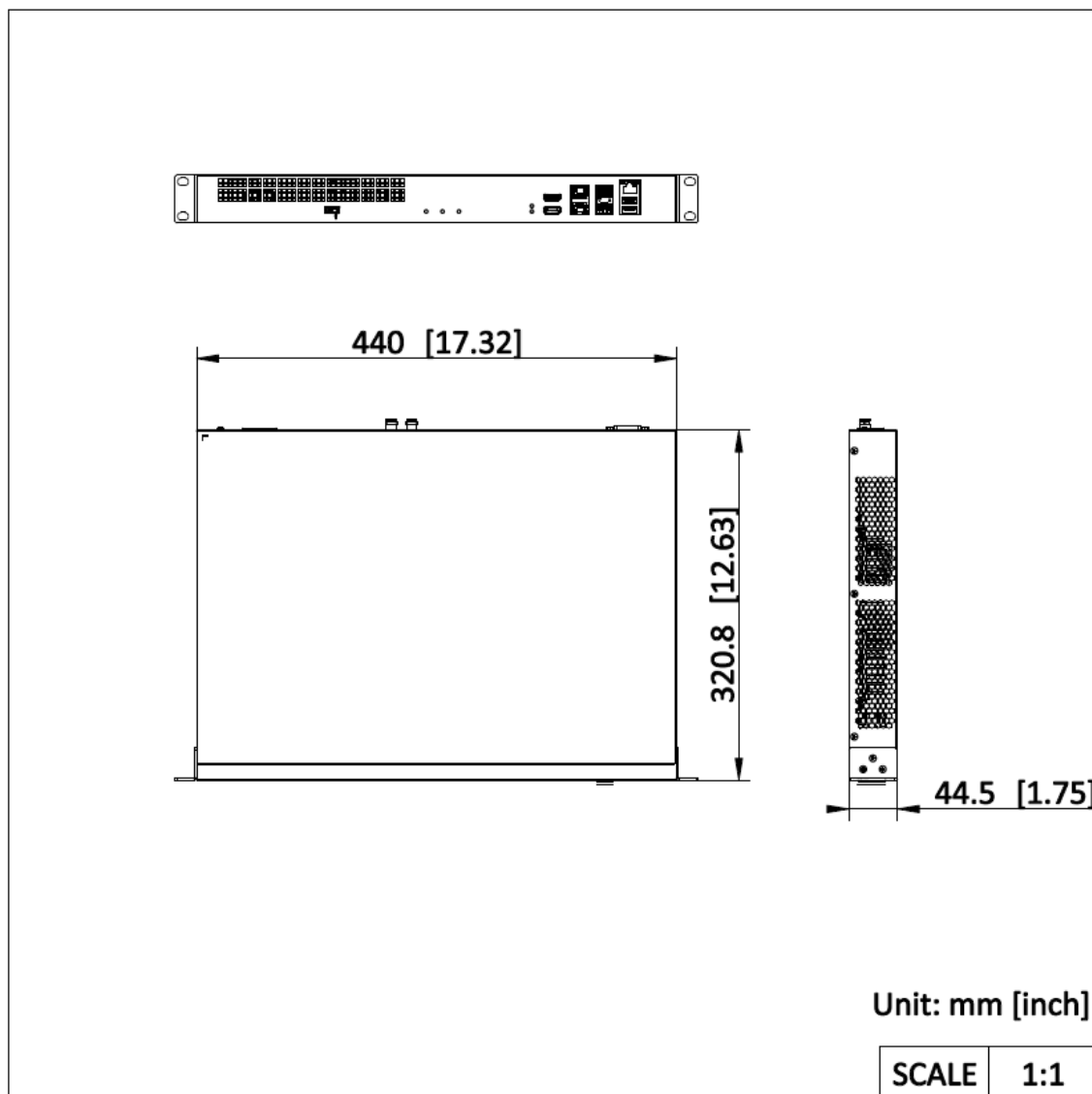


Front Panel	Description	Rear Panel	Description
SYS RUN	System running LED. It is steady green when the system runs normally.	AUDIO OUT	Audio output port
NET	Internal network LED. It is steady green when the internal network of the device is normal.	HDMI OUT	HDMI output port
PWR	Power status LED. It is steady green when the device is powered on.	VIDEO OUT	Video output port
HDMI IN1	HDMI input port 1. Its LED is steady green when the signal is connected.	RS485	RS-485 port
HDMI IN2	HDMI input port 2. Its LED is steady green when the signal is connected.	ALARM IN	Alarm input port
G	1000 Mbps electrical port 1	ALARM OUT	Alarm output port
OPT 1	1000 Mbps optical port 1		
RS232	Device debug serial port		
USB	USB 2.0 port		

▪ Available Model

DS-6904UDI(C)

▪ Dimension



See Far, Go Further



www.hikvision.com
support@hikvision.com



**CH 2005**

- » Suporte a resolução 4k / 60Hz
- » Largura de banda de 18 Gbps
- » Compatível com TVs LCD, LED, OLED, QLED, Plasma, videogames, notebooks e projetores.
- » Permite o uso de funções inerentes a tecnologia HDMI, tais como CEC e ARC.
- » Conectores banhados a ouro
- » Suporte a Ethernet
- » Cabo com comprimento de **5m**
- » Blindagem tripla para maior proteção contra interferências externas
- » Versão 2.0

CONECTORES
BANHADOS
A OURO**4K**

60 HZ

18
GbpsVELOCIDADE
DE TRANSMISSÃO**HDR**

SUPORTE HDR

3D

COMPATÍVEL

HDMI™
HIGH SPEED
WITH ETHERNET

O CH 2005 é um cabo com a tecnologia HDMI® (*High Definition Multimedia Interface*) versão 2.0 que permite a transmissão de vídeo e áudio de alta resolução entre aparelhos compatíveis com esta tecnologia, assim o cabo HDMI CH 2005 é ideal para interligar de forma simples e fácil os seus dispositivos, como TVs, DRV's, NVR's, projetores, notebooks, home theaters, sound bars, etc.

Especificações técnicas

Comprimento	5 metros
Versão	2.0

Construção do cabo	30 AWG / CCS (<i>copper clad steel</i>)
Material do cabo	PVC
Conector HDMI	Tipo A – Banhado a ouro
Quantidade de vias	19 vias + 1 Terra
sRGB	✓
YCbCr 4:2:2/4:4:4	✓
8 canais LPCM, 192 kHz, 24-bit áudio	✓
Imagem Blu-ray Full HD e DVD HD	✓
CEC (<i>Consumer Electronic Control</i>)	✓
Largura de Banda	18 Gbps
Áudio DVD	✓
Super Áudio CD (DSD - <i>Direct Stream Digital</i>)	✓
Deep Color	✓
xvYCC	✓
Auto lip-sync	✓
Áudio Dolby TrueHD / DTS-HD	✓
Lista atualizada de comandos CEC	✓
Suporte 3D	✓
Suporte Ethernet (100 Mbit/s)	✓
ARC (<i>Áudio Return Channel</i>)	✓
Máxima resolução de vídeo	4k (3840 x 2160 pixels) / 60 Hz
Máxima resolução de áudio	1536 kHz
Suporte de canais de áudio	32 canais
4 streams de áudio	✓
2 streams de vídeo	✓
HLG (<i>Hybrid Log-Gamma</i>)	✓
HDR (<i>High Dynamic Range</i>) Estático	✓
HDCP (<i>High-bandwidth Digital Content Protection</i>)	✓

Soluções Integradas

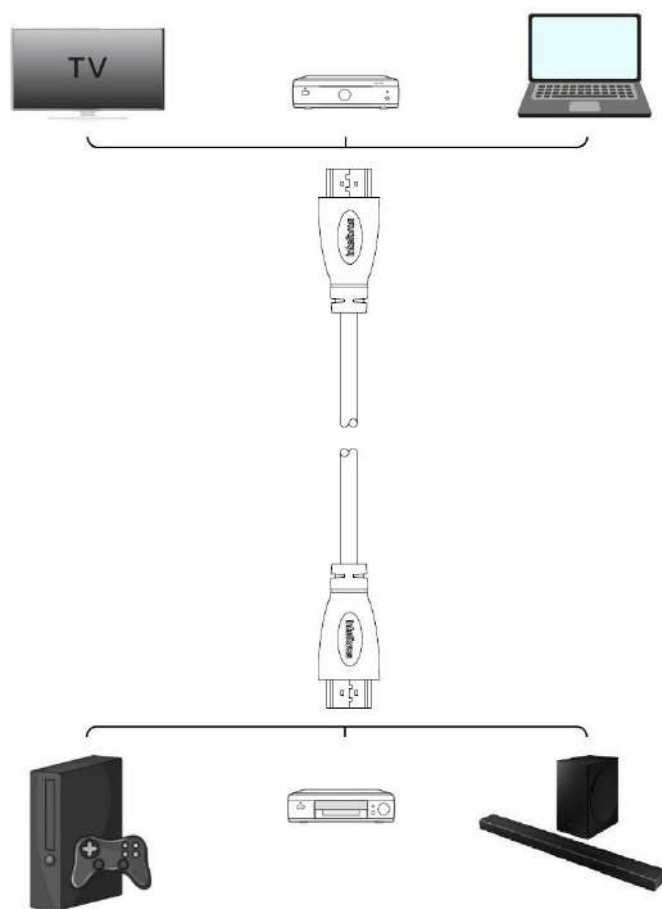
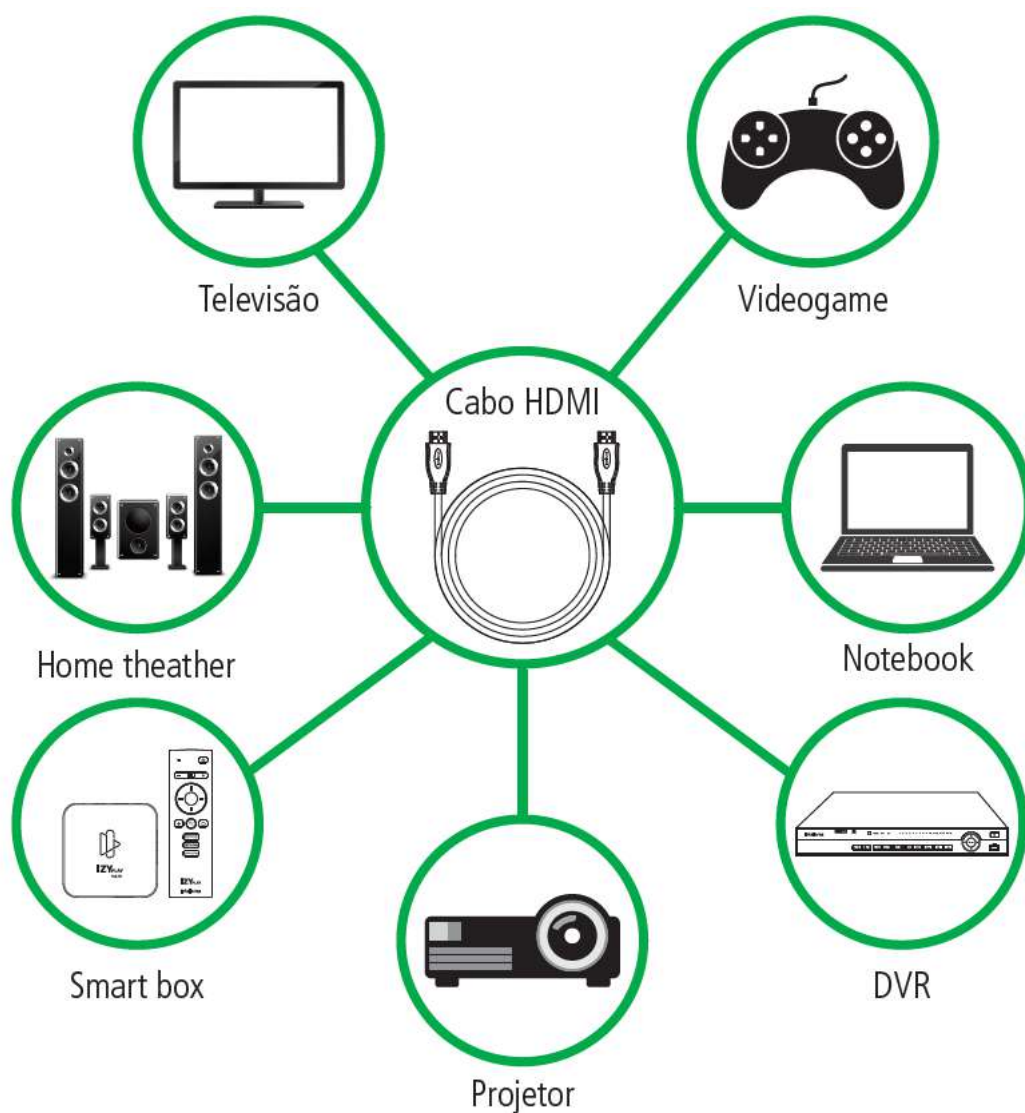
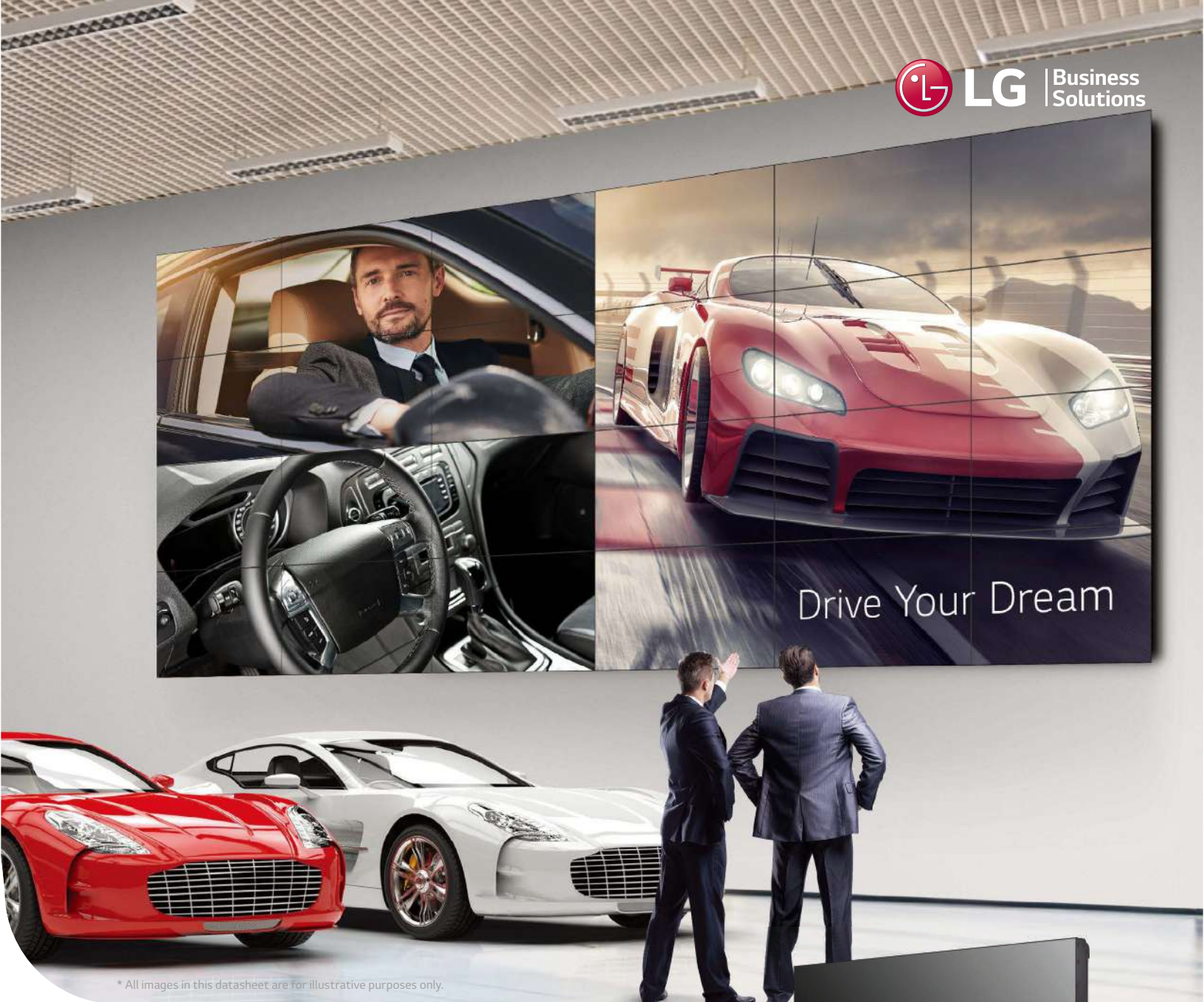


Figura 1 – Cenários de uso





* All images in this datasheet are for illustrative purposes only.

Video Wall 55VM5J-H

55" Narrow Bezel Video Wall with 1.74 mm BtB



Extreme-Narrow
Bezel



Wider
Viewing Angle



Easy Color
Adjustment



Efficient
Operation

55VM5J-H

Screen Size	55"
Aspect Ratio	16 : 9
Native Resolution	FHD (1,920 × 1,080)
Brightness	500 nits (Typ.)
Contrast Ratio	1,000:1



Large Screens with Narrow Bezel

The slim bezel, with its 1.74mm BtB (Bezel-to-Bezel) seams and delivers immersive content on assembled video wall screens.

* The 1.74mm BtB seams have been verified by Nemko, a global institution that tests and certifies electrical equipment.

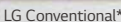


Image Gap Reduction

The 55VM5J-H includes an image improvement algorithm that can reduce perception of image gaps among tiled displays when playing back videos. Objects located on the bezel boundaries are adjusted for a smoother viewing experience.

* The "LG Conventional" refers to displays which do not include an image improvement algorithm.

** The image shown above are for illustration purposes only.



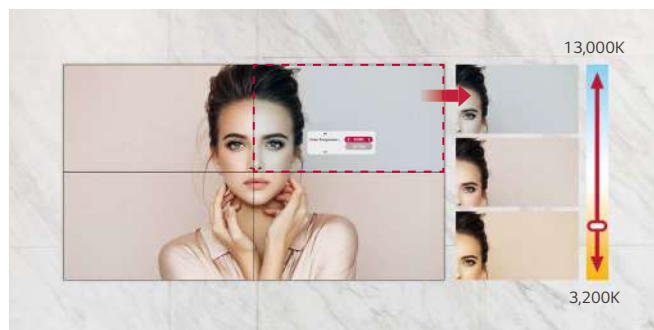
High Viewing Angle

Large screens are usually positioned higher than human-eye level. Wide half luminance angle (40°) enables effective picture quality for video walls. The viewing angle of the 55VM5J-H is high enough to display vivid colors throughout even up to 40 degrees of viewing angle difference.

* Results based on in-house testing. Actual test results may differ depending on environment and measuring equipment.



LG IPS panel technology enables stable and smooth control of liquid crystals, and allows the screen to be viewed from virtually any angle. Therefore, the 55VM5J-H captivates the attention of more viewers with lifelike colors, regardless of their horizontal viewing position.



Easy Color Adjustment

Depending on the content, the color temperature of the display can be easily adjusted in increments of 100K using a remote control.



Simple White Balance Adjustment

In conventional video walls, white balance was adjustable only in "full-white" mode, but the 55VM5J-H allows you to modify each value of grey scale to achieve more detailed and precise white balance adjustment.



High Performance and Great Scalability

Thanks to its built-in System-on-Chip and webOS smart signage platform, the 55VM5J-H can execute several tasks at once while providing smooth content playback without the need for a media player. As webOS supports HTML5 as a web-based platform and offers an SDK (Software Development Kit), it is even easier for system integrators to build and optimize their web apps.

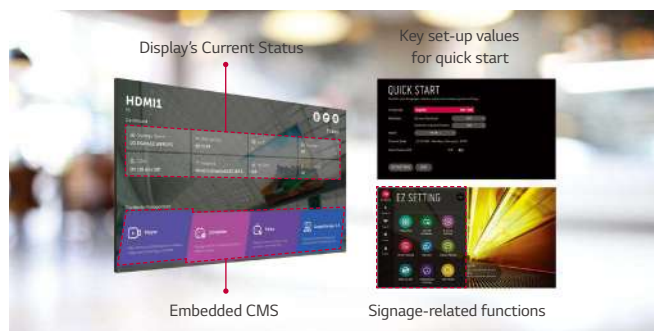
* SDK can be downloaded at
<https://webossignage.developer.lge.com>.



Flexible Content Creation

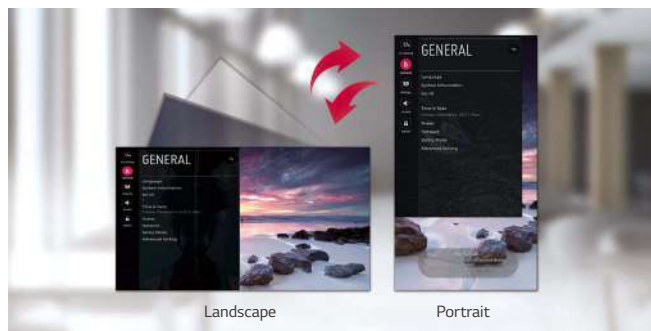
Four different videos can be played simultaneously via web apps, and various animation effects, such as scaling or rotating, are added to content using CSS (Cascading Style Sheets) transition effects. Real-time streaming is also available, providing the flexibility to organize and diversify content free from capacity limits.

* Supported protocols: RTSP, RTP, HLS, UDP Multicast



Intuitive Menu Structure

The menu structure has been optimized for commercial use. It simplifies approach flows and groups similar functions together, adopting a more intuitive GUI for ease of use. This way, users can avoid having to do trial-and-error when exploring desired functions and managing displays.



Dedicated User Interface for Portrait Orientation

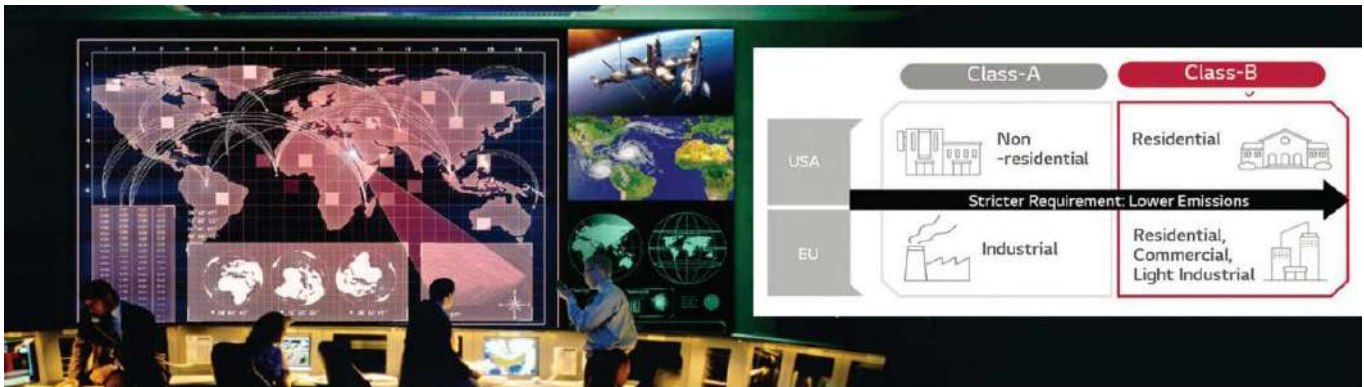
The user interface was designed based on landscape-oriented consumer TV usage, so on-screen display menu wasn't well-suited for screens in portrait mode. The OSD of the VM5J-H, however, consists of a long range menu with bigger font sizes and a 9:16 ratio, creating a comfortable and efficient business environment.



Conformal Coating

Video wall in various places can't avoid exposure to environments with dust, and humidity, which may lead to hampered performance over time. Conformal coating on the major circuit board (power board) offers protection from such environments by protecting video wall from salt, dust, iron powder, humidity, etc.

* Actual images available may differ from the example images shown.



EMC Class B Certified

The VM5J-H is certified as EMC Class B, which requires electronic equipment made for use in residential environments as well as commercial, industrial, or business environments. Therefore, it is suitable for up-close uses such as corporate meeting rooms, board rooms, etc.



Real-Time LG ConnectedCare

Maintenance is easy and fast with the optional LG ConnectedCare* service, a cloud service solution provided by LG. It remotely manages the status of displays in client workplaces for fault diagnosis and remote-control services, enabling the stable operation of clients' businesses.

* LG ConnectedCare is the brand name of LG Signage365Care Service. The availability differs by region.



Daisy Chain Capability

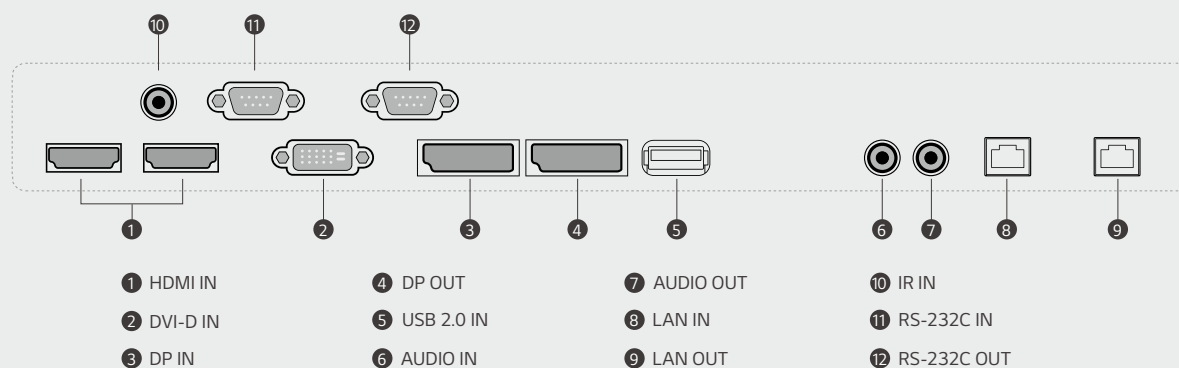
A LAN daisy chain allows you to control and monitor video walls and even update their firmwares at once. Also, through UHD daisy chain using HDMI and DisplayPort, you can set up a UHD video wall without the need of DisplayPort MST hub.



IP5x Certified Design

The IP5x Certification demonstrates protection of the internal parts of the product against dust particles.

CONNECTIVITY



* Jack Panels may differ from the above image, so please contact LG sales team to verify before ordering.



MODEL	55VM5J-H	
PANEL	Screen Size	55"
	Panel Technology	IPS
	Back Light Type	Direct
	Aspect Ratio	16:9
	Native Resolution	1920 X 1080 (FHD)
	Refresh Rate	60 Hz
	Brightness	500 nits
	Contrast Ratio	1,000:1
	Dynamic CR	500,000:1
	Color gamut	NTSC 72%
	Viewing Angle (H x V)	178° X 178°
	Color Depth	10 bit, 1.07 Billion colors
	Response Time	8ms (G to G)
	Surface Treatment (Haze)	28%
	Lifetime (Typ)	60,000 Hrs
	Operation Hours (Hours/Day)	24/7
	Portrait / Landscape	Yes / Yes
CONNECTIVITY IN	HDMI	Yes (x2), HDCP2.2
	DP	Yes (x1), HDCP2.2
	DVI-D	Yes (x1), HDCP1.4
	Audio In	Yes
	RS232C IN	Yes
	RJ45(LAN)	Yes
	IR IN	Yes
CONNECTIVITY OUT	USB	USB2.0 Type A
	DP Out	Yes (Input: HDMI / DVI / DP)
	Audio Out	Yes
	RS232C OUT	Yes
MECHANICAL	RJ45(LAN)	Yes
	Bezel Color	Black
	Bezel Width (Bezel-to-Bezel)	1.74mm BtB (1.3mm (T/L), 0.44 mm(B/R))
	Bezel Width (Active area to Active area)	2.49mm AtA (1.75mm (T/L), 0.74mm (B/R))
	Weight	41.4 lbs / 18.8 kg
	Shipping Weight	61.7 lbs / 28.0 kg
	Monitor Dimension (W x H x D)	47.7 x 26.9 x 3.4 in 1212.2 x 683.0 x 86.9 mm
	Carton Dimensions (W x H x D) (Box outer size)	54.8 x 37.6 x 11.9 in 1393 x 955 x 303 mm
	Handle	Yes
	VESA™ Standard Mount Interface	600 x 400
	Operation Temperature	32°F to 104°F 0°C to 40°C
	Operation Humidity	10% to 80%
	IP Rating	IP5X
HARDWARE FEATURES	Internal Memory	8GB
	Temperature Sensor	Yes
	BLU Sensor	Yes
	Acceleration (Gyro) Sensor	Yes
	Local Key Operation	Yes
	Fanless Design	Yes
	OPS type compatible	Yes (Piggyback)

MODEL	55VM5J-H	
SOFTWARE FEATURES	webOS ver.	webOS 4.1
	Local Contents Scheduling	Yes
	Group Manager	Yes
	USB Plug & Play	Yes
	Fail over	Yes
	No Signal Image	Yes
	RS-232C Sync	Yes
	Local Network Sync	Yes
	Video Tag	Yes (x4)
	Play via URL	Yes
	Screen Rotation	Yes
	External Input Rotation	Yes
	Gapless Playback	Yes
	Tile Mode Setting	Yes (Max. 15x15)
	Setting Data Cloning	Yes
	SNMP	Yes
	ISM Method	Yes
	Auto Set ID	Yes
	Status Mailing	Yes
	Control Manager	Yes
	Crestron Inside	Yes
	Smart Energy Saving	Yes
	PM mode	Yes
	Wake on LAN	Yes
	Network Ready	Yes
	HDMI-CEC	Yes
	SI Server Setting	Yes
	webRTC	Yes
	Pro:Idiom	Yes
	W/B Setting by Grey scale	Yes
	Scan Inversion	Yes
POWER	Power Supply	100-240 Vac, 50/60Hz
	Power Type	Built-In Power
	Typ. Power Consumption	160 W 546 BTU/hr
	Max. Power Consumption	190 W 648 BTU/hr
	Smart Energy Saving	90 W
	DPM	0.5 W
	Power off	0.5W
	FCC	Class "B"
CERTIFICATION	CE	Yes
	ErP / Energy Star	Yes / Energy Star 8.0
	SuperSign CMS	Yes
SOFTWARE COMPATIBILITY	SuperSign Control / Control+	Yes / Yes
	SuperSign WB	Yes
	SuperSign Media Editor	Yes
	LG Connected Care	Yes
ACCESSORIES & OTHER	Basic Accessories	Remote Controller(includes battery 2ea), Power Cord, RS232C cable, Lan cable, DP cable, IR Receiver, Guide Bracket, Screws, Manual
	Optional Accessories	OPS Kit (KT-OPSF)

BRACKETS STANDARD

Home > Produtos > Brackets > Brackets Standard

> RACKS FECHADOS

> Triunfo Standard

> Triunfo Server

> Triunfo Left

> Triunfo Left Server

> Rack Triunfo Plus

> Triunfo Industrial

> Rack Triunfo Flex

> RACKS ABERTOS

> Triunfo Plus

> Triunfo HD

> Rack Aberto Evo

> Rack Triunfo Open HD



Brackets Standard

Categoria: **Brackets**

Descrição

- Porta frontal em vidro temperado e fecho cilindro com chave.
- Estrutura em chapa de aço 0,75mm. e 1,2mm.
- Monobloco.
- Planos de montagem com marcação em meio "U" e regulagem na profundidade em chapa de aço 1,5mm.
- Teto com predisposição para instalação de 2 micro ventiladores
- Laterais removíveis em chapa de aço 0,75mm. com aletas de ventilação.
- Abertura superior e inferior para passagem de cabos.
- Acabamento: Toda a estrutura em aço é revestida com pintura eletrostática a pó na cor preta.

> Rack Open



CÓDIGO	UNIDADE	ALTURA	LARGURA	PROFUNDIDADE
BKS2-9350P	03U	171mm	530mm	350mm
BKS2-9450P	03U	171mm	530mm	450mm
BKS2-9550P	05U	260mm	530mm	350mm
BKS2-5450P	05U	349mm	530mm	350mm
BKS2-5550P	05U	349mm	530mm	450mm
BKS2-7350P	07U	349mm	530mm	350mm
BKS2-7450P	07U	349mm	530mm	450mm
BKS2-7550P	07U	349mm	530mm	550mm
BKS2-9350P	09U	438mm	530mm	350mm
BKS2-9450P	09U	438mm	530mm	450mm
BKS2-9550P	09U	438mm	530mm	550mm
BKS2-12350P	12U	572mm	530mm	350mm
BKS2-12450P	12U	572mm	530mm	450mm
BKS2-12550P	12U	572mm	530mm	550mm



EMPRESA

PRODUTOS

DISTRIBUIDORES

> Bracket
Standard Flex

> ACESSÓRIOS

> Guia de
Cabos
Fechado

> Guia de
Cabos Aberto

> Guia de
Cabos Anel

> Frente Falsa

> Bandeja Fixa
Light

> Bandeja Fixa
Estendida

> Bandeja Fixa
4 Pontos

> Bandeja
Telescópica

> Calhas de
tomadas

> DIO Rack
19"

> Mini Dio

> Caixa de
Emenda

> Unidade de
Ventilação

> Gaveta de
Ventilação

> Suporte para
servidor

> Base no-

Produtos relacionados



Bracket Standard Flex

break



EMPRESA

PRODUTOS

DISTRIBUIDORES



MENU

- Home
- Empresa
- Produtos
- Distribuidores
- Vídeos
- News
- Contato

CONTATO

📍 R. Antônio Lacerda Braga,
455
CIC - Curitiba - PR

✉️
racks@triunfometalurgica.co
m.br

☎️ (41) 3347.1850

UNIDADE DE VENTILAÇÃO

Home > Produtos > Acessórios > Unidade de Ventilação

> RACKS FECHADOS

- > Triunfo Standard
- > Triunfo Server
- > Triunfo Left
- > Triunfo Left Server
- > Rack Triunfo Plus
- > Triunfo Industrial
- > Rack Triunfo Flex

> RACKS ABERTOS

- > Triunfo Plus
- > Triunfo HD
- > Rack Aberto Evo
- > Rack Triunfo Open HD
- > Rack Open Plus

> BRACKETS

- > Brackets Standard
- > Bracket Standard Flex

> ACESSÓRIOS

- > Guia de Cabos Fechado
- > Guia de Cabos Aberto
- > Guia de Cabos Anel
- > Frente Falsa
- > Bandeja Fixa Light



Unidade de Ventilação

Categoria: **Acessórios**

Descrição

Utilizado para forçar a saída de ar quente e causar circulação de ar interna ao rack, auxiliando o funcionamento dos equipamentos. Possui chave liga/desliga, fusível e chave comutadora 110/220v.

Código	Ventiladores
UV02	2
UV04	4

Produtos relacionados





CALHA DE TOMADAS 19"



Calhas com 4, 6, 8, 10 e 12 tomadas com fixação para 19" Tomadas padrão brasileiro (NBR 14136) 2P +T (10A e 20A) 250V Cabo constituído de 3 via PP 2,5 m de Comprimento (10A e 20A) com plug; Montadas com barramento de latão

Estrutura em aço com pintura eletrostática poliéster, RAL 9011 preto texturizado; Cantoneira giratória para quatro posições de fixação.

Dados Técnicos			
Código	largura	Qtd de Tomadas	Amper
CALHA 0019	483(19")	4	10A
CALHA 0015	483(19")	4	20A
CALHA 0020	483(19")	6	10A
CALHA 0030	483(19")	6	20A
CALHA 0021	483(19")	8	10A
CALHA 0009	483(19")	8	20A
CALHA 0037	483(19")	10	10A
CALHA 0014	483(19")	10	20A
CALHA 0024	483(19")	12	10A
CALHA 0028	483(19")	12	20A

CALHA DE TOMADAS ESPECIAL 10 E 12