



Web Client HikCentral

Manual do Usuário

Informações Legais

Manual do Usuário

©2019 Hangzhou Hikvision Digital Technology Co., Ltd.

Acerca deste Manual

Este Manual está sujeito à proteção de direitos de autor doméstica e internacional. A Hangzhou Hikvision Digital Technology Co., Ltd. ("Hikvision") se reserva todos os direitos sobre este manual. Este manual não pode ser reproduzido, alterado, traduzido ou distribuído, total ou parcialmente, por nenhum meio, sem a prévia autorização escrita da Hikvision.

Utilize este manual do usuário sob a orientação de profissionais.

Marcas registradas

HIKVISION e outras marcas da Hikvision são de propriedade da Hikvision e marcas comerciais registradas ou objeto de aplicações para as mesmas pela Hikvision e/ou suas afiliadas. Outras marcas comerciais mencionadas neste manual são de propriedade de seus respectivos proprietários. Nenhum direito de licença é concedido para o uso dessas marcas comerciais sem autorização expressa.

Isenção de responsabilidade

ATÉ AO LIMITE MÁXIMO PERMITIDO PELA LEI APLICÁVEL, A HIKVISION NÃO OFERECE GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM FIM ESPECÍFICO, EM RELAÇÃO A ESTE MANUAL. A HIKVISION NÃO GARANTE NEM FAZ NENHUMA REPRESENTAÇÃO RELATIVA AO USO DO MANUAL OU A CORREÇÃO, PRECISÃO OU CONFIABILIDADE DAS INFORMAÇÕES AQUI CONTIDAS. SEU USO DESTES MANUAIS E QUALQUER CONFIANÇA NESTE MANUAL DEVEM SER INTEIRAMENTE POR SEU PRÓPRIO RISCO E RESPONSABILIDADE.

EM RELAÇÃO AO PRODUTO COM ACESSO À INTERNET, O USO DO MESMO SERÁ INTEIRAMENTE POR SUA CONTA E RISCO. A HIKVISION NÃO ASSUME NENHUMA RESPONSABILIDADE POR FUNCIONAMENTO ANORMAL, VAZAMENTO DE INFORMAÇÕES QUE AFETEM A PRIVACIDADE OU OUTROS DANOS RESULTANTES DE ATAQUES CIBERNÉTICOS, ATAQUES DE HACKERS, INSPEÇÃO DE VÍRUS OU OUTROS RISCOS DE SEGURANÇA NA INTERNET. NO ENTANTO, A HIKVISION FORNECERÁ APOIO TÉCNICO OPORTUNO, SE NECESSÁRIO.

LEIS DE VIGILÂNCIA VARIAM DE ACORDO COM A JURISDIÇÃO. VERIFIQUE TODAS AS LEIS PERTINENTES EM SUA JURISDIÇÃO ANTES DE UTILIZAR ESTE PRODUTO PARA GARANTIR QUE HAJA CONFORMIDADE COM A LEGISLAÇÃO APLICÁVEL. A HIKVISION NÃO SE RESPONSABILIZARÁ SE ESTE PRODUTO FOR UTILIZADO PARA PROPÓSITOS ILÍCITOS.

SE HOUVER ALGUM CONFLITO ENTRE ESTE MANUAL E A LEGISLAÇÃO APLICÁVEL, ESTA ÚLTIMA PREVALECERÁ.

Convenções dos símbolos

Os símbolos que podem ser encontrados neste documento são definidos da seguinte forma.

Símbolo	Descrição
 Perigo	Indica uma situação de perigo que, se não evitada, irá ou poderá resultar em morte ou lesão séria.
 Cuidado	Indica uma situação potencialmente perigosa, que se não for evitada, pode resultar em danos ao equipamento, perda de dados, degradação do desempenho ou resultados inesperados.
 Observação	Fornece informações adicionais para enfatizar ou complementar os pontos importantes do texto principal.

Índice

Capítulo 1 Acerca deste documento	1
Capítulo 2 Introdução.....	2
Capítulo 3 Introdução.....	4
Capítulo 4 Instalação e desinstalação	5
4.1 Instalação dos módulos.....	5
4.1.1 Instale o módulo de serviços no modo personalizado	5
4.1.2 Instalação do módulo de serviços no modo típico	7
4.2 Instalação do Control Client.....	8
4.3 Desinstalação dos módulos	8
4.3 Desinstalar todos os módulos.....	9
4.3.2 Desinstalação de módulos específicos	10
4.4 Gerenciador de Serviços.....	11
Capítulo 5 Iniciar sessão	13
5.1 Ambiente de execução recomendado.....	13
5.2 Iniciar sessão pela primeira vez	13
5.2.1 Iniciar sessão pela primeira vez para usuário admin	13
5.2.2 Iniciar sessão pela primeira vez para usuário normal	15
5.3 Iniciar sessão via Web Client.....	16
5.4 Alteração de senha para redefinição de usuário	17
5.5 Esquecimento da senha	18
Capítulo 6 Baixar o Mobile Client.....	20
Capítulo 7 Web Control	21
Capítulo 8 Assistente.....	22
Capítulo 9 Gerenciamento da Licença	23
9.1 Desativação da Licença on-line	23
9.2 Desativação da Licença off-line	25
9.3 Atualizar a Licença on-line	26
9.4 Atualização da Licença off-line	27
9.5 Desativação da Licença on-line.....	28

9.6 Desativação da Licença off-line	29
Capítulo 10 Gerenciamento de recursos	30
10.1 Criação de senha para dispositivos inativos	30
10.2 Editar informações de rede do Dispositivo On-Line	31
10.3 Gerenciamento do Dispositivo de Codificação	32
10.3.1 Adicionar Dispositivos On-Line	32
10.3.2 Adicionar dispositivo por endereço IP ou nome de domínio	40
10.3.3 Adicionar dispositivos por Segmento IP	44
10.3.4 Adicionar dispositivos por segmento de entrada	47
10.3.5 Adicionar dispositivo por Hik-Connect	50
10.3.6 Adicionar dispositivos em lote	53
10.4 Gerenciamento do Dispositivo de Controle de Acessos	55
10.4.1 Adicionar Dispositivos On-Line	55
10.4.2 Adicionar dispositivo por endereço IP	60
10.4.3 Adicionar dispositivos por Segmento IP	62
10.4.4 Adicionar dispositivos por segmento de entrada	64
10.4.5 Adicionar dispositivos em lote	66
10.5 Gerenciamento do Dispositivo de Controle de Segurança	67
10.5.1 Adicionar Dispositivos On-Line	67
10.5.2 Adicionar dispositivo por endereço IP	71
10.5.3 Adicionar dispositivo por Hik-Connect	73
10.5.4 Adicionar dispositivo por Segmento IP	75
10.5.5 Adicionar dispositivo por segmento de entrada	77
10.5.6 Adicionar dispositivos em lote	78
10.6 Restaurar/redefinir a senha do dispositivo	79
10.6.1 Redefinir a senha do dispositivo	80
10.6.2 Restaurar a senha padrão do dispositivo	81
10.7 Gerenciamento de local remoto	82
10.7.1 Adicionar Local Remoto por endereço IP ou nome de domínio	83
10.7.2 Adicionar Local Remoto registrado no Sistema Central	86
10.7.3 Adicionar Locais Remotos em lote	88

10.7.4	Faça cópia de segurança do banco de dados do Local Remoto no Sistema Central.....	90
10.7.5	Edição do Local Remoto	91
10.7.6	Exibição de alterações do Local Remoto	92
10.8	Gerenciamento do Servidor de Gravações.....	94
10.8.1	Gerenciamento do Servidor de Armazenamento em Nuvem	94
10.8.2	Adicionar Rede de Área de Armazenamento Híbrido	98
10.8.3	Adicionar pStor.....	101
10.8.4	Defina Hot Spare N+1.....	103
10.9	Gerenciamento do Servidor de Transmissões.....	105
10.9.1	Importação do Certificado de Componentes de Serviços para o Servidor de Transmissões	105
10.9.2	Adicionar Servidor de Transmissões	105
10.10	Gerenciamento do Smart Wall	107
10.10.1	Adicionar Dispositivo de Decodificação	107
10.10.2	Configuração em cascata	116
10.10.3	Adicionar Smart Wall	117
10.10.4	Vinculação de saída de decodificação com janela	118
Capítulo 11	Gerenciamento de Área	119
11.1	Adicionar área	119
11.1.1	Adicionar área para o Local Atual.....	119
11.1.2	Adicionar área para Local Remoto	121
11.2	Adicionar elemento a área.....	123
11.2.1	Adicionar câmera a área para o Local Atual	123
11.2.2	Adicionar câmera a área para Local Remoto	124
11.2.3	Adicionar ponto de acesso a área.....	126
11.2.4	Adicionar entrada de alarme a uma área.....	127
11.2.5	Vinculação de entradas de alarme à Partição do Controle de Segurança	128
11.2.6	Adicionar saída de alarme a uma área	129
11.2.7	Adicionar UVSS a área para o Local Atual	130
11.3	Editar elemento em área	131
11.3.1	Edição de câmera para o Local Atual.....	131

11.3.2 Edição de ponto de acesso para o Local Atual	133
11.3.3 Edição de entrada de alarme para o Local Atual	137
11.3.4 Edição de saída de alarme para o Local Atual.....	137
11.3.5 Edição de sistemas de vigilância sob veículos para o Local Atual	138
11.3.6 Editar elemento para o Local Remoto.....	139
11.4 Remover elemento de área	139
11.4.1 Remoção de elementos da área para o Local Atual	139
11.4.2 Remoção de elementos de uma área para o Local Remoto	140
11.5 Configuração do modelo de agendamento de defesa.....	140
Capítulo 12 Configurando a gravação.....	143
12.1 Configuração de gravações de câmeras em local atual	143
12.2 Configuração de gravações de câmeras em local remoto	148
12.3 Configurar armazenamento de imagens importadas	151
12.4 Configurar armazenamento para imagens carregadas.....	152
12.5 Configuração do modelo de programação de gravação	152
Capítulo 13 Configurar evento e alarme.....	155
13.1 Configurar evento monitorado pelo sistema	156
13.1.1 Adicionar evento para a câmera.....	156
13.1.2 Adicionar evento para ponto de acesso.....	161
13.1.3 Adicionar evento para entrada de alarme	164
13.1.4 Adicionar evento para a câmera ANPR	168
13.1.5 Adicionar evento por pessoa	172
13.1.6 Adicionar eventos monitorados no sistema ao UVSS.....	176
13.1.7 Adicionar evento para site remoto	180
13.1.8 Adicionar evento para dispositivo de codificação	183
13.1.9 Adicionar evento para o dispositivo de controle de acesso	187
13.1.10 Adicionar evento para o dispositivo de controle de segurança	190
13.1.11 Adicionar evento para servidor de transmissão ou servidor de gravação	194
13.1.12 Adicionar evento para o servidor HikCentral.....	197
13.1.13 Adicionar evento para usuário	201
13.1.13 Adicionar evento para o evento definido pelo usuário	204

13.1.15 Adicionar evento para Evento genérico	208
13.1 Editar evento monitorado pelo sistema.....	211
13.2 Configurar evento genérico	212
13.3 Configurar evento definido pelo usuário	215
13.4 Configurar alarme.....	216
13.4.1 Configurações de alarme	217
13.4.2 Adicionar alarme para câmera no local atual	219
13.4.3 Adicionar alarme para a câmera no local remoto	223
13.4.4 Adicionar alarme para ponto de acesso.....	227
13.4.5 Adicionar alarme para entrada de alarme	231
13.4.6 Adicionar alarme para a câmera ANPR	235
13.4.7 Adicionar alarme para pessoa	239
13.4.8 Adicionar alarme para UVSS	243
13.4.9 Adicionar alarme para dispositivo de codificação	247
13.4.10 Adicionar alarme para o dispositivo de controle de acesso.....	251
13.4.11 Adicionar alarme dispositivo de controle de segurança	255
13.4.12 Adicionar alarme para servidor de transmissão e servidor de gravação.....	258
13.4.13 Adicionar alarme para servidor HikCentral.....	262
13.4.14 Adicionar alarme para usuário	266
13.4.15 Adicionar alarme para evento definido pelo usuário.....	270
13.4.16 Adicionar alarme para evento genérico	274
13.4.17 Adicionar alarme para local remoto.....	278
13.5 Configurar modelo de agendamento de armar	282
Capítulo 14 Gerenciar mapa	285
14.1 Definir Mapa GIS e Ícones	285
14.2 Vincular e-map para a área.....	287
14.3 Pesquisa de Localização	288
14.4 Localizar locais no mapa	289
14.5 Adicionar área de destaque	290
14.6 Região da área de destaque.....	292
14.7 Adicionar etiquetas	293

Capítulo 15 Gerenciar veículo	294
15.1 Adicionar lista de veículos	294
15.2 Adicionar informação do Veículo	295
15.2.1 Importar informações do veículo em um lote	295
15.2.2 Adição manual de informações de veículo	296
Capítulo 16 Gerenciar lista de pessoas	299
16.1 Adicionar pessoa	299
16.2 Adicionar pessoas em lote	304
16.3 Importar pessoas do domínio	305
16.4 Adicionar perfil em lote	307
16.5 Cartões de emissão de lote para pessoas	308
16.6 Definir parâmetros de emissão de cartão	310
16.7 Informações adicionais personalizadas	311
Capítulo 17 Gerenciar controle de acesso	312
17.1 Adicionar grupo de acesso	312
17.2 Gerenciar nível de acesso	314
17.2.1 Gerenciar nível de acesso	314
17.2.2 Atribuir nível de acesso ao grupo de acesso	316
17.3 Aplicar os níveis de acesso das pessoas ao dispositivo	317
17.3.1 Aplicar manualmente os níveis de acesso das pessoas ao dispositivo	317
17.3.2 Aplicar regularmente os níveis de acesso da pessoa a dispositivos	319
17.4 Definir modelo de agendamento de acesso	320
17.5 Configurar regras de retorno do anti-retorno	321
Capítulo 18 gerenciar tempo e atendimento	323
18.1 Adicionar grupo de acesso	323
18.2 Adicionar agendamento de turno	325
18.3 Atribuir agendamento de turno ao grupo de atendimento	328
18.4 Adicionar ponto de verificação de atendimento	329
18.5 Gerenciar registro de atendimento	330
18.5.1 Pesquisa registro de atendimento	330
18.5.2 Registro de atendimento correto para pessoa singular	331

18.5.3 Registros de atendimento corretos para várias pessoas	332
Capítulo 19 Gerenciar grupo de comparação de face.....	334
19.1 Adicionar grupo de comparação de faces	334
19.2 Aplicar grupo de comparação de face ao dispositivo	336
Capítulo 20 Gerenciar função e usuário	338
20.1 Adicionar função	338
20.2 Adicionar usuário normal	341
20.3 Importar usuários do domínio	344
20.4 Alterar senha do usuário atual	346
20.5 Redefinir senha para usuário admin	347
20.6 Redefinir senha para usuário normal	350
Capítulo 21 Manutenção	351
21.1 Definir backup de dados do sistema	351
21.2 Restaurar banco de dados	353
21.3 Exportar arquivo de configuração	354
Capítulo 22 Gerenciar a segurança do sistema	355
Capítulo 23 Configuração do sistema	356
23.1 Definir nome do local	356
23.2 Definir limite de aviso para uso do servidor	356
23.3 Definir NTP.....	357
23.4 Definir o Active Directory.....	357
23.5 Ativar evento genérico de recebimento.....	360
23.6 Permitir registro de local remoto	360
23.7 Registre-se no sistema central.....	361
23.8 Definir acesso WAN.....	361
23.9 Definir tempo limite de rede	362
23.10 Definir modo de acesso a dispositivos	362
23.11 Definir NIC do servidor	363
23.12 Definir período de retenção de dados.....	363
23.13 Definir feriado	365
23.14 Definir modelo de email	365

23.14.1 Configurar conta de email.....	365
23.14.2 Adicionar modelo de email.....	367
23.15 Enviar relatório regularmente	368
23.15.1 Enviar relatório de eventos regularmente	368
23.15.2 Enviar relatório de alarme regularmente.....	370
23.15.3 Enviar relatório de passagem de veículo regularmente	371
23.15.4 Enviar relatório de contagem de pessoas regularmente.....	372
23.15.5 Enviar relatório de análise de filas regularmente.....	374
23.15.6 Enviar relatório de temperatura regularmente	376
23.16 Definir protocolo de transferência	378
23.17 Definir ID da câmera	379
23.18 Configuração do modo de funcionamento	379
23.19 Certificado de componente de serviço de exportação	380
23.20 Configurar o sistema de reposição qte.....	380
23.21 Redefinir informações de rede do dispositivo	381
Capítulo 24 Aplicações	382
24.1 Exibição ao vivo	382
24.1.1 Iniciar exibição ao vivo.....	382
24.1.2 Controle PTZ	384
24.2 Reprodução.....	390
24.2.1 Pesquisar Arquivo de Vídeo.....	390
24.2.2 Reproduzir Arquivo de Vídeo.....	392
24.3 Configuração Local	393
Capítulo 25 Entradas importantes	396

Capítulo 1 Acerca deste documento

Este Manual do Usuário se destina ao administrador do sistema.

O Manual orienta a estabelecer e configurar o sistema de vigilância. Consulte este Manual para realizar a instalação do sistema, ativação do VSM, acesso ao sistema e configuração da tarefa de vigilância por meio do Web Client etc. Para garantir adequação do uso e estabilidade do sistema, consulte o conteúdo abaixo e leia atentamente o Manual antes de instalação e operação.

Capítulo 2 Introdução

O sistema foi desenvolvido para gerenciamento central do sistema de monitoramento de vídeo e apresenta flexibilidade, alta confiabilidade para dimensionamento e funções avançadas. O sistema fornece gerenciamento central, compartilhamento de informações, conexão conveniente e cooperação entre múltiplos serviços. Ele pode adicionar dispositivos para gerenciamento, visualização em tempo real, armazenamento e reprodução de arquivos de vídeo, vinculação de alarmes, controle de acessos, tempo e frequência, comparação facial e assim por diante.

Observação

Os módulos exibidos na página inicial variam de acordo com a Licença adquirida. Para obter mais informações, entre em contato com nossa assistência técnica.

O sistema completo contém os seguintes módulos. Os módulos podem ser instalados de acordo com as reais necessidades. Consulte **Instalação e desinstalação** para obter orientação detalhada sobre a instalação do sistema.

Módulo	Introdução
VSM (Gerenciamento da Vigilância por Vídeo)	<ul style="list-style-type: none">● Fornecer serviço de autenticação unificada para conexão com clientes e servidores.● Fornecer gerenciamento centralizado para usuários, funções, permissões, dispositivos e serviços.● Fornecer interface de configuração para o módulo de vigilância e gerenciamento.● Fornecer a função de gerenciamento de registros e estatísticas.
Serviço de Transmissões (opcional)	Fornecer encaminhamento e distribuição de dados de áudio e vídeo da visualização em tempo real.

A tabela a seguir exibe os clientes fornecidos para acessar ou gerenciar o sistema.

Cliente	Introdução
Control Client	Control Client é um software C/S que fornece várias funcionalidades de operação, incluindo exibição em tempo real, controle de PTZ, reprodução e download de vídeos, recebimento de alarmes, pesquisa de registros etc.

Cliente	Introdução
Web Client	Web Client é um cliente B/S para gerenciamento do sistema. Ele apresenta várias funcionalidades, incluindo gerenciamento de dispositivos, Gerenciamento de Área, configurações de agendamento de gravações, configuração de eventos, gerenciamento de usuários e assim por diante.
Mobile Client	Mobile Client é o software projetado para obter acesso ao sistema via redes Wi-Fi, 3G e 4G com dispositivo móvel. Ele cumpre as funções dos dispositivos conectados ao sistema, como visualização em tempo real, reprodução remota, controle de PTZ e assim por diante.

Capítulo 3 Introdução

O conteúdo a seguir descreve as tarefas normalmente envolvidas na configuração de um sistema em funcionamento.

Verificação da configuração inicial de dispositivos e outros servidores

Antes de fazer qualquer coisa no sistema, verifique se os dispositivos (câmera, DVR, Servidor de Gravações e assim por diante) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para conectar os dispositivos ao sistema via rede.

Instalação do sistema

Consulte *Instalação e desinstalação* para conhecer as etapas detalhadas de instalação.

Abrir o Web Client e iniciar sessão

Consulte *Iniciar sessão pela primeira vez para usuário admin*.

Ativação da Licença

Consulte *Gerenciamento da Licença*.

Adicionar dispositivos ao sistema e configurar área

O sistema examinará rapidamente sua rede em busca de dispositivos relevantes (câmera, DVR e assim por diante) e adicioná-los ao seu sistema. Ou então adicione os dispositivos inserindo as informações necessárias manualmente. Os dispositivos adicionados devem ser organizados em áreas para gerenciamento conveniente. Consulte *Gerenciamento de recursos* e *Gerenciamento de Área*.

Configuração de definições de gravação

Grave os arquivos de vídeo das câmeras no dispositivo de armazenamento de acordo com o cronograma de gravação configurado. O agendamento pode ser definido como contínuo, acionado por alarme ou acionado como desejado. Consulte *Configuração das gravações*.

Configuração de eventos e alarmes

Exceção de câmera, exceção de dispositivo, exceção de servidor e entrada de alarme podem acionar ações de vinculação no sistema. Consulte *Configuração de eventos e alarmes*.

Configuração de usuários

Especifique quem deve poder acessar seu sistema e como. Defina as diferentes permissões para os usuários limitarem a operação do sistema. Consulte *Gerenciamento de funções e usuários*.

Capítulo 4 Instalação e desinstalação

Instale os módulos de serviço em seus servidores ou PCs para construir sua HikCentral. Dois pacotes de instalação estão disponíveis para construir seu sistema.

Pacote de instalação básica

Contém todos os módulos para construir o sistema, incluindo o Serviço de Gerenciamento da Vigilância por Vídeo (VSM), Serviços de transmissões e Control Client.

Pacote de instalação do Control Client

Contém somente o módulo do Control Client.

Observação

O Serviço de VSM e o Serviço de Transmissões não podem ser instalados no mesmo PC.

4.1 Instalação dos módulos

Dois métodos de instalação estão disponíveis para construir os módulos.

Modo típico

Instale todos os módulos de serviços (exceto o Serviço de Transmissões) e o Client.

Modo personalizado

Selecione o diretório de instalação e os módulos a serem instalados conforme desejado.

4.1.1 Instale o módulo de serviços no modo personalizado

Durante a instalação no modo personalizado, selecione o diretório de instalação e instale os módulos de serviço especificados conforme desejado.

Execute esta tarefa quando desejar instalar o módulo de serviço no modo personalizado.

Etapas

1. Clique duas vezes em  (HikCentral) para entrar no painel de Boas-Vindas no Assistente InstallShield.
2. Clique em **Avançar** para iniciar o Assistente InstallShield.
3. Leia o Contrato de Licença.
 - Clique em **Eu aceito os termos do Contrato de Licença** e continue.
 - Clique em **Eu não aceito os termos do Contrato de Licença** para cancelar a instalação.
4. Selecione **Personalizar** como tipo de configuração e clique em **Avançar**.
5. Opcional: Clique em **Alterar...** e selecione um diretório apropriado conforme desejado para instalar os módulos.
6. Clique em **Avançar** para continuar.

7. Selecione os módulos que desejar instalar e clique em **Avançar**.

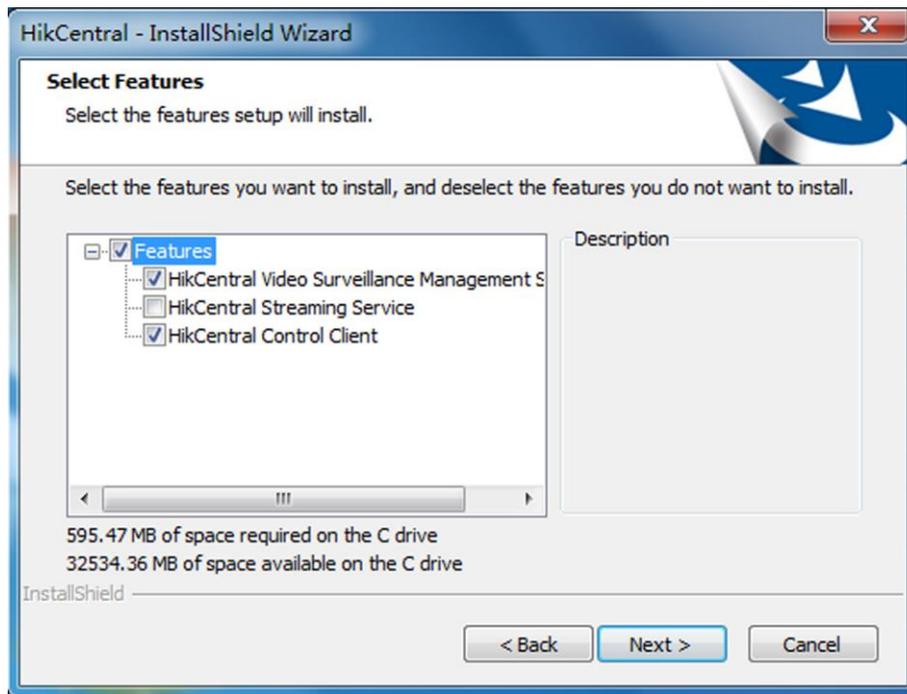


Figura 4-1 Selecione os módulos a instalar

Observação

O Serviço de VSM e o Serviço de Transmissões não podem ser instalados no mesmo PC.

Desta forma se pode instalar os módulos de serviço e cliente em diferentes PCs ou servidores, conforme desejado.

8. Opcional: Selecione o modo hot spare se optar por instalar o serviço VSM na etapa anterior.
- Selecione **Normal** se não precisar construir um sistema hot spare.
 - Selecione **Hot spare de espelho** para construir um sistema de hot spare de espelho. Existem dois servidores VSM no sistema hot spare: servidor host e servidor de reserva. Quando o servidor host funciona, os dados no servidor host são copiados para o servidor de reserva em tempo real. Quando o servidor host falha, o servidor de reserva entra em operação sem interrupções, aumentando assim a confiabilidade do sistema.
 - Selecione **Hot spare de armazenamento compartilhado** para construir um sistema hot spare de armazenamento compartilhado. Há dois servidores VSM e um disco rígido (instalado em outro servidor) no sistema hot spare: servidor host, servidor de reserva e o disco rígido selecionado. Quando o servidor host funciona, os dados são armazenados no disco rígido. Quando o servidor host falha, o servidor de reserva entra em operação e assume o disco rígido para utilizar o mesmo arquivo de dados.

 **Observação**

Para construir o sistema de hot spare, entre em contato com nossos engenheiros da assistência técnica.

9. Clique em **Instalar**.

Um painel indicador do andamento da instalação será exibido.

10. Leia as informações de pós-instalação e clique em **Terminar** para concluir a instalação.

 **Observação**

Marque **Executar Web Client** para abrir a página de início de sessão do Web Client via navegador da internet automaticamente. Se as configurações do seu navegador da internet bloquearem a abertura da página de iniciar sessão, siga o aviso no navegador da internet para permitir a exibição adequada da página.

4.1.2 Instalação do módulo de serviços no modo típico

Instale todos os módulos de serviço (exceto o Serviço de Transmissões) e o Client em um PC ou servidor.

Execute esta tarefa quando desejar instalar o módulo de serviço no modo típico.

Etapas

1. Clique duas vezes em  (HikCentral) para entrar no painel de Boas-Vindas no Assistente InstallShield.
2. Clique em **Avançar** para iniciar o Assistente InstallShield.
3. Leia o Contrato de Licença.
 - Clique em **Eu aceito os termos do Contrato de Licença** e continue.
 - Clique em **Eu não aceito os termos do Contrato de Licença** para cancelar a instalação.
4. Selecione **Típico** como tipo de configuração e clique em **Avançar**.
5. Opcional: Clique em **Alterar...** e selecione um diretório apropriado conforme desejar para instalar o módulo.
6. Clique em **Avançar** para continuar.
7. Opcional: Selecione o modo hot spare se optar por instalar o serviço VSM na etapa anterior.
 - Selecione **Normal** se não precisar construir um sistema hot spare.
 - Selecione **Hot spare de espelho** para construir um sistema de hot spare de espelho. Existem dois servidores VSM no sistema hot spare: servidor host e servidor de reserva. Quando o servidor host funciona, os dados no servidor host são copiados para o servidor de reserva em tempo real. Quando o servidor host falha, o servidor de reserva entra em operação sem interrupções, aumentando assim a confiabilidade do sistema.
 - Selecione **Hot spare de armazenamento compartilhado** para construir um sistema hot spare de armazenamento compartilhado. Há dois servidores VSM e um disco rígido (instalado em outro servidor) no sistema hot spare: servidor host, servidor de reserva e o disco rígido

selecionado. Quando o servidor host funciona, os dados são armazenados no disco rígido. Quando o servidor host falha, o servidor de reserva entra em operação e assume o disco rígido para utilizar o mesmo arquivo de dados.

Observação

Para construir o sistema de hot spare, entre em contato com nossos engenheiros da assistência técnica.

8. Leia as informações de pré-instalação e clique em **Instalar** para iniciar a instalação. Um painel indicador do andamento da instalação será exibido.
 9. Leia as informações de pós-instalação e clique em **Terminar** para concluir a instalação.
-

Observação

Marque **Executar Web Client** para abrir a página de início de sessão do Web Client via navegador da internet automaticamente. Se as configurações do seu navegador da internet bloquearem a abertura da página de início de sessão, siga o aviso no navegador da internet para permitir a exibição adequada da página.

4.2 Instalação do Control Client

Instale o Control Client HikCentral em seu computador antes de acessar o sistema por meio do Control Client.

Execute esta tarefa quando desejar instalar o Control Client.

Etapas

1. Clique duas vezes em  (HikCentral_Client) para entrar no painel de Boas-Vindas no Assistente InstallShield.
2. Clique em **Avançar** para iniciar o Assistente InstallShield.
3. Opcional: Clique em **Navegar** e selecione um diretório apropriado em seu computador para instalar o Control Client.
4. Clique em **Avançar** para continuar.
5. Leia as informações de pré-instalação e clique em **Instalar** para iniciar a instalação. Um painel indicador do andamento da instalação será exibido.
6. Leia as informações de pós-instalação e clique em **Terminar** para concluir a instalação.

4.3 Desinstalação dos módulos

Dois módulos de desinstalação estão disponíveis para desinstalar os módulos.

Desinstalação de todos os módulos

É possível remover o sistema inteiro do PC ou do servidor, incluindo o software de serviços de

vigilância, arquivos de instalação relacionados e o Control Client.

Desinstalação de módulos específicos

É possível remover os módulos específicos do sistema do PC ou do servidor como VSM, Serviço de Transmissões ou o Control Client.

4.3 Desinstalar todos os módulos

O sistema inteiro contém o software do serviço de vigilância, arquivos de instalação relacionados e o Control Client. É possível remover o sistema inteiro do PC ou do servidor se não precisar dele.

Antes de começar

- Desative o VSM ativado antes de remover o VSM para que a Licença possa ser utilizada para ativar outro VSM. Consulte **Desativar a Licença on-line** ou **Desativar a Licença off-line** para obter mais informações.
- Saia de todos os módulos do sistema e do Gerenciador de Serviços.

Execute esta tarefa quando desejar remover o sistema inteiro.

Etapas

Observação

Os procedimentos a seguir de remoção padrão do módulo do sistema podem ser um pouco diferentes, de acordo com as diferentes versões do sistema operacional.

1. Selecione **Painel de Controle** no menu Iniciar do Windows.
 - Se utilizar a exibição Categoria, encontre a categoria Programas e clique em **Desinstalar um programa**.
 - Se utilizar a exibição de ícones Pequenos ou Grandes, selecione **Programas e recursos**.
2. Clique com o botão direito no sistema que desejar remover na lista de programas instalados atualmente.
3. Selecione **Desinstalar** e siga as instruções para remoção.

Observação

Para desinstalar o VSM será exibida uma caixa de diálogo perguntando se você deseja manter o banco de dados. Se optar por manter o banco de dados, os dados do recurso e da configuração serão salvos e poderão ser utilizados ao instalar o sistema nesse servidor de hardware posteriormente.

4.3.2 Desinstalação de módulos específicos

É possível remover módulos específicos do sistema, como VSM, Serviço de Transmissões ou o Control Client, de seu PC ou servidor se não precisar deles.

Antes de começar

- Desative o VSM ativado antes de remover o VSM para que a Licença possa ser utilizada para ativar outro VSM. Consulte **Desativar a Licença on-line** ou **Desativar a Licença off-line** para obter mais informações.
- Saia de todos os módulos do sistema e do Gerenciador de Serviços.

Execute esta tarefa quando desejar remover módulos específicos do sistema.

Etapas

Observação

Os procedimentos a seguir de remoção padrão do módulo do sistema podem ser um pouco diferentes, de acordo com as diferentes versões do sistema operacional.

1. Selecione **Painel de Controle** no menu Iniciar do Windows.
 - Se utilizar a exibição Categoria, encontre a categoria Programas e clique em **Desinstalar um programa**.
 - Se utilizar a exibição de ícones Pequenos ou Grandes, selecione **Programas e recursos**.
2. Clique com o botão direito no sistema que desejar remover na lista de programas instalados atualmente.
3. Selecione **Alterar** e o Assistente InstallShield será exibido.
4. Selecione **Modificar** e clique em **Avançar** para continuar.
5. Desmarque o módulo que desejar desinstalar e clique em **Avançar**.

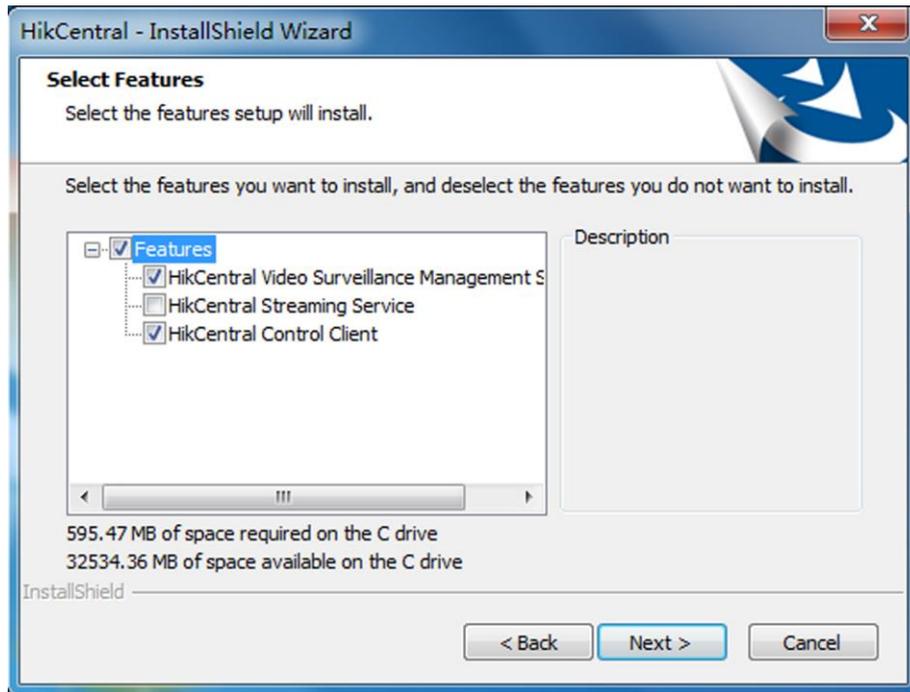


Figura 4-2 Selecione os módulos a desinstalar

6. Clique em **Desinstalar** e siga as instruções para remoção.

Observação

Para desinstalar o VSM será exibida uma caixa de diálogo perguntando se você deseja manter o banco de dados. Se você optar por manter o banco de dados, os dados de configuração e recurso serão mantidos e poderão ser utilizados quando você instalar o sistema neste servidor de hardware para a próxima vez.

Os módulos selecionados serão instalados e os módulos não selecionados serão removidos.

4.4 Gerenciador de Serviços

Após instalar com êxito os módulos de serviço será possível executar o Gerenciador de Serviços e as operações relacionadas ao serviço, como iniciar, parar ou reiniciar o serviço.

Execute esta tarefa quando precisar executar o Gerenciador de Serviços e executar as operações relacionadas.

Etapas

1. Clique com o botão direito  e selecione **Executar como administrador** para executar o Gerenciador de Serviços.

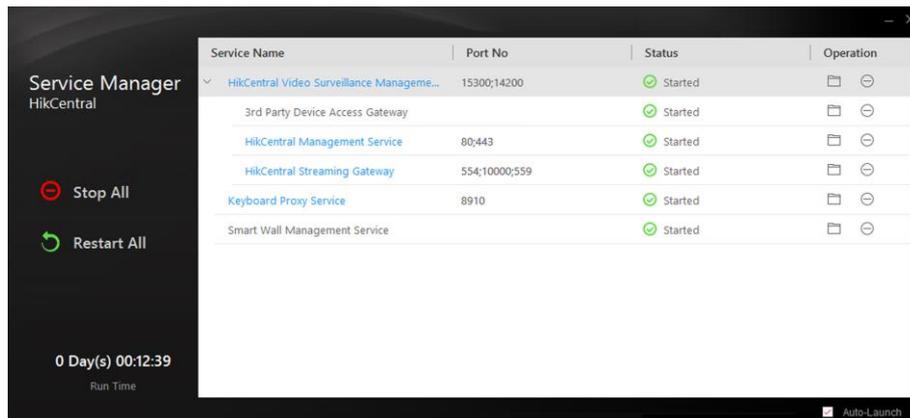


Figura 4-3 Página principal do Gerenciador de Serviços

Observação

Os itens exibidos variam de acordo com os módulos de serviço selecionados para a instalação.

2. Opcional: Execute as operações a seguir após iniciar o Gerenciamento dos Serviços.

Parar todos

Clique em **Parar todos** para parar todos os serviços.

Reiniciar todos

Clique em **Reiniciar todos** para executar os serviços novamente.

Parar serviços específicos

Selecione um serviço e clique em  para parar o serviço.

Editar serviço

Clique no nome do serviço para editar a entrada do serviço.

Observação

Se o número da entrada do serviço estiver ocupado por outro serviço, o número da entrada será exibido em vermelho. Deve-se alterar o número da entrada para outro valor antes que o serviço possa funcionar corretamente.

Abertura do local do serviço

Selecione um serviço e clique em  para ir para o diretório de instalação do serviço.

3. Opcional: Marque **Inicialização automática** para habilitar a inicialização do Gerenciador de Serviços automaticamente depois que o PC inicializou.

Observação

Se a função de inicialização automática não estiver ativada, todos os módulos de serviço instalados não poderão ser executados automaticamente após a inicialização do servidor.

Capítulo 5 Iniciar sessão

Acesse e configure o sistema diretamente via navegador da internet sem instalar nenhum software cliente no seu computador.

5.1 Ambiente de execução recomendado

A seguir o requisito de sistema recomendado para execução do Web Client.

CPU

Intel Pentium IV 3.0 GHz ou superior

Memória

1 GB e superior

Placa de vídeo

Série RADEON X700

Navegador da internet

Internet Explorer 10/11 e superior (32 bits), Firefox 32 e superior (32 bits), Google Chrome 35 e superior (32 bits)

Observação

Execute o navegador da internet como administrador.

5.2 Iniciar sessão pela primeira vez

Se esta é a primeira vez que você inicia sessão, poderá optar por fazer como administrador ou usuário normal de acordo com sua função de usuário.

5.2.1 Iniciar sessão pela primeira vez para usuário admin

Por padrão o sistema predefina o usuário administrador chamado admin. Ao iniciar sessão via Web Client pela primeira vez, você é obrigado a criar uma senha para o usuário admin antes de poder configurar e operar corretamente o sistema.

Etapas

1. Na barra de endereço do navegador da internet, digite o endereço do PC que estiver executando o serviço VSM e pressione a tecla **Enter**.

Exemplo:

Se o endereço IP do PC que estiver executando o VSM for 172.6.21.96, digite `http://172.6.21.96`

ou <https://172.6.21.96> na barra de endereços.

Observação

- Defina o protocolo de transferência antes de acessar o VSM. Para obter mais informações, consulte **Definir o protocolo de transferência**.
 - Defina o endereço IP do VSM antes de acessar o VSM via WAN. Para obter mais informações, consulte **Definir o acesso WAN**.
-

2. Digite a senha e confirme para o usuário admin na janela pop-up Criar senha.

Observação

A força da senha pode ser verificada pelo sistema e deve atender aos requisitos dele. A força padrão mínima da senha deve ser **Média**. Para definir a força mínima da senha, Consulte **Gerenciamento da segurança do sistema**.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

3. Clique em **OK**.

A página inicial do Web Client é exibida depois de criar com êxito a senha do administrador.

Resultado

Depois de iniciar sessão, a janela Nome do Local será aberta e se poderá definir o nome do local para o sistema atual conforme desejar.

Observação

Também se pode definir em **Sistema** → **Nome do local**. Consulte **Definir o nome do local** para obter mais informações.

5.2.2 Iniciar sessão pela primeira vez para usuário normal

Ao iniciar sessão no sistema como usuário normal via Web Client pela primeira vez, deve-se alterar a senha inicial e definir uma nova senha para iniciar sessão.

Etapas

1. Na barra de endereço do navegador da internet, digite o endereço do PC que estiver executando o serviço VSM e pressione a tecla **Enter**.

Exemplo:

Se o endereço IP do PC que estiver executando o VSM for 172.6.21.96, digite `http://172.6.21.96` ou `https://172.6.21.96` na barra de endereços.

Observação

Configure o endereço IP do VSM no Acesso WAN de Configuração do Sistema antes de acessar VSM via WAN. Para obter mais informações, consulte **Definir o acesso WAN**.

2. Digite o nome de usuário e a senha.

Observação

Entre em contato com o administrador para obter o nome de usuário e a senha inicial.

3. Clique em **Login** e a janela de **Alterar a senha** abrirá.
4. Insira uma nova senha e confirme-a.

Observação

A força da senha pode ser verificada pelo sistema e deve atender aos requisitos dele. Se a força da senha for inferior à força mínima exigida, será solicitado que você a altere. Para definir a força mínima da senha, Consulte **Gerenciamento da segurança do sistema**.

Cuidado

A força da senha do dispositivo pode ser verificada pelo sistema. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Clique em **OK** para alterar a senha.

Resultado

A página inicial do Web Client será exibida depois que a sessão for iniciada com êxito.

5.3 Iniciar sessão via Web Client

Acesse o sistema por meio do navegador da internet e configure o sistema.

Etapas

1. Na barra de endereço do navegador da internet, digite o endereço do PC que estiver executando o serviço VSM e pressione a tecla **Enter**.

Exemplo:

Se o endereço IP do PC que estiver executando o VSM for 172.6.21.96, digite `http://172.6.21.96` ou `https://172.6.21.96` na barra de endereços.

Observação

Configure o endereço IP do VSM no Acesso WAN de Configuração do Sistema antes de acessar VSM via WAN. Para obter mais informações, consulte ***Definir o acesso WAN***.

2. Digite o nome de usuário e a senha.
3. Clique em **Login** para entrar no sistema.

Observação

- Se tentativa de senha com falha do usuário atual for detectada, será necessário inserir o código de verificação. Tentativas de senha com falha do cliente atual, outro cliente e outro endereço exigirão o código de verificação.
 - Tentativa de senha com falha e tentativa de código de verificação do cliente atual, outro cliente (por exemplo, Control Client) e outro endereço serão todos acumuladas. Seu endereço IP será bloqueado por um período de tempo especificado após uma determinada quantidade de tentativas falhas de inserção de senha ou de código de verificação ser detectada. Para definir tentativas de iniciar sessão com falha e duração de bloqueio, consulte ***Gerenciamento da segurança do sistema***.
 - A conta será congelada por 30 minutos após 5 tentativas falhas de inserção de senha. A falha em tentativas de inserção de senha proveniente de cliente atual, outros clientes (por exemplo, Control Client) e outros endereços se acumulará.
 - A força da senha pode ser verificada pelo sistema e deve atender aos requisitos dele. Se a força da senha for inferior à força mínima exigida, será solicitado que você a altere. Para definir a força mínima da senha, Consulte ***Gerenciamento da segurança do sistema***.
 - Se sua senha tiver expirado, será solicitado que você a altere ao fazer logon. Para definir a idade máxima da senha, consulte ***Gerenciamento da segurança do sistema***.
-

Resultado

A página inicial do Web Client será exibida depois que a sessão for iniciada com êxito no sistema.

5.4 Alteração de senha para redefinição de usuário

Quando a senha do usuário normal é redefinida para a senha inicial pelo usuário admin, ele deve alterar a senha inicial e definir uma nova senha ao registrar em HikCentral via Web Client.

Execute esta tarefa quando precisar acessar o sistema via Web Client por usuário normal cuja senha tenha sido redefinida para a inicial.

Etapas

1. Na barra de endereço do navegador da internet, digite o endereço do PC que estiver executando o serviço VSM (Gerenciamento da Vigilância por Vídeo) e pressione a tecla **Enter**.

Exemplo:

Se o endereço IP do PC que estiver executando o VSM for 172.6.21.96, digite `http://172.6.21.96` ou `https://172.6.21.96` na barra de endereços.

Observação

Configure o endereço IP do VSM no Acesso WAN de Configuração do Sistema antes de acessar VSM via WAN. Para obter mais informações, consulte ***Definir o acesso WAN***.

2. Digite o nome de usuário e a senha.

Observação

A senha inicial para o usuário normal é Abc123.

3. Clique em **Login** e a janela de **Alterar a senha** abrirá.
4. Insira uma nova senha e confirme-a.

Observação

A força da senha pode ser verificada pelo sistema e deve atender aos requisitos dele. Se a força da senha for inferior à força mínima exigida, será solicitado que você a altere. Para definir a força mínima da senha, Consulte ***Gerenciamento da segurança do sistema***.

Cuidado

A força da senha do dispositivo pode ser verificada pelo sistema. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Clique em **OK**.

Resultado

A página inicial do Web Client será exibida depois que a senha for alterada com êxito.

5.5 Esquecimento da senha

Se você esqueceu a senha da sua conta, poderá redefini-la e definir uma nova.

Execute esta tarefa se esquecer a senha do usuário.

Etapas

1. Abra a página de início de sessão.
2. Digite um nome de usuário no campo Nome de usuário.
3. Clique em **Esqueci a senha**.
4. Defina a nova senha para o usuário.
 - Para o usuário administrador, insira o código de ativação, a nova senha e confirme a senha na janela Redefinir senha.
 - Para o usuário normal, se o endereço de e-mail for definido ao adicionar o usuário e o servidor de e-mail for testado com êxito, clique em **Obter código** e você receberá um e-mail com o código de verificação em seu endereço de e-mail. Em dez minutos, insira o código de verificação recebido, a nova senha e confirme a senha para definir a nova senha para o usuário normal.

Observação

Se um endereço de e-mail não estiver definido para o usuário normal, entre em contato com o usuário administrador para redefinir a senha para você e altere a senha quando iniciar sessão. Consulte ***Redefinição de senha para usuário normal*** para obter mais informações.

-
- Para o usuário do domínio, entre em contato com o usuário administrador para redefinir a senha.

Observação

A força da senha pode ser verificada pelo sistema e deve atender aos requisitos dele. Se a força da senha for inferior à força mínima exigida, será solicitado que você a altere. Para definir a força mínima da senha, Consulte ***Gerenciamento da segurança do sistema***.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Clique em **OK**.

Capítulo 6 Baixar o Mobile Client

Na página de início de sessão do Web Client é possível fazer a varredura do código QR para baixar o Mobile Client que é utilizado para acessar o sistema via terminal móvel (por exemplo, telefone celular).

Execute esta tarefa quando desejar baixar o Mobile Client.

Observação

Também se pode pesquisar e baixar o Mobile Client em App Store ou Google Play.

Etapas

1. Na barra de endereço do navegador da internet, digite o endereço do PC que estiver executando o serviço VSM (Gerenciamento da Vigilância por Vídeo) e pressione a tecla **Enter**.

Exemplo:

Se o endereço IP do PC que estiver executando o VSM for 172.6.21.96, digite `http://172.6.21.96` na barra de endereços.

Observação

Configure o endereço IP do VSM no Acesso WAN de Configuração do Sistema antes de acessar VSM via WAN. Para obter mais informações, consulte ***Definir o acesso WAN***.

2. Digitalize o código QR correspondente com o seu terminal móvel para baixar o Mobile Client.
-

Observação

Para obter informações introdutórias detalhadas sobre o Mobile Client, consulte o *Manual do Usuário do Mobile Client HikCentral* e o *Manual do Usuário do Mobile Client HD HikCentral*.

Capítulo 7 Web Control

Para acessar o Web Client via navegador da internet, instale um Web Control no PC pelo qual acessará o Web Client ao executar algumas funções como, por exemplo, visualização em tempo real, reprodução e pesquisa de Dispositivos On-Line. O Web Client automaticamente pedirá a instalação do Web Control quando você desejar acessar as funções correspondentes e você poderá seguir as instruções para instalá-lo no PC.

Capítulo 8 Assistente

O assistente pode guiá-lo para percorrer as operações básicas do sistema, incluindo adicionar os Dispositivos de Codificação, adicionar dispositivos de controle de acesso, configurar parâmetros de eventos e gerenciar os usuários.

Clique em  na página inicial para entrar na página de Iniciar o Assistente.

Vídeo

Adicione os Dispositivos de Codificação on-line ativos na mesma sub-rede local ao Web Client, adicione os dispositivos por endereço IP, segmento IP ou segmento de entrada e importe câmeras em lote, etc. Consulte ***Gerenciamento de Dispositivos de Codificação*** para obter as configurações detalhadas.

Controle de acesso

Adicione os dispositivos de controle de acesso ao sistema para outras operações e defina a permissão de acesso para as pessoas acessarem a entrada etc. Consulte ***Gerenciamento de dispositivos de controle de acessos*** para obter as configurações detalhadas.

Eventos

Configure os eventos detectados com ações de vinculação para notificação. Por exemplo, quando um movimento for detectado, acionará um evento definido pelo usuário. Consulte ***Configuração de eventos e alarmes*** para obter as configurações detalhadas.

Usuário

Adicione várias contas de usuário ao sistema para acessar Web Client, Control Client ou Mobile Client e terá permissão para atribuir diferentes funções para diferentes usuários. As funções poderão ser especificadas com diferentes permissões. Consulte ***Gerenciamento de funções e usuários*** para obter as configurações detalhadas.

Capítulo 9 Gerenciamento da Licença

Após instalar HikCentral, você tem uma Licença temporária para um número especificado de câmeras e funções limitadas. Para garantir o uso adequado da HikCentral, ative o VSM para acessar mais funções e gerenciar mais dispositivos. Se não desejar ativar o VSM agora poderá ignorar este Capítulo e ativar o sistema mais tarde.

Dois tipos de Licença estão disponíveis para HikCentral:

- **Base:** Você precisa comprar pelo menos uma Licença básica para ativar HikCentral.
- **Expansão:** Se desejar aumentar a capacidade do seu sistema (por exemplo, conectar mais câmeras), poderá adquirir uma Licença expandida para obter recursos adicionais.

Observação

- Apenas o usuário administrador pode executar a operação de ativação, atualização e desativação.
 - Se encontrar algum problema durante ativação, atualização e desativação, envie os registros do servidor para nossos engenheiros da assistência técnica.
-

9.1 Desativação da Licença on-line

Se o VSM a ser ativado puder se conectar corretamente à internet, será possível ativar o VSM no modo on-line.

Execute esta tarefa quando precisar ativar a Licença no modo on-line.

Etapas

1. Inicie sessão em HikCentral via Web Client. Consulte *Iniciar sessão via Web Client*.
2. Clique em **Ativação on-line** na área de Licença para abrir a janela de configuração da Licença.

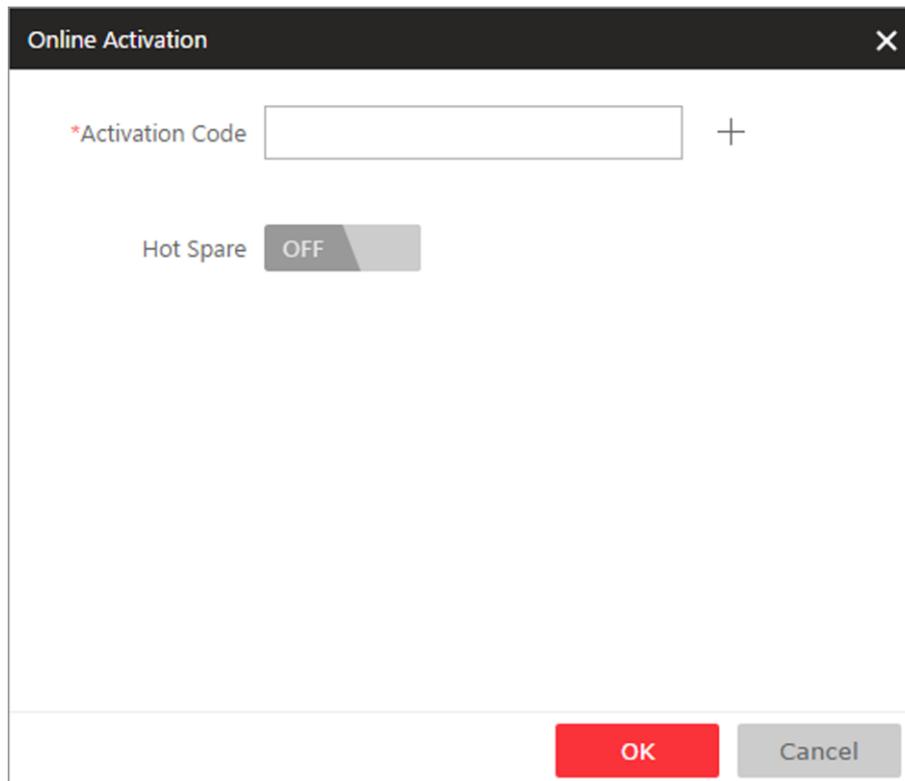


Figura 9-1 Janela de configuração da Licença

3. Digite o código de ativação recebido quando a Licença foi adquirida.

 Observação

Se tiver adquirido mais de uma Licença, clique em + e insira outros códigos de ativação.

4. Opcional: Configure o interruptor **Hot Spare** como **ligado** e insira os parâmetros exigidos se desejar construir um sistema de hot spare.

 Observação

- Selecione o modo Hot Spare ao instalar o sistema. Para obter mais informações, consulte ***Instalação de módulo***.
 - Em relação a construir o sistema de hot spare, entre em contato com nossos engenheiros da assistência técnica.
-

5. Clique em **OK** e a caixa de diálogo Contrato de Licença abrirá.

6. Leia o Contrato de Licença.

- Se aceitar os termos do Contrato de Licença, marque **Eu aceito os termos do contrato** e clique em **OK** para continuar.
- Se não aceitar o contrato, clique em **Cancelar** para cancelar a ativação.

Resultado

O aviso **Operação concluída** será exibido quando a Licença for ativada.

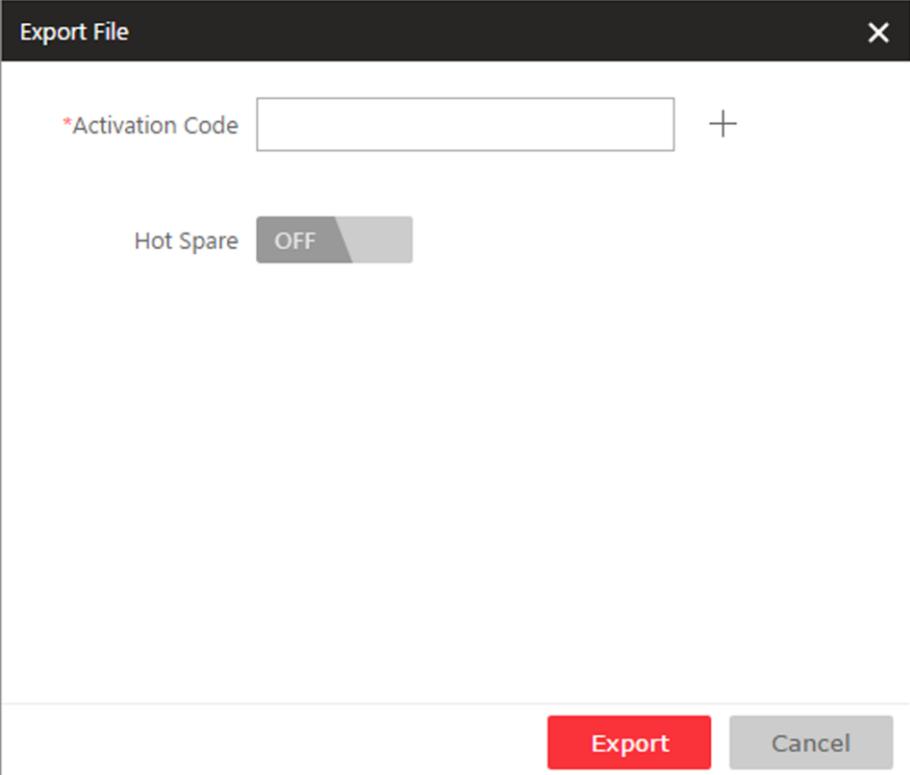
9.2 Desativação da Licença off-line

Se o VSM a ser ativado não puder se conectar à internet, será possível ativar a Licença no modo off-line.

Execute esta tarefa quando precisar ativar a Licença no modo off-line.

Etapas

1. Inicie sessão em HikCentral via Web Client. Consulte ***Iniciar sessão via Web Client***.
2. Clique em **Exportar o arquivo de solicitação da Licença** na área de Licença para abrir a janela de configuração da Licença.



The image shows a dialog box titled "Export File" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "*Activation Code" with a "+" icon to its right. Below this, there is a "Hot Spare" toggle switch currently set to "OFF". At the bottom of the dialog, there are two buttons: "Export" (red) and "Cancel" (grey).

Figura 9-2 Janela de configuração da Licença

3. Digite o código de ativação recebido quando a Licença foi adquirida.

Observação

Se tiver adquirido mais de uma Licença, clique em + e insira outros códigos de ativação.

4. Opcional: Configure o interruptor **Hot Spare** como **ligado** e insira os parâmetros exigidos se desejar construir um sistema de hot spare.

Observação

- Selecione o modo Hot Spare ao instalar o sistema. Para obter mais informações, consulte ***Instalação de módulo***.

- Em relação a construir o sistema de hot spare, entre em contato com os engenheiros da assistência técnica da Hikvision.
-

5. Clique em **Exportar** e salve o arquivo de solicitação no diretório apropriado ou na mídia removível de armazenamento (por exemplo, pen drive USB).
 6. Copie o arquivo de solicitação para o PC que pode se conectar à internet.
-

Observação

Se o PC que estiver acessando HikCentral via Web Client puder se conectar à internet, esta etapa poderá ser ignorada.

7. Entre no site da HIKVISION (<http://www.hikvision.com/en>) e vá para a página **VMS** → **Assistência a VMS** → **Gerenciamento da Licença**.
8. Entre em sua conta.
9. Selecione **Como ativar a sua conta** e clique em **Procurar** na parte inferior da página para selecionar o arquivo de solicitação de Licença exportado na Etapa 5.
10. Na caixa de diálogo pop-up, clique em **Baixar** para baixar o arquivo de ativação gerado e defina o nome e o caminho de salvamento.
11. Salve o arquivo de ativação no diretório apropriado do PC que acessa HikCentral via Web Client.
12. Na janela de configuração da Licença, clique em **Importar o arquivo de ativação** para importar o arquivo de ativação e a caixa de diálogo do Contrato de Licença abrirá.
13. Leia o Contrato de Licença.
 - Se aceitar os termos do Contrato de Licença, marque **Eu aceito os termos do contrato** e clique em **OK** para continuar.
 - Se não aceitar o contrato, clique em **Cancelar** para cancelar a ativação.

Resultado

O aviso **Operação concluída** será exibido quando o VSM for ativado com êxito.

9.3 Atualizar a Licença on-line

À medida que seu projeto cresce, pode ser necessário aumentar o número de recursos conectáveis (por exemplo, câmeras) para HikCentral. Se o VSM a ser atualizado puder se conectar corretamente à internet, será possível atualizar a Licença no modo on-line.

Antes de começar

Entre em contato com seu revendedor ou nossa equipe de vendas para adquirir uma Licença para recursos adicionais.

Etapas

1. Inicie sessão em HikCentral via Web Client. Consulte **Iniciar sessão via Web Client** para obter mais informações.
 2. Clique em **Atualizar a Licença** na área de Licença para abrir o painel de atualização.
-

3. Digite o código de ativação recebido ao adquirir sua Licença.

Observação

Se tiver adquirido mais de uma Licença, clique em + e insira outros códigos de ativação.

4. Clique em **Atualizar** e a caixa de diálogo Contrato de Licença abrirá.

5. Leia o Contrato de Licença.

- Se aceitar os termos do Contrato de Licença, marque **Eu aceito os termos do contrato** e clique em **OK** para continuar.
- Se não aceitar o contrato, clique em **Cancelar** para cancelar a atualização.

Resultado

O aviso **Operação concluída** será exibido quando o VSM for atualizado com êxito.

9.4 Atualização da Licença off-line

À medida que seu projeto cresce, pode ser necessário aumentar o número de câmeras conectáveis para HikCentral. Se o VSM a ser atualizado não puder se conectar à internet, será possível atualizar o sistema no modo off-line.

Antes de começar

Entre em contato com seu revendedor ou nossa equipe de vendas para adquirir uma Licença para recursos adicionais.

Etapas

1. Inicie sessão em HikCentral via Web Client. Consulte **Iniciar sessão via Web Client** para obter mais informações.
2. Clique em **Atualizar a Licença** na área de Licença para abrir o painel de atualização.
3. Clique em **Exportar o arquivo de solicitação da Licença** na área de Licença para abrir a janela de configuração da Licença.
4. Digite o código de ativação da sua Licença adicional.

Observação

Se tiver adquirido mais de uma Licença, clique em + e insira outros códigos de ativação.

5. Clique em **Exportar** e salve o arquivo de solicitação no diretório apropriado ou na mídia removível de armazenamento (por exemplo, pen drive USB).

6. Copie o arquivo de solicitação para o PC que pode se conectar à internet.

Observação

Se o PC que estiver acessando HikCentral via Web Client puder se conectar à internet, esta etapa poderá ser ignorada.

7. Entre no site da HIKVISION (<http://www.hikvision.com/en>) e vá para a página **VMS** → **Assistência a VMS** → **Gerenciamento da Licença**.
8. Acesse a sua conta.
9. Selecione **Como atualizar a sua conta** e clique em **Procurar** na parte inferior da página para selecionar o arquivo de solicitação de Licença exportado na Etapa 5.
10. Clique em **Enviar** para gerar o arquivo de atualização.
11. Na caixa de diálogo pop-up, clique em **Baixar** para baixar o arquivo de atualização gerado e defina o nome e o caminho de salvamento.
12. Salve o arquivo de atualização no diretório apropriado do PC que acessa HikCentral via Web Client.
13. Na janela de configuração da Licença, clique em **Importar o arquivo de atualização** para importar o arquivo de atualização e a caixa de diálogo do Contrato de Licença abrirá.
14. Leia o Contrato de Licença.
 - Se aceitar os termos do Contrato de Licença, marque **Eu aceito os termos do contrato** e clique em **OK** para continuar.
 - Se não aceitar o contrato, clique em **Cancelar** para cancelar a atualização.

Resultado

O aviso **Operação concluída** será exibido quando o VSM for atualizado com êxito.

9.5 Desativação da Licença on-line

Se desejar executar o VSM em outro PC ou servidor, desative o VSM primeiro e depois ative o outro VSM novamente. Se o VSM a ser desativado puder se conectar corretamente à internet, será possível desativar a Licença no modo on-line.

Etapas

1. Inicie sessão em HikCentral via Web Client. Consulte **Iniciar sessão via Web Client**.
2. Clique em **Desativar a Licença** na área de Licença para abrir o painel de desativação.
3. Clique em **Desativação on-line** e marque os códigos de ativação a desativar.
4. Clique em **OK** para desativar a Licença.

Resultado

O aviso **Operação concluída** será exibido quando o VSM for desativado com êxito. Ative outro VSM com a Licença.

9.6 Desativação da Licença off-line

Se desejar executar o VSM em outro PC ou servidor, desative o VSM primeiro e depois ative o VSM novamente. Se o VSM a ser desativado não puder se conectar à internet, será possível desativar a Licença no modo off-line.

Etapas

1. Inicie sessão em HikCentral via Web Client. Consulte **Iniciar sessão via Web Client** para obter mais informações.
2. Clique em **Desativar a Licença** na área de Licença para abrir o painel de desativação.
3. Clique em **Exportar o arquivo de solicitação da Licença** e selecione os códigos de ativação a desativar.
4. Clique em **Exportar** e salve o arquivo de solicitação no diretório apropriado ou na mídia removível de armazenamento (por exemplo, pen drive USB).
5. Copie o arquivo de solicitação para o PC que pode se conectar à internet.

Observação

Se o PC que estiver acessando HikCentral via Web Client puder se conectar à internet, esta etapa poderá ser ignorada.

6. Entre no site da HIKVISION (<http://www.hikvision.com/en>) e vá para a página **VMS** → **Assistência** → **Gerenciamento da Licença**.
7. Acesse a sua conta.
8. Selecione **Como desativar a sua conta** e clique em **Procurar** na parte inferior da página para selecionar o arquivo de solicitação de Licença exportado na Etapa 4.
9. Na caixa de diálogo pop-up, clique em **Baixar** para baixar o arquivo de desativação gerado e defina o nome e o caminho de salvamento.
10. Salve o arquivo de desativação no diretório apropriado do PC que acessa HikCentral via Web Client.
11. Na janela de configuração da Licença, clique em **Importar o arquivo de desativação** para importar o arquivo de desativação.
12. Desative novamente para concluir a operação de desativação.
 - 1) Um novo arquivo de solicitação será gerado automaticamente e solicitará que você o exporte novamente. Ou então clique em **Exportar o arquivo de solicitação da Licença** para exportar o arquivo de solicitação manualmente.
 - 2) Salve o arquivo de solicitação no diretório apropriado ou na mídia de armazenamento removível e execute as Etapas 4-9 novamente para concluir a operação de desativação.

Resultado

O aviso **Operação concluída** será exibido quando o VSM for desativado com êxito. Ative outro VSM com a Licença.

Capítulo 10 Gerenciamento de recursos

A HikCentral apresenta vários tipos de recursos, como dispositivo de codificação, dispositivo de controle de acessos, local remoto, dispositivo de decodificação e Smart Wall. Depois de adicioná-los ao sistema, gere-os, defina as configurações necessárias e realize outras operações. Por exemplo, adicione Dispositivos de Codificação para visualização em tempo real, reprodução, configurações de gravação, configuração de eventos etc., adicione dispositivos de controle de acesso para controle de acessos, gerenciamento de horários e presença etc., adicione Local Remoto para gerenciamento central de vários sistemas, adicione Servidor de Gravações para armazenar vídeos, adicione Servidor de Transmissões para obter a transmissão de dados de vídeo do servidor e adicione Smart Wall para exibir vídeo decodificado no Smart Wall.

10.1 Criação de senha para dispositivos inativos

Devido à senha padrão simples, os dispositivos podem ser acessados facilmente por usuário não autorizado. Para maior segurança, a senha padrão não é fornecida para alguns dispositivos. Você é obrigado a criar a senha para ativá-los antes de adicioná-los e executar algumas operações neles por meio do sistema. Além de ativar o dispositivo um por um, você também pode lidar com vários ao mesmo tempo. Os dispositivos que forem ativados em lote terão a mesma senha

Antes de começar

- Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Esta função deve ser aceita pelo dispositivo. Verifique se os dispositivos que desejam ativar permitem essa função.

Execute esta tarefa quando precisar ativar os Dispositivos On-Line detectados. Aqui tomamos como exemplo a criação de senha para o Dispositivo de Codificação.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.

Observação

- Para os dispositivos de controle de acesso, clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de gerenciamento do Dispositivo de Controle de Acessos.
- Para os dispositivos de controle de acesso, clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de gerenciamento do Dispositivo de Controle de Segurança.
- Para Dispositivos de Decodificação, clique em **Exibição física** → **Smart Wall**. Na área do Dispositivo de Decodificação, clique em **Adicionar** e marque **Dispositivos on-line** como Modo

de Adição.

A lista de Dispositivos On-Line detectados está na área de Dispositivos On-Line.

2. Veja o status do dispositivo (exibido na coluna de Segurança) e selecione um ou vários dispositivos inativos.
 3. Clique em  para abrir a janela de Ativação de Dispositivos.
 4. Crie uma senha no campo de senha e confirme-a.
-



Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Clique em **Salvar** para criar a senha para o dispositivo.
Uma mensagem de **Operação concluída** será exibida quando a senha for definida com êxito.
6. Clique em  na coluna Operação do dispositivo e altere seu endereço IP, máscara de sub-rede e gateway para a mesma sub-rede com seu computador se precisar adicionar o dispositivo no sistema. Consulte *Editar informações de rede do Dispositivo On-Line*.

10.2 Editar informações de rede do Dispositivo On-Line

Dispositivos On-Line que possuem endereços IP na mesma sub-rede local com o servidor VSM ou o Web Client podem ser detectados por HikCentral. Para os Dispositivos On-Line detectados, edite as informações da rede conforme desejado via HikCentral de forma conveniente e remota. Por exemplo, modifique o endereço IP do dispositivo devido às alterações da rede.

Antes de começar

Para alguns dispositivos é necessário ativá-los antes de editar suas informações de rede. Consulte *Criação de senha para dispositivos inativos* para obter mais informações.

Execute esta tarefa quando precisar editar as informações da rede para os Dispositivos On-Line detectados. Aqui tomamos como exemplo o Dispositivo de Codificação de edição.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
-



Observação

- Para os dispositivos de controle de acesso, clique em **Exibição física** → **Dispositivo de**
-

Controle de Acessos para entrar na página de gerenciamento do Dispositivo de Controle de Acessos.

- Para os dispositivos de controle de acesso, clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de gerenciamento do Dispositivo de Controle de Segurança.
 - Para Dispositivos de Decodificação, clique em **Exibição física** → **Smart Wall**. Na área do Dispositivo de Decodificação, clique em **Adicionar** e marque **Dispositivos on-line** como Modo de Adição.
-

2. Na área Dispositivos On-Line, selecione um tipo de rede.

Rede do servidor

Os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client serão relacionados na área dos Dispositivos On-Line.

3. Veja o status do dispositivo (exibido na coluna Segurança) e clique em  na coluna Operação de um dispositivo ativo.
 4. Altere os parâmetros exigidos como endereço IP, entrada do dispositivo, entrada HTTP, máscara de sub-rede e gateway.
-

Observação

Os parâmetros podem variar para diferentes tipos de dispositivos.

5. Clique em .
6. Digite a senha do dispositivo.
7. Clique em **Salvar**.

10.3 Gerenciamento do Dispositivo de Codificação

Dispositivos de Codificação (por exemplo, câmera, NVR, DVR) podem ser adicionados ao sistema para gerenciamento, incluindo edição e exclusão de dispositivos, configuração remota, alteração da senha de Dispositivos On-Line etc. Também se pode realizar outras operações com base nos dispositivos adicionados, como visualização em tempo real, gravação de vídeo e configurações de eventos.

10.3.1 Adicionar Dispositivos On-Line

O sistema pode realizar uma detecção automatizada dos Dispositivos de Codificação disponíveis na rede onde estão localizados o Web Client ou o servidor, o que torna as informações dos dispositivos sobre si mesmas (por exemplo, endereço IP) reconhecidas pelo sistema. Com base nas

informações, adicione os dispositivos rapidamente.

Adicione um Dispositivo On-Line de cada vez ou vários Dispositivos On-Line em lote.

Observação

Instale o Web Control de acordo com as instruções e, em seguida, a função de detecção on-line de dispositivos estará disponível.

Adicionar Dispositivos On-Line

Quando desejar adicionar um dos Dispositivos On-Line detectados no momento ou adicionar alguns desses dispositivos com nomes de usuário e senhas diferentes, será necessário selecionar um único dispositivo a cada vez para adicioná-lo a HikCentral. O endereço IP, o número da entrada e o nome de usuário serão reconhecidos automaticamente, o que pode reduzir algumas operações manuais de alguma forma.

Antes de começar

- Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos a serem adicionados devem ser ativados. Consulte ***Criação de senha para dispositivos inativos*** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar adicionar um único dispositivo detectado on-line.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
2. Na área Dispositivos On-Line, selecione um tipo de rede.

Rede do servidor

Como seleção padrão os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client serão relacionados na área dos Dispositivos On-Line.

3. Na área de Dispositivos On-Line, selecione o dispositivo ativo a ser adicionado.
4. Clique em **Adicionar à lista de dispositivos** para abrir a janela de Adicionar Dispositivos On-Line.

Add Online Device

Basic Information

* Device Address

* Device Port

i Verify Stream Encryption Key

* Alias

* User Name

* Password

Risky

Channel Information

i Add Channel to Area

* Channel All Channels
 Specified Channel

* Area Create Area by Device Name
 Existing Area

i Streaming Server

Video Storage

*Storage Location

Get Device's Recording Settings

Add **Cancel**

Figura 10-1 Janela de Adicionar Dispositivos On-Line

5. Preencha as informações solicitadas.

Endereço do dispositivo

O endereço IP do dispositivo que é exibido automaticamente.

Entrada do dispositivo

O número da entrada do dispositivo, que é exibido automaticamente. O padrão é 8000.

Verificação da chave de criptografia de transmissões

Configure o interruptor de **Verificação da chave de criptografia de transmissões** como ligado

e insira a chave de criptografia de transmissões no campo **Chave de criptografia de transmissões no dispositivo**. Então, ao iniciar a visualização em tempo real ou a reprodução remota do dispositivo, o cliente verificará a chave armazenada no servidor VSM para fins de segurança.

Observação

Esta função deve ser aceita pelos dispositivos. Consulte o Manual do Usuário do dispositivo para obter a chave.

Pseudônimo

Crie um nome descritivo para o dispositivo. Por exemplo, utilize um pseudônimo que exiba a localização ou o recurso do dispositivo.

Nome de usuário

O nome de usuário da conta do administrador criada ao ativar o dispositivo ou a conta não administrativa adicionada, como a operadora. Ao adicionar o dispositivo a HikCentral utilizando a conta não administrativa, suas permissões podem restringir seu acesso a determinados recursos.

Senha

A senha necessária para acessar a conta.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

6. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais dos dispositivos adicionados a uma área.
-

Observação

- Importe todos os canais, incluindo câmeras, entradas e saídas de alarmes ou câmeras especificadas para a área correspondente.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se você não importar canais para a área, não será possível executar a exibição em tempo real, reprodução, configurações de evento etc. para as câmeras.
-

7. Opcional: Se optar por adicionar canais à área, selecione um servidor de transmissões para obter a transmissão de vídeo dos canais por meio do servidor.
-

 **Observação**

Marque **Exibição em mural via servidor de transmissões** para transmitir por meio do servidor de transmissões selecionado ao exibir a visualização em tempo real no Smart Wall.

8. Opcional: Se optar por adicionar canais à área, ative a função **Armazenamento de vídeo** e selecione o local de armazenamento para gravações.

Dispositivo de codificação

Os arquivos de vídeo serão armazenados no dispositivo de acordo com o cronograma de gravação configurado.

Rede de Área de Armazenamento Híbrido

Os arquivos de vídeo serão armazenados na Rede de Área de Armazenamento Híbrido de acordo com o cronograma de gravação configurado.

Servidor de Armazenamento em Nuvem

Os arquivos de vídeo serão armazenados no Servidor de Armazenamento em Nuvem de acordo com o cronograma de gravação configurado.

pStor

De acordo com o cronograma de gravação configurado, os arquivos de vídeo serão armazenados no pStor, que é o serviço de acesso a armazenamento para gerenciamento de discos rígidos locais e discos lógicos.

 **Observação**

- Para adicionar o Dispositivo de Codificação por nome de domínio, os arquivos de vídeo só podem ser armazenados no armazenamento local do dispositivo.
 - Configure a Rede de Área de Armazenamento Híbrido, o Servidor de Armazenamento em Nuvem ou pStor antecipadamente. Caso contrário, seu local de armazenamento não poderá ser exibido na lista suspensa. Clique em **Adicionar um novo** para adicionar uma nova Rede de Área de Armazenamento Híbrido, Servidor de Armazenamento em Nuvem ou pStor.
-

9. Defina o agendamento de gravação rápida para os canais adicionados.
- Marque **Obter configurações de gravações do dispositivo** para obter o cronograma de gravações do dispositivo e os canais do dispositivo iniciarão gravação de acordo com o cronograma.
 - Desmarque **Obter configurações de gravações do dispositivo** e defina as informações obrigatórias como modelo de cronograma de gravações, tipo de transmissão etc. Consulte **Configuração de gravações para câmeras no Local Atual** para obter mais informações.
10. Clique em **Adicionar**.
11. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo On-Line.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

 **Observação**

Para conhecer as etapas de funcionamento detalhadas acerca da configuração remota, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Adicionar Dispositivos On-Line em lote

Para os Dispositivos de Codificação on-line detectados, se tiverem os mesmos nome de usuário e senha, adicione vários dispositivos a HikCentral de uma vez. Os dispositivos adicionados por esse método serão definidos como as mesmas informações de canal, que se poderá editar posteriormente, se necessário.

Antes de começar

- Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos a serem adicionados devem ser ativados. Consulte ***Criação de senha para dispositivos inativos*** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar adicionar os Dispositivos On-Line detectados em lote.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
2. Na área Dispositivos On-Line, selecione um tipo de rede.

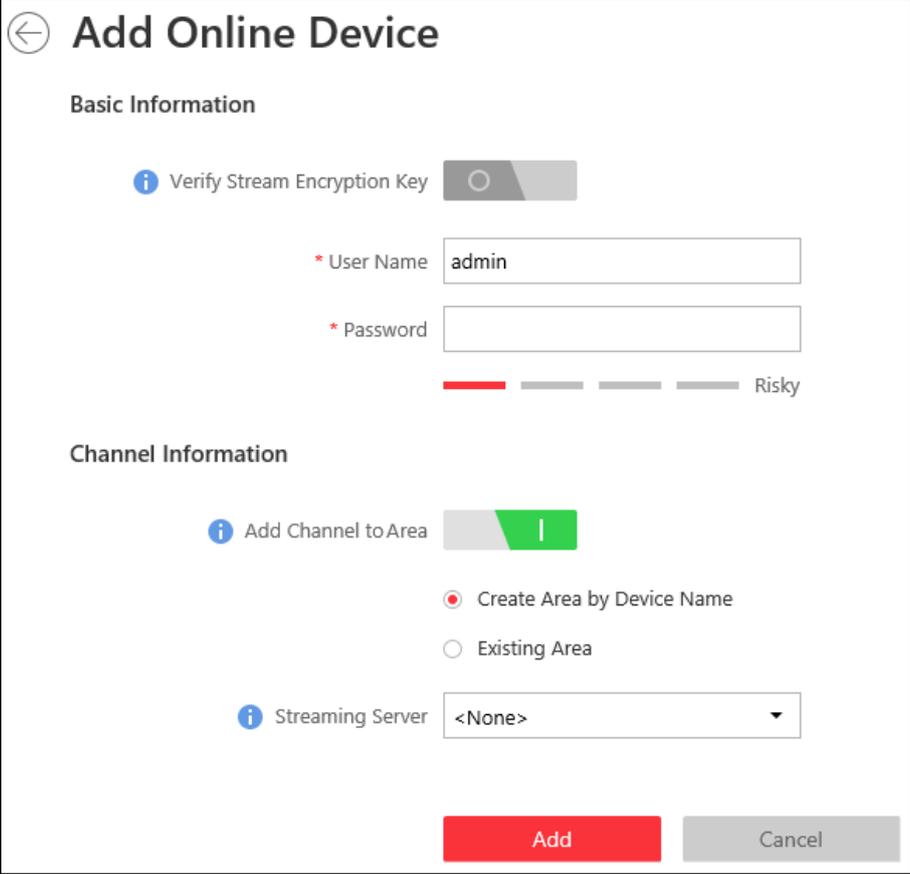
Rede do servidor

Como seleção padrão os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client serão relacionados na área dos Dispositivos On-Line.

3. Na área de Dispositivos On-Line, marque o dispositivo ativo a ser adicionado.
4. Clique em **Adicionar à lista de dispositivos** para abrir a caixa de diálogo de Adicionar Dispositivos On-Line.



Add Online Device

Basic Information

Verify Stream Encryption Key

* User Name: admin

* Password: [Empty]

Risky

Channel Information

Add Channel to Area

Create Area by Device Name

Existing Area

Streaming Server: <None>

Add Cancel

Figura 10-2 Caixa de diálogo de Adicionar Dispositivos On-Line

5. Opcional: Configure o interruptor de **Verificação da chave de criptografia de transmissões** como ligado e insira a chave de criptografia de transmissões no campo **Chave de criptografia de transmissões no dispositivo**.

Então, ao iniciar a visualização em tempo real ou a reprodução remota da câmera, o cliente verificará a chave armazenada no servidor VSM para fins de segurança.

Observação

Esta função deve ser aceita pelos dispositivos. Consulte o Manual do Usuário do dispositivo para obter a chave.

6. Digite os mesmos nome de usuário e senha.

Nome de usuário

O nome de usuário da conta do administrador criada ao ativar o dispositivo ou a conta não administrativa adicionada, como a operadora. Ao adicionar o dispositivo a HikCentral utilizando a conta não administrativa, suas permissões podem restringir seu acesso a

determinados recursos.

Senha

A senha necessária para acessar a conta.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

7. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais dos dispositivos adicionados a uma área.
-

Observação

- Importe todos os canais, incluindo câmeras, entradas e saídas de alarmes ou câmeras especificadas para a área correspondente.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se você não importar canais para a área, não será possível executar a exibição em tempo real, reprodução, configurações de evento etc. para as câmeras.
-

8. Opcional: Selecione a Servidor de Transmissões para obter a transmissão de vídeo dos canais via servidor.
-

Observação

Marque **Exibição em mural via servidor de transmissões** para obter transmissão via servidor de transmissões selecionadas ao iniciar a visualização em tempo real no Smart Wall.

9. Clique em **Adicionar**.

10. Opcional: Execute as operações a seguir depois de adicionar os Dispositivos On-Line em lote.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.3.2 Adicionar dispositivo por endereço IP ou nome de domínio

Quando se conhece endereço IP ou nome de domínio do dispositivo a adicionar se pode adicionar os dispositivos ao sistema especificando-se o endereço IP (ou nome de domínio), nome de usuário, senha e outros parâmetros relacionados.

Antes de começar

Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivo por endereço IP ou nome de domínio.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Codificação.

Figura 10-3 Página de Adicionar Dispositivo de Codificação

3. Selecione **IP/Domínio** como modo de adicionar.
4. Defina as informações obrigatórias, incluindo protocolo de acesso, endereço de dispositivo, entrada de dispositivo, chave de criptografia de transmissões, pseudônimo, nome de usuário e senha.

Protocolo de acesso

Selecione **Protocolo Hikvision** para adicionar os dispositivos e selecione **Protocolo ONVIF** para adicionar dispositivos de terceiros.

Endereço do dispositivo

O endereço IP ou nome de domínio do dispositivo.

Entrada do dispositivo

Por padrão o número da entrada do dispositivo é 8000.

Verificação da chave de criptografia de transmissões

Configure o interruptor de **Verificação da chave de criptografia de transmissões** como ligado e insira a chave de criptografia de transmissões no campo **Chave de criptografia de transmissões no dispositivo**. Então, ao iniciar a visualização em tempo real ou a reprodução

remota do dispositivo, o cliente verificará a chave armazenada no servidor VSM para fins de segurança.

Observação

Esta função deve ser aceita pelos dispositivos. Consulte o Manual do Usuário do dispositivo para obter a chave.

Pseudônimo

Crie um nome descritivo para o dispositivo. Por exemplo, utilize um pseudônimo que exiba a localização ou o recurso do dispositivo.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais dos dispositivos adicionados a uma área.
-

Observação

- Importe todos os canais, incluindo câmeras, entradas e saídas de alarmes ou câmeras especificadas para a área correspondente.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se você não importar canais para a área, não será possível executar a exibição em tempo real, reprodução, configurações de evento etc. para as câmeras.
-

6. Opcional: Se optar por adicionar canais à área, selecione um servidor de transmissões para obter a transmissão de vídeo dos canais por meio do servidor.
-

Observação

Marque **Exibição em mural via servidor de transmissões** para transmitir por meio do servidor de transmissões selecionado ao exibir a visualização em tempo real no Smart Wall.

7. Opcional: Se optar por adicionar canais à área, ative a função **Armazenamento de vídeo** e selecione o local de armazenamento para gravações.

Dispositivo de codificação

Os arquivos de vídeo serão armazenados no dispositivo de acordo com o cronograma de

gravação configurado.

Rede de Área de Armazenamento Híbrido

Os arquivos de vídeo serão armazenados na Rede de Área de Armazenamento Híbrido de acordo com o cronograma de gravação configurado.

Servidor de Armazenamento em Nuvem

Os arquivos de vídeo serão armazenados no Servidor de Armazenamento em Nuvem de acordo com o cronograma de gravação configurado.

pStor

De acordo com o cronograma de gravação configurado, os arquivos de vídeo serão armazenados no pStor, que é o serviço de acesso a armazenamento para gerenciamento de discos rígidos locais e discos lógicos.

Observação

- Para adicionar o Dispositivo de Codificação por nome de domínio, os arquivos de vídeo só podem ser armazenados no armazenamento local do dispositivo.
 - Configure a Rede de Área de Armazenamento Híbrido, o Servidor de Armazenamento em Nuvem ou pStor antecipadamente. Caso contrário, seu local de armazenamento não poderá ser exibido na lista suspensa. Clique em **Adicionar um novo** para adicionar uma nova Rede de Área de Armazenamento Híbrido, Servidor de Armazenamento em Nuvem ou pStor.
-

8. Defina o agendamento de gravação rápida para os canais adicionados.

- Marque **Obter configurações de gravações do dispositivo** para obter o cronograma de gravações do dispositivo e os canais do dispositivo iniciarão gravação de acordo com o cronograma.
- Desmarque **Obter configurações de gravações do dispositivo** e defina as informações obrigatórias como modelo de cronograma de gravações, tipo de transmissão etc. Consulte **Configuração de gravações para câmeras no Local Atual** para obter mais informações.

9. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar o Dispositivo de Codificação e volte à página com a lista de Dispositivos de Codificação.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Dispositivos de Codificação.

10. Opcional: Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para conhecer as etapas de funcionamento detalhadas acerca da configuração remota, consulte o Manual do Usuário do dispositivo.

Alteração da senha Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.3.3 Adicionar dispositivos por Segmento IP

Quando vários Dispositivos de Codificação a adicionar têm os mesmos número de entrada, nome de usuário e senha mas diferentes endereços IP dentro de um intervalo, selecione este modo de adicionar e especifique o intervalo de IP onde seus dispositivos estiverem localizados e outros parâmetros relacionados. O sistema fará a varredura desde o endereço IP inicial até o endereço IP final para os dispositivos a fim de adicioná-los rapidamente.

Antes de começar

Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Codificação.

Figura 10-4 Página de Adicionar Dispositivo de Codificação

3. Selecione **Segmento IP** como modo de adicionar.
4. Digite as informações obrigatórias.

Protocolo de acesso

Selecione **Protocolo Hikvision** para adicionar os dispositivos e selecione **Protocolo ONVIF** para adicionar dispositivos de terceiros.

Endereço do dispositivo

Digite o endereço IP inicial e o endereço IP final onde os dispositivos estiverem localizados.

Entrada do dispositivo

O mesmo número de entrada dos dispositivos. Por padrão o número da entrada do dispositivo é 8000.

Verificação da chave de criptografia de transmissões

Configure o interruptor de **Verificação da chave de criptografia de transmissões** como ligado e insira a chave de criptografia de transmissões no campo **Chave de criptografia de transmissões no dispositivo**. Então, ao iniciar a visualização em tempo real ou a reprodução remota do dispositivo, o cliente verificará a chave armazenada no servidor VSM para fins de segurança.

Observação

Esta função deve ser aceita pelos dispositivos. Consulte o Manual do Usuário do dispositivo para obter a chave.

Nome de usuário

O nome de usuário do administrador criado ao ativar o dispositivo ou usuários não administrativos adicionados. Ao adicionar o dispositivo a HikCentral utilizando usuário não administrativo, suas permissões podem restringir seu acesso a determinados recursos.

Senha

A senha necessária para acessar o dispositivo.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais dos dispositivos adicionados a uma área.
-

Observação

- Importe todos os canais, incluindo câmeras, entradas e saídas de alarmes ou câmeras especificadas para a área correspondente.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se você não importar canais para a área, não será possível executar a exibição em tempo real, reprodução, configurações de evento etc. para os canais.
-

6. Opcional: Se optar por adicionar canais à área, selecione um servidor de transmissões para obter a transmissão de vídeo dos canais por meio do servidor.
-

Observação

Marque **Exibição em mural via servidor de transmissões** para transmitir por meio do servidor de transmissões selecionado ao exibir a visualização em tempo real no Smart Wall.

7. Termine de adicionar o dispositivo.
 - Clique em **Adicionar** para adicionar os dispositivos dos quais os endereços IP estejam entre os endereços IP inicial e final e volte à página com a lista de dispositivos.
-

- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Dispositivos de Codificação.

8. Opcional: Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.3.4 Adicionar dispositivos por segmento de entrada

Quando vários Dispositivos de Codificação a adicionar tiverem os mesmos endereço IP, nome de usuário e senha mas diferentes números de entrada dentro de um intervalo, selecione este modo de adicionar e especifique o intervalo de entrada, endereço IP, nome de usuário, senha e outros parâmetros relacionados para adicioná-los.

Antes de começar

Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por segmento de entrada.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Codificação.

Figura 10-5 Página de Adicionar Dispositivo de Codificação

3. Selecione **Segmento de entrada** como modo de adicionar.
4. Preencha as informações solicitadas.

Protocolo de acesso

Selecione **Protocolo Hikvision** para adicionar os dispositivos e selecione **Protocolo ONVIF** para adicionar dispositivos de terceiros.

Endereço do dispositivo

Digite o endereço IP para adicionar os dispositivos que tiverem o mesmo endereço IP.

Entrada do dispositivo

Digite o número de entrada inicial e o número de entrada final.

Verificação da chave de criptografia de transmissões

Configure o interruptor de **Verificação da chave de criptografia de transmissões** como ligado e insira a chave de criptografia de transmissões no campo **Chave de criptografia de transmissões no dispositivo**. Então, ao iniciar a visualização em tempo real ou a reprodução remota do dispositivo, o cliente verificará a chave armazenada no servidor VSM para fins de segurança.

Observação

Esta função deve ser aceita pelos dispositivos. Consulte o Manual do Usuário do dispositivo para obter a chave.

Nome de usuário

O nome de usuário da conta do administrador criada ao ativar o dispositivo ou a conta não administrativa adicionada, como a operadora. Ao adicionar o dispositivo a HikCentral utilizando a conta não administrativa, suas permissões podem restringir seu acesso a determinados recursos.

Senha

A senha necessária para acessar a conta.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais dos dispositivos adicionados a uma área.
-

Observação

- Importe todos os canais, incluindo câmeras, entradas e saídas de alarmes ou câmeras especificadas para a área correspondente.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se você não importar canais para a área, não será possível executar a exibição em tempo real, reprodução, configurações de evento etc. para os canais.
-

6. Opcional: Se optar por adicionar canais à área, selecione um servidor de transmissões para obter a transmissão de vídeo dos canais por meio do servidor.
-

Observação

Marque **Exibição em mural via servidor de transmissões** para transmitir por meio do servidor de transmissões selecionado ao exibir a visualização em tempo real no Smart Wall.

7. Termine de adicionar o dispositivo.
 - Clique em **Adicionar** para adicionar os dispositivos dos quais o número de entrada seja entre
-

o número de entrada inicial e o número de entrada final e volte à página com a lista de dispositivos.

- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros dispositivos.

8. Opcional: Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.3.5 Adicionar dispositivo por Hik-Connect

Adicione o Dispositivo de Codificação que foi adicionado à conta Hik-Connect ao sistema.

Antes de começar

Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por Hik-Connect.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Codificação.

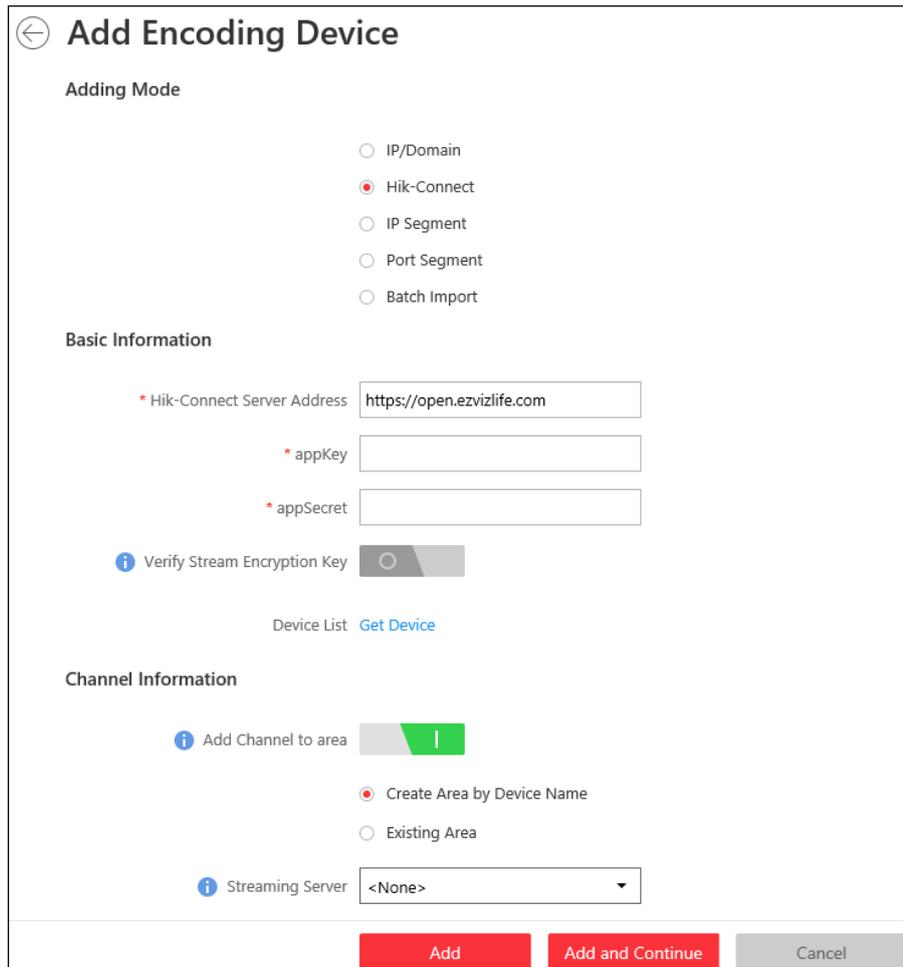


Figura 10-6 Página de Adicionar Dispositivo de Codificação

3. Selecione **Hik-Connect** como modo de adicionar.
4. Digite as informações obrigatórias.

Endereço do servidor de Hik-Connect

Digite o endereço do serviço Hik-Connect. Por padrão é ***https://open.ezvizlife.com***.

appKey

Digite appKey do serviço Hik-Connect.

appSecret

Digite o appSecret do serviço Hik-Connect.

Verificação da chave de criptografia de transmissões

Configure o interruptor de **Verificação da chave de criptografia de transmissões** como ligado e insira a chave de criptografia de transmissões no campo **Chave de criptografia de transmissões no dispositivo**. Então, ao iniciar a visualização em tempo real ou a reprodução remota da câmera, o cliente verificará a chave armazenada no servidor VSM para fins de segurança.

Esta função deve ser aceita pelos dispositivos. Consulte o Manual do Usuário do dispositivo

para obter a chave.

Lista de dispositivos

Clique em **Obter dispositivo** para exibir os dispositivos adicionados à conta, selecione o dispositivo e digite nome de usuário e senha do dispositivo.

The screenshot shows the 'Device List' interface. At the top, there are three input fields: '*Hik-Connect Server Address' with the value 'https://open.ezvizlife.com', '*appKey', and '*appSecret'. Each has a green checkmark to its right. Below these is a 'Device List' section with a search bar and a 'Show Added Device' checkbox. A table displays two devices: 'DS-7' and 'DS-2', both with 'Not Added' status. At the bottom, there are fields for 'User Name' and 'Password'.

Figura 10-7 Lista de dispositivos adicionados

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Configure o interruptor **Adicionar canal a área** como ligado para importar os canais dos dispositivos adicionados a uma área.

Observação

- Importe todos os canais, incluindo câmeras, entradas e saídas de alarmes ou câmeras especificadas para a área correspondente.
- Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
- Se você não importar canais para a área, não será possível executar a exibição em tempo real, reprodução, configurações de evento etc. para os canais.

6. Opcional: Se optar por adicionar canais à área, selecione um servidor de transmissões para obter a transmissão de vídeo dos canais por meio do servidor.

 **Observação**

Marque **Exibição em mural via servidor de transmissões** para transmitir por meio do servidor de transmissões selecionado ao exibir a visualização em tempo real no Smart Wall.

7. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar o Dispositivo de Codificação e volte à página com a lista de Dispositivos de Codificação.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Dispositivos de Codificação.

8. Opcional: Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

 **Observação**

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.3.6 Adicionar dispositivos em lote

Quando há um lote de dispositivos a adicionar a HikCentral se pode editar o modelo predefinido que contém as informações obrigatórias do dispositivo e importar para adicionar vários dispositivos ao mesmo tempo. Esse também é um método altamente eficaz se configurar vários sistemas semelhantes.

Antes de começar

Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos importando o modelo que contém informações de vários dispositivos.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Codificação.

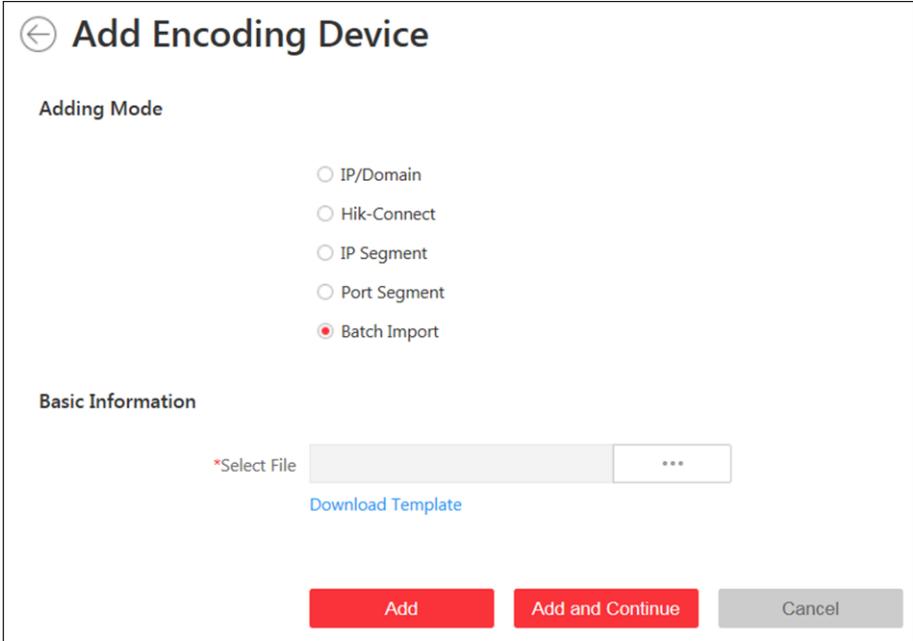


Figura 10-8 Página de Adicionar Dispositivo de Codificação

3. Selecione **Importação em lote** como modo de adicionar.
4. Clique em **Baixar modelo** e salve o modelo predefinido (arquivo CSV) em seu PC.
5. Abra o arquivo de modelo exportado e insira as informações obrigatórias dos dispositivos a serem adicionados na coluna correspondente.
6. Clique em **...** e selecione o arquivo de modelo.
7. Termine de adicionar os dispositivos.
 - Clique em **Adicionar** para adicionar os dispositivos e volte à página com a lista de dispositivos.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros dispositivos.
8. Opcional: Execute as operações a seguir depois de adicionar os dispositivos em lote.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.4 Gerenciamento do Dispositivo de Controle de Acessos

Adicione o Dispositivo de Controle de Acessos ao sistema para configuração de permissão de acesso, horários e gerenciamento de frequência etc.

10.4.1 Adicionar Dispositivos On-Line

O Dispositivo de Controle de Acessos on-line na mesma sub-rede local que o Web Client ou servidor VSM atuais será exibido em uma lista. Adicione um Dispositivo On-Line de cada vez ou vários Dispositivos On-Line em lote.

 **Observação**

Instale o Web Control de acordo com as instruções e, em seguida, a função de detecção on-line de dispositivos estará disponível.

Adicionar Dispositivos On-Line únicos

Adicione os dispositivos de controle de acessos on-line detectados e aqui apresentamos o processo para adicionar dispositivo único.

Antes de começar

- Verifique se os dispositivos de controle de acesso que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos a serem adicionados devem ser ativados. Consulte ***Criação de senha para dispositivos inativos*** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar adicionar um único dispositivo detectado on-line.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de Gerenciamento de Dispositivo de Controle de Acessos.
2. Na área Dispositivos On-Line, selecione um tipo de rede.

Rede do servidor

Como seleção padrão os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client atual serão relacionados na área dos Dispositivos On-Line.

Observação

Para a série DS-K5600 de reconhecimento facial, os Dispositivos On-Line exibidos são diferentes de acordo com as configurações de modo de funcionamento. Consulte **Configuração do modo de funcionamento** para obter mais informações.

3. Na área de Dispositivos On-Line, selecione o dispositivo ativo a adicionar.
 4. Clique em **Adicionar à lista de dispositivos** para abrir a janela de Adicionar Dispositivos On-Line.
 5. Digite as informações obrigatórias.
-

Observação

O endereço IP do dispositivo pode ser exibido automaticamente no campo **Endereço do dispositivo**.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

6. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os pontos de acesso do dispositivo adicionado a uma área.
-

Observação

- Importe todos os pontos de acesso ou pontos de acesso especificados do dispositivo para a área correspondente.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os pontos de acesso para a área não será possível realizar as configurações adicionais para os pontos de acesso.
-

7. Clique em **Adicionar**.

8. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo On-Line.

Configurações remotas

Clique em  para editar os parâmetros de tempo, reinicializar o dispositivo, restaurar o dispositivo ou definir outras configurações dos dispositivos correspondentes.

 **Observação**

- Para alguns Dispositivo de Controle de Acessos se pode personalizar regras de comunicação Wiegand para conectar o leitor de cartões Wiegand personalizado.
 - Depois de restaurar o dispositivo é necessário aplicar os parâmetros no sistema para o dispositivo (clique em **Aplicar as configurações de aplicativo** na página de Gerenciamento do Dispositivo de Controle de Acessos).
 - Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.
-

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Aplicar as configurações de aplicativo

Após restaurar o banco de dados ou as configurações padrão do dispositivo, se os parâmetros (tais como antirretorno abertura de entrada com primeiro cartão) no sistema forem incoerentes com os parâmetros no Dispositivo de Controle de Acessos, um ícone vermelho  será exibido na lateral direita de **Aplicar as configurações de aplicativo**. Clique em **Aplicar as configurações de aplicativo** para apagar os dados originais no dispositivo e aplicar as configurações atuais no sistema para o dispositivo.

Adicionar Dispositivos On-Line em lote

Para os Dispositivo de Controle de Acessos on-line detectados, se tiverem a mesma senha para o mesmo nome de usuário, se pode adicionar vários dispositivos ao mesmo tempo.

Antes de começar

- Verifique se os dispositivos de controle de acesso que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos a serem adicionados devem ser ativados. Consulte ***Criação de senha para dispositivos inativos*** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar adicionar os Dispositivos On-Line detectados em lote.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de Gerenciamento de Dispositivo de Controle de Acessos.
2. Na área Dispositivos On-Line, selecione um tipo de rede.

Rede do servidor

Os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client serão relacionados na área dos Dispositivos On-Line.

Observação

Para a série DS-K5600 de reconhecimento facial, os Dispositivos On-Line exibidos são diferentes de acordo com as configurações de modo de funcionamento. Consulte ***Configuração do modo de funcionamento*** para obter mais informações.

3. Na área de Dispositivos On-Line, selecione os dispositivos ativo a adicionar.
 4. Clique em **Adicionar à lista de dispositivos** para abrir a janela de Adicionar Dispositivos On-Line.
 5. Digite as informações obrigatórias.
-

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

6. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os pontos de acesso dos dispositivos adicionados a uma área.

Observação

- Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os pontos de acesso para a área não será possível realizar as operações adicionais para os pontos de acesso.
-

7. Clique em **Adicionar**.

8. Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para editar os parâmetros de tempo, reinicializar o dispositivo, restaurar o dispositivo ou definir outras configurações dos dispositivos correspondentes.

Observação

- Para alguns Dispositivo de Controle de Acessos se pode personalizar regras de comunicação Wiegand para conectar o leitor de cartões Wiegand personalizado.
 - Depois de restaurar o dispositivo é necessário aplicar os parâmetros no sistema para o dispositivo (clique em **Aplicar as configurações de aplicativo** na página de Gerenciamento do Dispositivo de Controle de Acessos).
 - Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.
-

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Aplicar as configurações de aplicativo

Após restaurar o banco de dados ou as configurações padrão do dispositivo, se os parâmetros (tais como antirretorno abertura de entrada com primeiro cartão) no sistema forem incoerentes com os parâmetros no Dispositivo de Controle de Acessos, um ícone vermelho  será exibido na lateral direita de **Aplicar as configurações de aplicativo**. Clique em **Aplicar as configurações de**

aplicativo para apagar os dados originais no dispositivo e aplicar as configurações atuais no sistema para o dispositivo.

10.4.2 Adicionar dispositivo por endereço IP

Quando se conhece endereço IP ou o Dispositivo de Controle de Acessos a adicionar se pode adicionar os dispositivos ao sistema especificando-se o endereço IP, nome de usuário, senha e outros parâmetros relacionados.

Antes de começar

Verifique se os dispositivos de controle de acesso que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por endereço IP.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de Gerenciamento de Dispositivo de Controle de Acessos.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Acessos.
3. Selecione **Endereço IP** como modo de adicionar.
4. Digite as informações obrigatórias.

Observação

Por padrão o número da entrada do dispositivo é 8000.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os pontos de acesso dos dispositivos adicionados a uma área.

Observação

- Importe todos os pontos de acesso ou pontos de acesso especificados do dispositivo para a área correspondente.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os pontos de acesso para a área não será possível realizar as operações adicionais para os pontos de acesso.
-

6. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar os Dispositivo de Controle de Acessos e volte à página com a lista de Dispositivos de Controle de Acessos.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar o próximo Dispositivo de Controle de Acessos.

7. Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para editar os parâmetros de tempo, reinicializar o dispositivo, restaurar o dispositivo ou definir outras configurações dos dispositivos correspondentes.

Observação

- Para alguns Dispositivo de Controle de Acessos se pode personalizar regras de comunicação Wiegand para conectar o leitor de cartões Wiegand personalizado.
 - Depois de restaurar o dispositivo é necessário aplicar os parâmetros no sistema para o dispositivo (clique em **Aplicar as configurações de aplicativo** na página de Gerenciamento do Dispositivo de Controle de Acessos).
 - Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.
-

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Aplicar as configurações de aplicativo

Após restaurar o banco de dados ou as configurações padrão do dispositivo, se os parâmetros (tais como antirretorno abertura de entrada com primeiro cartão) no sistema forem incoerentes com os

parâmetros no Dispositivo de Controle de Acessos, um ícone vermelho  será exibido na lateral direita de **Aplicar as configurações de aplicativo**. Clique em **Aplicar as configurações de aplicativo** para apagar os dados originais no dispositivo e aplicar as configurações atuais no sistema para o dispositivo.

10.4.3 Adicionar dispositivos por Segmento IP

Se o Dispositivo de Controle de Acessos tiver os mesmos nome de usuário e senha e seus endereços IP estiverem entre o segmento IP se pode especificar os endereços IP inicial e final, nome de usuário, senha e outros parâmetros relacionados para adicioná-los.

Antes de começar

Verifique se os dispositivos de controle de acesso que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por segmento IP.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de Gerenciamento de Dispositivo de Controle de Acessos.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Acessos.
3. Selecione **Segmento IP** como modo de adicionar.
4. Digite as informações obrigatórias.

Observação

Por padrão o número da entrada do dispositivo é 8000.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os pontos de acesso dos dispositivos adicionados a uma área.

Observação

- Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os pontos de acesso para a área não será possível realizar as operações adicionais para os pontos de acesso.
-

6. Termine de adicionar o dispositivo.
- Clique em **Adicionar** para adicionar os Dispositivo de Controle de Acessos e volte à página com a lista de Dispositivos de Controle de Acessos.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar o próximo Dispositivo de Controle de Acessos.
7. Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para editar os parâmetros de tempo, reinicializar o dispositivo, restaurar o dispositivo ou definir outras configurações dos dispositivos correspondentes.

Observação

- Para alguns Dispositivo de Controle de Acessos se pode personalizar regras de comunicação Wiegand para conectar o leitor de cartões Wiegand personalizado.
 - Depois de restaurar o dispositivo é necessário aplicar os parâmetros no sistema para o dispositivo (clique em **Aplicar as configurações de aplicativo** na página de Gerenciamento do Dispositivo de Controle de Acessos).
 - Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.
-

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Aplicar as configurações de

Após restaurar o banco de dados ou as configurações padrão do dispositivo, se os parâmetros (tais como antirretorno abertura de

aplicativo

entrada com primeiro cartão) no sistema forem incoerentes com os parâmetros no Dispositivo de Controle de Acessos, um ícone vermelho  será exibido na lateral direita de **Aplicar as configurações de aplicativo**. Clique em **Aplicar as configurações de aplicativo** para apagar os dados originais no dispositivo e aplicar as configurações atuais no sistema para o dispositivo.

10.4.4 Adicionar dispositivos por segmento de entrada

Se o Dispositivo de Controle de Acessos tiver os mesmos endereço IP, nome de usuário e senha e seu número de entrada estiver entre o segmento de entrada se pode especificar os números de entrada inicial e final, endereço IP, nome de usuário, senha e outros parâmetros relacionados para adicioná-los.

Antes de começar

Verifique se os dispositivos de controle de acesso que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por segmento de entrada.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de Gerenciamento de Dispositivo de Controle de Acessos.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Acessos.
3. Selecione **Segmento de entrada** como modo de adicionar.
4. Digite as informações obrigatórias.



Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

-
5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os pontos de acesso dos dispositivos adicionados a uma área.



Observação

- Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.

- Se não forem importados os pontos de acesso para a área não será possível realizar as operações adicionais para os pontos de acesso.
-

6. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar os Dispositivo de Controle de Acessos e volte à página com a lista de Dispositivos de Controle de Acessos.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar o próximo Dispositivo de Controle de Acessos.

7. Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para editar os parâmetros de tempo, reinicializar o dispositivo, restaurar o dispositivo ou definir outras configurações dos dispositivos correspondentes.

Observação

- Para alguns Dispositivo de Controle de Acessos se pode personalizar regras de comunicação Wiegand para conectar o leitor de cartões Wiegand personalizado.
 - Depois de restaurar o dispositivo é necessário aplicar os parâmetros no sistema para o dispositivo (clique em **Aplicar as configurações de aplicativo** na página de Gerenciamento do Dispositivo de Controle de Acessos).
 - Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.
-

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Aplicar as configurações de aplicativo

Após restaurar o banco de dados ou as configurações padrão do dispositivo, se os parâmetros (tais como antirretorno abertura de entrada com primeiro cartão) no sistema forem incoerentes com os parâmetros no Dispositivo de Controle de Acessos, um ícone vermelho  será exibido na lateral direita de **Aplicar as configurações de aplicativo**. Clique em **Aplicar as configurações de aplicativo** para apagar os dados originais no dispositivo e aplicar as

configurações atuais no sistema para o dispositivo.

10.4.5 Adicionar dispositivos em lote

Digite as informações do Dispositivo de Controle de Acessos no modelo predefinido para adicionar diversos dispositivos ao mesmo tempo.

Antes de começar

Verifique se os dispositivos de controle de acesso que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos em lote.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de Gerenciamento de Dispositivo de Controle de Acessos.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Acessos.
3. Selecione **Importação em lote** como modo de adicionar.
4. Clique em **Baixar modelo** e salve o modelo predefinido (arquivo CSV) em seu PC.
5. Abra o arquivo de modelo exportado e insira as informações obrigatórias dos dispositivos a serem adicionados na coluna correspondente.
6. Clique em **...** e selecione o arquivo de modelo.
7. Termine de adicionar os dispositivos.
 - Clique em **Adicionar** para adicionar os dispositivos e volte à página com a lista de dispositivos.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros dispositivos.
8. Execute as operações a seguir depois de adicionar os dispositivos em lote.

Configurações remotas

Clique em  para editar os parâmetros de tempo, reinicializar o dispositivo, restaurar o dispositivo ou definir outras configurações dos dispositivos correspondentes.

Observação

- Para alguns Dispositivo de Controle de Acessos se pode personalizar regras de comunicação Wiegand para conectar o leitor de cartões Wiegand personalizado.
 - Depois de restaurar o dispositivo é necessário aplicar os parâmetros no sistema para o dispositivo (clique em **Aplicar as configurações de aplicativo** na página de Gerenciamento do Dispositivo de Controle de Acessos).
 - Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.
-

Alteração da senha Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Aplicar as configurações de aplicativo

Após restaurar o banco de dados ou as configurações padrão do dispositivo, se os parâmetros (tais como antirretorno abertura de entrada com primeiro cartão) no sistema forem incoerentes com os parâmetros no Dispositivo de Controle de Acessos, um ícone vermelho  será exibido na lateral direita de **Aplicar as configurações de aplicativo**. Clique em **Aplicar as configurações de aplicativo** para apagar os dados originais no dispositivo e aplicar as configurações atuais no sistema para o dispositivo.

10.5 Gerenciamento do Dispositivo de Controle de Segurança

Adicione os Dispositivos de Controle de Segurança ao sistema para gerenciar partição, zona, armar/desarmar, manuseio de alarmes etc.

O Dispositivo de Controle de Segurança inclui Painel de Controle de Segurança, estação de alarme para pânico etc., que são amplamente utilizados em muitos cenários.

Um Painel de Controle de Segurança é utilizado para monitoramento de zonas de armar, manuseando sinais de alarmes provenientes de acionadores e enviando relatórios de alarmes à estação central de monitoramento de alarmes. O Painel de Controle de Segurança é muito importante para impedir roubos, furtos ou outros acidentes.

Uma estação de alarme para pânico é instalada principalmente em áreas com multidões ou alta incidência de casos, como escolas, praças, atrações turísticas, hospitais, portões de supermercados, mercados, estações, estacionamentos etc. Quando ocorre alguma emergência ou alguém pede ajuda, a pessoa pode pressionar o botão de pânico para enviar alarme para a central de monitoramento e o operador na central adotará as medidas apropriadas. A estação de alarme para pânico ajuda a soar alarmes em emergências.

10.5.1 Adicionar Dispositivos On-Line

O Dispositivo de Controle de Segurança on-line na mesma sub-rede local que o Web Client ou servidor VSM atuais será exibido em uma lista. Adicione um Dispositivo On-Line de cada vez ou

vários Dispositivos On-Line em lote.

Observação

Instale o Web Control de acordo com as instruções e, em seguida, a função de detecção on-line de dispositivos estará disponível.

Adicionar Dispositivos On-Line únicos

Adicione os dispositivos de controle de segurança on-line detectados e aqui apresentamos o processo para adicionar dispositivo único.

Antes de começar

- Verifique se os dispositivos de controle de segurança que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos a serem adicionados devem ser ativados. Consulte ***Criação de senha para dispositivos inativos*** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar adicionar um único dispositivo detectado on-line.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de Gerenciamento de Dispositivo de Controle de Segurança.
2. Na área Dispositivos On-Line, selecione um tipo de rede.

Rede do servidor

Como seleção padrão os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client atual serão relacionados na área dos Dispositivos On-Line.

3. Na área de Dispositivos On-Line, selecione o dispositivo ativo a adicionar.
4. Clique em **Adicionar à lista de dispositivos** para abrir a janela de Adicionar Dispositivos On-Line.
5. Digite as informações obrigatórias.

Observação

O endereço IP do dispositivo pode ser exibido automaticamente no campo **Endereço do dispositivo**.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

6. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais (incluindo câmeras e entradas e saídas de alarmes) dos Dispositivos de Controle de Segurança adicionados a uma área.
-

Observação

- Selecione **Entrada de alarme especificado** e selecione entradas de alarme para importar para a área.
 - O sistema irá gerar partições de controle de segurança na área com base nas configurações do dispositivo.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os canais para a área não será possível realizar as configurações adicionais para os canais.
-

7. Clique em **Adicionar**.

8. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo On-Line.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

Adicionar Dispositivos On-Line em lote

Para os Dispositivos de Controle de Segurança on-line detectados, se tiverem a mesma senha para o mesmo nome de usuário, se pode adicionar vários dispositivos ao mesmo tempo.

Antes de começar

- Verifique se os dispositivos de controle de segurança que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos a serem adicionados devem ser ativados. Consulte ***Criação de senha para dispositivos inativos*** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar adicionar os Dispositivos On-Line detectados em lote.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de Gerenciamento de Dispositivo de Controle de Segurança.
2. Na área Dispositivos On-Line, selecione um tipo de rede.

Rede do servidor

Os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client serão relacionados na área dos Dispositivos On-Line.

3. Na área de Dispositivos On-Line, selecione os dispositivos ativo a adicionar.
4. Clique em **Adicionar à lista de dispositivos** para abrir a janela de Adicionar Dispositivos On-Line.
5. Digite as informações obrigatórias.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

6. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais (incluindo câmeras e entradas e saídas de alarmes) dos Dispositivos de Controle de Segurança adicionados a uma área.

 **Observação**

- Selecione **Entrada de alarme especificado** e selecione entradas de alarme para importar para a área.
 - O sistema irá gerar partições de controle de segurança na área com base nas configurações do dispositivo.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os canais para a área não será possível realizar as configurações adicionais para os canais.
-

7. Clique em **Adicionar**.

8. Opcional: Execute as operações a seguir depois de adicionar os Dispositivos On-Line em lote.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

 **Observação**

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.5.2 Adicionar dispositivo por endereço IP

Quando se conhece endereço IP ou o Dispositivo de Controle de Segurança a adicionar se pode adicionar os dispositivos ao sistema especificando-se o endereço IP, nome de usuário, senha e outros parâmetros relacionados.

Antes de começar

Verifique se os dispositivos de controle de segurança que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial

é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por endereço IP.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de Gerenciamento de Dispositivo de Controle de Segurança.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Segurança.
3. Selecione **Endereço IP** como modo de adicionar.
4. Digite as informações obrigatórias.

Observação

Por padrão o número da entrada do dispositivo é 8000.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais (incluindo câmeras e entradas e saídas de alarmes) dos Dispositivos de Controle de Segurança adicionados a uma área.

Observação

- Selecione **Entrada de alarme especificado** e selecione entradas de alarme para importar para a área.
 - O sistema irá gerar partições de controle de segurança na área com base nas configurações do dispositivo.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Até 64 entradas de alarme podem ser importadas em uma área. Se não forem importados os canais para a área não será possível realizar operações adicionais para os canais.
-

6. Termine de adicionar o dispositivo.
 - Clique em **Adicionar** para adicionar os Dispositivo de Controle de Segurança e volte à lista de Dispositivos de Controle de Segurança.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar o

próximo Dispositivo de Controle de Segurança.

7. Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.5.3 Adicionar dispositivo por Hik-Connect

O endereço IP que se pode adicionar aos Dispositivos de Controle de Segurança que foram adicionados à conta de Hik-Connect para o sistema.

Antes de começar

Verifique se os dispositivos de controle de segurança que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por Hik-Connect.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de Gerenciamento de Dispositivo de Controle de Segurança.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Segurança.
3. Selecione **Hik-Connect** como modo de adicionar.
4. Digite as informações obrigatórias.

Endereço do servidor de Hik-Connect

Digite o endereço do serviço Hik-Connect. Por padrão é <https://open.ezvizlife.com>.

appKey

Digite appKey do serviço Hik-Connect.

appSecret

Digite o appSecret do serviço Hik-Connect.

Lista de dispositivos

Clique em **Obter dispositivo** para exibir os dispositivos adicionados à conta, selecione o dispositivo e digite nome de usuário e senha do dispositivo.



Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais (incluindo câmeras e entradas e saídas de alarmes) dos Dispositivos de Controle de Segurança adicionados a uma área.
-



Observação

- O sistema irá gerar partições de controle de segurança na área com base nas configurações do dispositivo.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os canais para a área não será possível realizar as configurações adicionais para os canais.
-

6. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar os Dispositivo de Controle de Segurança e volte à página com a lista de Dispositivos de Controle de Segurança.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar o próximo Dispositivo de Controle de Segurança.

7. Opcional: Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.



Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.5.4 Adicionar dispositivo por Segmento IP

Se o Dispositivo de Controle de Segurança tiver os mesmos número de entrada, nome de usuário e senha e seus endereços IP estiverem entre o segmento IP se pode especificar os endereços IP inicial e final, número de entrada, nome de usuário, senha e outros parâmetros relacionados para adicioná-los.

Antes de começar

Verifique se os dispositivos de controle de segurança que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por segmento IP.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de Gerenciamento de Dispositivo de Controle de Segurança.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Segurança.
3. Selecione **Segmento IP** como modo de adicionar.
4. Digite as informações obrigatórias.

 **Observação**

Por padrão o número da entrada do dispositivo é 8000.

 **Cuidado**

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais (incluindo câmeras e entradas e saídas de alarmes) dos Dispositivos de Controle de Segurança adicionados a uma área.
-

 **Observação**

- O sistema irá gerar partições de controle de segurança na área com base nas configurações do dispositivo.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os canais para a área não será possível realizar as configurações adicionais para os canais.
-

6. Termine de adicionar o dispositivo.
- Clique em **Adicionar** para adicionar os Dispositivo de Controle de Segurança e volte à página com a lista de Dispositivos de Controle de Segurança.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar o próximo Dispositivo de Controle de Segurança.
7. Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

 **Observação**

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

 **Observação**

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
-

- Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.5.5 Adicionar dispositivo por segmento de entrada

Se o Dispositivo de Controle de Segurança tiver os mesmos nome de usuário e senha e seu número de entrada estiver entre o segmento de entrada se pode especificar os números de entrada inicial e final, nome de usuário, senha e outros parâmetros relacionados para adicioná-los.

Antes de começar

Verifique se os dispositivos de controle de segurança que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos por segmento de entrada.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de Gerenciamento de Dispositivo de Controle de Segurança.
 2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Segurança.
 3. Selecione **Segmento de entrada** como modo de adicionar.
 4. Digite as informações obrigatórias.
-

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Configure o interruptor **Adicionar canal a área** como ligado para importar os canais (incluindo câmeras e entradas e saídas de alarmes) dos Dispositivos de Controle de Segurança adicionados a uma área.
-

Observação

- O sistema irá gerar partições de controle de segurança na área com base nas configurações do dispositivo.
 - Crie uma nova área pelo nome do dispositivo ou selecione uma área existente.
 - Se não forem importados os canais para a área não será possível realizar as configurações
-

adicionais para os canais.

6. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar os Dispositivo de Controle de Segurança e volte à página com a lista de Dispositivos de Controle de Segurança.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar o próximo Dispositivo de Controle de Segurança.

7. Execute as operações a seguir depois de adicionar os dispositivos.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.5.6 Adicionar dispositivos em lote

Edite o modelo predefinido com as informações do dispositivo de controle de segurança para adicionar vários dispositivos de uma vez.

Antes de começar

Verifique se os dispositivos de controle de segurança que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar dispositivos em lote.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Controle de Segurança** para entrar na página de Gerenciamento de Dispositivo de Controle de Segurança.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Controle de Segurança.
3. Selecione **Importação em lote** como modo de adicionar.

4. Clique em **Baixar modelo** e salve o modelo predefinido (arquivo CSV) em seu PC.
5. Abra o arquivo de modelo exportado e edite as informações obrigatórias dos dispositivos a serem adicionados na coluna correspondente.
6. Clique em **...** e selecione o arquivo de modelo.
7. Termine de adicionar os dispositivos.
 - Clique em **Adicionar** para adicionar os dispositivos e volte à página com a lista de dispositivos.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros dispositivos.
8. Execute as operações a seguir depois de adicionar os dispositivos em lote.

Configurações remotas

Clique em  para definir as configurações remotas dos dispositivos correspondentes.

Observação

Para obter mais informações acerca das configurações remotas, consulte o Manual do Usuário do dispositivo.

Alteração da senha

Selecione os dispositivos adicionados e clique em  para alterar a senha do dispositivo.

Observação

- Atualmente só se pode alterar a senha on-line para dispositivos HIKVISION.
 - Se os dispositivos tiverem a mesma senha, selecione vários dispositivos para alterar a senha ao mesmo tempo.
-

10.6 Restaurar/redefinir a senha do dispositivo

Se você esqueceu a senha dos dispositivos on-line detectados, poderá restaurar a senha padrão do dispositivo ou redefinir a senha do dispositivo pelo sistema. Então será possível acessar o dispositivo ou adicioná-lo ao sistema utilizando a senha.

Quanto a operações detalhadas para restaurar a senha padrão do dispositivo, consulte **Restauração da senha padrão do dispositivo**.

Quanto a operações detalhadas para redefinição da senha do dispositivo, consulte **Redefinição da senha do dispositivo**.

10.6.1 Redefinir a senha do dispositivo

Se você esqueceu a senha que utiliza para acessar o Dispositivo On-Line, poderá solicitar um arquivo de chave junto à assistência técnica e redefinir a senha do dispositivo pelo sistema.

Antes de começar

- Verifique se os dispositivos (câmeras, DVR, dispositivo de controle de acesso etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos devem ser ativados. Consulte **Criação de senha para dispositivos inativos** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar redefinir a senha do dispositivo. Aqui tomamos como exemplo o Dispositivo de Codificação.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.

Observação

- Para os dispositivos de controle de acesso, clique em **Exibição física** → **Dispositivo de Controle de Acessos** para entrar na página de gerenciamento do Dispositivo de Controle de Acessos.
- Para Dispositivos de Decodificação, clique em **Exibição física** → **Smart Wall**. Na área do Dispositivo de Decodificação, clique em **Adicionar** e marque **Dispositivos on-line** como Modo de Adição.

A lista de Dispositivos On-Line detectados está na área de Dispositivos On-Line.

2. Na área de Dispositivos On-Line, veja o status do dispositivo (exibido na coluna Segurança) e clique em ícone  na coluna Operação de um dispositivo ativo. Uma caixa de diálogo com o arquivo de importação e o arquivo de exportação, senha e confirmação dos campos de senha é aberta.
3. Clique em **Exportar** para salvar o arquivo do dispositivo em seu PC.
4. Envie o arquivo para nossos engenheiros técnicos.

Observação

Para as operações a seguir sobre como redefinir a senha, entre em contato com o engenheiro da assistência técnica.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

10.6.2 Restaurar a senha padrão do dispositivo

Para alguns Dispositivos de Codificação com versão de firmware antiga, se você esqueceu a senha utilizada para acessar o Dispositivo On-Line, poderá restaurar a senha padrão do dispositivo pelo sistema e alterar a senha padrão para uma mais forte para melhor segurança.

Antes de começar

- Verifique se os dispositivos (câmeras, DVR etc.) que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Os dispositivos devem ser ativados. Consulte **Criação de senha para dispositivos inativos** para obter mais informações sobre a ativação de dispositivos.

Execute esta tarefa quando precisar restaurar a senha padrão do dispositivo.

Etapas

1. Clique em **Exibição física** → **Dispositivo de Codificação** para entrar na página de Gerenciamento do Dispositivo de Codificação.
A lista de Dispositivos On-Line detectados está na área de Dispositivos On-Line.
2. Na área de Dispositivos On-Line, veja o status do dispositivo (exibido na coluna Segurança) e clique em ícone  na coluna Operação de um dispositivo ativo.
Uma caixa de diálogo com código de segurança é exibida.
3. Digite o código de segurança e restaure a senha padrão do dispositivo selecionado.

Observação

Entre em contato com nossa assistência técnica para obter um código de segurança.

O que fazer em seguida

Altere essa senha padrão para proteger melhor contra riscos de segurança como acesso não autorizado de outras pessoas ao produto, que pode impedir o funcionamento correto do produto e/ou levar a outras consequências indesejáveis.



Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

10.7 Gerenciamento de local remoto

Adicione outra HikCentral sem módulo de RSM (Gerenciamento de Local Remoto) para a HikCentral com o módulo de RSM como Local Remoto para gerenciamento central.

Depois de adicionar o Local Remoto ao Sistema Central será possível gerenciar as câmeras do Local Remoto (como visualização em tempo real e reprodução), adicionar os alarmes configurados do Local Remoto para poder gerenciar os alarmes via Sistema Central e definir o agendamento de gravação para as câmeras do Local Remoto e armazenar os arquivos de vídeo gravados no Servidor de Gravações adicionado ao Sistema Central. Também se pode visualizar o local GIS do Local Remoto, pontos de acesso e configurações de região de destaque no módulo Mapa.

Local remoto

Se a HikCentral não tiver o módulo de RSM (com base na Licença adquirida), é possível adicioná-la ao Sistema Central como Local Remoto.

Sistema Central

Se a HikCentral tiver o módulo de RSM (com base na Licença adquirida), é possível adicionar outros Locais Remotos a este sistema. Este sistema e os Locais Remotos adicionados são chamados de Sistema Central.



Observação

- O sistema com o módulo de RSM não pode ser adicionado ao outro Sistema Central como Local Remoto.
 - Se um Local Remoto tiver sido adicionado a um Sistema Central, não poderá ser adicionado ao outro Sistema Central.
-

10.7.1 Adicionar Local Remoto por endereço IP ou nome de domínio

Quando se conhece endereço IP ou nome de domínio do Local Remoto a adicionar se pode adicionar o local ao Sistema Central especificando-se o endereço IP (ou nome de domínio), nome de usuário, senha e outros parâmetros relacionados.

Execute esta tarefa quando precisar adicionar Local Remoto por endereço IP ou nome de domínio.

Etapas

Observação

Ao adicionar o Local Remoto, câmeras e informações de área lógica do local são importadas para a Sistema Central como padrão.

1. Clique em **Gerenciamento do Local Remoto** na página inicial para abrir a página do Gerenciamento do Local Remoto.
2. Entre na página de Adicionar Local Remoto.
 - Se nenhum Local Remoto tiver sido adicionado, clique em **Adicionar Site** para entrar na página de Adicionar Local Remoto.
 - Se já tiver adicionado o Local Remoto, clique em **+** à esquerda para entrar na página de Adicionar Local Remoto.

← Add Remote Site

Adding Mode

IP/Domain
 Site Registered to Central System
 Batch Import

Basic Information

*Site Address

*Site Port

Alias Synchronize Name

*User Name

*Password

Description

Channel Information

Add Add and Continue Cancel

Figura 10-9 Página de Adicionar Local Remoto

3. Selecione **IP/Domínio** como modo de adicionar.
4. Digite as informações obrigatórias.

Endereço do local

O endereço IP ou nome de domínio do Local Remoto.

Entrada do local

Insira o número de entrada do Local Remoto. Por padrão é 80.

Pseudônimo

Edite um nome para o Local Remoto conforme desejar. Marque **Sincronizar nome** para sincronizar automaticamente o nome do Local Remoto.

Nome de usuário

O nome de usuário para o Local Remoto, como usuário admin e usuário normal.

Senha

A senha necessária para acessar o Local Remoto.

Descrição

Opcionalmente se pode digitar as informações descritivas para o Local Remoto, como local e implementação.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Opcional: Habilite o recebimento dos alarmes configurados no Local Remoto.

1) Configure o interruptor **Selecionar alarme** como **ligado** para exibir todos os alarmes configurados em um Local Remoto.

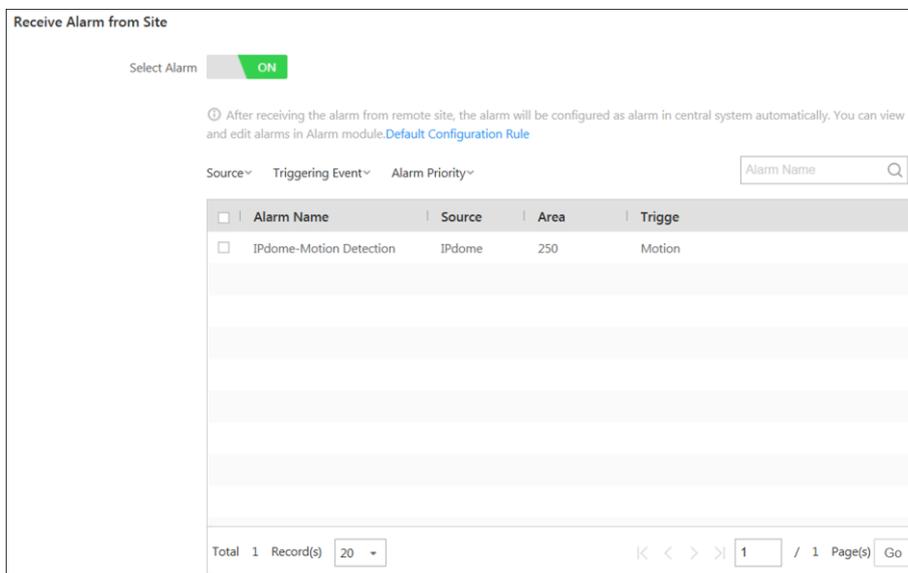


Figura 10-10 Recebimento de alarme proveniente da página do local

2) Opcional: Filtre os alarmes configurados pela origem do alarme, evento que acionou e prioridade do alarme.

3) Selecione os alarmes configurados.

Observação

- Após receber o alarme do Local Remoto, o alarme será automaticamente configurado como alarme no Sistema Central. Clique em **Regra padrão de configuração** para ver as configurações padrão dos alarmes importados, incluindo nome do alarme, prioridade do alarme, ações etc.
- É possível visualizar e editar alarmes no módulo Alarmes. Para obter mais informações acerca da configuração de alarmes, consulte **Configuração de alarmes**.

6. Faça cópia de segurança do banco de dados dos Locais Remotos no Sistema Central e será possível definir o número máximo de cópias de seguranças e visualizar o caminho de salvamento do banco de dados no Sistema Central.

Número máximo de cópias de segurança

Defina o número máximo de arquivos de cópia de segurança disponíveis no sistema.

7. Opcional: Habilite a cópia de segurança do banco de dados do Local Remoto no agendamento.
 - 1) Configure o interruptor **Cópia de segurança agendada para o banco de dados** como **ligado**.
 - 2) Selecione com que frequência será feita cópia de segurança do banco de dados.

Observação

Se selecionar **Semanalmente** ou **Mensalmente** para realizar a tarefa de cópia de segurança, selecione em qual dia executar.

- 3) Selecione uma hora do dia para iniciar o cópia de segurança.
8. Termine de adicionar o Local Remoto.
 - Clique em **Adicionar** para adicionar o Local Remoto e retorne à página com a lista de Locais Remotos.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Locais Remotos.

10.7.2 Adicionar Local Remoto registrado no Sistema Central

Se os Locais Remotos tiverem sido registrados no Sistema Central e o Sistema Central também habilitou o recebimento da função de registro de local, os Locais Remotos registrados serão exibidos na lista de locais. Adicione-os ao Sistema Central digitando nomes de usuários e senhas.

Antes de começar

- O Local Remoto deve ser registrado no Sistema Central informando-se os parâmetros de rede do Sistema Central (consulte **Registro no Sistema Central** para obter mais informações).
- O Sistema Central irá habilitar o recebimento da função de registro do local (consulte **Permitir registro do Local Remoto** para obter mais informações).

Execute esta tarefa quando precisar adicionar o local que foi registrado no Sistema Central.

Etapas

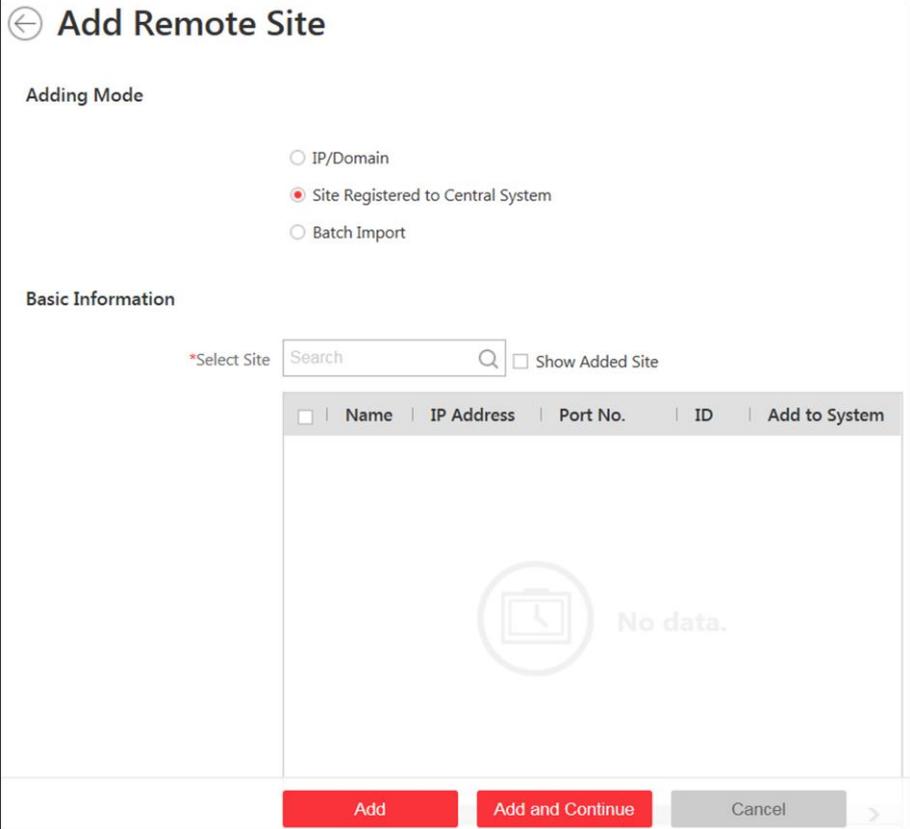
Observação

Ao adicionar o Local Remoto, câmeras e informações de área lógica do local são importadas para a Sistema Central como padrão.

1. Clique em **Gerenciamento do Local Remoto** na página inicial para entrar na página do Gerenciamento do Local Remoto.
2. Entre na página de Adicionar Local Remoto.
 - Se nenhum Local Remoto tiver sido adicionado, clique em **Adicionar Site** para entrar na

página de Adicionar Local Remoto.

- Se já tiver adicionado o Local Remoto, clique em + à esquerda para entrar na página de Adicionar Local Remoto.



Add Remote Site

Adding Mode

IP/Domain

Site Registered to Central System

Batch Import

Basic Information

*Select Site Show Added Site

Name	IP Address	Port No.	ID	Add to System
No data.				

Figura 10-11 Página de Adicionar Local Remoto

3. Selecione **Local registrado no Sistema Central** como modo de adicionar.
Os locais que já foram registrados no Sistema Central serão exibidos na lista.
4. Selecione o Local Remoto e digite o nome de usuário e senha do Local Remoto.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

-
5. Faça cópia de segurança do banco de dados dos Locais Remotos no Sistema Central e será possível definir o número máximo de cópias de segurança e visualizar o caminho de salvamento do banco de dados no Sistema Central.

Número máximo de cópias de segurança

Defina o número máximo de arquivos de cópia de segurança disponíveis no sistema.

Observação

O valor do número máximo de cópia de segurança varia de 1 a 5.

6. Opcional: Faça cópia de segurança do banco de dados do Local Remoto no agendamento.

- 1) Configure o interruptor **Cópia de segurança agendada para o banco de dados** como **ligado** para habilitar a cópia de segurança agendada.
- 2) Selecione com que frequência será feita cópia de segurança do banco de dados.

Observação

Se selecionar **Semanalmente** ou **Mensalmente** para realizar a tarefa de cópia de segurança, selecione em qual dia executar.

3) Selecione uma hora do dia para iniciar o cópia de segurança.

7. Termine de adicionar o Local Remoto

- Clique em **Adicionar** para adicionar o Local Remoto e retorne à página com a lista de Locais Remotos.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Locais Remotos.

10.7.3 Adicionar Locais Remotos em lote

Quando desejar adicionar Locais Remotos de uma vez para conveniência, será possível editar o modelo predefinido ao informar os parâmetros dos locais e importar o modelo para o Sistema Central para adicionar.

Execute esta tarefa quando precisar adicionar Locais Remotos em lote.

Etapas

Observação

Ao adicionar o Local Remoto, câmeras e informações de área lógica do local são importadas para a Sistema Central como padrão.

1. Clique em **Gerenciamento do Local Remoto** na página inicial para entrar na página do Gerenciamento do Local Remoto.
2. Entre na página de Adicionar Local Remoto.
 - Se nenhum Local Remoto tiver sido adicionado, clique em **Adicionar Site** para entrar na página de Adicionar Local Remoto.
 - Se já tiver adicionado o Local Remoto, clique em **+** à esquerda para entrar na página de Adicionar Local Remoto.

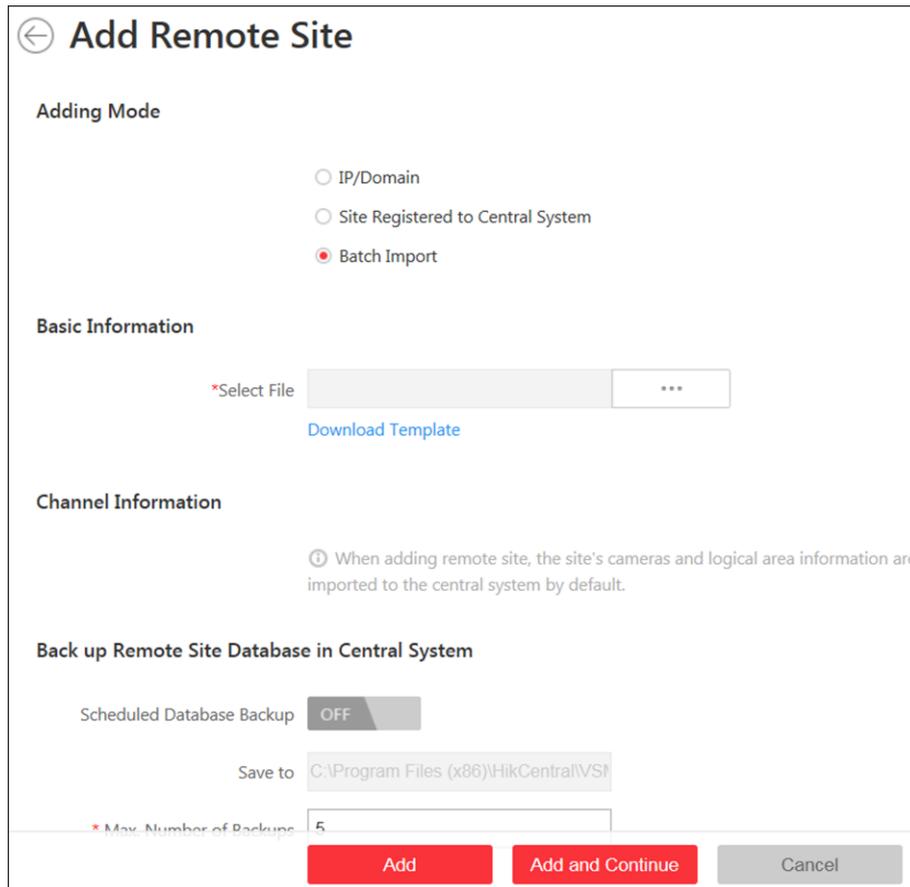


Figura 10-12 Adicionar Local Remoto

3. Selecione **Importação em lote** como modo de adicionar.
4. Clique em **Baixar modelo** e salve o modelo predefinido (arquivo CSV) em seu PC.
5. Abra o arquivo de modelo exportado e insira as informações obrigatórias dos Locais Remotos a serem adicionados na coluna correspondente.
6. Clique em **...** e selecione o arquivo de modelo.
7. Faça cópia de segurança do banco de dados dos Locais Remotos no Sistema Central e será possível definir o número máximo de cópias de segurança e visualizar o caminho de salvamento do banco de dados no Sistema Central.

Número máximo de cópias de segurança

Defina o número máximo de arquivos de cópia de segurança disponíveis no sistema.

8. Opcional: Faça cópia de segurança do banco de dados do Local Remoto no agendamento.
 - 1) Configure o interruptor **Cópia de segurança agendada para o banco de dados** como **ligado** para habilitar a cópia de segurança agendada.
 - 2) Selecione com que frequência será feita cópia de segurança do banco de dados.

Observação

Se selecionar **Semanalmente** ou **Mensalmente** para realizar a tarefa de cópia de segurança, selecione em qual dia executar.

- 3) Selecione uma hora do dia para iniciar o cópia de segurança.
9. Termine de adicionar o Local Remoto
 - Clique em **Adicionar** para adicionar o Local Remoto e retorne à página com a lista de Locais Remotos.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Locais Remotos.

10.7.4 Faça cópia de segurança do banco de dados do Local Remoto no Sistema Central

Depois de adicionar o Local Remoto, faça cópia de segurança do banco de dados do Local Remoto no Sistema Central. A cópia de segurança do banco de dados pode ser executada de acordo com agendamento configurado ou imediatamente. Em caso de exclusão ou corrupção de dados após desastre natural ou induzido por pessoas será possível recuperar os dados para garantir a continuidade dos negócios.

Execute esta tarefa quando precisar fazer cópia de segurança do banco de dados do Local Remoto no Sistema Central.

Etapas

1. Clique em **Gerenciamento do Local Remoto** na página inicial para abrir a página do Gerenciamento do Local Remoto.
2. Na lista de locais à esquerda, clique no nome do Local Remoto para visualizar os detalhes.

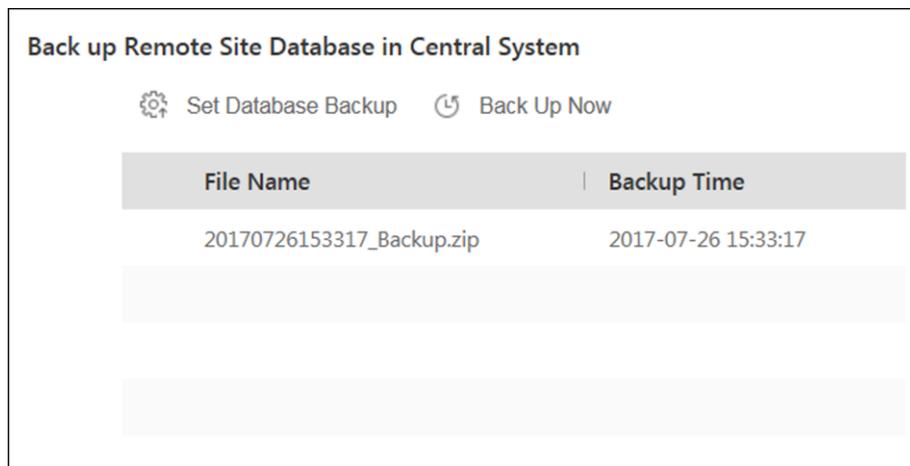


Figura 10-13 Faça cópia de segurança do banco de dados do Local Remoto no Sistema Central

3. Clique em **Fazer cópia de segurança agora** para fazer cópia de segurança manualmente do banco de dados do Local Remoto.
4. Opcional: Defina os parâmetros da cópia de segurança e habilite a cópia de segurança agendada do banco de dados se for necessário fazer cópia de segurança do banco de dados do Local Remoto regularmente.
 - 1) Clique em **Definir cópia de segurança do banco de dados** para abrir a caixa de diálogo Definir cópia de segurança do banco de dados.

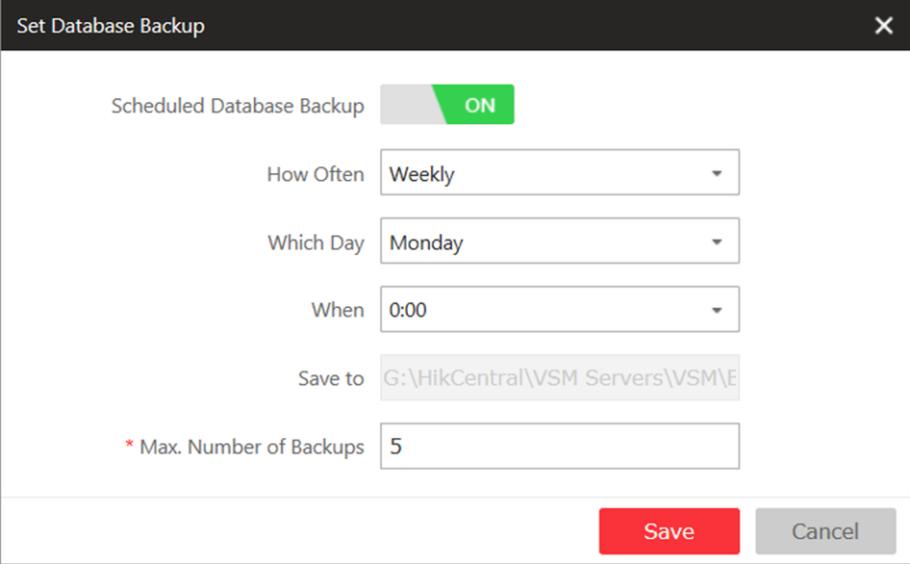


Figura 10-14 Definir cópia de segurança do banco de dados

- 2) Configure o interruptor **Cópia de segurança agendada para o banco de dados** como **ligado** para habilitar a cópia de segurança agendada.
- 3) Selecione com que frequência será feita cópia de segurança do banco de dados.

Observação

Se selecionar **Semanalmente** ou **Mensalmente** para realizar a tarefa de cópia de segurança, selecione em qual dia executar.

- 4) Selecione uma hora do dia para iniciar o cópia de segurança.
- 5) Defina o **Número máximo de cópias de segurança** para definir o número máximo de arquivos de cópias de segurança disponíveis no sistema.

Observação

O número máximo de cópias de segurança deve ficar entre 1 e 5.

- 6) Clique em **Salvar**.

Resultado

O arquivo de cópia de segurança (incluindo cópia de segurança manual e cópia de segurança agendada) será exibido na lista, exibindo o nome do arquivo e o horário da cópia de segurança.

10.7.5 Edição do Local Remoto

Após adicionar o Local Remoto é possível visualizar e editar as informações do Local Remoto adicionado e definir a localização GPS.

Execute esta tarefa quando precisar editar as informações sobre o Local Remoto adicionado.

Etapas

1. Clique em **Gerenciamento do Local Remoto** na página inicial para abrir a página do Gerenciamento do Local Remoto.
2. Na lista de locais à esquerda, clique no nome do Local Remoto para visualizar os detalhes.
3. Visualize e edite as informações básicas do Local Remoto, incluindo endereço IP, entrada, pseudônimo etc.

Observação

Não é possível editar o endereço e a entrada do local registrado no Sistema Central.

4. No campo de informações originais, veja o nome do local, identificação do sistema, versão do sistema e localização GPS do Local Remoto.

Observação

Se localização GPS não estiver configurada, clique em **Configurações** para definir sua localização no módulo Mapa. Consulte **Gerenciar mapas** para obter mais informações.

5. Opcional: Clique em **Configurações no local** para abrir o Web Client do Local Remoto e inicie sessão para configurações adicionais.

Observação

O local deverá estar on-line se precisar inserir seu Web Client.

6. Clique em **Salvar**.

10.7.6 Exibição de alterações do Local Remoto

Quando houver recursos alterados no Local Remoto, como câmeras recém-adicionadas, excluídas e com nomes alterados, será possível exibir os recursos alterados e sincronizá-los no Sistema Central com o Local Remoto.

Execute esta tarefa quando precisar exibir alterações do Local Remoto.

Etapas

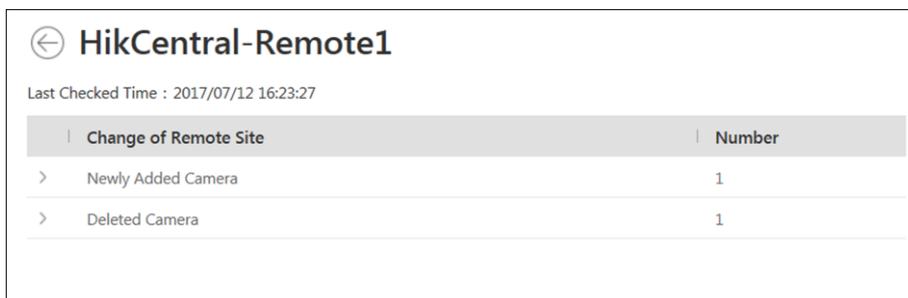
Observação

O local deverá estar on-line se precisar exibir os recursos alterados.

1. Clique em **Gerenciamento do Local Remoto** na página inicial para abrir a página do Gerenciamento do Local Remoto.
2. Clique em  na lista de locais à esquerda para obter o estado mais recente dos Locais Remotos.
Se os recursos no Local Remoto estiverem alterados, um ponto vermelho será exibido no ícone

do Local Remoto como .

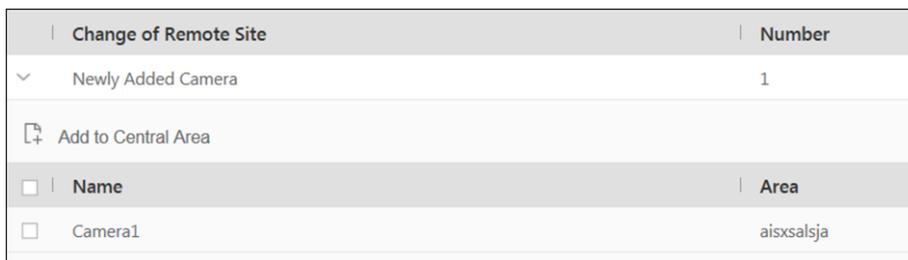
3. Clique no nome do local cujos recursos estiverem alterados para entrar na página dos detalhes.
4. Clique em **Alterações do Local Remoto** para exibir as alterações.



HikCentral-Remote1	
Last Checked Time : 2017/07/12 16:23:27	
Change of Remote Site	Number
> Newly Added Camera	1
> Deleted Camera	1

Figura 10-15 Gerenciamento do Local Remoto

5. Quando houver câmeras recém-adicionadas no local será possível exibir as câmeras adicionadas e adicioná-las à área no Sistema Central.
 - 1) Se houver alguma câmera recém-adicionada no Local Remoto, clique em **Câmera recém-adicionada** para expandir a lista de câmeras recém-adicionadas.

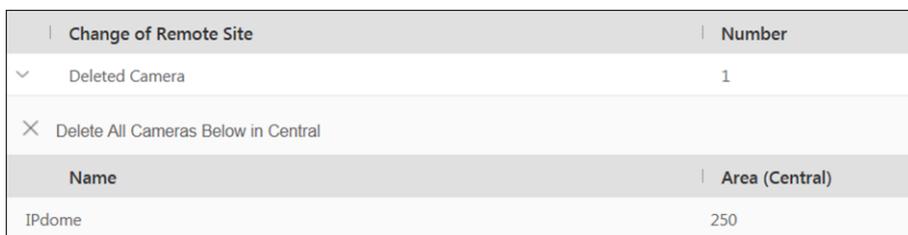


Change of Remote Site	Number
▼ Newly Added Camera	1
 Add to Central Area	
Name	Area
<input type="checkbox"/> Camera1	aisxsalsja

Figura 10-16 Alterações do Local Remoto

É possível exibir o nome da câmera e o nome da área no Local Remoto.

- 2) Selecione a câmera e clique em **Adicionar à Área Central** para sincronizar as câmeras recém-adicionadas ao Sistema Central.
- 3) Selecione a área no Sistema Central.
- 4) Clique em **Salvar**.
6. Quando houver algumas câmeras excluídas do local será possível exibi-las e removê-las do Sistema Central.
 - 1) Se houver alguma câmera excluída do Local Remoto, clique em **Câmera excluída** para expandir a lista de câmeras excluídas.

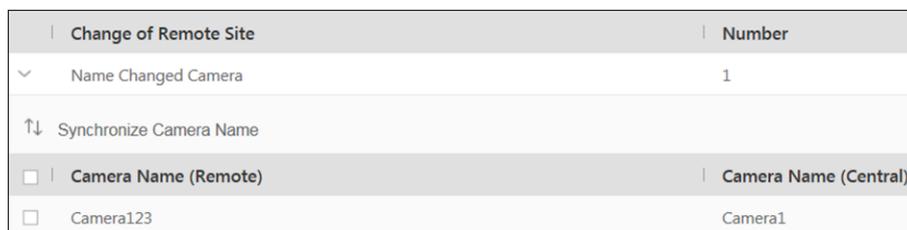


Change of Remote Site	Number
▼ Deleted Camera	1
 Delete All Cameras Below in Central	
Name	Area (Central)
IPdome	250

Figura 10-17 Alteração do Local Remoto

É possível exibir o nome da câmera e sua área no Sistema Central.

- 2) Clique em **Excluir todas as câmeras abaixo na Central** para excluir as câmeras excluídas no Sistema Central.
7. Quando houver algumas câmeras cujos nomes estejam alterados no local será possível exibir as câmeras com nome alterado e sincronizá-las ao Sistema Central.
 - 1) Se o nome da câmera do Local Remoto estiver alterado, clique em **Câmera com nome alterado** para expandir a lista de câmeras com nomes alterados.



Change of Remote Site	Number
▼ Name Changed Camera	1
↕ Synchronize Camera Name	
Camera Name (Remote)	Camera Name (Central)
<input type="checkbox"/> Camera123	Camera1

Figura 10-18 Câmera com nome alterado

É possível exibir os nomes da câmera no Local Remoto e no Sistema Central.

- 2) Selecione as câmeras e clique em **Sincronizar nome da câmera** para sincronizar o nome da câmera no Sistema Central.

10.8 Gerenciamento do Servidor de Gravações

Adicione o Servidor de Gravações ao sistema para armazenamento de arquivos de vídeo. Atualmente, o Servidor de Gravações permite Rede de Área de Armazenamento Híbrido, Servidor de Armazenamento em Nuvem e pStor. Forme também um sistema hot spare N+1 com várias Redes de Área de Armazenamento Híbridos para aumentar a confiabilidade de armazenamento de vídeo do sistema.

10.8.1 Gerenciamento do Servidor de Armazenamento em Nuvem

Adicione um Servidor de Armazenamento em Nuvem como Servidor de Gravações a HikCentral para armazenamento de arquivos de vídeo.

Importação de Certificado de Componentes de Serviços para o Servidor de Armazenamento em Nuvem

Para finalidades de segurança de dados, o certificado do Servidor de Armazenamento em Nuvem deve ser o mesmo que o do servidor do VSM. Antes de adicionar o Servidor de Armazenamento em Nuvem ao sistema, primeiramente importe o certificado armazenado no servidor do VSM para o Servidor de Armazenamento em Nuvem.

Antes de começar

Verifique se o servidor de armazenamento em nuvem que será utilizado está corretamente instalado e conectado à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Etapas

Observação

Se o Certificado de Componentes de Serviços estiver atualizado, exporte o novo certificado e importe novamente para o Servidor de Armazenamento em Nuvem para atualizar.

1. Clique em **Sistema** → **Certificado de Componentes de Serviços**.
2. Clique em **Exportar** para exportar o certificado armazenado no servidor do VSM.
3. Entre na página de configuração do Servidor de Armazenamento em Nuvem via navegador da internet.
4. Clique em **Sistema** → **Configurações** → **Configurações de nuvem**.
5. Insira as chaves root keys salt e componentes de chaves de acordo com os parâmetros no certificado exportados na Etapa 3.



Encryption & Decryption: <input checked="" type="radio"/> Open <input type="radio"/> Close	Digest Algorithm: sha256
Root Keys Salt: F140BA81E408461A	Keys Component: F140BA81E408461A
Keys Security Level: <input type="radio"/> High <input type="radio"/> Medium <input checked="" type="radio"/> Low	

6. Clique em **Definir**.

O que fazer em seguida

Depois de importar o certificado para o Servidor de Armazenamento em Nuvem, adicione o servidor ao sistema para gerenciamento. Consulte **Adicionar Servidor de Armazenamento em Nuvem** para obter mais informações.

Adicionar Servidor de Armazenamento em Nuvem

Adicione o Servidor de Armazenamento em Nuvem como Servidor de Gravações a HikCentral para armazenamento de arquivos de vídeo e imagens.

Antes de começar

- Verifique se os Servidores de Armazenamento em Nuvem que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- Primeiramente, importe o Certificado de Componentes de Serviços para o Servidor de Armazenamento em Nuvem antes de adicioná-lo ao sistema. Consulte **Importação do Certificado de Componentes de Serviços para o Servidor de Armazenamento em Nuvem** para obter mais informações.

Execute esta tarefa quando precisar adicionar o Servidor de Armazenamento em Nuvem ao sistema.

Etapas

1. Clique em **Exibição física** → **Servidor de Gravações** para entrar na página do Servidor de Gravações.
2. Clique em **Adicionar** para entrar na página de adicionar servidor.

Add Recording Server

Server Type

pStor

Hybrid Storage Area Network

Cloud Storage Server

Basic Information

* Address

* Control Port

* Network Port

* Signaling Gateway Port

* Access Key

* Secret Key

Enable Picture Storage

Enable WAN Access

* Alias

* User Name

* Password

Figura 10-19 Adicionar Servidor de Gravações

3. Selecione **Servidor de Armazenamento em Nuvem**.
4. Entre nos parâmetros de rede.

Endereço

O endereço IP do servidor em LAN que pode se comunicar com o VSM.

Entrada de controle

O número da entrada de controle do servidor. Se não tiver sido alterado, utilize o valor padrão.

Entrada de rede

O número da entrada de rede do servidor. Se não tiver sido alterado, utilize o valor padrão.

Entrada de gateway de sinalização

O número da entrada de gateway de sinalização do servidor. Se não tiver sido alterado, utilize o valor padrão.

5. Insira a chave de acesso do usuário e a chave secreta do Servidor de Armazenamento em Nuvem para pesquisa de arquivos de vídeo armazenados neste Servidor de Armazenamento em Nuvem via Mobile Client HikCentral ou baixar imagens via Control Client.

Observação

- Baixe essas duas chaves na página de configuração do Servidor de Armazenamento em Nuvem (clique em **Virtualização** → **Gerenciamento de usuários**).
- Para obter mais informações sobre a pesquisa de arquivos de vídeo armazenados no Servidor de Armazenamento em Nuvem via Mobile Client, consulte *Manual do Usuário do Mobile Client HikCentral*.

-
6. Opcional: Configure o interruptor **Habilitar armazenamento de imagens** como ligado para armazenamento de imagens neste Servidor de Armazenamento em Nuvem.

Observação

Se esta função estiver habilitada, será necessário configurar o número de entrada para baixar imagens, o que se utiliza para baixar imagens via Control Client.

-
7. Opcional: Se precisar acessar o servidor via WAN, configure o interruptor **Ativar acesso WAN** como ligado e configure os parâmetros correspondentes que ficam disponíveis quando se acessa o servidor via WAN.
8. Digite pseudônimo, nome de usuário e senha do servidor.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

-
9. Termine de adicionar o servidor.
- Clique em **Adicionar** para adicionar o servidor e volte à página com a lista de servidores.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros servidores.
10. Opcional: Execute as operações a seguir depois de adicionar o servidor:

Editar o servidor	Clique no campo Pseudônimo do servidor e edite as informações do servidor e veja as informações de armazenamento e da câmera.
Exclusão do servidor	Selecione o servidor na lista e clique em Excluir para remover o servidor selecionado.
Configuração do servidor	Clique em  , e a interface de início de sessão do Servidor de Armazenamento em Nuvem será exibida. Inicie sessão e configure o Servidor de Armazenamento em Nuvem.

10.8.2 Adicionar Rede de Área de Armazenamento Híbrido

Adicione a Rede de Área de Armazenamento Híbrido como Servidor de Gravações a HikCentral para armazenamento de arquivos de vídeo e imagens.

Antes de começar

Verifique se as Redes de Área de Armazenamento Híbrido que serão utilizadas estão corretamente instaladas e conectadas à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar a Rede de Área de Armazenamento Híbrido ao sistema.

Etapas

1. Clique em **Exibição física** → **Servidor de Gravações** para entrar na página do Servidor de Gravações.
2. Clique em **Adicionar** para entrar na página de Adicionar Servidor de Gravações.

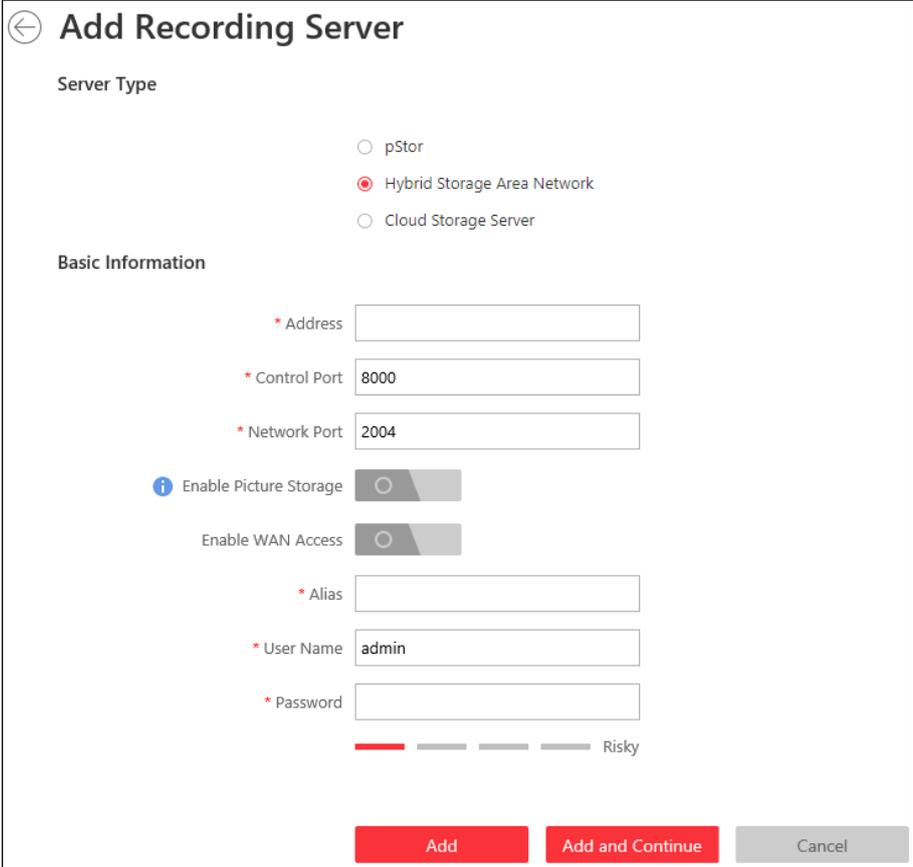


Figura 10-20 Adicionar Servidor de Gravações

3. Selecione **Rede de Área de Armazenamento Híbrido**.
4. Entre nos parâmetros de rede.

Endereço

O endereço IP do servidor em LAN que pode se comunicar com o VSM.

Entrada de controle

O número da entrada de controle do servidor. Se não tiver sido alterado, utilize o valor padrão.

Entrada de rede

O número da entrada de rede do servidor. Se não tiver sido alterado, utilize o valor padrão.

5. Opcional: Habilitar a função de armazenamento de imagens para armazenamento de imagens nesta Rede de Área de Armazenamento Híbrido.
 - 1) Configure o interruptor **Habilitar armazenamento de imagens** como ligado.
 - 2) Configure o número de entrada para baixar imagens para baixar imagens via Control Client. Se o número da entrada para baixar imagens não tiver sido alterado, utilize os padrão.
 - 3) Configure o número de entrada do gateway de sinalização. Se o número da entrada para baixar imagens não tiver sido alterado, utilize os padrão.
 - 4) Insira a chave de acesso e a chave secreta.

Observação

A chave de acesso e a chave secreta são utilizadas para baixar imagens via Control Client. Se necessário, entre em contato com nossa assistência técnica para obtê-las.

6. Opcional: Se precisar acessar o servidor via WAN, configure o interruptor **Ativar acesso WAN** como ligado e configure os parâmetros correspondentes que ficam disponíveis quando se acessa o servidor via WAN.
 7. Digite pseudônimo, nome de usuário e senha do servidor.
-

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

8. Termine de adicionar o servidor.
 - Clique em **Adicionar** para adicionar o servidor e volte à página com a lista de servidores.
 - Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros servidores.
9. Opcional: Execute as operações a seguir depois de adicionar o servidor:

Editar o servidor Clique no campo **Pseudônimo** do servidor e edite as informações do servidor e veja as informações de armazenamento e da câmera.

Exclusão do servidor Selecione o servidor na lista e clique em **Excluir** para remover o servidor selecionado.

Configuração do servidor Clique em , e a interface de início de sessão da Rede de Área de Armazenamento Híbrido será exibida. Inicie sessão e configure SAN Híbrido.

Configuração em um toque Se a Rede de Área de Armazenamento Híbrido não tiver sido configurada com configurações de armazenamento, clique em  para realizar configuração com um toque antes de armazenar os arquivos de vídeo da câmera na Rede de Área de Armazenamento Híbrido.

10.8.3 Adicionar pStor

Adicione pStor como Servidor de Gravações a HikCentral para armazenamento dos arquivos de vídeo e imagens.

Antes de começar

Verifique se os pStors que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar adicionar pStor ao sistema.

Etapas

1. Clique em **Exibição física** → **Servidor de Gravações** para entrar na página do Servidor de Gravações.
2. Clique em **Adicionar** para entrar na página de adicionar servidor.

← Add Recording Server

Server Type

pStor

Hybrid Storage Area Network

Cloud Storage Server

Basic Information

* Address

* Control Port

* Network Port

* Signaling Gateway Port

* Access Key

* Secret Key

Enable Picture Storage

Enable WAN Access

* Alias

* User Name

* Password

Add Add and Continue Cancel

Figura 10-21 Adicionar Servidor de Gravações

3. Selecione **pStor**.
4. Entre nos parâmetros de rede.

Endereço

O endereço IP do servidor em LAN que pode se comunicar com o VSM.

Entrada de controle

O número da entrada de controle do pStor. Se não tiver sido alterado, utilize o valor padrão.

Entrada de rede

O número da entrada de rede do pStor. Se não tiver sido alterado, utilize o valor padrão.

Entrada de gateway de sinalização

O número da entrada de gateway de sinalização do pStor. Se não tiver sido alterado, utilize o valor padrão.

5. Insira a chave de acesso e a chave secreta do usuário de pStor para baixar imagens via Control Client.

Observação

Baixe essas duas chaves na página do Web Client de pStor.

6. Opcional: Configure o interruptor **Habilitar armazenamento de imagens** como ligado for armazenamento imagens em pStor.

Observação

Se esta função estiver habilitada, será necessário configurar o número de entrada para baixar imagens, o que se utiliza para baixar imagens via Control Client.

7. Opcional: Se precisar acessar o servidor via WAN, configure o interruptor **Ativar acesso WAN** como ligado e configure os parâmetros correspondentes que ficam disponíveis quando se acessa o servidor via WAN.
8. Digite pseudônimo, nome de usuário e senha do pStor.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

9. Termine de adicionar o servidor.

- Clique em **Adicionar** para adicionar o servidor e volte à página com a lista de servidores.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros servidores.

10. Opcional: Execute as operações a seguir depois de adicionar o servidor:

Editar o servidor	Clique no campo Pseudônimo do servidor e edite as informações do servidor e veja as informações de armazenamento e da câmera.
Exclusão do servidor	Selecione o servidor na lista e clique em Excluir para remover o servidor selecionado.
Configuração do servidor	Clique em  , e a interface de início de sessão de pStor será exibida. Inicie sessão e configure pStor.

10.8.4 Defina Hot Spare N+1

Forme um sistema hot spare N+1 com vários Servidores de Gravações. O sistema consiste em vários servidores host e um servidor de reserva. Quando o servidor host falha, o servidor de reserva entra em operação, aumentando assim a confiabilidade do armazenamento de vídeo de HikCentral.

Antes de começar

- Pelo menos duas Redes de Área de Armazenamento Híbridos on-line devem ser adicionadas para formar um sistema hot spare N+1.
- Verifique se as Redes de Área de Armazenamento Híbrido que serão utilizadas estão corretamente instaladas e conectadas à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Execute esta tarefa quando precisar configurar hot spare N+1 para os Servidores de Gravações adicionados.

Etapas

Observação

- A função hot spare N+1 é possível somente nas Redes de Área de Armazenamento Híbridos.
 - O servidor de reserva não pode ser selecionado para armazenamento de vídeos enquanto não alternar para servidor host.
 - O servidor host não pode ser configurado como servidor de reserva e o servidor de reserva não pode ser configurado como servidor host.
-

1. Clique em **Exibição física** → **Servidor de Gravações** → **hot spare N+1** para entrar na página de configurações de N+1.



Figura 10-22 N+1 Página de configurações

2. Clique em **Adicionar** para configurar hot spare N+1.
3. Selecione a Rede de Área de Armazenamento Híbrido na lista suspensa de servidores de reserva para configurar o servidor de reserva.
4. Selecione a Rede de Área de Armazenamento Híbrido no campo de servidores host como servidor host.
5. Clique em **Adicionar**.

 **Observação**

Os agendamentos de gravações configurados na Rede de Área de Armazenamento Híbrido serão excluídos após configuração como Servidor de Gravações de reserva.

6. Opcional: Após configurar o hot spare, faça um ou mais do seguinte:

Editar

Clique em  na coluna Operações para editar as configurações dos servidores de reserva e host.

Excluir

Clique em  na coluna Operações para cancelar as configurações de hot spare N+1.

 **Observação**

O cancelamento de hot spare N+1 cancelará todas as associações de host spare e apagará o agendamento de gravações no servidor de reserva.

7. Opcional: Se o servidor host falhou ao enviar o agendamento de gravações para o servidor de reserva, clique em  na coluna Operações para enviar novamente o agendamento de gravações no servidor host para o servidor de reserva.

10.9 Gerenciamento do Servidor de Transmissões

Adicione o Servidor de Transmissões a HikCentral para obter a transmissão de dados de vídeo data do Servidor de Transmissões e com isso reduzir a carga do dispositivo.

Observação

Para sistema que admita Gerenciamento do Local Remoto, câmeras importadas do Local Remoto adotam o Servidor de Transmissões configurado no Local Remoto por padrão. Não é necessário adicionar o Servidor de Transmissões ao Sistema Central e configurar novamente.

10.9.1 Importação do Certificado de Componentes de Serviços para o Servidor de Transmissões

Para finalidades de segurança de dados, o certificado do Servidor de Transmissões deve ser o mesmo que o do servidor do VSM. Antes de adicionar o Servidor de Transmissões ao sistema, primeiramente importe o certificado armazenado no servidor do VSM para o Servidor de Transmissões.

Execute esta tarefa quando precisar importar o Certificado de Componentes de Serviços para o Servidor de Transmissões.

Etapas

Observação

Se o Certificado de Componentes de Serviços estiver atualizado, importe novamente o novo certificado para o Servidor de Transmissões para atualizar.

1. Inicie sessão no Web Client no servidor do VSM localmente.
Você entrará na página inicial do Web Client.
2. Entre em **Sistema** → **Certificado de Componentes de Serviços**.
3. Clique em **Exportar** para exportar o certificado armazenado no servidor do VSM.
4. Copie o certificado para computador que tiver o Serviço de Transmissões instalado.
5. Abra o Gerenciador de Serviços, selecione o Serviço de Transmissões e clique em  para importar o certificado que foi exportado na Etapa 3.

10.9.2 Adicionar Servidor de Transmissões

Adicione a Servidor de Transmissões ao sistema para encaminhar a transmissão de vídeo.

Execute as Etapas a seguir quando precisar adicionar o Servidor de Transmissões ao sistema.

Etapas

1. Clique em **Exibição física** → **Servidor de Transmissões** para entrar na página de gerenciamento do Servidor de Transmissões.
-

2. Clique em **Adicionar** para entrar na página de Adicionar Servidor de Transmissões.

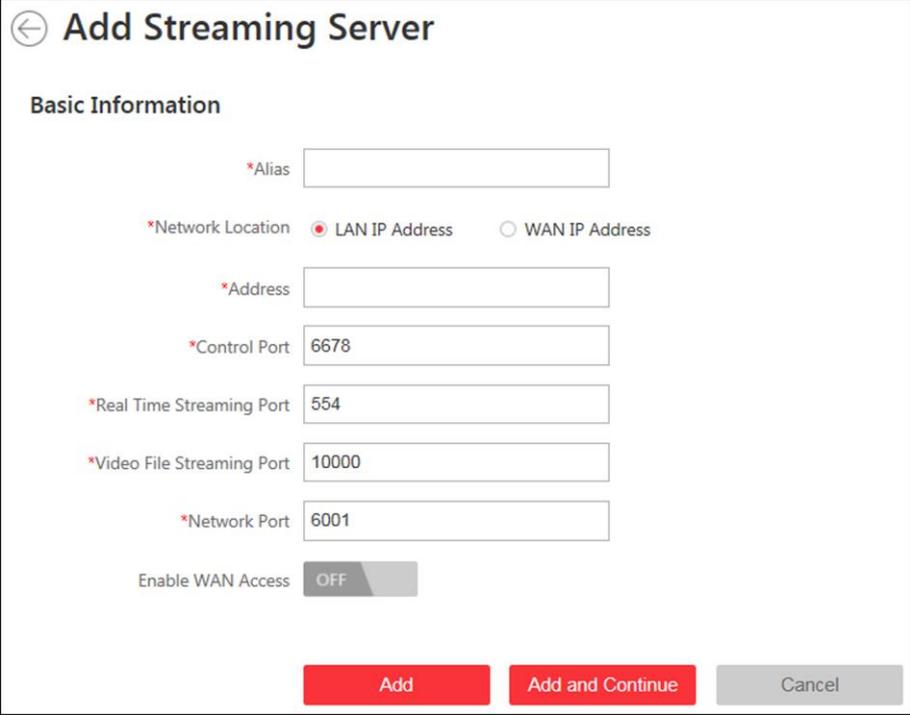


Figura 10-23 Página de Adicionar Servidor de Transmissões

3. Digite as informações obrigatórias.

Local da rede

Selecione **Endereço IP de LAN** se o Servidor de Transmissões e o VSM estiverem na mesma LAN. Caso contrário, selecione **Endereço IP de WAN**.

4. Opcional: Se precisar acessar o servidor via WAN, configure o interruptor **Ativar acesso WAN** como **ligado** como ligado e configure os parâmetros correspondentes que ficam disponíveis quando se acessa o servidor via WAN.

Observação

O interruptor de **Ativar acesso WAN** fica disponível quando se configura Local de Rede como **Endereço IP de LAN**.

5. Termine de adicionar o servidor de transmissões.
 - Clique em **Adicionar** para adicionar o servidor e volte à página com a lista de servidores.
 - Clique em **Adicionar e continuar** para salvar o servidor e continuar a adicionar outros servidores.

Os servidores serão exibidos na lista de servidores para gerenciamento depois que foram adicionados com êxito. Marque as informações relacionadas dos servidores adicionados na lista.

10.10 Gerenciamento do Smart Wall

O Smart Wall pode proporcionar ao pessoal da segurança uma visualização geral abrangente das áreas que se deseja observar. Antes de exibir vídeos no Smart Wall primeiramente é necessário configurar o Smart Wall e também editar, excluir o Smart Wall ou gerenciar os Dispositivos de Decodificação aqui.

Isto inclui principalmente o seguinte:

- Dispositivos de Decodificação que podem ser adicionados ao sistema e utilizados para decodificação de transmissões de vídeo provenientes de Dispositivos de Codificação.
- O Smart Wall Virtual que define o layout e o nome do Smart Wall.
- Vinculação entre as saídas de decodificação do Dispositivo de Decodificação e as janelas do Smart Wall.

10.10.1 Adicionar Dispositivo de Decodificação

Dispositivos de Decodificação podem ser adicionados ao sistema para vinculação com o Smart Wall. Adicione Dispositivos de Decodificação on-line com os endereços IP dentro do servidor do VSM ou sub-rede do Web Client e também se pode adicionar Dispositivos de Decodificação por endereço IP, segmento IP ou por segmento de entrada.

Adicionar Dispositivo de Decodificação on-line

O sistema pode realizar uma detecção automatizada dos Dispositivos de Decodificação disponíveis na rede onde estão localizados o Web Client ou o servidor VSM, o que torna as informações dos dispositivos sobre si mesmas (por exemplo, endereço IP) reconhecidas pelo sistema. Com base nas informações, adicione os dispositivos rapidamente.

Antes de começar

Verifique se os dispositivos que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Etapas

Observação

- Para Google Chrome, instale o Serviço SADP de acordo com as instruções e, em seguida, a função de detecção on-line de dispositivos estará disponível.
 - Para Firefox, instale o Serviço SADP e importe o certificado de acordo com as instruções e, em seguida, a função de detecção on-line de dispositivos estará disponível.
-

1. Clique em **Exibição física** → **Smart Wall** para entrar na página de gerenciamento do Smart Wall.
2. Clique em **Adicionar** no painel do Dispositivo de Decodificação para entrar na página de Adicionar Dispositivo de Decodificação.
3. Selecione **Dispositivos On-Line** como modo de adicionar.

4. Na área Dispositivos On-Line, selecione um tipo de rede.

Rede do servidor

Os Dispositivos On-Line detectados na mesma sub-rede local com o servidor VSM serão relacionados na área dos Dispositivos On-Line.

Redes locais

Os Dispositivos On-Line detectados na mesma sub-rede local com o Web Client serão relacionados na área dos Dispositivos On-Line.

5. Marque a caixa de seleção dos dispositivos a adicionar.

Observação

- Para dispositivos inativos será necessário criar a senha para eles antes de adicionar apropriadamente. Quanto às Etapas detalhadas, consulte ***Criar senha para dispositivo inativo***.
 - Se os dispositivos detectados tiverem os mesmos nome de usuário e senha, adicione vários dispositivos de uma vez. Caso contrário, adicione um por um.
-

6. Digite as informações obrigatórias.

Nome de usuário

O nome de usuário da conta do administrador criada ao ativar o dispositivo ou a conta não administrativa adicionada, como a operadora. Ao adicionar o dispositivo a HikCentral utilizando a conta não administrativa, suas permissões podem restringir seu acesso a determinados recursos.

Senha

A senha necessária para acessar a conta.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

7. Termine de adicionar o Dispositivo de Decodificação.

- Clique em **Adicionar** para adicionar o Dispositivo de Decodificação e volte à página com a lista de Dispositivos de Decodificação.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Dispositivos de Decodificação.

8. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo de Decodificação.

Exibição da saída de decodificação	Clique em  para exibir as saídas de decodificação. É possível exibir a resolução de saída e status de vinculação após vincular a saída ao Smart Wall. Para obter mais informações sobre vinculação de saída de decodificação com Smart Wall, consulte Adicionar Smart Wall .
Editar	Clique em  para editar o Dispositivo de Decodificação. Modifique o Local de Rede como Endereço IP de LAN ou Endereço IP de WAN.
Configurações remotas	Clique em  para definir as configurações remotas do dispositivo.
	<hr/> Observação Para obter mais informações acerca das operações, consulte o Manual do Usuário do dispositivo. <hr/>
Excluir	Clique em  para excluir o dispositivo.

Adicionar Dispositivo de Decodificação por endereço IP

Quando se conhece endereço IP ou o Dispositivo de Decodificação a adicionar se pode adicionar os dispositivos ao sistema especificando-se o endereço IP, nome de usuário, senha e outros parâmetros relacionados. Este modo de adicionar requer que se adicione os dispositivos um por um. Portanto, é uma boa escolha quando se deseja adicionar poucos dispositivos e se conhece todos os detalhes mencionados acima.

Antes de começar

Verifique se os dispositivos que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Etapas

1. Clique em **Exibição física** → **Smart Wall** para entrar na página de gerenciamento do Smart Wall.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Decodificação.

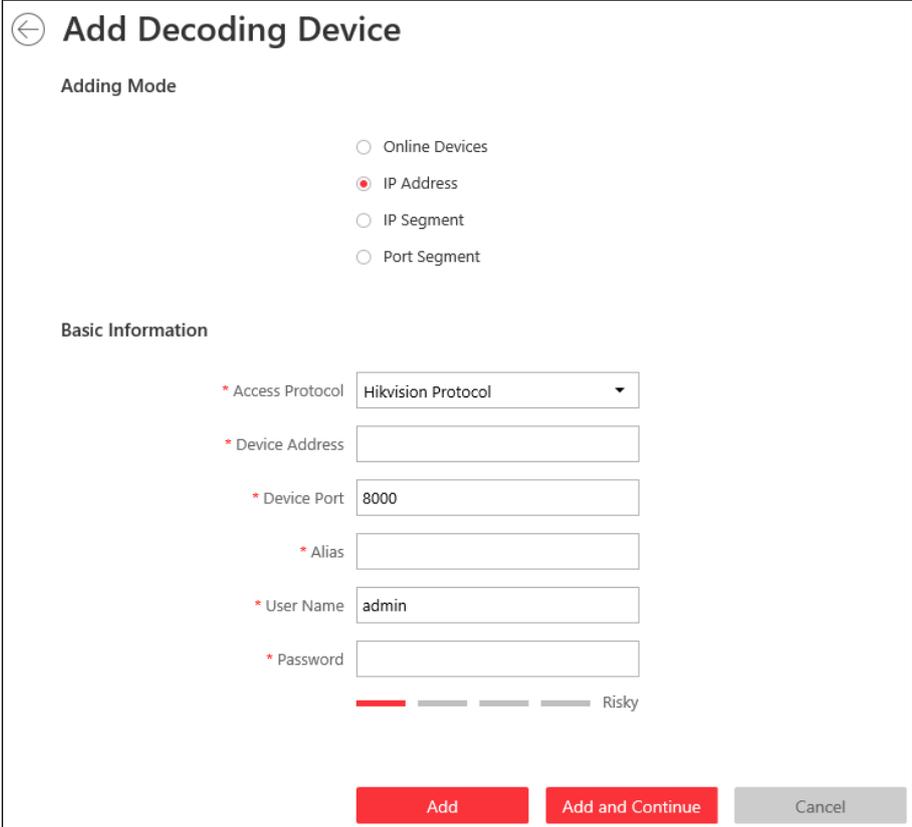


Figura 10-24 Página de adicionar dispositivo de decodificação

3. Selecione **Endereço IP** como modo de adicionar.
4. Digite as informações obrigatórias.

Protocolo de acesso

Selecione **Protocolo Hikvision** para adicionar os dispositivos e selecione **Protocolo ONVIF** para adicionar dispositivos de terceiros.

Endereço do dispositivo

O endereço IP do dispositivo.

Entrada do dispositivo

O número da entrada na qual realizar a varredura. O padrão é 8000.

Se o dispositivo estiver localizado atrás de um roteador habilitado por NAT (Tradução de Endereço de Rede) ou um firewall, pode ser necessário especificar um número de entrada diferente. Nesses casos, lembre-se de configurar o roteador/firewall para que mapeie a entrada e o endereço IP utilizados pelo dispositivo.

Pseudônimo

Crie um nome descritivo para o dispositivo. Por exemplo, utilize um pseudônimo que exiba a localização ou o recurso do dispositivo.

Nome de usuário

O nome de usuário da conta do administrador criada ao ativar o dispositivo ou a conta não

administrativa adicionada, como a operadora. Ao adicionar o dispositivo a HikCentral utilizando a conta não administrativa, suas permissões podem restringir seu acesso a determinados recursos.

Senha

A senha necessária para acessar a conta.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar o Dispositivo de Decodificação e volte à página com a lista de Dispositivos de Decodificação.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Dispositivos de Decodificação.

6. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo de Decodificação.

Exibição da saída de decodificação Clique em  para exibir as saídas de decodificação. É possível exibir a resolução de saída e status de vinculação após vincular a saída ao Smart Wall. Para obter mais informações sobre vinculação de saída de decodificação com Smart Wall, consulte **Adicionar Smart Wall**.

Editar Clique em  para editar o Dispositivo de Decodificação. Modifique o Local de Rede como Endereço IP de LAN ou Endereço IP de WAN.

Configurações remotas Clique em  para definir as configurações remotas do dispositivo.

Observação

Para obter mais informações acerca das operações, consulte o Manual do Usuário do dispositivo.

Excluir Clique em  para excluir o dispositivo.

Adicionar Dispositivos de Decodificação por segmento IP

Se vários Dispositivos de Decodificação a adicionar têm os mesmos número de entrada, nome de usuário e senha mas diferentes endereços IP que estejam dentro de um intervalo, selecione este

modo de adicionar e especifique o intervalo de IP onde seus dispositivos estiverem localizados e outros parâmetros relacionados. O sistema fará a varredura desde o endereço IP inicial até o endereço IP final para os dispositivos a fim de adicioná-los rapidamente.

Antes de começar

Verifique se os dispositivos que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Etapas

1. Clique em **Exibição física** → **Smart Wall** para entrar na página de gerenciamento do Smart Wall.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Decodificação.

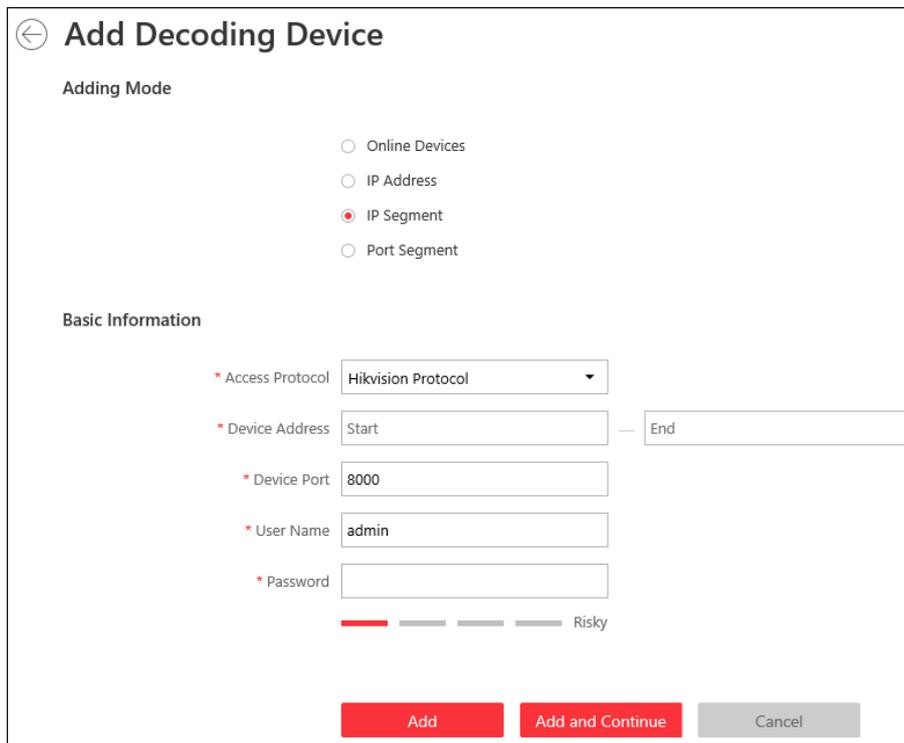


Figura 10-25 Página de Adicionar dispositivo de decodificação

3. Selecione **Segmento IP** como modo de adicionar.
4. Digite as informações obrigatórias.

Protocolo de acesso

Selecione **Protocolo Hikvision** para adicionar os dispositivos e selecione **Protocolo ONVIF** para adicionar dispositivos de terceiros.

Endereço do dispositivo

Digite o endereço IP inicial e o endereço IP final onde os dispositivos estiverem localizados.

Entrada do dispositivo

O mesmo número de entrada dos dispositivos. Por padrão o número da entrada do

dispositivo é 8000.

Nome de usuário

O nome de usuário da conta do administrador criada ao ativar o dispositivo ou a conta não administrativa adicionada, como a operadora. Ao adicionar o dispositivo a HikCentral utilizando a conta não administrativa, suas permissões podem restringir seu acesso a determinados recursos.

Senha

A senha necessária para acessar a conta.

Cuidado

A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar o Dispositivo de Decodificação e volte à página com a lista de Dispositivos de Decodificação.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Dispositivos de Decodificação.

6. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo de Decodificação.

Exibição da saída de decodificação Clique em  para exibir as saídas de decodificação. É possível exibir a resolução de saída e status de vinculação após vincular a saída ao Smart Wall. Para obter mais informações sobre vinculação de saída de decodificação com Smart Wall, consulte **Adicionar Smart Wall**.

Editar Clique em  para editar o Dispositivo de Decodificação. Modifique o Local de Rede como Endereço IP de LAN ou Endereço IP de WAN.

Configurações remotas Clique em  para definir as configurações remotas do dispositivo.

Observação

Para obter mais informações acerca das operações, consulte o Manual do Usuário do dispositivo.

Excluir Clique em  para excluir o dispositivo.

Adicionar Dispositivos de Decodificação por segmento de entrada

Quando vários Dispositivos de Decodificação a adicionar tiverem os mesmos endereço IP, nome de usuário e senha mas diferentes números de entrada que estejam dentro de um intervalo, selecione este modo de adicionar e especifique o intervalo de entrada, endereço IP, nome de usuário, senha e outros parâmetros relacionados para adicioná-los.

Antes de começar

Verifique se os dispositivos que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.

Etapas

1. Clique em **Exibição física** → **Smart Wall** para entrar na página de gerenciamento do Smart Wall.
2. Clique em **Adicionar** para entrar na página de Adicionar Dispositivo de Decodificação.

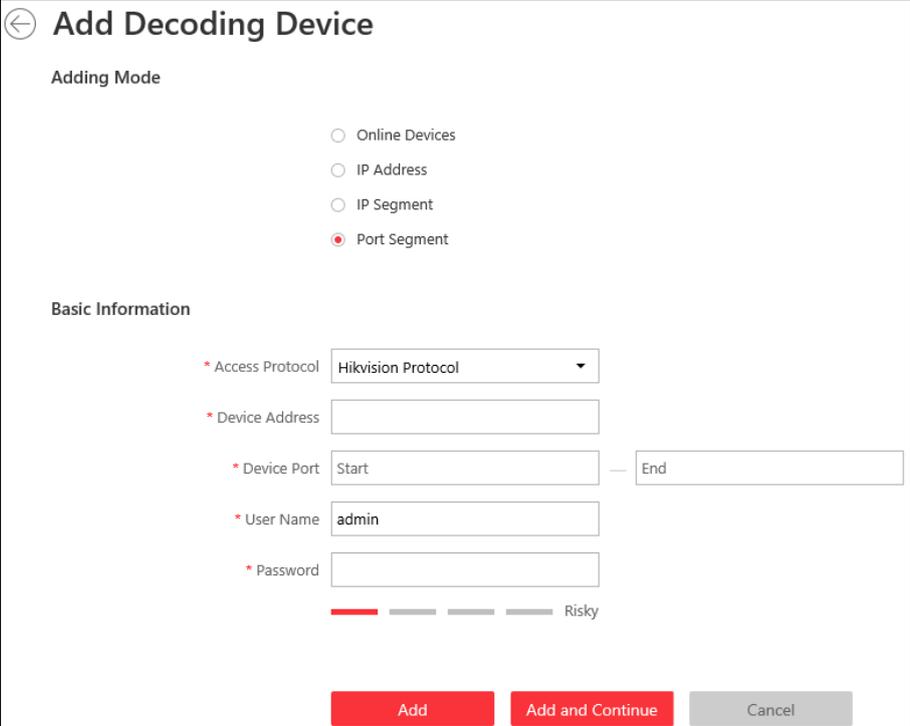


Figura 10-26 Página de adicionar dispositivo de decodificação

3. Selecione **Segmento de entrada** como modo de adicionar.
4. Digite as informações obrigatórias.

Protocolo de acesso

Selecione **Protocolo Hikvision** para adicionar os dispositivos e selecione **Protocolo ONVIF** para adicionar dispositivos de terceiros.

Endereço do dispositivo

O mesmo endereço IP onde os dispositivos estão localizados.

Entrada do dispositivo

Digite os números inicial e final de entrada em que realizar varredura.

Nome de usuário

O nome de usuário da conta do administrador criada ao ativar o dispositivo ou a conta não administrativa adicionada, como a operadora. Ao adicionar o dispositivo a HikCentral utilizando a conta não administrativa, suas permissões podem restringir seu acesso a determinados recursos.

Senha

A senha necessária para acessar a conta.



A força da senha do dispositivo pode ser verificada automaticamente. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

5. Termine de adicionar o dispositivo.

- Clique em **Adicionar** para adicionar o Dispositivo de Decodificação e volte à página com a lista de Dispositivos de Decodificação.
- Clique em **Adicionar e continuar** para salvar as configurações e continuar a adicionar outros Dispositivos de Decodificação.

Após adicionar o Dispositivo de Decodificação, os dispositivos serão exibidos na lista no painel de Dispositivos de Decodificação.

6. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo de Decodificação.

Exibição da saída de decodificação Clique em  para exibir as saídas de decodificação. É possível exibir a resolução de saída e status de vinculação após vincular a saída ao Smart Wall. Para obter mais informações sobre vinculação de saída de decodificação com Smart Wall, consulte **Adicionar Smart Wall**.

Editar Clique em  para editar o Dispositivo de Decodificação. Modifique o Local de Rede como Endereço IP de LAN ou Endereço IP de WAN.

Configurações remotas Clique em  para definir as configurações remotas do dispositivo.

Observação

Para obter mais informações acerca das operações, consulte o Manual do Usuário do dispositivo.

Excluir

Clique em ✕ para excluir o dispositivo.

10.10.2 Configuração em cascata

Em algumas situações reais para exibição em tela grande, o número de telas do Smart Wall ultrapassará o número de saídas de decodificação de um decodificador. Ou então funções de decodificação cruzada como roaming e extensão serão necessárias. Coloque dois decodificadores em cascata com o controlador de video wall para atender a várias demandas de exibição.

Antes de começar

- Verifique se os dispositivos que serão utilizados estão corretamente instalados e conectados à rede, conforme especificado pelos fabricantes. Essa configuração inicial é necessária para poder conectar os dispositivos a HikCentral via rede.
- As interfaces dos decodificadores foram conectadas com o controlador de video wall utilizando fios combinados.
- Os decodificadores e o controlador de video wall são adicionados a HikCentral. Consulte **Adicionar Dispositivo de Decodificação** para obter mais informações.

Execute esta tarefa quando precisar configurar colocação em cascata para os Dispositivos de Decodificação como segue.

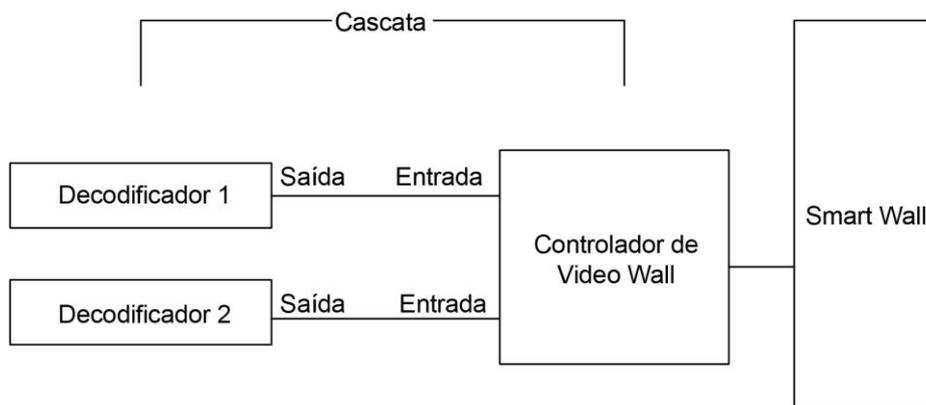


Figura 10-27 Cascata

Etapas

1. Clique em **Exibição física** → **Smart Wall** para entrar na página de gerenciamento do Smart Wall. Os Dispositivos de Decodificação adicionados e o Smart Wall serão exibidos.
2. Clique em  por trás do controlador de video wall adicionado para entrar na página de Colocação em cascata.

 **Observação**

Somente os controladores de video wall DS-CS10S e DS-C10S-T apresentam esta função.

3. Selecione o canal de sinal do controlador de video wall e clique em .
 4. Selecione a saída de decodificação do decodificador para configurar como entrada de sinal do controlador de video wall.
-

 **Observação**

Se os decodificadores estiverem em cascata com o controlador de video wall, as saídas de decodificação de reserva dos decodificadores não poderão mais ser utilizadas para exibição no Smart Wall.

5. Clique em **Salvar** para salvar a cascata.

Resultado

Após configurar a cascata será necessário adicionar um Smart Wall e vincular as saídas de decodificação do controlador de video wall para exibir as saídas de sinal dos dois decodificadores no Smart Wall.

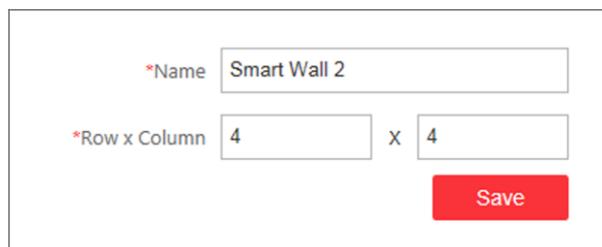
10.10.3 Adicionar Smart Wall

Adicione o Smart Wall ao sistema e configure linhas e colunas.

Execute esta tarefa quando precisar adicionar um Smart Wall ao sistema.

Etapas

1. Clique em **Exibição física** → **Smart Wall** para entrar na página de gerenciamento do Smart Wall.
2. Clique em **Adicionar** no painel do Smart Wall para abrir a caixa de diálogo de Adicionar Smart Wall.



The image shows a dialog box for adding a Smart Wall. It contains the following elements:

- A text input field labeled '*Name' with the value 'Smart Wall 2'.
- A text input field labeled '*Row x Column' with the value '4' in the first box and '4' in the second box, separated by an 'x' symbol.
- A red button labeled 'Save'.

Figura 10-28 Caixa de diálogo de Adicionar Smart Wall

3. Defina o nome do Smart Wall.
4. Configure os números de linha e coluna.
5. Clique em **Salvar**.
6. Opcional: Execute as operações a seguir depois de adicionar o Dispositivo de Decodificação.

Vinculação de saída Para obter mais informações acerca das operações, consulte

de decodificação com janela *Vinculação de saída de decodificação com janela.*

Editar o Smart Wall Edite o nome do Smart Wall.

Excluir o Smart Wall Exclua o Smart Wall.

10.10.4 Vinculação de saída de decodificação com janela

Após adicionar o Dispositivo de Decodificação e o Smart Wall, vincule a saída de decodificação do Dispositivo de Decodificação à janela do Smart Wall.

Execute esta tarefa quando precisar vincular a saída de decodificação ao Smart Wall.

Etapas

1. Clique em **Exibição física** → **Smart Wall** para entrar na página de gerenciamento do Smart Wall. Os Dispositivos de Decodificação adicionados e o Smart Wall serão exibidos.
2. Clique em > na dianteira do Dispositivo de Decodificação para exibir as saídas de decodificação.
3. Clique em > na dianteira do Smart Wall para exibir as janelas.
4. Arraste a saída de decodificação do painel do Dispositivo de Decodificação para a janela de exibição do Smart Wall para configurar a correspondência de um por um.

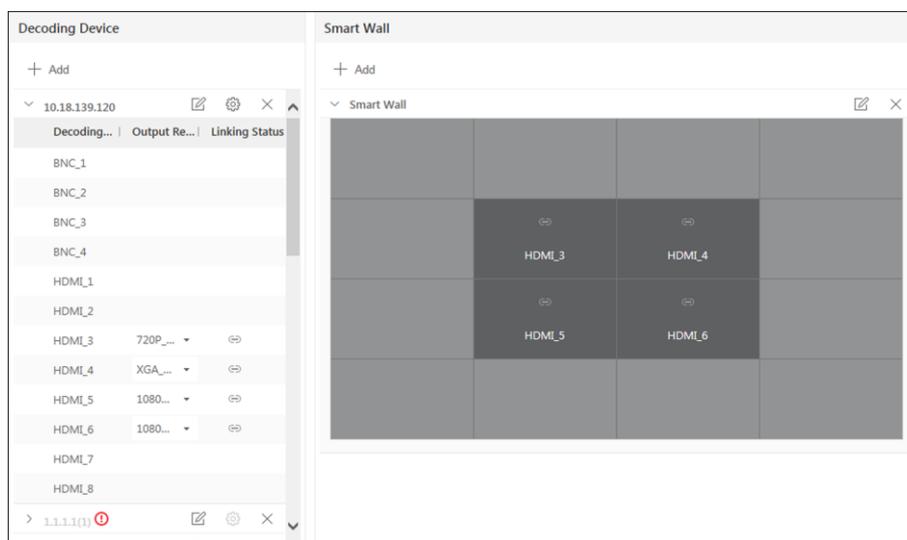


Figura 10-29 Vinculação do Dispositivo de Decodificação com janela

5. Opcional: Clique em ✕ para liberar a vinculação.

Capítulo 11 Gerenciamento de Área

HikCentral proporciona áreas para gerenciar os recursos adicionados em diferentes grupos. Agrupe os recursos em diferentes áreas de acordo com os locais dos recursos. Por exemplo, no primeiro andar há 64 câmeras fixadas, 16 pontos de acesso, 64 entradas de alarmes e 16 saídas de alarmes. Organize esses recursos em uma área (chamada primeiro andar) para aprimorar o gerenciamento. Obtenha exibição em tempo real, reprodução de arquivos de vídeo e executar algumas outras operações dos dispositivos depois de gerenciar os recursos por áreas.

Observação

Se o sistema atual for um Sistema Central com um módulo de Gerenciamento do Local Remoto, gerencie também as áreas em um Local Remoto e adicione câmeras no Local Remoto em áreas.

11.1 Adicionar área

Adicione uma área antes de gerenciar os elementos por áreas.

11.1.1 Adicionar área para o Local Atual

Adicione uma área para o Local Atual para gerenciar os dispositivos.

Execute esta tarefa quando precisar adicionar uma área para o local atual.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Exibição Lógica.
2. Opcional: Selecione a área pai no painel com a lista de áreas para adicionar uma sub-área.

Observação

- Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o Local Atual na lista suspensa de locais para exibir suas áreas.
 - O ícone  indica que o local é um Local Atual.
-

3. Clique em **+** no painel com a lista de áreas para abrir a janela de Adicionar área.

← Add Area

Basic Information

i *Parent Area 0314_01

*Area Name Area_20180316161219

i Streaming Server <None>

Map

Related Map

Save Cancel

Figura 11-1 Adicionar área para o Local Atual

4. Selecione a área pai para adicionar uma sub-área.
5. Crie um nome para a área.
6. Opcional: Selecione um Servidor de Transmissões para a área para obter transmissão de vídeo das câmeras que pertencem a esta área via servidor.
7. Opcional: Se selecionar um Servidor de Transmissões para a área, marque **Exibição em mural via Servidor de Transmissões** para exibir os recursos da área no Smart Wall por meio deste Servidor de Transmissões.
8. Opcional: Configure o interruptor **Mapa relacionado** como ligado e vincule os mapas eletrônicos à área. Consulte **Vinculação de mapa eletrônico a uma área** para obter mais informações.
9. Clique em **Salvar**.
10. Opcional: Após adicionar a área, faça um ou mais do seguinte:

Editar área Clique em  para editar a área.

Excluir área Clique em  para excluir a área selecionada.

 **Observação**

Após excluir a área, os recursos na área (câmeras, entradas de alarmes, saídas de alarmes, pontos de acesso e UVSSs) serão removidos da área, bem como as configurações de gravações correspondentes, configurações de eventos e configurações de mapas.

Pesquisar área

Digite uma palavra-chave no campo de pesquisas para pesquisar a área.

11.1.2 Adicionar área para Local Remoto

Adicione uma área para Local Remoto para gerenciar os dispositivos no Sistema Central.

Execute esta tarefa quando precisar adicionar área ao Local Remoto.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Exibição Lógica.
2. No painel com a lista de áreas, selecione o Local Remoto adicionado na lista suspensa de locais para exibir as áreas.

 **Observação**

O ícone  indica que o local é um Local Remoto.

3. Clique em **+** no painel com a lista de áreas para abrir a janela de Adicionar área.

← Add Area

Basic Information

*Parent Area None

*Mode Import Area with New Cameras Add New Area

*Area Refresh

Search

No data.

Streaming Server <None>

Save Cancel

Figura 11-2 Adicionar área no Local Remoto

4. Selecione a área pai para adicionar uma sub-área.
5. Configure o modo de adicionar para adicionar a área.

Importação de área com novas câmeras

Se houver algumas câmeras recém-adicionadas às áreas em um Local Remoto, importe as áreas, bem como as câmeras recém-adicionadas. As áreas com câmeras recém-adicionadas serão exibidos. Selecione as áreas a adicionar.

Adicionar nova área

Adicionar uma nova área à área pai.

6. Opcional: Selecione um Servidor de Transmissões para a área para obter transmissão de vídeo das câmeras que pertencem a esta área via servidor.
7. Opcional: Se selecionar um Servidor de Transmissões para a área, marque **Exibição em mural via Servidor de Transmissões** se desejar exibir os recursos da área no Smart Wall por meio deste Servidor de Transmissões.
8. Clique em **Salvar**.
9. Após adicionar a área, faça um ou mais do seguinte:

Editar área

Clique em  para editar a área.

Excluir área

Clique em  para excluir a área selecionada.

 **Observação**

Após excluir a área, as câmeras serão removidas da área, bem como as configurações de gravações correspondentes e configurações de eventos.

Pesquisar área

Digite uma palavra-chave no campo de pesquisas para pesquisar a área.

11.2 Adicionar elemento a área

Adicione elementos incluindo câmeras, entradas de alarmes, saídas de alarmes, pontos de acesso e sistemas de vigilância sob veículos (UVSS) em áreas para gerenciamento.

11.2.1 Adicionar câmera a área para o Local Atual

Adicione câmeras a áreas para o Local Atual. Após gerenciar as câmeras em áreas, obtenha a exibição em tempo real, reproduza os arquivos de vídeo e assim por diante.

Antes de começar

Os dispositivos precisam ser adicionados a HikCentral para Gerenciamento de Área. Consulte **Gerenciamento de recursos** para obter as configurações detalhadas sobre adicionar dispositivos.

Execute esta tarefa quando precisar adicionar câmeras do Local Atual a áreas.

Etapas

 **Observação**

Uma câmera só pode pertencer a uma área. Não é possível adicionar uma câmera a várias áreas.

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
 2. Selecione uma área a que adicionar câmeras.
-

 **Observação**

- Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o Local Atual na lista suspensa de locais para exibir suas áreas.
 - O ícone  indica que o local é um Local Atual.
-

3. Selecione a guia **Câmeras**.

- Clique em **Adicionar** para entrar na página de Adicionar câmera.
- Selecione o tipo de dispositivo como **Dispositivo de Codificação** ou **Dispositivo de Controle de Segurança**.

 **Observação**

Alguns dispositivos de controle de segurança como estações de alarme para pânico também contêm as câmeras.

- Selecione as câmeras a adicionar.
- Opcional: Marque **Obter configurações de gravações do dispositivo** para obter o agendamento de gravações configurado no dispositivo local e o dispositivo poderá começar a gravar de acordo com o agendamento.

 **Observação**

Se o agendamento de gravações configurado no dispositivo não for de gravação contínua, será alterado para gravação de evento no dispositivo local.

- Opcional: Marque **Adicionar a um mapa** para adicionar a câmera ao mapa.
- Clique em **Adicionar**.
- Opcional: Após adicionar as câmeras, faça um ou mais do seguinte:

Obtenha o nome da câmera Selecione as câmeras e clique em **Obter o nome da câmera** para obter os nomes das câmeras do dispositivo em lote.

 **Observação**

Só se pode sincronizar o nome da câmera de um dispositivo HIKVISION on-line.

Mover para outra área Selecione as câmeras e clique em **Mover para outra área**. Em seguida, selecione a área de destino para mover as câmeras selecionadas e clique em **Mover**.

Exibição de câmeras de áreas filhas Marque **Incluir sub-área** para exibir as câmeras de áreas filhas.

11.2.2 Adicionar câmera a área para Local Remoto

Se o sistema atual for um Sistema Central com um módulo de Gerenciamento do Local Remoto, adicione também câmeras de Locais Remotos para áreas no Sistema Central para gerenciamento.

Antes de começar

Os dispositivos de codificação precisam ser adicionados ao HikCentral para fins de gerenciamento

de área. Consulte **Gerenciamento de Dispositivo de Codificação** para obter as configurações detalhadas sobre adicionar dispositivos.

Execute esta tarefa quando precisar adicionar câmera de Local Remoto a área central.

Etapas

Observação

Uma câmera só pode pertencer a uma área. Não é possível adicionar uma câmera a várias áreas.

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
 2. No painel com a lista de áreas, selecione o Local Remoto adicionado na lista suspensa de locais para exibir as áreas.
-

Observação

O ícone  indica que o local é um Local Remoto.

3. Selecione uma área a que adicionar elementos.
4. Clique em **Adicionar** para entrar na página de Adicionar câmera.

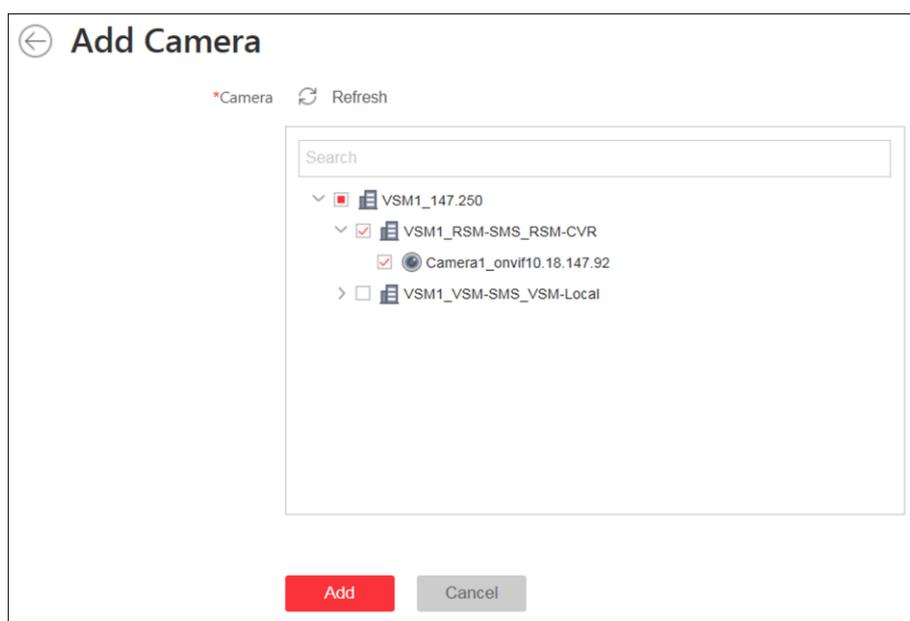


Figura 11-3 Página de Adicionar câmera

5. Selecione as câmeras a adicionar.
-

Observação

Podem ser adicionadas até 64 câmeras a uma área.

6. Clique em **Adicionar**.
-

7. Opcional: Após adicionar as câmeras, faça um ou mais do seguinte:

Sincronização do nome da câmera	Selecione as câmeras e clique em  para obter os nomes das câmeras do dispositivo em lote.
Mover para outra área	Selecione as câmeras e clique em  . Em seguida, selecione a área de destino para mover as câmeras selecionadas e clique em Mover .
Exibição de câmeras de áreas filhas	Selecione Incluir sub-área para exibir as câmeras de áreas filhas.

11.2.3 Adicionar ponto de acesso a área

Adicione pontos de acesso a áreas para o Local Atual para gerenciamento.

Antes de começar

Dispositivos de controle de acesso precisam ser adicionados a HikCentral para Gerenciamento de Área. Consulte **Gerenciamento de recursos** para obter as configurações detalhadas sobre adicionar dispositivos.

Execute esta tarefa quando precisar adicionar pontos de acesso do Local Atual a áreas.

Etapas

Observação

Um ponto de acesso só pode pertencer a uma área. Não é possível adicionar um ponto de acesso a várias áreas.

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
 2. Selecione uma área a que adicionar pontos de acesso.
-

Observação

- Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o Local Atual na lista suspensa de locais para exibir suas áreas.
 - O ícone  indica que o local é um Local Atual.
-

3. Selecione a guia **Pontos de acesso**.
 4. Clique em **Adicionar** para entrar na página de Adicionar Pontos de Acesso.
 5. Selecione os pontos de acesso a adicionar.
 6. Opcional: Marque **Obter nome do ponto de acesso** para obter o nome do ponto de acesso do dispositivo.
-

Observação

Só se pode sincronizar o nome do ponto de acesso de um dispositivo HIKVISION on-line.

7. Opcional: Marque **Adicionar a um mapa** para adicionar o ponto de acesso ao mapa.
8. Clique em **Adicionar**.
9. Opcional: Após adicionar os pontos de acesso, faça um ou mais do seguinte:

Obter o nome do ponto de acesso

Selecione os pontos de acesso e clique em **Obter o nome do ponto de acesso** para obter os nomes dos pontos de acesso do dispositivo em lote.

 **Observação**

Só se pode sincronizar o nome do ponto de acesso de um dispositivo HIKVISION on-line.

Mover para outra área

Selecione os pontos de acesso e clique em **Mover para outra área**. Em seguida, selecione a área de destino para mover os pontos de acesso selecionados e clique em **Mover**.

Exibição de pontos de acesso de áreas filhas

Marque **Incluir sub-área** para exibir os pontos de acesso de áreas filhas.

11.2.4 Adicionar entrada de alarme a uma área

Adicione entradas de alarme acesso a áreas para o Local Atual para gerenciamento.

Antes de começar

Dispositivos precisam ser adicionados a HikCentral para Gerenciamento de Área. Consulte **Gerenciamento de recursos** para obter as configurações detalhadas sobre adicionar dispositivos.

Execute esta tarefa quando precisar adicionar entradas de alarme do Local Atual a áreas.

Etapas

 **Observação**

Entrada de alarme só pode pertencer a uma área. Não é possível adicionar uma entrada de alarme a várias áreas.

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. Selecione uma área a que adicionar entradas de alarme.

 **Observação**

- Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o Local Atual na lista suspensa de locais para exibir suas áreas.
- O ícone  indica que o local é um Local Atual.

3. Selecione a guia **Entradas de alarmes**.
4. Clique em **Adicionar** para entrar na página de Adicionar Entradas de alarme.
5. Selecione o tipo de dispositivo.
6. Selecione as entradas de alarme a adicionar.

 **Observação**

For o dispositivo de controle de segurança é necessário selecionar suas zonas como entradas de alarme para adicionar à área.

7. Opcional: Marque **Adicionar a um mapa** para adicionar a entrada de alarme ao mapa.
8. Clique em **Adicionar**.
9. Opcional: Após adicionar as entradas de alarme, faça um ou mais do seguinte:

Mover para outra área Selecione as entradas de alarme e clique em **Mover para outra área**. Em seguida, selecione a área de destino para mover as entradas de alarme selecionadas e clique em **Mover**.

Exibição de entradas de alarme de áreas filhas Marque **Incluir sub-área** para exibir as entradas de alarme de áreas filhas.

11.2.5 Vinculação de entradas de alarme à Partição do Controle de Segurança

Após adicionar as zonas do dispositivo de controle de segurança ao sistema (chamadas “entradas de alarme” depois de adicionadas ao sistema), vincule-as a diferentes partições de controle de segurança no sistema de acordo com a relação entre zonas e partições configurada no dispositivo. Depois de agrupar entradas de alarme nas partições de controle de segurança no sistema, defina um agendamento de defesa para as entradas de alarme em uma partição de controle de segurança. O agendamento de defesa define quando e como armar as entradas de alarme nesta partição de controle de segurança. Por exemplo, área 1 foi criada para o primeiro andar e todos os recursos no primeiro andar são gerenciados na área 1. Se houver algum dispositivo de controle de segurança fixado no primeiro andar, adicione suas zonas na área 1 primeiramente. Em seguida, vincule as zonas (entradas de alarme) na partição de controle de segurança e defina um agendamento de defesa para essas partições de controle de segurança. Depois disso, as zonas (entradas de alarme) poderão ser armadas de acordo com os agendamentos, respectivamente.

Antes de começar

Verifique se as zonas do dispositivo de controle de segurança foram adicionadas ao sistema e agrupadas em áreas. Para obter mais informações, consulte **Adicionar entrada alarme a uma área**.

Etapas

1. Clique em **Exibição Lógica** na página inicial.
2. Selecione uma área que contenha entradas de alarme em que desejar definir um agendamento de defesa e clique em  para entrar na página da área de edição.
3. No campo Partição de controle de segurança, clique em **Adicionar**.
4. Crie um nome para a partição de controle de segurança.
5. Na lista suspensa do campo entrada de alarme, selecione um dispositivo de controle de segurança.
As entradas de alarme do dispositivo de controle de segurança adicionadas a esta área e que não foram adicionadas a nenhuma partição de controle de segurança serão exibidas.
6. Selecione as entradas de alarme que desejar adicionar à partição de controle de segurança.
7. Selecione o número de partição de controle de segurança na lista suspensa que se obtém no dispositivo que foi selecionado na Etapa 5.
8. Opcional: Defina um agendamento de defesa para esta partição, que especifica como e quando armar as entradas de alarme na partição de controle de segurança.

Observação

Para definir um novo agendamento de defesa, consulte **Configuração de modelo de agendamento de defesa**.

9. Clique em **Adicionar**.

11.2.6 Adicionar saída de alarme a uma área

Adicione saídas de alarme acesso a áreas para o Local Atual para gerenciamento. Quando alarme ou evento vinculados com saída de alarme são detectados, os dispositivos de alarme (por exemplo, sirene, lâmpada de alarme etc.) conectados com saída de alarme realizam ações. Por exemplo, ao receber o sinal de saída de alarme do sistema, a lâmpada de alarme piscará.

Antes de começar

Dispositivos precisam ser adicionados a HikCentral para Gerenciamento de Área. Consulte **Gerenciamento de recursos** para obter as configurações detalhadas sobre adicionar dispositivos.

Execute esta tarefa quando precisar adicionar saídas de alarme do Local Atual a áreas.

Etapas

Observação

Uma saída de alarme só pode pertencer a uma área. Não é possível adicionar uma saída de alarme a várias áreas.

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. Selecione uma área a que adicionar saídas de alarme.

 **Observação**

- Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o Local Atual na lista suspensa de locais para exibir suas áreas.
 - O ícone  indica que o local é um Local Atual.
-

3. Selecione a guia **Saídas de alarmes**.

4. Clique em **Adicionar** para entrar na página de Adicionar Saídas de alarme.

5. Selecione o tipo de dispositivo.

6. Selecione as saídas de alarme a adicionar.

7. Opcional: Marque **Adicionar a um mapa** para adicionar a saída de alarme ao mapa.

8. Clique em **Adicionar**.

9. Opcional: Após adicionar as saída de alarme, faça um ou mais do seguinte:

Mover para outra área Selecione as saída de alarme e clique em **Mover para outra área**. Em seguida, selecione a área de destino para mover as saída de alarme selecionadas e clique em **Mover**.

Exibição de saída de alarme de áreas filhas Marque **Incluir sub-área** para exibir as saída de alarme de áreas filhas.

11.2.7 Adicionar UVSS a área para o Local Atual

Adicione sistemas de vigilância sob veículos (UVSS) a áreas para o Local Atual para gerenciamento.

Execute esta tarefa quando precisar adicionar sistemas de vigilância sob veículos (UVSS) do Local Atual a áreas.

Etapas

 **Observação**

UVSS só pode pertencer a uma área. Não é possível adicionar UVSS a várias áreas.

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.

2. Selecione uma área a que adicionar UVSSs.

 **Observação**

- Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o Local Atual na lista suspensa de locais para exibir suas áreas.
 - O ícone  indica que o local é um Local Atual.
-

3. Selecione a guia **Sistemas de vigilância sob veículos**.

 **Observação**

Se a função de mapa estiver ativada, clique em  e clique em **UVSSs**.

4. Clique em **Adicionar** para entrar na página de Adicionar UVSS.
5. Digite as informações obrigatórias sobre UVSS.
6. Vinculação de câmeras a UVSS.
 - 1) Configure o interruptor **Relacionar câmera** como ligado.
 - 2) Selecione as câmeras.
7. Marque **Adicionar a um mapa** para adicionar UVSS ao mapa.
8. Clique em **Adicionar**.

11.3 Editar elemento em área

Edite os elementos adicionados da área como configurações de gravações, configurações de eventos e configurações de mapas para câmeras, configurações de aplicações, configurações de hardware e configurações de frequência para portas e assim por diante.

11.3.1 Edição de câmera para o Local Atual

Edite as informações básicas, configurações de gravações, configurações de armazenamento de imagens, configurações de eventos e configurações de mapa da câmera para o Local Atual. Edite também as configurações do grupo de comparações faciais das câmeras que permitem comparação de imagens faciais.

Execute esta tarefa quando precisar editar alguma câmera para o Local Atual.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. No painel com a lista de áreas, selecione o Local Atual adicionado na lista suspensa de locais para exibir as áreas.

 **Observação**

O ícone  indica que o local é um Local Atual.

3. Selecione uma área.
4. Selecione a guia **Câmeras** para exibir as câmeras adicionadas.
5. Clique na coluna **Nome** para entrar na página de Editar câmera.
6. Edite as informações básicas da, incluindo nome da câmera e tipo de protocolo.
7. Opcional: Clique em  para visualizar a exibição em tempo real da câmera e passar o mouse pela janela e clique em  no canto inferior direito para alternar para reprodução.

 **Observação**

As funções de exibição em tempo real e reprodução na página de detalhes da câmera são permitidas somente pelo Internet Explorer.

8. Edite as configurações de gravações da câmera. Consulte **Configuração de gravações** para obter mais informações.
-

 **Observação**

Se nenhuma configuração de gravações tiver sido definida para a câmera, clique em **Configurações** para configurar os parâmetros.

9. Opcional: Para câmeras que permitem comparações de imagens faciais, edite as configurações de grupo de comparação facial.
- 1) Configure o grupo de pessoas para comparação facial. Exclua o agrupo aplicado e exiba detalhes do grupo.
-

 **Observação**

Se nenhum grupo de comparação facial tiver sido aplicado à câmera, clique em **Aplicação de grupo de configuração facial**. Consulte **Aplicação de grupo de configuração facial a dispositivo** para obter mais informações.

- 2) Configure o limite de semelhança de comparação facial que afeta frequência e precisão do alarme de comparação de imagem facial.
10. Opcional: Configure o interruptor **Armazenamento de imagens** como ligado e selecione o local de armazenamento na lista suspensa para armazenamento das imagens enviadas da câmera para o local especificado.
-

 **Observação**

Consulte **Configuração de armazenamento para imagens enviadas** para obter mais informações.

11. Edite as configurações de eventos da câmera. Consulte **Configuração de eventos e alarmes** para obter mais informações.
-

 **Observação**

Se nenhuma configuração de eventos tiver sido definida para a câmera, clique em **Configurações** para configurar os parâmetros.

12. Adicione a câmera ao mapa.
- 1) Configure o interruptor **Adicionar ao mapa** como ligado.
- 2) Selecione o ícone estilo e cor do nome para exibir a câmera no mapa.
-

13. Opcional: Clique em **Configurações no dispositivo** para definir as configurações remotas dos dispositivos correspondentes, se necessário.

Observação

Para obter mais informações acerca de configuração remota, consulte o Manual do Usuário do dispositivo.

14. Clique em **Salvar**.
15. Opcional: Entre novamente na página de Editar câmera e clique em **Copiar para** para selecionar item de configuração e copiar as configurações desta câmera para outras câmeras.

11.3.2 Edição de ponto de acesso para o Local Atual

Edite informações básicas, câmeras relacionadas, configurações de aplicação, configurações de hardware, nível de acesso, configurações de frequência, configurações de eventos e configurações de mapas do ponto de acesso para o Local Atual.

Execute esta tarefa quando precisar editar o ponto de acesso para o Local Atual.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. No painel com a lista de áreas, selecione o Local Atual adicionado na lista suspensa de locais para exibir as áreas.

Observação

O ícone  indica que o local é um Local Atual.

3. Selecione uma área.
4. Selecione a guia **Pontos de acesso** para exibir os pontos de acesso adicionados.
5. Clique na coluna Nome para entrar na página de Editar ponto de acesso.
6. Edite as informações básicas do ponto de acesso.

Contato de porta

O modo de conexão do contato da porta.

Tipo de botão de saída

O modo de conexão do botão de saída.

Duração da abertura

O intervalo de tempo entre o ponto de acesso é desbloqueado e bloqueado novamente.

Duração estendida da abertura

O intervalo de tempo entre o ponto de acesso é desbloqueado e bloqueado novamente quando a função de acesso estendido de uma pessoa está ativada.

Alarme do limite de tempo de abertura da porta

Depois de ativar, se o ponto de acesso tiver sido configurado com evento ou alarme, quando a duração de abertura do contato da porta tiver chegado ao limite, evento ou alarme serão enviados ao sistema.

Código da ameaça

Se inserir este código no teclado do leitor de cartões, o Control Client receberá um evento de ameaça. Deve ser diferente da super senha e do código de dispensar.

Super senha

Se inserir esta senha no teclado do leitor de cartões, haverá isenção de todas as restrições de autorização restantes bloqueadas (falha na credencial), antirretorno e de primeiro cartão. Deve ser diferente do código de ameaça e do código de dispensar.

Código de dispensar

Se inserir este código no teclado do leitor de cartões, o som da campainha será interrompido. Deve ser diferente do código de ameaça e da super senha.

Agendamento de acesso livre

Durante este agendamento, o ponto de acesso permanece aberto. O usuário pode entrar ou sair por meio do ponto de acesso sem nenhuma credencial. Para catraca, defina agendamentos para entrada e saída, respectivamente.

7. Vincule as câmeras ao ponto de acesso e poderá visualizar exibição em tempo real, vídeo gravado, imagens capturadas via Control Client.



Observação

Até duas câmeras podem ser relacionadas a um ponto de acesso.

8. Edição das configurações de aplicação.

Antirretorno:

A pessoa sai por meio do ponto de acesso no antirretorno se entrar por meio do ponto de acesso no antirretorno. Isso minimiza mau uso ou uso fraudulento de credenciais de acesso como cartão de passagem para alguma pessoa não autorizada ou acesso pela traseira. Para configurar a regra de antirretorno, consulte **Configuração de regras de antirretorno**.

Abertura da porta com o primeiro cartão

Depois de passar o primeiro cartão, o ponto de acesso permanecerá desbloqueado ou será autorizado. O status depende da quantidade de vezes em que se passa o cartão (par ou ímpar). Para ímpar, o ponto de acesso permanecerá desbloqueado ou será autorizado. Para par, haverá os modos desbloqueado ou autorizado.

9. Edite as configurações de hardware.

- 1) Configure o interruptor **Leitor de cartões** como ligado e configure os parâmetros relacionados do leitor de cartões.

Polaridade LED OK

Disponível somente quando o dispositivo estiver conectado via interface Wiegand. A

polaridade para conexão com fio de núcleo OK na placa principal do leitor de cartões.

Erro na polaridade LED

Disponível somente quando o dispositivo estiver conectado via interface Wiegand. A polaridade para conexão com fio do núcleo ERR na placa principal do leitor de cartões.

Polaridade da campainha

Disponível somente quando o dispositivo estiver conectado via interface Wiegand. A polaridade para conexão da campainha na placa principal do leitor de cartões.

- 2) Configure o modo de acesso do leitor de cartões em períodos de tempo normais.
-

Observação

Os modos de acesso do leitor de cartões são aceitos pelo dispositivo.

Exemplo:

Se selecionar **Cartão**, abra o ponto de acesso passando o cartão o tempo todo.

- 3) Opcional: Quando desejar abrir o ponto de acesso via outro modo de acesso em alguns períodos de tempo especiais, configure o modo de acesso do leitor de cartões e selecione o período de tempo personalizado.

Exemplo:

Se selecionar **Impressão digital** e **Agendamento de final de semana**, abra o ponto de acesso com impressão digital nos finais de semana.

Observação

Adicione um modelo de agendamento personalizado e até três períodos de tempo podem ser definidos para cada dia. Consulte **Configuração do modelo de agendamento de acesso** para obter mais informações.

- 4) Configure o interruptor **Intervalo mínimo de passagem do cartão** como ligado e defina o intervalo.

Intervalo mínimo de passagem do cartão

Depois de ativado, não se pode passar o mesmo cartão novamente dentro do intervalo mínimo de passagem do cartão.

- 5) Configure o intervalo máximo de tempo de pressionar duas teclas no teclado. Se expirar, a primeira entrada será redefinida.
- 6) Configure o interruptor **Alarme para falhas em tentativas com o cartão** como ligado e configure a quantidade máxima de falhas de tentativas.

Alarme para falhas em tentativas com o cartão

Depois de ativar, se o ponto de acesso tiver sido configurado com evento ou alarme, quando o número de excesso de falhas em tentativas de passar o cartão chegar ao limite, o evento ou o alarme serão enviados ao sistema.

Detecção de manipulações indevidas

Depois de ativar, se o ponto de acesso tiver sido configurado com evento ou alarme para dispositivo adulterado, quando o corpo ou o painel do dispositivo se separarem o alarme será acionado e enviado ao sistema.

10. Opcional: Para ponto de acesso de catraca, configure o interruptor **Terminal de reconhecimento facial** como ligado e adicione os terminais de reconhecimento facial para vincular o ponto de acesso selecionado.
 - 1) Configure o interruptor **Terminal de reconhecimento facial** como ligado para adicionar os terminais de reconhecimento facial.
 - 2) Clique em **Adicionar** para entrar na página de Adicionar Terminal de reconhecimento facial.
 - 3) Selecione **IP** ou **Dispositivos on-line** como modo de adicionar e configure os parâmetros necessários, o que pode variar de acordo com diferentes terminais.
 - 4) Clique em **Adicionar** para vincular o terminal ao ponto de acesso.
-

Observação

Depois de adicionar à lista de terminais, edite ou exclua os dispositivos ou execute outras operações.

11. Adicione o ponto de acesso a um nível de acesso.
 12. Configure o ponto de acesso como ponto de verificação de frequência.
 13. Edite as configurações de eventos do ponto de acesso. Consulte **Configuração de eventos e alarmes** para obter mais informações.
-

Observação

Se nenhuma configuração de eventos tiver sido definida para o ponto de acesso, clique em **Configurações** para configurar os parâmetros.

14. Adicione o ponto de acesso ao mapa.
 - 1) Configure o interruptor **Adicionar ao mapa** como ligado.
 - 2) Selecione o ícone estilo e cor do nome para exibir o ponto de acesso no mapa.
-

Observação

Podem ser adicionados até 128 pontos de acesso em um mapa.

15. Clique em **Salvar**.
16. Opcional: Se necessário, entre novamente na página de Editar ponto de acesso e clique em **Copiar para** para aplicar as configurações atuais do ponto de acesso a outros pontos de acesso.

11.3.3 Edição de entrada de alarme para o Local Atual

Edite informações básicas, configurações de eventos e configurações de mapa da entrada de alarme para o Local Atual.

Execute esta tarefa quando precisar editar entrada de alarme para o Local Atual.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. No painel com a lista de áreas, selecione o Local Atual adicionado na lista suspensa de locais para exibir as áreas.

Observação

O ícone  indica que o local é um Local Atual.

3. Selecione a guia **Entradas de alarme** para exibir as entradas de alarme adicionadas.
4. Clique na coluna Nome para entrar na página de Editar entrada de alarme.
5. Edite o nome de entrada do alarme.
6. Opcional: Para a entrada de alarme do dispositivo de controle de segurança, selecione **Tipo de detector** e **Tipo de zona** de acordo com a real implementação.
7. Edite as configurações de evento da entrada de alarme. Consulte **Configuração de eventos e alarmes** para obter mais informações.

Observação

Se nenhuma configuração de eventos tiver sido definida para a entrada de alarme, clique em **Configurações** para configurar os parâmetros.

8. Adicione a entrada de alarme ao mapa.
 - 1) Configure o interruptor **Adicionar ao mapa** como ligado.
 - 2) Selecione o ícone estilo e cor do nome para exibir a entrada de alarme no mapa.
9. Clique em **Salvar**.

11.3.4 Edição de saída de alarme para o Local Atual

Edite informações básicas e configurações de mapa da saída de alarme para o Local Atual.

Execute esta tarefa quando precisar editar saída de alarme para o Local Atual.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. No painel com a lista de áreas, selecione o Local Atual adicionado na lista suspensa de locais para exibir as áreas.

 **Observação**

O ícone  indica que o local é um Local Atual.

3. Selecione a guia **Saídas de alarme** para exibir as saídas de alarme adicionadas.
4. Clique na coluna Nome para entrar na página de Editar saída de alarme.
5. Edite o nome de saída do alarme.
6. Adicione a saída de alarme ao mapa.
 - 1) Configure o interruptor **Adicionar ao mapa** como ligado.
 - 2) Selecione o ícone estilo e cor do nome para exibir a saída de alarme no mapa.
7. Clique em **Salvar**.

11.3.5 Edição de sistemas de vigilância sob veículos para o Local Atual

Edite as informações básicas, câmeras relacionadas e configurações de mapas no sistema de vigilância sob veículos (UVSS) para o Local Atual.

Execute esta tarefa quando precisar editar UVSS para o Local Atual.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. No painel com a lista de áreas, selecione o Local Atual adicionado na lista suspensa de locais para exibir as áreas.

 **Observação**

O ícone  indica que o local é um Local Atual.

3. Selecione uma área.
4. Selecione a guia **Sistema de vigilância sob veículos** para exibir os UVSSs adicionados.

 **Observação**

Se a função de mapa estiver ativada, clique em  e clique em **UVSSs**.

5. Clique na coluna Nome para entrar na página de Editar UVSS.
6. Edite as informações básicas de UVSS, como endereço IP, número de entrada e assim por diante.
7. Vinculação de câmeras a UVSS.
 - 1) Configure o interruptor **Relacionar câmera** como ligado.
 - 2) Selecione a câmera.
8. Adicione UVSS ao mapa.
 - 1) Configure o interruptor **Adicionar ao mapa** como ligado.
 - 2) Selecione o ícone estilo e cor do nome para exibir o UVSS no mapa.
9. Clique em **Salvar**.

11.3.6 Editar elemento para o Local Remoto

Se o sistema atual for um Sistema Central com um módulo de Gerenciamento do Local Remoto, edite as câmeras adicionadas provenientes do Local Remoto.

Execute esta tarefa quando precisar editar os parâmetros de câmera para o Local Remoto.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. No painel com a lista de áreas, selecione o Local Remoto adicionado na lista suspensa de locais para exibir as áreas.

Observação

O ícone  indica que o local é um Local Remoto.

3. Selecione uma área para exibir suas câmeras adicionadas.
4. Clique no campo Nome para editar os parâmetros das câmeras, incluindo informações básicas e configurações de gravações.

Observação

Para configurações de gravações, se nenhuma configuração de gravações tiver sido definida para a câmera, clique em **Configurações** para definir os parâmetros (para obter mais informações, consulte **Configuração de gravações para câmeras em Local Remoto**).

5. Opcional: Clique em  para visualizar a exibição em tempo real da câmera e passar o mouse pela janela e clique em  no canto inferior direito para alternar para reprodução.

Observação

As funções de exibição em tempo real e reprodução na página de detalhes da câmera são permitidas somente pelo Internet Explorer.

6. Opcional: Clique em **Copiar para** para copiar os parâmetros atuais especificados de configuração da câmera para outras câmeras do Local Remoto.
7. Clique em **Salvar**.

11.4 Remover elemento de área

Remova as câmeras adicionadas, entradas de alarme, saídas de alarme, portas e sistemas de vigilância sob veículos (UVSSs) da área.

11.4.1 Remoção de elementos da área para o Local Atual

Remova as câmeras adicionadas, entradas de alarme, saídas de alarme, portas e sistemas de

vigilância sob veículos (UVSSs) da área para o Local Atual.

Execute esta tarefa quando precisar remover o elemento da área para o Local Atual.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. Selecione uma área no painel com a lista de áreas para exibir seus elementos adicionados.

Observação

- Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o Local Atual na lista suspensa de locais para exibir suas áreas.
- O ícone  indica que o local é o Local Atual.

-
3. Selecione as câmeras, entradas de alarme, saídas de alarme, portas ou a guia UVSSs para exibir os elementos adicionados.
 4. Selecione os elementos.
 5. Clique em **Excluir**.

11.4.2 Remoção de elementos de uma área para o Local Remoto

Se o sistema atual for um Sistema Central com um módulo de Gerenciamento do Local Remoto, remova as câmeras adicionadas de sua área.

Execute esta tarefa quando precisar remover o elemento da área para o Local Remoto.

Etapas

1. Clique em **Exibição Lógica** na página inicial para entrar na página de Gerenciamento de Área.
2. No painel com a lista de áreas, selecione o Local Remoto adicionado na lista suspensa de locais para exibir as áreas.

Observação

O ícone  indica que o local é um Local Remoto.

-
3. Selecione uma área para exibir suas câmeras adicionadas.
 4. Selecione as câmeras.
 5. Clique em **Excluir**.
 6. Opcional: Se  aparecer perto do nome da câmera, significa que a câmera foi excluída do Local Remoto. Passe o cursor sobre  e clique em **Excluir** para excluir a câmera da área.

11.5 Configuração do modelo de agendamento de defesa

O agendamento de defesa define o modo de armar em diferentes períodos de tempo para as partições dos dispositivos de controle de segurança adicionados. Defina um agendamento semanal para períodos de tempo de agendamento para permanência de armar, armar

instantaneamente ou armar à distância em uma semana. O sistema predefine dois modelos padrão de agendamento de defesa: Modo para o dia todo e modelo para dias úteis. Adicione também um modelo personalizado de acordo com as reais necessidades.

Etapas

1. Clique em **Sistema** na página inicial e entre na página **Agendamento** → **Modelo de agendamento de defesa**.
2. Clique em **Adicionar** para entrar na página de adicionar modelo de agendamento de defesa.
3. Preencha as informações solicitadas.

Nome

Defina um nome para o modelo.

Copiar de

Opcionalmente, selecione copiar as configurações de outros modelos definidos.

4. Selecione um modo de armar e arraste na barra de tempo para desenhar um período de tempo.

Observação

Por padrão, o que se baseia em tempo é selecionado.

Armar instantaneamente

Utiliza-se quando as pessoas saem da área de detecção. A zona será acionada imediatamente quando detectar evento ou alarme sem atraso e notificar o pessoal da segurança.

Armar à distância

Utiliza-se quando as pessoas saem da área de detecção. Eventos ou alarmes serão ativados quando a zona for ativada ou adulterada. Para zona atrasada, o alarme não será ativado quando a zona detectar evento de ativação durante atraso de entrada/saída.

Permanecer armado

Utiliza-se quando as pessoas permanecem dentro da área de detecção. Durante permanência de armar, todas as detecções de arrombamentos no perímetro (como detector de perímetro, contatos magnéticos, detector de cortina em sacada) serão ativadas. Enquanto isso, detectores dentro da área de detecção serão desviados (como detectores PIR). As pessoas podem se mover dentro da área e não ativar eventos ou alarmes.

Observação

Podem ser configurados até 8 períodos de tempo a cada dia.

5. Opcional: Clique em **Apagar** e clique no período de tempo desenhado para limpar o período de tempo correspondente ao desenho.
6. Termine de adicionar o modelo de agendamento de defesa.
 - Clique em **Adicionar** para adicionar o modelo e retorne à página com a lista de modelos de agendamento de defesa.
 - Clique em **Adicionar e continuar** para adicionar o modelo e continue a adicionar outros

modelos.

O modelo de agendamento de defesa será exibido na lista de modelos de agendamento de defesa.

7. Opcional: Execute as seguintes operações depois de adicionar o modelo.

Exibir Detalhes do Modelo	Clique no modelo para exibir seus detalhes.
Edição do modelo	Clique em  na coluna Operação para editar detalhes do modelo (exceto modelos em uso).
Exclusão do modelo	Clique em  na coluna Operação para excluir o modelo.
Exclusão de todos os modelos	Clique em Excluir todos para excluir todos os modelos de agendamento (exceto os modelos padrão e os modelos em uso).

Capítulo 12 Configurando a gravação

As definições de gravação são para definir quando e como a gravação começa com os parâmetros pré-definidos. Você também pode definir as configurações de armazenamento para armazenar imagens importadas e imagens carregadas.

O HikCentral fornece quatro locais de armazenamento - armazenamento em dispositivos de codificação, Rede de Área de Armazenamento Híbrido, Servidor de Armazenamento em Nuvem ou pStor - para armazenar os arquivos de vídeo gravados das câmeras.

Dispositivo de codificação

Os dispositivos de codificação, incluindo os DVRs, NVRs e câmeras de rede, devem fornecer dispositivos de armazenamento, como HDDs, HDDs de Rede e cartões SD/SDHC para arquivos de vídeo. Os dispositivos de armazenamento recém-instalados precisam ser formatados. Vá para a página de configuração remota do dispositivo (**Physical View (Exibição física) → Configuration (Configuração)**), clique em **Storage (Armazenamento) → General (Geral)**, selecione o HD, cartão HD de Rede ou SD/SDHC, e clique em **Format (Formatar)** para inicializar o dispositivo de armazenamento selecionado.

Rede de área de armazenamento híbrido

Armazene os arquivos de vídeo na rede de área de armazenamento híbrido adicionada. Para obter detalhes sobre como adicionar a rede de área de armazenamento híbrido, consulte **Add Hybrid Storage Area Network (Adicionar rede de área de armazenamento híbrido)**.

Servidor de armazenamento em nuvem

Armazene os arquivos de vídeo no Servidor de armazenamento em nuvem adicionado. Para obter detalhes sobre como adicionar este servidor, consulte **Add Cloud Storage Server (Adicionar Servidor de Armazenamento em nuvem)**.

pStor

Armazene os arquivos de vídeo no pStor adicionado, que é o serviço de acesso ao armazenamento usado para gerenciar HDs locais e discos lógicos. Para detalhes sobre como adicionar o pStor, consulte **Add pStor (Adicionar pStor)**.

12.1 Configuração de gravações de câmeras em local atual

Para as câmeras no local atual, o HikCentral oferece quatro métodos de armazenamento (armazenamento em dispositivos de codificação, Rede de área de armazenamento híbrido, Servidor de armazenamento em nuvem ou pStor) para armazenar os arquivos de vídeo das câmeras de acordo com a programação de gravação configurada. Você pode obter as configurações de gravação do dispositivo ao adicionar a câmera a uma área.

Antes de começar

Os dispositivos de codificação precisam ser adicionados ao HikCentral para fins de gerenciamento

de área. Consulte **Gerenciamento de recursos** para obter as configurações detalhadas sobre adicionar dispositivos.

Execute esta tarefa quando precisar gravar vídeos das câmeras no local atual.

Etapas

1. Entre na página de configuração de gravação.
 - 1) Clique em **Logical View (Exibição lógica) → Camera (Câmeras)** para entrar na interface de Gerenciamento de área.
 - 2) Selecione uma área para exibir suas câmeras.
-

Observação

Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o local atual (marcado com o ícone ) na lista suspensa de locais para exibir suas câmeras.

- 3) Selecione uma câmera e clique no campo Name (Nome) para entrar na página Editar Câmera.

The screenshot shows the 'Camera 01' configuration page in the HikCentral Web Client. At the top, there is a back arrow, the title 'Camera 01', and links for 'Configuration on Device' and 'Copy to'. The 'Basic Information' section includes a text input for '*Name' (Camera 01) and a dropdown for '*Protocol Type' (TCP). Below this is a large black video player area with a play button. The 'Recording Settings' section features a 'Main Storage' slider (set to 'On'), a 'Get Device's Recording Settings' link, a '*Storage Location' dropdown (Encoding Device), a '*Recording Schedule Template' dropdown (All-day Event-based Template) with a 'View' button, a '*Stream Type' dropdown (Main Stream), a 'Pre-record' checkbox (unchecked), a '*Post-record' dropdown (10s), and a 'Video Expiration' slider (set to 'Off'). At the bottom, there is an 'Enable ANR' checkbox, a red 'Save' button, and a grey 'Cancel' button.

Figura 12-1 Editar página da câmera

2. Alterne o interruptor **Main Storage (Armazenamento principal)** para ligado.
3. Selecione o local de armazenamento para armazenar o arquivo de vídeo gravado.

Observação

Se você selecionar **Hybrid Storage Area Network (rede de área de armazenamento híbrido)**, **Cloud Storage Server (Servidor de armazenamento em nuvem)** ou **pStor**, especifique um servidor e (opcional) selecione um Servidor de Tipo de Fluxo (Stream Type) para obter o fluxo de vídeo da câmera através dele.

4. Selecione o tipo de armazenamento e configure os parâmetros necessários.
 - Selecione **Real-Time Storage (Armazenamento em Tempo Real)** como o tipo de local para armazenar os arquivos de vídeo gravados no local de armazenamento especificado em tempo

real.

Observação

Se você escolher **Encoding Device (Dispositivo de codificação)** como o local de armazenamento, você não precisa selecionar o tipo de armazenamento, mas configure os parâmetros seguintes como configurações de armazenamento em tempo real por padrão.

Modelo de programação de gravação

Configura o modelo que define quando gravar o vídeo da câmera.

Modelo com base em horário no dia inteiro

Grava o vídeo para o dia inteiro de maneira contínua.

Modelo com base em evento no dia inteiro

Grava o vídeo quando o alarme ocorre.

Adicionar Novo

Define o modelo personalizado. Para detalhes sobre como configurar um modelo personalizado, consulte *Configure Recording Schedule Template (Configurar o modelo de programação de gravação)*.

Exibir

Exibe os detalhes do modelo.

Observação

A programação de gravação baseada em eventos não pode ser configurada no **Cloud Storage Server (Servidor de armazenamento em nuvem)**, e o cronograma de gravação baseado em comando não pode ser configurado no **Cloud Storage Server (Servidor de armazenamento em nuvem)** e pStor.

Tipo de transmissão

Selecione o tipo de transmissão para transmissão principal, transmissão secundária ou transmissão dupla.

Observação

Para armazenar na Hybrid Storage Area Network (rede de área de armazenamento híbrido), Cloud Storage Server (Servidor de armazenamento em nuvem) ou pStor, a transmissão dupla não é suportada.

Pré-gravação

Grava vídeos de períodos que precedem eventos detectados. Por exemplo, quando alguém abre uma porta, você pode ver o que acontece logo antes da porta se abrir.

Este campo é exibido quando o local de armazenamento é definido como Encode Device

(Dispositivo de codificação) ou pStor e está disponível para a câmera que esteja configurada com gravação baseada em evento.

Pós-gravação

Grava vídeos de períodos após eventos detectados.

Este campo é exibido quando o local de armazenamento é definido como Encode Device (Dispositivo de codificação) ou Hybrid Storage Area Network (rede de área de armazenamento híbrido). Está disponível para a câmera que está configurada com gravação baseada em evento.

Validade do vídeo

Se você selecionar Encoding Device (Dispositivo de codificação) como local de armazenamento, defina a opção Video Expiration (Validade de vídeo) para ON (ligado) e insira o(s) dia(s) de validade.

Exclua automaticamente os vídeos mais antigos após o período de retenção especificado. Esse método permite definir o período mais longo de tempo para manter os vídeos conforme desejado e o período de retenção real para os vídeos depende da cota alocada.

Ativar ANR

Se você selecionar Encoding Device (Dispositivo de codificação) ou Hybrid Storage Area Network (rede de área de armazenamento híbrido) como local de armazenamento, marque Enable ANR (Habilitar ANPR) para ativar o reabastecimento automático de rede para armazenar temporariamente o vídeo na câmera quando a rede falhar e transportar o vídeo para o dispositivo de armazenamento quando a rede se recuperar.

- Selecione **Scheduled Uploading (Carregamento programado)** como o tipo de armazenamento para carregar os arquivos de vídeo gravados do dispositivo de codificação ou pStor para o local de armazenamento especificado de acordo com o período programado.



Observação

- Certifique-se de ter configurado a programação de gravação armazenada no dispositivo de armazenamento local ou pStor para armazenamento auxiliar primeiro. Caso contrário, o carregamento da programação não será configurável.
 - As gravações só podem ser enviadas do dispositivo de codificação para a Rede de Área de Armazenamento híbrido, o Servidor de Armazenamento em Nuvem ou o pStor, ou de pStor para outro pStor.
-

Carregar intervalo

Especifique o período de tempo para carregar os arquivos de vídeo gravados no local de armazenamento especificado durante o período.

Gravar para carregamento

Selecione o tipo de arquivo de vídeo gravado para backup.

5. Opcional: Defina **Auxiliary Storage (Armasenamento auxiliar)** para ON (ligado) e configure outro local de armazenamento para os arquivos de vídeo.

Observação

- Se o Servidor de Armazenamento em Nuvem, a Rede de Área de Armazenamento híbrido ou pStor estiverem definidos como o local de armazenamento auxiliar, você poderá selecionar Real-Time Storage (Armazenamento em tempo real) para armazenar arquivos de vídeos gravados ou selecionar Scheduled Uploading (Carregamento programado) para carregar gravações do dispositivo de codificação ou pStor (armazenamento principal) para o local de armazenamento auxiliar especificado de acordo com o período programado.
 - Antes de configurar o **Scheduled Uploading (carregamento programado)**, certifique-se de ter configurado a programação de gravações em tempo real armazenado no objeto local do dispositivo ou o pStor do objeto principal.
 - As gravações só podem ser enviadas do dispositivo de codificação para a Rede de Área de Armazenamento híbrido, o Servidor de Armazenamento em Nuvem ou o pStor, ou de pStor para outro pStor.
-

6. Clique em **Salvar**.

12.2 Configuração de gravações de câmeras em local remoto

Você pode definir a programação de gravação para gravar o vídeo de câmeras em locais remotos e lojas nos Servidores de Gravação do Sistema Central (Rede de Área de Armazenamento Híbrido, Servidor de Armazenamento em Nuvem ou pStor).

Execute esta tarefa quando precisar gravar vídeos de câmeras em local remoto.

Etapas

1. Entre na página de configuração de gravação.
 - 1) Clique em **Logical View (Exibição lógica) → Camera (Câmeras)** para entrar na interface de Gerenciamento de área.
 - 2) Selecione o modelo do local remoto adicionado na lista suspensa.
-

Observação

O ícone  indica que o local é um Local Remoto.

- 3) Selecione uma área para exibir suas câmeras.
- 4) Selecione uma câmera e clique no campo **Name (Nome)** para entrar na página Editar Câmera.
- 5) Na área Configurações de gravação, defina **Storage in Central System (Armazenamento no Sistema Central)** para ON (ativado) para mostrar a área de definição da gravação.

The screenshot shows the configuration page for 'Camera 06' in the HikCentral Web Client. The page is titled 'Camera 06' and includes a 'Configuration on Site' icon and a 'Copy to' button. The main content is divided into two sections: 'Basic Information' and 'Recording Settings'. In the 'Basic Information' section, the 'Name' is set to 'Camera 06' and the 'Protocol Type' is set to 'TCP'. Below this is a video player area with a play button and a message: 'The camera element does not exist. {Er...'. The 'Recording Settings' section includes a 'Storage in Central System' progress bar, a 'Storage Location' dropdown set to 'Hybrid Storage Area Network' with a server dropdown set to 'CVR_10.41.7.232'. Below this is a storage status box for 'RV_1' showing '250.8GB Free of 802.3GB'. The 'Storage Type' is set to 'Real-Time Storage' (selected) with 'Scheduled Uploading' as an option. The 'Recording Schedule Template' is set to 'All-day Time-based Template' with a 'View' button. The 'Stream Type' is set to 'Main Stream', 'Post-record' is set to '10s', and 'Streaming Server' is set to '10.18.64.32'. At the bottom, there is an 'Enable ANR' checkbox, a red 'Save' button, and a grey 'Cancel' button.

Figura 12-2 Adicionar Página de Configurações de Gravação

2. Selecione o local de armazenamento para armazenar o arquivo de vídeo gravado.

Observação

Você pode selecionar **Hybrid Storage Area Network (rede de área de armazenamento híbrido)**, **Cloud Storage Server (Servidor de armazenamento em nuvem)** ou **pStor**, especificar um servidor e (opcional) selecionar um Servidor de Tipo de Fluxo (Stream Type) para obter o fluxo de vídeo da câmera através dele.

3. Selecione o tipo de armazenamento e configure os parâmetros necessários.

- Selecione **Real-Time Storage (Armazenamento em Tempo Real)** como o tipo de local para armazenar os arquivos de vídeo gravados no local de armazenamento especificado em tempo real.

Observação

Se você escolher **Encoding Device (Dispositivo de codificação)** como o local de armazenamento, você não precisa selecionar o tipo de armazenamento, mas configure os parâmetros seguintes como configurações de armazenamento em tempo real por padrão.

Modelo de programação de gravação

Configura o modelo que define quando gravar o vídeo da câmera.

Modelo com base em horário no dia inteiro

Grava o vídeo para o dia inteiro de maneira contínua.

Modelo com base em evento no dia inteiro

Grava o vídeo quando o alarme ocorre.

Adicionar Novo

Define o modelo personalizado. Para detalhes sobre como configurar um modelo personalizado, consulte *Configure Recording Schedule Template (Configurar o modelo de programação de gravação)*.

Exibir

Exibe os detalhes do modelo.

Tipo de transmissão

Selecione o tipo de transmissão para transmissão principal, transmissão secundária ou transmissão dupla.

Observação

Para armazenar na Hybrid Storage Area Network (rede de área de armazenamento híbrido), Cloud Storage Server (Servidor de armazenamento em nuvem) ou pStor, a transmissão dupla não é suportada.

Pré-gravação

Grava vídeos de períodos que precedem eventos detectados. Por exemplo, quando alguém abre uma porta, você pode ver o que acontece logo antes da porta se abrir.

Este campo é exibido quando o local de armazenamento é definido como Cloud Storage Server (Servidor de armazenamento em nuvem) e está disponível para a câmera que esteja configurada com gravação baseada em evento.

Pós-gravação

Comece a gravar o vídeo a partir de períodos após os eventos detectados.

Este campo é exibido quando o local de armazenamento é definido como Rede de área de armazenamento híbrida e está disponível para a câmera que esteja configurada com gravação baseada em evento.

Servidor de transmissões

Opcionalmente, selecione Streaming Server (Servidor de transmissões) para obter o fluxo de vídeo da câmera através dele.

Ativar ANR

Se você selecionar o Local de Armazenamento como Rede de Área de Armazenamento Híbrida, marque Ativar ANR para ativar o reabastecimento automático de rede para armazenar temporariamente o vídeo na câmera quando a rede desconectar e transportar o vídeo para a Rede de Armazenamento Híbrida quando a rede for recuperada.

- Selecione Scheduled Uploading (Carregamento programado) como tipo de armazenamento e especifique o período, armazenamento principal / auxiliar, tipo de gravação e velocidade de carregamento para carregar os arquivos de vídeo gravados do armazenamento local do dispositivo ou pStor no site remoto de acordo com o período programado.

Observação

Certifique-se de que você configurou a programação de gravação armazenada no dispositivo de codificação ou o pStor da câmera no local remoto.

4. Clique em **Salvar**.

12.3 Configurar armazenamento de imagens importadas

As imagens importadas pelos usuários, como as imagens originais de material rodante importadas na página Vehicle, as imagens de mapas estáticos, as imagens de rosto na lista de pessoas, podem ser armazenadas no HDD do servidor VSM.

Antes de começar

Certifique-se de que você tenha pelo menos 1GB de espaço livre para armazenamento de fotos.

Execute esta tarefa quando precisar armazenar as imagens importadas.

Etapas

1. Faça o login no Web Client em execução no servidor VSM.
2. Clique em System (Sistema) → Storage (Armazenamento) → Storage on VSM Server (Armazenamento no servidor VSM) para entrar no armazenamento na página do servidor VSM.

Observação

Este módulo exibe quando o Web Client corrente está sendo executado no servidor VSM.

Os discos do servidor VSM são exibidos com o espaço livre e a capacidade total.

3. Selecione o HD para armazenar as fotos importadas.
4. Opcional: Defina Restrict Quota for Pictures (restringir cota para fotos) para ON (ativado) para alocar a cota para armazenar as imagens.
5. Clique em **Salvar**.

12.4 Configurar armazenamento para imagens carregadas

As imagens carregadas dos dispositivos, como imagens disparadas por alarme, imagens de rosto capturadas e imagens de licença de placa capturadas, podem ser armazenadas no HD do servidor VSM, na rede de área de armazenamento híbrida, no servidor de armazenamento em nuvem ou no pStor.

Execute esta tarefa quando precisar armazenar as imagens carregadas dos dispositivos.

Etapas

1. Entre na página de configuração de armazenamento de fotos.
 - 1) Clique em **Logical View (Exibição lógica) → Camera (Câmeras)** para entrar na interface de Gerenciamento de área.
 - 2) Selecione uma área para exibir suas câmeras.

Observação

Para um Sistema Central com um módulo de Gerenciamento do Local Remoto, selecione o local atual (marcado com o ícone ) na lista suspensa de locais para exibir suas câmeras.

- 3) Selecione uma câmera e clique no campo Name (Nome) para entrar na página Editar Câmera.
2. Defina **Picture Storage (armazenamento de fotos)** para ON (ativado) para habilitar o armazenamento de fotos para a câmera.
3. Selecione o local de armazenamento na lista suspensa.

Observação

- Se você selecionar Video Surveillance Management (Gerenciamento de videomonitoramento), as imagens serão armazenadas no servidor VSM. Clique em **Configuration (Configuração)** para exibir o disco no servidor VSM e a cota de armazenamento, que pode ser editada por meio do Web Client em execução no servidor VSM. Consulte **Configure Storage for Imported Pictures (Configurar o armazenamento de imagens importadas)** para obter mais detalhes.
 - Você não pode configurar o local de armazenamento das imagens de material circulante capturadas, que são armazenadas no dispositivo UVSS.
-

4. Clique em **Save (Salvar)** para salvar  salvar as fotos enviadas no local especificado.

12.5 Configuração do modelo de programação de gravação

A programação de gravação é um gerenciamento de tempo para gravação de vídeo. Você pode configurar as programações de gravação para gravar vídeo em um determinado período. Dois programas de gravação padrão estão disponíveis: Modelo baseado no tempo o dia todo e Modelo baseado em eventos o dia todo. O Modelo baseado no tempo o dia todo pode ser usado para gravar vídeos durante o dia todo continuamente, e o Modelo baseado em eventos o dia todo é para gravar vídeos quando o alarme é acionado. Você também pode personalizar a programação

de gravação.

Execute esta tarefa quando precisar personalizar a programação para gravar os arquivos de vídeo.

Etapas

1. Clique em **System (Sistema)** na página inicial e acesse a página **Schedule (Programação) → Recording Schedule Template (Modelo de programação de gravação)**.
 2. Clique em **Add (Adicionar)** para adicionar a página de programação de gravação.
-

Observação

Podem ser adicionados até 32 modelos.

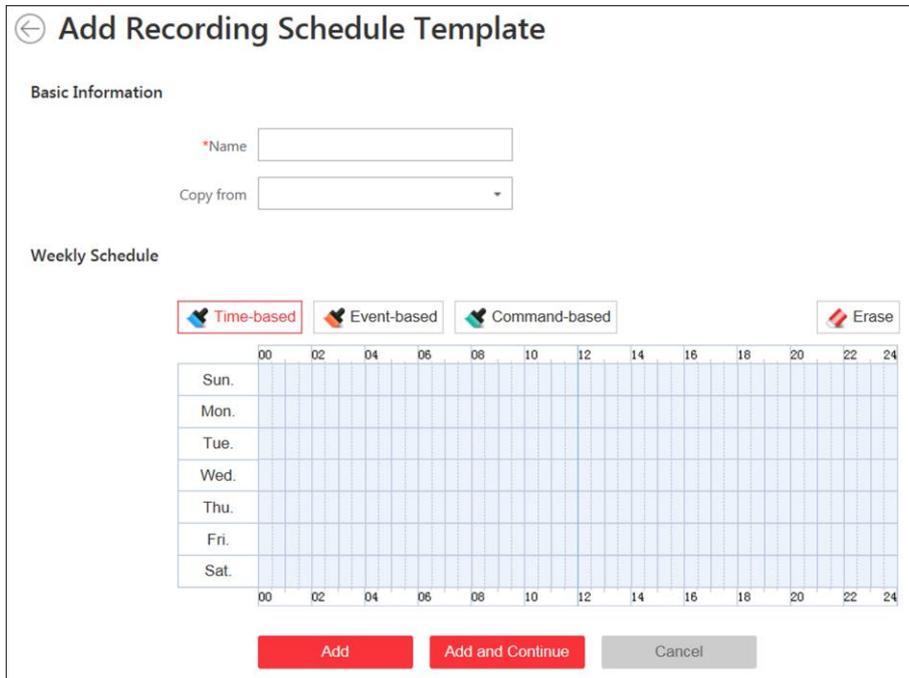


Figura 12-3 Adicionar página de modelo de programação de gravação

3. Preencha as informações solicitadas.

Nome

Defina um nome para o modelo.

Copiar de

Opcionalmente, selecione copiar as configurações de outros modelos definidos.

4. Selecione um tipo de gravação e arraste na barra de tempo para determinar um período de tempo.
-

Observação

Por padrão, o que se baseia em tempo é selecionado.

Baseado em horário

Gravação contínua de acordo com o horário que você definiu. A barra de tempo da programação fica marcada em azul.

Baseado em evento

Gravação acionada pelo alarme (p. ex., alarme, entrada de alarme ou alarme de detecção de movimento). A barra de horário da programação fica marcada em laranja.

Baseado em comando

A gravação é acionada pelo comando ATM. A barra de horário da programação fica marcada em verde.

Observação

Até 8 períodos de tempo podem ser definidos para cada dia na programação de gravação.

5. Opcional: Clique em **Erase** (Apagar) e clique na barra de horário para limpar o período de tempo.
6. Termine de adicionar o modelo.
 - Clique em **Add (Adicionar)** para adicionar o modelo e retornar à página de lista de modelos de programação de gravação.
 - Clique em **Add and Continue (Adicionar e continuar)** para salvar as configurações e continuar a adicionar outros modelos.
7. Opcional: Execute as seguintes operações na página da lista de modelos de programação de gravação.

Exibir detalhes do modelo	Clique no modelo para marcar as configurações detalhadas.
Edição do modelo	Clique em  na coluna de operação para editar detalhes do modelo (exceto os modelos em uso).
Exclusão do modelo	Clique em  na coluna Operação para excluir o modelo.
Exclusão de todos os modelos	Clique em Excluir todos para excluir todos os modelos de agendamento (exceto os modelos padrão e os modelos em uso).

Capítulo 13 Configurar evento e alarme

Você pode definir as ações de ligação para os eventos e alarmes detectados. As informações detalhadas dos eventos e alarmes podem ser recebidas e verificadas através do Control Client e do Mobile Client.

Eventos

Eventos podem ser divididos em:

Evento monitorado pelo sistema

O sinal que o recurso (por exemplo, câmera, dispositivo, servidor) envia quando algo ocorre. O sistema pode acionar ações de vinculação (como gravação, captura, envio de email, etc.) para registrar o evento recebido para verificação.

Evento genérico

O sinal que o recurso (p. ex., outro software, dispositivo) envia quando algo ocorre e pode ser recebido na forma de pacotes de dados TCP ou UDP, que o sistema pode analisar e gerar eventos se eles corresponderem à expressão configurada.

Evento definido pelo usuário

O evento definido pelo usuário pode ser usado para:

- O usuário pode acionar um evento definido pelo usuário manualmente no módulo Monitoramento e Central de Alarme no Control Client ao visualizar o vídeo ou verificar as informações de alarme.
- Um evento definido pelo usuário pode acionar um alarme, se configurado.
- Um alarme será armado ou desarmado quando o evento definido pelo usuário for acionado.
- Um alarme pode ser acionado por um evento definido pelo usuário como ações de alarme.

Alarme

O alarme é usado para notificar o pessoal de segurança sobre a situação específica que ajuda a lidar com a situação imediatamente. Um alarme pode acionar uma série de ações de vinculação (p. ex., janela pop-up) para notificação e manuseio de alarmes.

Ação de vinculação

Você pode definir ações de vinculação para eventos e alarmes.

- As ações de vinculação de um evento são usadas para registrar os detalhes do evento (como gravação e captura) e acionar ações básicas (como vincular o ponto de acesso a bloqueio ou desbloqueio, acionamento de saída de alarme, envio de email, etc.).
- As ações de vinculação de um alarme são usadas para registrar os detalhes do alarme e fornecer aos destinatários várias maneiras de exibir informações de alarme para reconhecimento e manuseio de alarmes, como janela pop-up, smart wall, aviso sonoro, etc.

13.1 Configurar evento monitorado pelo sistema

Evento monitorado pelo sistema é o sinal que o recurso (por exemplo, dispositivo, câmera, servidor) envia quando algo ocorre. O sistema pode receber e registrar eventos para verificação e também pode acionar uma série de ações de vinculação para notificação. O evento também pode acionar um alarme para novas ações de notificação e vinculação (como destinatários de alarme, janela pop-up no Control Client, exibição no Smart Wall, etc.). Você pode verificar o vídeo relacionado ao evento e as imagens capturadas através do Control Client, se você definir a gravação e a captura como vinculação do evento.

Suporta os seguintes tipos de evento:

- **Evento de câmera:** refere-se à exceção de vídeo ou ao evento detectado na área de monitoramento da câmera, como detecção de movimento, perda de vídeo, atravessamento de linha e assim por diante.
- **Evento de ponto de acesso:** o evento de controle de acesso acionado no ponto de acesso, como evento de acesso, evento de status da porta etc.
- **Evento de entrada de alarme:** o evento acionado pela entrada de alarme.
- **Evento ANPR:** o evento correspondente da placa de licença e evento incompatível detectado pela câmera ANPR ou UVSS.
- **Evento pessoa:** o evento de combinação de face e evento incompatível detectado pela câmera de reconhecimento facial.
- **Evento UVSS:** o evento acionado pelo UVSS, inclusive ficando on-line ou off-line.
- **Evento de local remoto:** o evento acionado pelo Local Remoto adicionado, incluindo o local ficando offline.
- **Evento de dispositivo:** o evento acionado por dispositivo de codificação, dispositivo de controle de acesso, exceção do painel de controle de segurança.
- **Evento do servidor:** os eventos acionados pelo Servidor de Gravação, Servidor de Fluxo ou o Servidor HikCentral.
- **Evento do usuário:** o evento acionado pelos usuários do sistema, incluindo login e logout do usuário.
- **Evento genérico:** o evento acionado pelo evento genérico adicionado no sistema.
- **Evento definido pelo usuário:** o evento acionado pelo evento definido pelo usuário adicionado no sistema.

13.1.1 Adicionar evento para a câmera

Você pode adicionar um evento para as câmeras no local atual. Quando o evento é acionado na câmera, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute esta tarefa quando você precisar adicionar um evento monitorado pelo sistema acionado pelas câmeras no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.

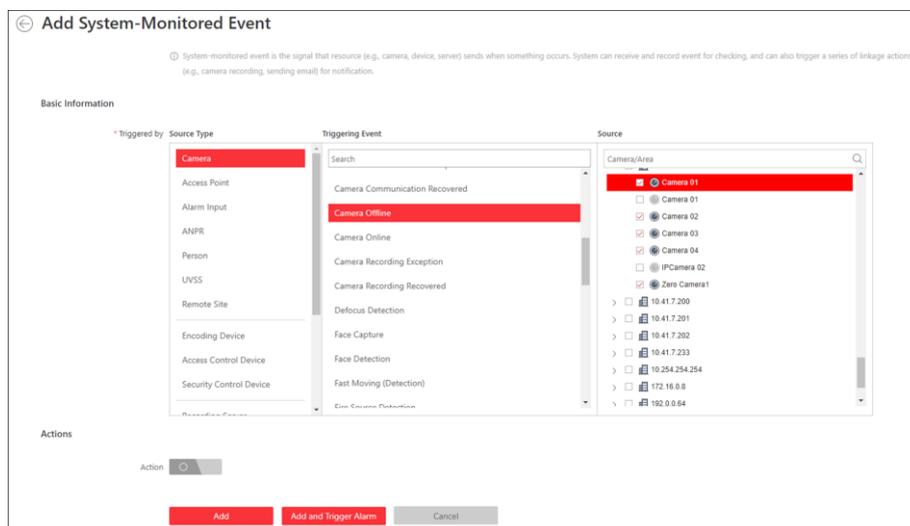


Figura 13-1 Adicionar um Evento Monitorado Pelo Sistema

2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de fonte como Câmera.

Acionamento de evento

O evento detectado na câmera acionará um evento monitorado pelo sistema no sistema.

Origem

A(s) câmera(s) específica(s) que pode(m) acionar este evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

A câmera é armada durante o horário de armação e o evento de disparo ocorrido na câmera durante o programa de armação irá acionar as ações de vinculação configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Selecione a câmera para gravar o vídeo quando o evento ocorrer. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a própria câmera de origem para gravação, selecione Source Camera (Câmera

de origem) e selecione o local de armazenamento para armazenar os arquivos de vídeo.

- Para acionar outras câmeras, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Grava vídeos de períodos após eventos detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o evento parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Selecione a(s) câmera(s) para gravar vídeo quando o evento ocorrer e adicione uma tag ao vídeo acionado por evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

- Para acionar a própria câmera de origem para gravação com tag, selecione Source Camera (Câmera de origem) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras por gravação com tag, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a própria câmera de origem para capturar fotos, selecione Source Camera (Câmera de origem).
- Para acionar outra câmera para capturar fotos, selecione **Specified Camera (Câmera especificada)** e selecione uma câmera para capturar fotos.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos para definir quando a câmera

irá capturar imagens para o evento. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

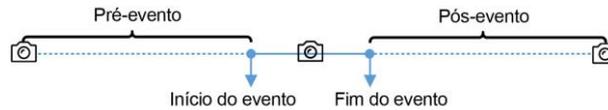


Figura 13-2 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

Observação

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

Observação

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte *Definir modelo de e-mail*.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte *Configurar o evento definido pelo usuário*.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte *Configurar Alarme*.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

Observação

Para obter mais detalhes, consulte *Configurar Alarme*.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.2 Adicionar evento para ponto de acesso

Você pode adicionar um evento para os pontos de acesso no sistema. Quando o evento é acionado no ponto de acesso, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (p. ex., envio de email) para notificação.

Execute esta tarefa quando você precisar adicionar um evento monitorado pelo sistema acionado pelo ponto de acesso no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **Ponto de Acesso**.

Acionamento de evento

O evento detectado no ponto de acesso acionará o evento monitorado pelo sistema no sistema.

Origem

Ponto(s) de acesso específico(s) que podem acionar esse evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O ponto de acesso é armado durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.



Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Selecione a câmera para gravar o vídeo quando o evento ocorrer. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a(s) câmera(s) relacionada(s) do ponto de acesso para gravação, selecione **Source Related Camera (Câmera de origem relacionada)** e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento,

você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Selecione a câmera para gravar vídeo quando o evento ocorrer e adicione uma tag ao vídeo acionado por evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

- Para acionar a(s) câmera(s) relacionada(s) do ponto de acesso para gravação com tag, selecione Source Related Camera (Câmera de origem relacionada) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras por gravação com tag, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).



Figura 13-3 Captura de fotos

 **Observação**

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

 **Observação**

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

 **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte *Definir modelo de e-mail*.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
- Para definir o evento definido pelo usuário, consulte *Configurar o evento definido pelo usuário*.

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.3 Adicionar evento para entrada de alarme

Você pode adicionar um evento para as entradas de alarme do sistema. Quando a entrada de alarme é acionada, o sistema pode receber e gravar eventos para verificar e acionar uma série de ações de vinculação (por exemplo, envio de e-mail) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelas entradas de alarme no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.

- Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **Entrada de alarme**.

Acionamento de evento

O evento detectado na entrada de alarme acionará os eventos monitorados pelo sistema no sistema.

Origem

A(s) entrada(s) de alarme específica(s) que pode(m) acionar este evento.

- Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

A entrada de alarme é armada durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a(s) câmera(s) para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a(s) câmera(s) para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é

possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

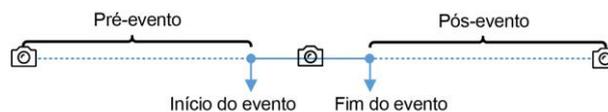


Figura 13-4 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

 **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte ***Definir modelo de e-mail***.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte ***Configurar o evento definido pelo usuário***.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte ***Configurar Alarme***.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte ***Configurar Alarme***.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s)

selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.4 Adicionar evento para a câmera ANPR

Você pode adicionar um evento para as câmeras que possuem a função ANPR (Reconhecimento Automático de Placas Numéricas) (como câmeras ANPR e UVSS) no sistema. Quando os números reconhecidos da placa coincidirem ou não corresponderem aos números da placa na lista de veículos, o sistema pode receber e registrar eventos para verificação e acionar uma série de ações de ligação (por exemplo, envio de e-mail) para notificação.

Execute esta tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pela câmera ANPR no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **ANPR**.

Acionamento de evento

Selecione a lista de veículos que acionará o evento correspondido da placa de veículo correspondente / incompatível.

Origem

As câmeras ANPR específicas que podem acionar esse evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

A câmera ANPR é armada durante a programação de armação e a placa de veículo correspondente ou incompatível, reconhecida durante a programação de armação, acionará as ações de vínculo configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Selecione a câmera para gravar o vídeo quando o evento ocorrer. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a câmera de origem (quando a fonte é a câmera ANPR) ou acionar a câmera relacionada à fonte (quando a fonte é UVSS) para gravação, selecione Câmera Fonte ou Câmera Relacionada e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Visualizar vídeo pré-evento: Se a câmera tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Selecione a(s) câmera(s) para gravar vídeo quando o evento ocorrer e adicione uma tag ao vídeo acionado por evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

- Para acionar a câmera de origem (quando a fonte é a câmera ANPR) ou acionar a câmera relacionada à fonte (quando a fonte é UVSS) para gravação com tag, selecione Câmera Fonte ou Câmera Relacionada e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras por gravação com tag, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Você pode inserir o nome como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a câmera de origem (quando a fonte é a câmera ANPR) ou acionar a câmera relacionada à fonte (quando a fonte é UVSS) para imagens capturadas, selecione Câmera Fonte ou Câmera Relacionada.
- Para acionar outra câmera para capturar fotos, selecione **Specified Camera (Câmera especificada)** (opcional) e selecione uma câmera para capturar fotos.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

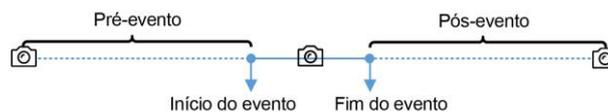


Figura 13-5 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

 **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte ***Definir modelo de e-mail***.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte ***Configurar o evento definido pelo usuário***.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte ***Configurar Alarme***.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte ***Configurar Alarme***.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s)

selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.5 Adicionar evento por pessoa

Você pode adicionar um evento correspondido e incompatível à câmera de reconhecimento facial adicionada no sistema. Quando a câmera reconhece um rosto de pessoa correspondente ou incompatível, o sistema pode receber e registrar eventos para verificar e acionar uma série de ações de vinculação (por exemplo, envio de e-mail) para notificação.

Execute esta tarefa quando você precisar adicionar um evento monitorado pelo sistema acionado pelas pessoas no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **Pessoa**.

Acionamento de evento

Selecione o grupo de comparação facial que acionará o evento correspondente de rosto correspondente / incompatível.

Origem

A(s) câmera(s) específica(s) que pode(m) acionar este evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

A câmera de reconhecimento facial é armada durante a programação de armação e a placa de veículo correspondente ou incompatível, reconhecida durante a programação de armação, acionará as ações de vínculo configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Selecione a câmera para gravar o vídeo quando o evento ocorrer. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a própria câmera de reconhecimento facial para gravação, selecione Source Camera (Câmera de origem) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Visualizar vídeo pré-evento: Se a câmera tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Selecione a câmera para gravar vídeo quando o evento ocorrer e adicione uma tag ao vídeo acionado por evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

- Para acionar a própria câmera de reconhecimento facial para gravação com tag, selecione Source Camera (Câmera de origem) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras por gravação com tag, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as

imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a própria câmera de reconhecimento facial para capturar fotos, selecione Source Camera (Câmera de origem).
- Para acionar outra câmera para capturar fotos, selecione **Specified Camera (Câmera especificada)** e selecione uma câmera para capturar fotos.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).



Figura 13-6 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

Observação

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s)

automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

Observação

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

Observação

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.6 Adicionar eventos monitorados no sistema ao UVSS

Você pode adicionar um evento ao UVSS no sistema. Quando o evento é acionado no UVSS, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelo UVSS no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **UVSS**.

Acionamento de evento

O evento detectado na entrada de alarme acionará os eventos monitorados pelo sistema no sistema.

Origem

O(s) UVSS(s) específico(s) que pode(m) acionar este evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O UVSS é armado durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.



Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Selecione a câmera para gravar o vídeo quando o evento ocorrer. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a(s) câmera(s) relacionada(s) do UVSS para gravação, selecione Source Related Camera (Câmera de origem relacionada) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Visualizar vídeo pré-evento: Se a câmera tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Selecione a(s) câmera(s) para gravar vídeo quando o evento ocorrer e adicione uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

- Para acionar a(s) câmera(s) relacionada(s) do UVSS para gravação com tag, selecione Source Related Camera (Câmera de origem relacionada) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para acionar outras câmeras por gravação com tag, selecione **Specified Camera (Câmera especificada)** e clique em **Add (Adicionar)** para adicionar outras câmeras. Selecione o local de armazenamento para armazenar os arquivos de vídeo.

Você pode inserir o nome como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

- Para acionar a câmera relacionada do UVSS para capturar fotos, selecione Source Camera (Câmera de origem).
- Para acionar outra câmera para capturar fotos, selecione **Specified Camera (Câmera especificada)** (opcional) e selecione uma câmera para capturar fotos.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

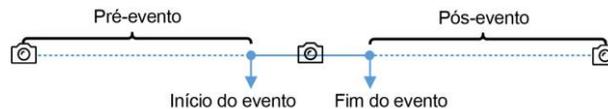


Figura 13-7 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

Observação

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as

condições.

13.1.7 Adicionar evento para site remoto

Você pode adicionar um evento para os sites remotos gerenciados no sistema. Quando o site remoto fica offline, o sistema central pode receber e registrar eventos para verificar e acionar uma série de ações de vinculação (por exemplo, envio de e-mail) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelo site remoto offline no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **Site remoto**

Acionamento de evento

Se o site remoto ficar offline, ele acionará um evento monitorado pelo sistema no sistema central.

Origem

O(s) recurso(s) específico(s) que pode(m) acionar este evento.

Observação

Para o tipo de origem do evento genérico e o evento definido pelo usuário, você deve selecionar o evento genérico configurado ou o evento definido pelo usuário como a origem do evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O site remoto é armado durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a câmera para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode

reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmera tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a câmera para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

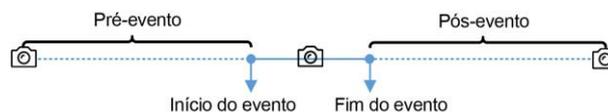


Figura 13-8 Captura de fotos

 **Observação**

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

 **Observação**

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

 **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
- Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.8 Adicionar evento para dispositivo de codificação

Você pode adicionar um evento aos dispositivo de codificação do sistema. Quando o evento é acionado no dispositivo, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelos dispositivos de codificação no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.

- Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **dispositivo de codificação**.

Acionamento de evento

O evento detectado no dispositivo de codificação acionará os eventos monitorados pelo sistema no sistema.

Origem

O(s) dispositivo(es) específico(s) que pode(m) acionar este evento.

- Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

A origem do evento é armada durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.



Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a(s) câmera(s) para gravar vídeo, quando o evento ocorre. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a câmera para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Você pode inserir o nome como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos

antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

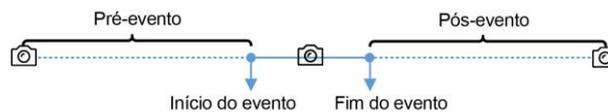


Figura 13-9 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

Observação

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

Observação

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

Observação

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o

cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.9 Adicionar evento para o dispositivo de controle de acesso

Você pode adicionar um evento aos dispositivos de controle de acesso do sistema. Quando o evento é acionado no dispositivo, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute esta tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelos dispositivos de controle de acesso no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **dispositivo de controle de acesso**.

Acionamento de evento

O evento detectado no dispositivo de controle de acesso acionará os eventos monitorados pelo sistema no sistema.

Origem

O(s) dispositivo(s) de controle de acesso específico(s) que pode acionar este evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O dispositivo de controle de acesso é armado durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a(s) câmera(s) para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a(s) câmera(s) para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.



Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

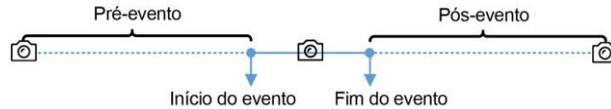


Figura 13-10 Captura de fotos

i **Observação**

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

i **Observação**

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

i **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

i **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.10 Adicionar evento para o dispositivo de controle de segurança

Você pode adicionar um evento ao dispositivo de controle de segurança do sistema. Quando o evento é acionado no dispositivo, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute esta tarefa quando você precisar adicionar um evento monitorado pelo sistema acionado pelo dispositivo de controle de segurança no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **dispositivo de controle de segurança**.

Acionamento de evento

O evento detectado no dispositivo de controle de segurança acionará os eventos monitorados pelo sistema no sistema.

Origem

O(s) dispositivo(s) de controle de segurança específico(s) que pode acionar este evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O dispositivo de controle de segurança é armado durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.



Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a(s) câmera(s) para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a(s) câmera(s) para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag

pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

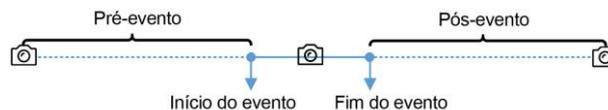


Figura 13-11 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser

ativado quando o evento ocorrer.

 **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s)

selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.11 Adicionar evento para servidor de transmissão ou servidor de gravação

Você pode adicionar um evento para os servidores de transmissão e servidores de gravação adicionados no sistema. Quando o evento é acionado nesses servidores, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelo servidor de transmissão ou pelo servidor de gravação no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de fonte como **Servidor de transmissão** ou **Gravação**.

Acionamento de evento

O evento detectado no servidor acionará um evento monitorado pelo sistema no sistema.

Origem

O(s) servidor(es) específico(s) que pode(m) acionar este evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O servidor é armado durante a programação de arme e o evento de disparo ocorrido na câmera durante a programação de arme irá acionar as ações de vinculação configuradas.

 **Observação**

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a câmera para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmera tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a câmera para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

 **Observação**

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura

abaixo).



Figura 13-12 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

Observação

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

Observação

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

Observação

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.12 Adicionar evento para o servidor HikCentral

Você pode definir um evento para a exceção (incluindo exceção de hardware e exceção de serviço) dos servidores que foram instalados com os serviços do sistema (como o serviço VSM, gateway de acesso de dispositivo de terceiros, serviço NGINX, serviço de proxy de teclado, Smart Wall serviços de gestão, etc.). Quando o evento é acionado, o sistema pode receber e registrar um evento para

verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelo servidor HikCentral no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **servidor HikCentral**.

Acionamento de evento

O evento detectado no HikCentral Server acionará o evento monitorado pelo sistema no sistema.

Origem

Selecione o **Servidor HikCentral** para acionar esse evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O servidor é armado durante a programação de arme e o evento de disparo ocorrido na câmera durante a programação de arme irá acionar as ações de vinculação configuradas.



Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a câmera para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmera tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a câmera para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

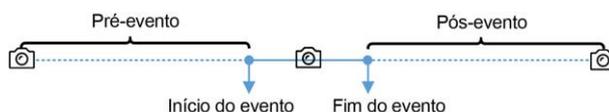


Figura 13-13 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

 **Observação**

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

 **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte ***Definir modelo de e-mail***.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte ***Configurar o evento definido pelo usuário***.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte ***Configurar Alarme***.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento	Selecione o(s) evento(s) e clique em Delete para excluir o(s) evento(s) selecionado(s).
Gerenciar eventos inválidos	Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em Delete na dica de ferramenta e exclua o evento.
Excluir todos os eventos inválidos	Clique Excluir todos os itens inválidos para excluir todos os alarmes inválidos em um lote.
Filtrar Evento	Clique em  para expandir as condições de filtro. Defina as condições e clique em Filter para filtrar os eventos de acordo com as condições.

13.1.13 Adicionar evento para usuário

Você pode adicionar um evento para os usuários no sistema. Quando o usuário entra ou sai, o sistema pode receber e registrar o evento para verificar e acionar uma série de ações de vinculação (por exemplo, envio de e-mail) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelos usuários no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como **Usuário**.

Acionamento de evento

O evento detectado na origem do evento acionará os eventos monitorados pelo sistema no sistema.

Origem

O(s) usuário(es) específico(s) que pode(m) acionar este evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O usuário é armado durante programação de arme e o evento de disparo ocorrido na fonte de evento durante a programação de arme irá acionar as ações de vínculo configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a câmera para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Selecione a câmera para gravar vídeo quando o evento ocorrer e adicione uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client. Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo,

respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

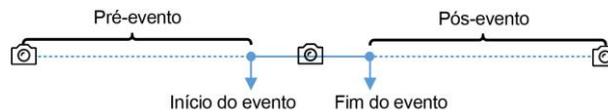


Figura 13-14 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

Observação

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

Observação

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo

modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

Observação

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1.13 Adicionar evento para o evento definido pelo usuário

Você pode adicionar um evento para o evento definido pelo usuário adicionado no sistema.

Quando o evento definido por usuário é acionado, o sistema pode receber e registrar um evento

para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute essa tarefa quando precisar adicionar um evento monitorado pelo sistema acionado pelo evento definido pelo usuário no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de origem e a origem do evento.

Tipo de origem

Selecione o tipo de origem como **Evento definido pelo usuário**.

Origem

Selecione o evento definido pelo usuário configurado como a origem do evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O evento definido pelo usuário é armado durante a programação de arme e o evento definido pelo usuário acionado durante a programação de arme acionará as ações de vinculação configuradas.



Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a câmera para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmara tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a câmera para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag

pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

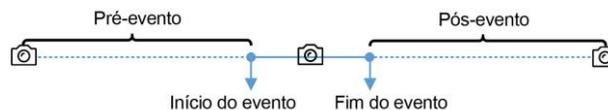


Figura 13-15 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser

ativado quando o evento ocorrer.

 **Observação**

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

 **Observação**

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento	Selecione o(s) evento(s) e clique em Delete para excluir o(s) evento(s) selecionado(s).
Gerenciar eventos inválidos	Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em Delete na dica de ferramenta e exclua o evento.
Excluir todos os eventos inválidos	Clique Excluir todos os itens inválidos para excluir todos os alarmes inválidos em um lote.
Filtrar Evento	Clique em  para expandir as condições de filtro. Defina as condições e clique em Filter para filtrar os eventos de acordo com as condições.

13.1.15 Adicionar evento para Evento genérico

Você pode adicionar um evento para os eventos genéricos adicionados no sistema. Quando o evento genérico é acionado, o sistema pode receber e registrar um evento para verificação e acionar uma série de ações de vinculação (por exemplo, envio de email) para notificação.

Execute essa tarefa quando você precisar adicionar um evento monitorado pelo sistema acionado pelo evento genérico no sistema.

Etapas

1. Clique em **Evento & Alarme** → **Evento monitorado pelo sistema** → **Adicionar** para entrar na página de adição de evento.
2. Configure as informações básicas do evento, incluindo o tipo de fonte, o evento de acionamento e a fonte do evento.

Tipo de origem

Selecione o tipo de origem como evento genérico.

Origem

Selecione o evento genérico configurado como a origem do evento.

3. Opcional: Defina **Action (Ação)** para ON (ativado) para definir as ações de vinculação ao evento.

Modelo de programação de arme

O evento é armado durante a programação de arme e o evento genérico acionado durante a programação de arme acionará as ações de vinculação configuradas.

Observação

Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Acionamento de gravações

Clique em **Adicionar** para selecionar a câmera para gravar vídeo, quando o evento ocorre. Selecione o local de armazenamento para armazenar os arquivos de vídeo. Você pode reproduzir os arquivos de vídeo gravados ao verificar eventos em Pesquisa de Alarme & Evento do Control Client.

Visualizar vídeo pré-evento: Se a câmera tiver gravado arquivos de vídeo antes do evento, você pode ver o vídeo gravado a partir de períodos anteriores ao evento. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do evento. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Pós-gravação: Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Bloqueio de arquivos de vídeo por: Defina os dias para proteger o arquivo de vídeo de ser substituído.

Criação de tag

Clique em **Add (Adicionar)** para selecionar a câmera para gravar vídeo quando o evento ocorrer e adicionar uma tag ao vídeo acionado por evento. Selecione o local de armazenamento para armazenar os arquivos de vídeo. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Você pode inserir o nome da tag como desejar. Você também pode clicar no botão abaixo para adicionar as informações relacionadas ao nome.

Configure a faixa de tempo para definir a duração do vídeo etiquetado. Por exemplo, é possível configurar para gravar o vídeo com a marcação de uma tag começando 5 segundos antes do evento e terminando até 10 segundos depois do evento. O vídeo com a marcação de uma tag pode ser procurado e verificado via Control Client.

Adicione a descrição ao vídeo etiquetado conforme necessário.

Capturar uma imagem

Selecione uma câmera para capturar imagens durante o evento e você poderá visualizar as imagens capturadas ao verificar o evento em Pesquisa de Alarme & Evento do Control Client.

Observação

Apenas uma câmera pode ser definida para captura de fotos.

Capturar imagem quando: Especifique o número de segundos em que a câmera irá capturar antes/depois do evento começar/terminar. Depois de definir o número de segundos para pré/pós-evento, a câmera irá capturar uma imagem em três pontos de tempo, respectivamente: nos segundos configurados antes do início do evento, nos segundos configurados após o término do evento e no meio do evento (como mostrado na figura abaixo).

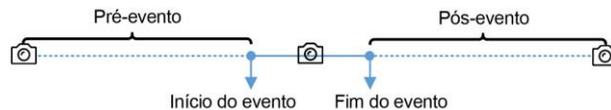


Figura 13-16 Captura de fotos

Observação

A imagem pré-evento é capturada a partir dos arquivos de vídeo gravados da câmera. Esta função de captura de pré-evento é suportada apenas pela câmera que está configurada para armazenar os arquivos de vídeo no Servidor de Gravação (servidor de armazenamento em nuvem, SAN híbrido ou pStor).

Ponto de acesso vinculado

Selecione o(s) ponto(s) de acesso como destino(s) de vinculação. Você pode definir a ação do ponto de acesso para que o ponto de acesso seja desbloqueado, bloqueado, permaneça desbloqueado ou permaneça bloqueado quando o evento ocorrer.

Observação

Até 16 pontos de acesso podem ser selecionados como vínculo de evento.

Saída de alarme vinculada

Selecione a saída de alarme (se disponível) e o dispositivo externo conectado pode ser ativado quando o evento ocorrer.

Observação

Até 64 saídas de alarme podem ser selecionadas como vínculo de evento.

Fechar a saída de alarme: A(s) saída(s) de alarme adicionada(s) pode(m) ser fechada(s) manualmente ou você pode definir o número de segundos em que ela(s) será (ão) fechada(s) automaticamente.

Acionamento de PTZ

Acione a predefinição, patrulha ou padrão da(s) câmera(s) selecionada(s) quando o evento ocorrer.

Observação

Até 64 vínculos PTZ podem ser selecionadas como vínculo de evento.

Enviar e-mail

Selecione um modelo de e-mail para enviar as informações do evento de acordo com as configurações de e-mail definidas. Você pode selecionar **Adicionar novo** para criar um novo modelo de e-mail. Para obter mais detalhes, consulte **Definir modelo de e-mail**.

Acionar Eventos de Movimento

Acione eventos definidos pelo usuário quando o evento monitorado pelo sistema é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como vinculação de evento.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

4. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e acionar alarme** para acionar esse evento como um alarme para posterior notificação. Para obter mais detalhes, consulte **Configurar Alarme**.

Depois de adicionar o evento, ele é exibido na lista de eventos e você pode visualizar o nome do evento, a origem do evento e o evento de disparo.

5. Opcional: Execute as seguintes operações após adicionar o evento.

Evento de disparo como alarme

Clique em  na coluna Operação da página de configurações de eventos monitorados pelo sistema para definir as propriedades do alarme, os destinatários, as ações e outros parâmetros.

 **Observação**

Para obter mais detalhes, consulte **Configurar Alarme**.

Excluir evento

Selecione o(s) evento(s) e clique em **Delete** para excluir o(s) evento(s) selecionado(s).

Gerenciar eventos inválidos

Se  aparecer perto do nome do evento, isso significa que o evento não é suportado pelo dispositivo e é inválido. Você deve passar o cursor sobre o  e clique em **Delete** na dica de ferramenta e exclua o evento.

Excluir todos os eventos inválidos

Clique **Excluir todos os itens inválidos** para excluir todos os alarmes inválidos em um lote.

Filtrar Evento

Clique em  para expandir as condições de filtro. Defina as condições e clique em **Filter** para filtrar os eventos de acordo com as condições.

13.1 Editar evento monitorado pelo sistema

Depois de adicionar o evento monitorado pelo sistema, você pode editar as configurações do evento e acionar o evento como alarme.

Antes de começar

Adicione o evento monitorado pelo sistema. Consulte **Configuração de eventos monitorados no sistema** para obter mais informações.

Execute esta tarefa quando você precisa editar o evento adicionado sistema monitorado ou acioná-lo como alarme.

Etapas

1. Clique em **Evento & alarme** na página inicial.
2. Clique na guia **Evento monitorado pelo sistema** para entrar na página de lista de eventos.
3. Clique no nome do evento para entrar na página de detalhes do evento.
4. Opcional: Execute as seguintes operações para editar os detalhes do evento.

Configurar o evento no dispositivo (se suportado) Para alguns dos tipos de fonte, clique em  para acessar o dispositivo e configurar o evento. Consulte o manual do usuário do dispositivo para obter detalhes.

Editar o nome do evento Edite o nome do evento conforme desejado.

Editar ações Edite as configurações de ação de vinculação de eventos. Para obter mais detalhes, consulte **Configurar os eventos monitorados no sistema**.

5. Salve as configurações do evento.
 - Clique em **Salvar** para salvar as configurações do evento e retornar à página de lista de eventos.
 - Clique em **Salvar e acionar alarme** para salvar o evento como alarme e entrar na página de configurações de alarme para definir o alarme. Consulte **Configurar o alarme** para obter mais informações.

13.2 Configurar evento genérico

Você pode personalizar a expressão para criar um evento genérico para analisar os pacotes de dados TCP e/ou UDP recebidos e acionar eventos quando as condições especificadas forem atendidas. Desta forma, você pode facilmente integrar o seu sistema com uma ampla gama de fontes externas, tais como sistemas de controle de acesso e sistemas de alarme.

Execute essa tarefa quando você precisar configurar o evento genérico.

Etapas

1. Clique em **Evento & alarme** → **Evento genérico** para entrar na página de configurações de evento genérico.



<input type="checkbox"/>	Event Name	Transport Type	Match Type	Expression
<input type="checkbox"/>	Generic Event 1	TCP	Search	"Motion" AND "Line Crossing"

Figura 13-17 Página de configurações de evento genérico

2. Clique em **Adicionar** para entrar na página de Adicionar evento genérico

← Add Generic Event

Generic event is the signal that resource (e.g., other software, device) sends when something occurs, and is received by system in TCP or UDP data packages.

Basic Information

*Event Name

Copy from

Event Definition

*Transport Type TCP UDP

*Match Type Search Match

*Expression

Figura 13-18 Adicionar página de eventos genéricos

3. Defina um nome para o evento no campo Nome do evento.
4. Opcional: Copie as configurações de outros eventos genéricos definidos no campo **Copiar de**.
5. Selecione **TCP** ou **UDP** para analisar os pacotes usando o protocolo TCP ou UDP.
6. Selecione o tipo correspondente que indica como o sistema deve ser determinado ao analisar os pacotes de dados recebidos:

Pesquisar

O pacote recebido deve conter o texto definido no campo expressão.

Por exemplo, se você definiu que os pacotes recebidos devem conter "Movimento" e "Cruzamento de linha", o alarme será acionado quando os pacotes recebidos contiverem "Movimento", "Intrusão" e "Cruzamento de linha".

Correspondência

O pacote recebido deve conter exatamente o texto definido no campo de Expressão e nada mais.

7. Defina a regra de evento para analisar o pacote recebido no campo Expressão.
 - 1) Digite o termo que deve estar contido na expressão no campo de texto.
 - 2) Clique em **Adicionar** para adicioná-lo à expressão.
 - 3) Clique em parêntese ou no botão do operador para adicioná-lo à expressão.

- 4) Para adicionar um termo, parêntese ou operador à expressão, posicione o cursor dentro do campo de expressão para determinar onde um novo item (termo, parêntese ou o operador) deve ser incluído e clique em Adicionar ou em um dos botões de parêntese ou operador.
- 5) Para remover um item da expressão, posicione o cursor dentro do campo para determinar onde um item deve ser removido e clique em . O item imediatamente à esquerda do cursor será removido.

Os botões de parêntese ou operador são descritos no seguinte:

E

Você especifica que os termos em ambos os lados do E operador devem ser incluídos. Por exemplo, se você definir a regra como "Movimento" e "Cruzamento de linha" e "Intrusão", o termo movimento, e cruzamento de linha, bem como o termo intrusão devem estar no pacote recebido para as condições a serem cumpridas.

Observação

Em geral, quanto mais termos você combinar com E, menos eventos serão detectados.

OU

Você especifica que todos esses termos devem estar presentes. Por exemplo, se você definir a regra como "Movimento" ou "Cruzamento de linha" ou "Intrusão", qualquer um dos termos (movimento, cruzamento de linha ou intrusão) deve estar no pacote recebido para as condições a serem atendidas.

Observação

Em geral, quanto mais termos você combinar com o OU, mais eventos serão detectados.

(

Adicione o parêntese esquerdo à regra. Os parênteses podem ser usados para garantir que os termos relacionados sejam processados juntos como uma unidade; em outras palavras, eles podem ser usados para forçar uma determinada ordem de processamento na análise. Por exemplo, se você definir a regra como ("Movimento" ou "Cruzamento de linha") e "Intrusão", os dois termos dentro dos parênteses serão processados primeiro, em seguida, o resultado será combinado com a última parte da regra. Em outras palavras, o sistema irá primeiro procurar todos os pacotes que contenham qualquer um dos termos Movimento ou Cruzamento de linha, em seguida, ele procurará os resultados em busca dos pacotes que contenham o termo Intrusão.

)

Adicione o parêntese direito à regra.

8. Termine de adicionar o evento.

- Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
- Clique em **Adicionar e continuar** para salvar as configurações de evento e continuar adicionando eventos.

9. Opcional: Execute as seguintes operações após adicionar o evento.

Editar configurações de evento	Clique no nome na coluna nome do evento para editar as configurações de evento correspondentes.
Excluir configurações de evento	Verifique os eventos e clique em Delete para excluir as configurações de evento selecionadas.
Excluir todas as configurações do evento	Marque a caixa de seleção na linha de título e clique em Delete para excluir todas as configurações do evento.

13.3 Configurar evento definido pelo usuário

Se o evento que você precisa não está na lista de eventos monitorados pelo sistema fornecido, ou o evento genérico não pode definir corretamente o evento recebido do sistema de terceiros, você pode personalizar um evento definido pelo usuário.

Execute esta tarefa se você precisar adicionar um evento definido pelo usuário.

Etapas

1. Clique em **Evento e alarme** → **Evento definido pelo usuário** para entrar na página de gerenciamento de eventos definida pelo usuário.
2. Clique em **Adicionar** para abrir a janela seguinte.

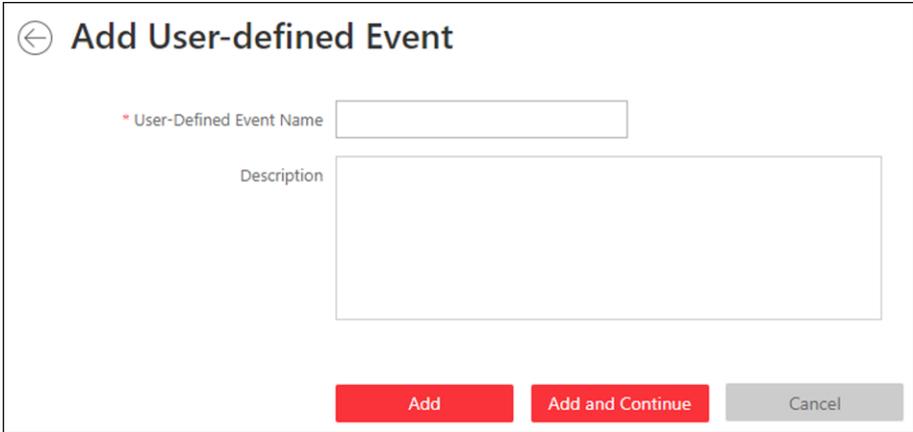


Figura 13-19 Adicionar evento definido pelo usuário

3. Crie um nome para o evento.
4. Opcional: Insira as informações de descrição para descrever os detalhes do evento.
5. Termine de adicionar o evento.
 - Clique em **Adicionar** para adicionar o evento e retornar à página de lista de eventos.
 - Clique em **Adicionar e continuar** para adicionar o evento e continue a adicionar outros eventos.

Com o evento personalizado definido pelo usuário, ele fornece as seguintes funções:

- O usuário pode acionar um evento definido pelo usuário manualmente no módulo Monitoramento e Central de Alarme no Control Client ao visualizar o vídeo ou verificar as informações de alarme.
- Um evento definido pelo usuário pode acionar um alarme, se configurado.
- É possível definir o período de tempo de armar pelo evento definido pelo usuário: O agendamento de armar de um alarme iniciará ou terminará quando o evento definido pelo usuário for acionado.
- Um alarme pode ser acionado por um evento definido pelo usuário como ações de alarme.
- Integre outros sistemas de terceiros com o HikCentral usando os dados recebidos do sistema de terceiros. Você pode acionar os eventos definidos pelo usuário fora do HikCentral. Para mais informações, entre em contato com o nosso suporte técnico.

Observação

- Para configurar a origem do alarme, a programação de arme, e a ação do alarme, consulte **Configurar alarme**.
 - Para acionar o evento definido pelo usuário no Control Client, consulte o Manual do usuário do HikCentral Control Client.
-

13.4 Configurar alarme

O alarme é usado para notificar o pessoal de segurança sobre a situação específica que ajuda a lidar com a situação imediatamente. O alarme pode desencadear uma série de ações de vinculação (por exemplo, a janela pop-up no Control Client, mostrando os detalhes do alarme) para notificação e manuseio de alarmes.

Você pode definir os alarmes para os recursos no local atual.

Se o sistema é um sistema central com módulo de gerenciamento de site remoto, você também pode definir o alarme para a câmera no site remoto que configurou com alarme, para que você possa receber alarmes no sistema central quando o alarme é acionado.

Você pode definir diferentes ações de ligação para os seguintes alarmes:

- Alarme da câmera: a exceção de vídeo ou os eventos detectados na área de monitoramento das câmeras, tais como detecção de movimento, perda de vídeo, cruzamento de linha, etc.
- Alarme do ponto de acesso: o alarme acionado nos pontos de acesso (porta, pista, etc.), tais como o evento de acesso, o evento do status da porta, etc.
- Alarme de entrada de alarme: o alarme acionado pelas entradas de alarme (incluindo entradas de alarme de dispositivos de codificação, dispositivos de controle de acesso e dispositivos de controle de segurança).
- Alarme ANPR: o alarme acionado quando as placas de veículo detectadas pela câmera ANPR e UVSS correspondem ou descombinam com as informações do veículo na lista de veículos.
- Alarme de pessoa: o alarme acionado quando o rosto da pessoa detectado pelo dispositivo de reconhecimento facial corresponde ou não à imagem facial no grupo de comparação facial.
- Alarme UVSS: o alarme acionado pelo dispositivo UVSS, incluindo o dispositivo ficar online e

offline.

- Alarme de local remoto: o alarme acionado pelo Local Remoto adicionado, incluindo o local ficando offline.

Observação

O alarme do local remoto está disponível para o sistema com módulo de gerenciamento remoto do local (baseado na licença que você comprou).

- Exceção de dispositivo: o alarme acionado pelo dispositivo de codificação, dispositivo de controle de acesso ou exceções de dispositivos de controle de segurança.
 - Exceção do servidor: o alarme acionado pelo servidor de gravação, pelo servidor de transmissão ou pelo servidor HikCentral.
 - Alarme do usuário: o alarme acionado por usuários do sistema, incluindo o login do usuário e logout.
 - Evento definido pelo usuário: o alarme acionado pelo evento configurado definido pelo usuário.
 - Evento genérico: o alarme acionado pelo evento genérico configurado.
-

Observação

Você pode verificar a mensagem de alarme recebidos através do Control Client. Para mais detalhes, consulte o *Manual do HikCentral Control Client*.

13.4.1 Configurações de alarme

O sistema predefine várias prioridades de alarme e categorias de alarmes para as necessidades básicas. Você pode editar a prioridade de alarme predefinida e categoria de alarme, e definir a prioridade de alarme personalizado e categoria de alarme de acordo com as necessidades reais.

Execute esta tarefa quando precisar configurar a prioridade e a categoria do alarme.

Prioridade de alarme

Defina a prioridade para o alarme ao adicionar o alarme e os filtros de alarme no Control Client.

Categoria de alarme

A categoria de alarme é usada quando o usuário reconhece o alarme no Control Client e indica qual é o tipo de alarme, p.ex., alarme falso ou alarme que deve ser verificado. Você pode procurar os alarmes por tipo de alarme na Central de alarmes do Control Client.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Configurações de alarme** para entrar na página de configuração do alarme.
2. Defina a prioridade de alarme de acordo com as necessidades reais. Por padrão, existem três tipos de prioridade de alarme.



Figura 13-20 Página de prioridade de alarme

- 1) Clique em **Adicionar** para adicionar uma prioridade personalizada.

Observação

Podem ser adicionados até 255 níveis de prioridade de alarme. Os níveis de prioridade podem ser usados para classificar alarmes no Centro de alarmes do Control Client.

- 2) Selecione um nº de nível para a prioridade.
- 3) Insira um nome descritivo para a prioridade.
- 4) Selecione a cor para a prioridade.

*Level 8

*Name

*Color #ff0000

Save

Figura 13-21 Janela de configurações de prioridade de alarme

- 5) Clique em **Salvar** para adicionar a prioridade.
A prioridade será exibida na lista de prioridades de alarme.
3. Defina a categoria de alarme de acordo com as necessidades reais. Por padrão, existem quatro categorias de alarme.

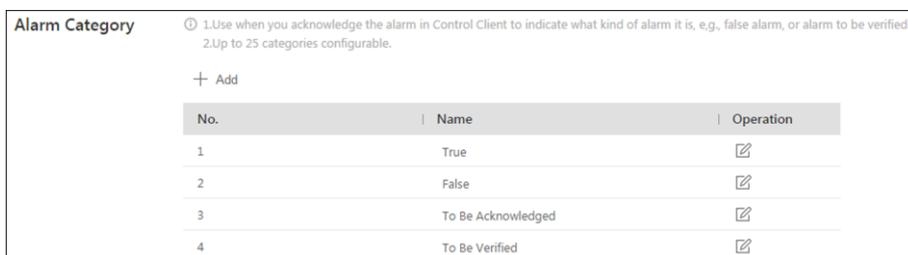


Figura 13-22 Página de categoria de alarme

- 1) Clique em **Adicionar** para adicionar a categoria de alarme personalizada.

 **Observação**

Podem ser adicionadas até 25 categorias de alarme.

- 2) Selecione um número para a categoria de alarme.
- 3) Insira um nome descritivo para a categoria de alarme.



Figura 13-23 Janela de configurações de categoria de alarme

- 4) Clique em **Salvar** para adicionar a categoria de alarme.
A categoria de alarme será exibida na lista de categoria de alarme.
4. Execute as seguintes operações após adicionar a prioridade e a categoria do alarme.

Editar

Clique em  para editar a prioridade e a categoria do alarme.

 **Observação**

Não é possível editar o nº de prioridades e categorias de alarme predefinidas.

Excluir

Clique em  para excluir a prioridade e a categoria do alarme.

 **Observação**

Não é possível excluir as prioridades e categorias de alarme predefinidas.

13.4.2 Adicionar alarme para câmera no local atual

Você pode definir alarmes para câmeras adicionadas no site atual e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme for acionado.

Execute esta tarefa quando precisar adicionar um novo alarme para as câmeras no local atual.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

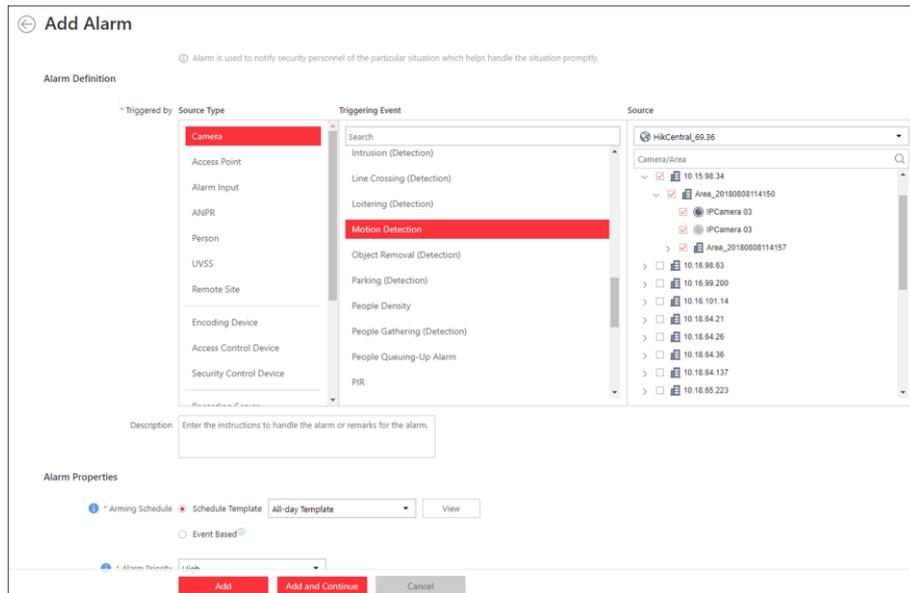


Figura 13-24 Adicionar alarme para câmera no local atual

2. Defina o tipo de origem como **Câmera** no campo **Acionado por**.
3. Selecione um evento de acionamento como a origem para acionar o alarme.
4. Na lista suspensa do local, selecione o local atual.
5. Selecione uma câmera específica para acionar o alarme.
6. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
7. Preencha as informações solicitadas.

Agendamento de armar

A câmera é armada durante a programação de armar e o evento ocorrido durante a programação de armar será acionado como alarme e notificará o usuário. Ele fornece dois tipos de programação de arme:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

8. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de vinculação de alarme

Câmera relacionada

Selecione as câmeras relacionadas para gravar o vídeo do alarme quando o alarme é acionado. Você pode exibir o vídeo ao vivo e reproduzir esses arquivos de vídeo na central de alarmes do Control Client.

- Para relacionar a própria câmera de origem para gravação, selecione **Source Camera** (Câmera de origem) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para relacionar outras câmeras, selecione **Câmera especificada** e clique em **Adicionar** para adicionar outras câmeras como câmeras relacionadas. Selecione o local de armazenamento para armazenar os arquivos de vídeo.
- **Ver vídeo de pré-alarme:** É possível ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.

Observação

- Certifique-se de que as câmeras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Mapa relacionado

Selecione um mapa para mostrar as informações de alarme e você deve adicionar a câmera ao mapa como um ponto de destaque (consulte **Adicionar ponto de destaque**). Você pode marcar o mapa na Central de alarmes e na pesquisa de alarmes e eventos do Control Client.

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e a reprodução quando ocorrer um alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo no smart wall e qual janela e definir o tipo de transmissão do vídeo de alarme.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a

correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.

- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

9. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

10. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique em Excluir tudo para excluir todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.4.3 Adicionar alarme para a câmera no local remoto

Se o sistema é um sistema central com módulo de gerenciamento de site remoto (com base na licença que você comprou), você também pode adicionar os alarmes configurados para as câmeras no site remoto para o sistema central, e configurar séries de ações de vinculação para a notificação no Sistema central quando o alarme é acionado.

Antes de começar

Você deve configurar o alarme para a câmera no local remoto por meio do Web Client do site remoto.

Execute esta tarefa se você precisar adicionar os alarmes configurados para as câmeras no local remoto para o sistema central.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

Alarm Definition

Alarm Properties

Alarm Recipients

Figura 13-25 Adicionar alarme para câmera no local remoto

2. Defina o tipo de origem como **Câmera** no campo **Acionado por**.
3. Selecione a origem de alarme.
 - 1) Na lista de **Eventos de acionamento**, selecione o tipo de evento de origem.
 - 2) Na lista **Origem**, selecione um local remoto na lista suspensa.

Os alarmes configurados no local remoto do tipo de evento de acionamento selecionado serão exibidos.
 - 3) Selecione o alarme configurado no local remoto como a origem para acionar um alarme no sistema central.

Observação

Certifique-se de que o alarme configurado no local remoto está habilitado. O alarme será efetivo após ativado no local remoto e no sistema central

4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione um usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o login no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, como ações de vinculação de alarme.

Câmera relacionada

Se o alarme selecionado estiver configurado com a câmera relacionada no Local remoto, você poderá visualizar seus arquivos de vídeo ao verificar o alarme no sistema central.

Mapa relacionado

Se o alarme selecionado estiver configurado com o mapa relacionado no local remoto, você poderá visualizar o local de origem do alarme ao verificar o alarme no sistema central.

Janela Pop-up de acionamento

Ele mostra a janela de alarme no Control Client para exibir os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e a reprodução quando ocorrer um alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes. Será possível ver o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique em habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os	Clique Desabilitar Tudo para desabilitar todos os alarmes

alarmes adicionados.

Alarme de teste Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.4 Adicionar alarme para ponto de acesso

Você pode definir alarmes para os pontos de acesso dos dispositivos de controle de acesso adicionados e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando você precisar adicionar um novo alarme para os pontos de acesso.

Etapas

1. Clique em Evento & Alarme → Alarme → Adicionar entrar na Página de Adicionar Alarme.

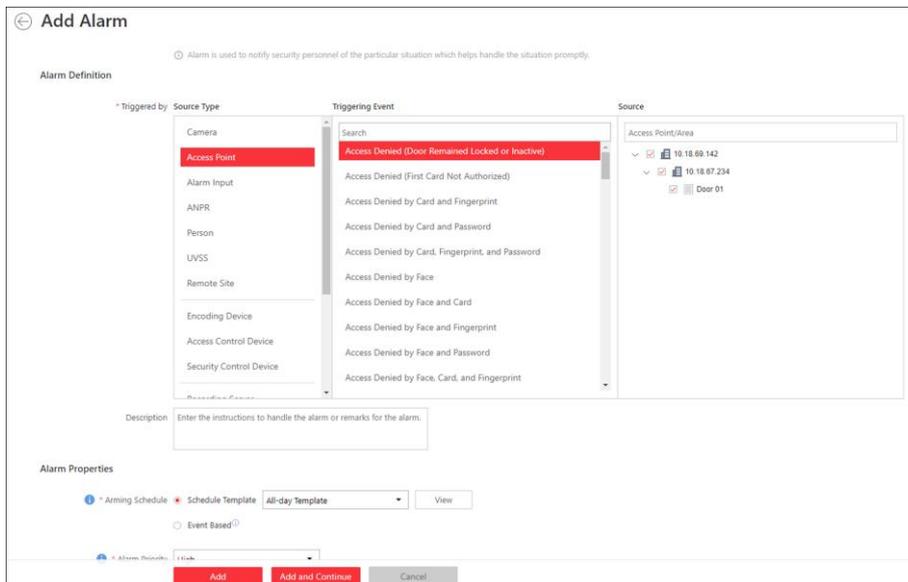


Figura 13-26 Adicionar alarme para ponto de acesso

2. Defina o tipo de origem como **Ponto de Acesso** no campo **Acionado por**.
3. Selecione um evento de acionamento e um ponto de acesso específico como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O ponto de acesso é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme

para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários de alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

Câmera relacionada

Selecione as câmeras relacionadas para gravar o vídeo do alarme quando o alarme é acionado. Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Para relacionar a câmera relacionada do ponto de acesso para gravação, selecione Source Related Camera (Câmera de origem relacionada) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para relacionar outras câmeras, selecione **Câmera especificada** e clique em **Adicionar** para adicionar outras câmeras como câmeras relacionadas. Selecione o local de armazenamento para armazenar os arquivos de vídeo.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Para definir a câmera relacionada do ponto de acesso na Exibição Lógica, consulte **Editar Ponto de Acesso do Local Atual**.
- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
- Até 16 câmeras podem ser definidas como câmera relacionada.

Mapa relacionado

Selecione o mapa para mostrar as informações de alarme e você deve adicionar o ponto de acesso ao mapa como um local de destaque (consulte **Adicionar local de destaque**). Você pode marcar o mapa na Central de alarmes e na pesquisa de alarmes e eventos do Control Client.

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e a reprodução quando ocorrer um alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.



Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

 **Observação**

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

6. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

Depois de adicionar o alarme, ele é exibido na lista de alarmes e você pode visualizar o nome do alarme e o status do alarme.

7. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique em Excluir tudo para excluir todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.

Alarme de teste

Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.4.5 Adicionar alarme para entrada de alarme

Você pode definir o alarme de entrada de alarme para entradas de alarme do dispositivo adicionado e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando precisar adicionar alarme para as entradas de alarme do dispositivo adicionado.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

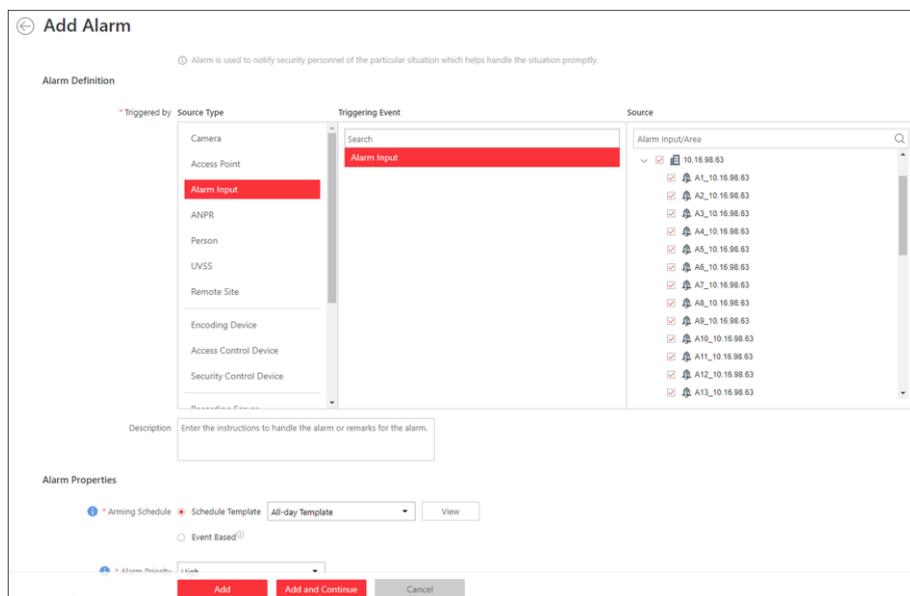


Figura 13-27 Adicionar alarme para entrada de alarme

2. Defina o tipo de origem como **Entrada de alarme** no campo **Acionado por**.
3. Selecione uma entrada de alarme específica como a fonte para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

A entrada de alarme é armada durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Mapa relacionado

Selecione o mapa para mostrar as informações de alarme e você deve adicionar a entrada de alarme ao mapa como um local de destaque (consulte **Adicionar local de destaque**). Você pode verificar o mapa na Central de Alarmes e na Pesquisa de Alarmes & Eventos do Control Client.

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os

vídeos ao vivo das câmeras relacionadas ao alarme e arquivos de vídeo gravados quando o alarme ocorrer.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

Depois de adicionar o alarme, ele é exibido na lista de alarmes e você pode visualizar o nome do alarme e o status do alarme.

8. Opcional: Execute as operações a seguir depois de adicionar o alarme:

Editar alarme	Clique em  na coluna operação para editar o alarme.
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique em Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.6 Adicionar alarme para a câmera ANPR

Você pode definir o alarme compatível e incompatível de número de placa para a câmera ANPR adicionada (incluindo câmeras de trânsito ANPR profissionais e câmera em UVSS (sob sistema de vigilância veicular)) e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando precisar adicionar o alarme para a câmera adicionada de ANPR.

Etapas

1. Clique em Evento & Alarme → Alarme → Adicionar entrar na Página de Adicionar Alarme.

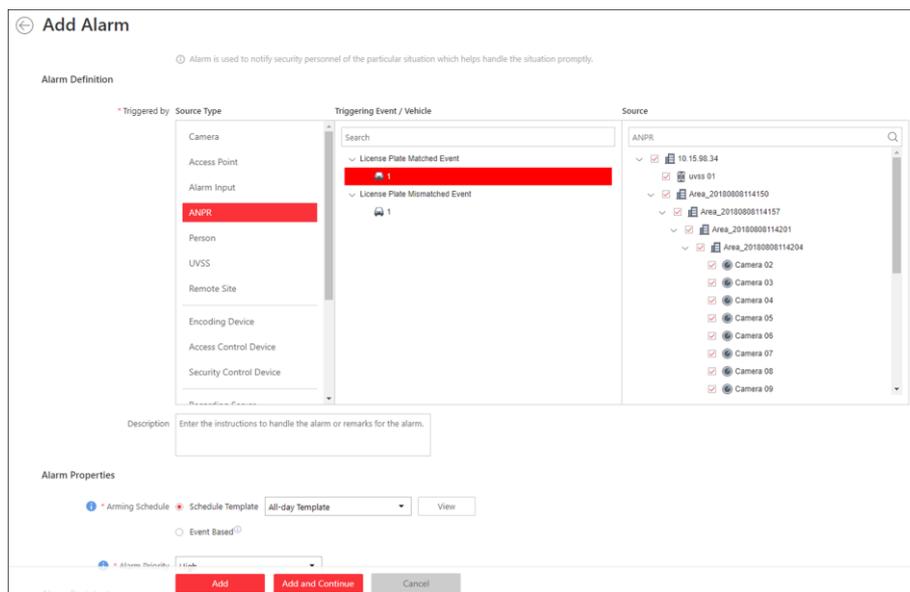


Figura 13-28 Adicionar alarme para câmera ANPR

2. Defina o tipo de origem como **ANPR** no campo **Acionado por**.
3. Selecione uma lista de veículos definida como a fonte para a correspondência ou incompatibilidade da placa reconhecida por e, em seguida, selecione uma câmera ANPR específica ou uma câmera UVSS como a fonte para acionar o alarme.

Observação

Antes de configurar o alarme ANPR, os veículos de informação devem ser adicionados por correspondência de placa de licença reconhecida pelo dispositivo ANPR. Para adicionar lista de veículos e informações do veículo, consulte **Gerenciar veículo**.

4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O dispositivo é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Selecione as câmeras relacionadas para gravar o vídeo do alarme quando o alarme é acionado. Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Para relacionar a própria câmera ANPR de origem, ou a câmera relacionada ao UVSS para gravação, selecione **Origem ou Câmera relacionada à origem** e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para relacionar outras câmeras, selecione **Câmera especificada** e clique em **Adicionar** para adicionar outras câmeras como câmeras relacionadas. Selecione o local de armazenamento para armazenar os arquivos de vídeo.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
- Até 16 câmeras podem ser definidas como câmera relacionada.

Mapa relacionado

Selecione o mapa para mostrar as informações de alarme e você deve adicionar a câmera ou UVSS ao mapa como um local de destaque (consulte **Adicionar local de destaque**). Você pode verificar o mapa na Central de Alarmes e na Pesquisa de Alarmes & Eventos do Control Client.

Janela Pop-up de acionamento

Ele mostra a janela de alarme no Control Client para exibir os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e a reprodução quando ocorrer um alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

 **Observação**

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

Depois de adicionar o alarme, ele é exibido na lista de alarmes e você pode visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme Clique em  na coluna operação para editar as informações do alarme.

Copiar para outros alarmes Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote.
Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em **Copiar para**.
Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em **OK**.

Excluir alarme Clique em  na coluna Operação para excluir o alarme.

Excluir todos os alarmes Clique **Deletar Tudo** para deletar todos os alarmes adicionados.

Excluir todos os alarmes inválidos Clique **Deletar todos os itens inválidos** para deletar todos os alarmes inválidos em um lote.

Habilitar alarme Clique em  na coluna operação para ativar o alarme.

Habilitar todos os alarmes Clique em **habilitar tudo** para habilitar todos os alarmes adicionados.

Desativar alarme Clique em  na coluna operação para desabilitar o alarme.

Desabilitar todos os Clique em **Desabilitar Tudo** para desabilitar todos os alarmes

alarmes

adicionados.

Alarme de teste

Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.7 Adicionar alarme para pessoa

Você pode definir o alarme de face compatível e incompatível para a câmera de reconhecimento de face adicionada e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme for acionado.

Execute esta tarefa quando precisar adicionar um alarme de face compatível ou incompatível para a pessoa.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

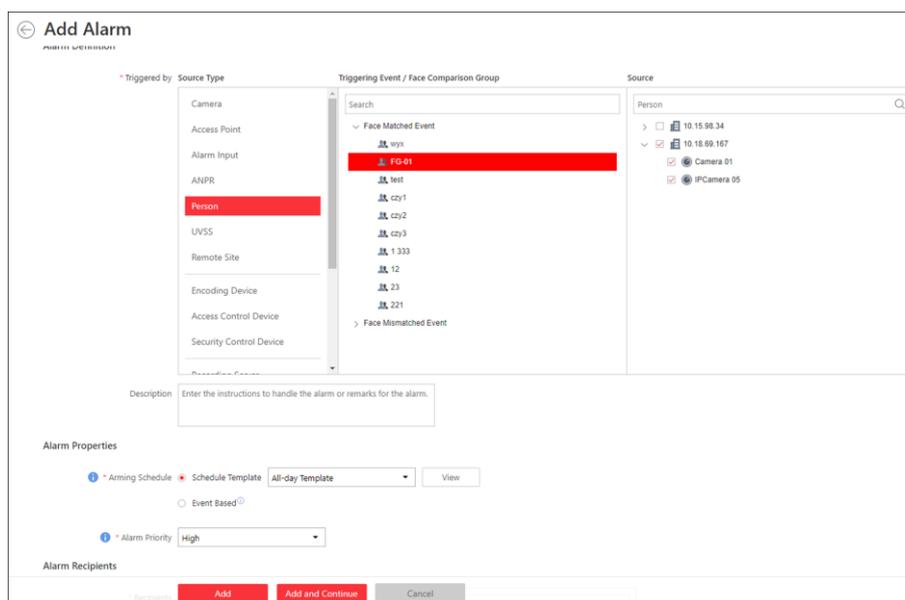


Figura 13-29 Adicionar alarme para pessoa

2. Defina o tipo de origem como **Pessoa** no campo **Acionado por**.
3. Selecione um grupo de comparação de rostos aplicado à câmera e selecione uma câmera de reconhecimento de rostos específica como fonte para correspondência ou incompatibilidade da face da pessoa reconhecida pela câmera de reconhecimento facial.

Observação

Para configurar o grupo de comparação de faces e aplicá-lo ao dispositivo, consulte **Gerenciar grupo de comparação facial**.

4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

A câmera é armada durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

Modelo de cronograma

Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Baseado em evento

Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Selecione as câmeras relacionadas para gravar o vídeo do alarme quando o alarme é acionado. Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Para relacionar a própria câmera de origem para gravação, selecione Source Camera (Câmera de origem) e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para relacionar outras câmeras, selecione **Câmera especificada** e clique em **Adicionar** para adicionar outras câmeras como câmeras relacionadas. Selecione o local de armazenamento para armazenar os arquivos de vídeo.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o

número de segundos que você deseja gravar vídeo para depois que o alarme parar.

- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.

Observação

- Certifique-se de que as câmeras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Mapa relacionado

Selecione um mapa para mostrar as informações de alarme e você deve adicionar a câmera ao mapa como um ponto de destaque (consulte **Adicionar ponto de destaque**). Você pode verificar o mapa na Central de Alarmes e na Pesquisa de Alarmes & Eventos do Control Client.

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e arquivos de vídeo gravados quando o alarme ocorrer.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

 **Observação**

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

 **Observação**

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

Depois de adicionar o alarme, ele é exibido na lista de alarmes e você pode visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique em Excluir tudo para excluir todos os alarmes adicionados.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.

Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em ☹ na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Alarme de teste	Clique em 🕒 para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.8 Adicionar alarme para UVSS

Você pode definir alarmes para adicionar UVSSs, incluindo UVSS online e offline, e acionar uma série de ações de vinculação (por exemplo, acionando janela pop-up no Control Client) para notificação.

Execute esta tarefa quando precisar adicionar alarmes para o UVSS adicionado.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

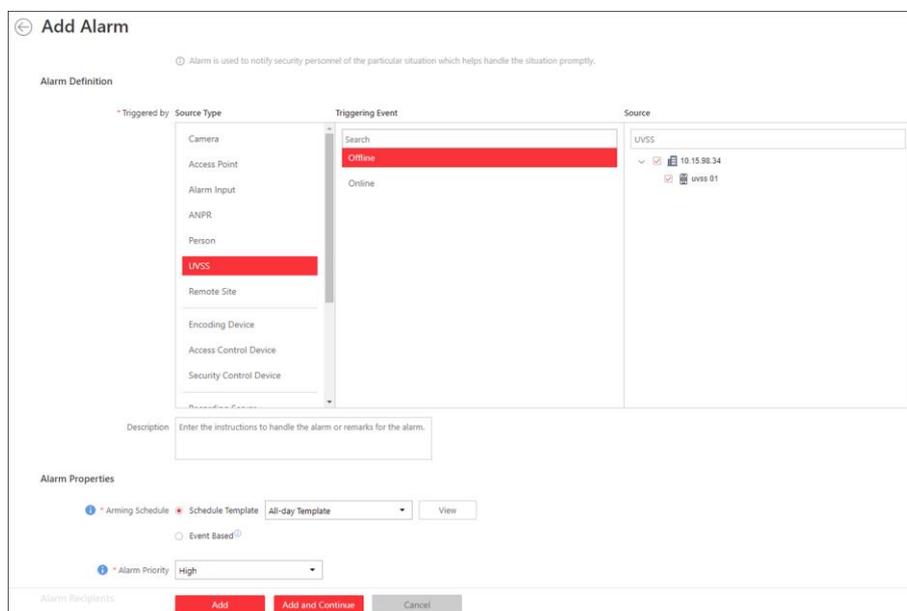


Figura 13-30 Adicionar alarme para UVSS

2. Defina **UVSS** como o tipo de origem no campo **Acionado por**.

3. Selecione um evento de acionamento específico e um UVSS específico como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O UVSS é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Para relacionar a câmera relacionada do UVSS para gravação, selecione **Source Related Camera (Câmera de origem relacionada)** e selecione o local de armazenamento para armazenar os arquivos de vídeo.
- Para relacionar outras câmeras, selecione **Câmera especificada** e clique em **Adicionar** para adicionar outras câmeras como câmeras relacionadas. Selecione o local de armazenamento para armazenar os arquivos de vídeo.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser

substituído.

- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Para configurar a câmera relacionada ao UVSS, consulte ***Editar sistema de vigilância sob o veículo para local atual***
 - Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Exiba a janela de alarme no Control Client para mostrar os detalhes do alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte ***Configurar o evento definido pelo usuário***.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

Depois de adicionar o alarme, ele é exibido na lista de alarmes e você pode visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.

Desabilitar todos os alarmes

Clique **Desabilitar Tudo** para desabilitar todos os alarmes adicionados.

Alarme de teste

Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.4.9 Adicionar alarme para dispositivo de codificação

Você pode definir alarmes para os dispositivos de codificação adicionados e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme for acionado.

Execute esta tarefa quando precisar adicionar um alarme para dispositivo de codificação adicionado.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

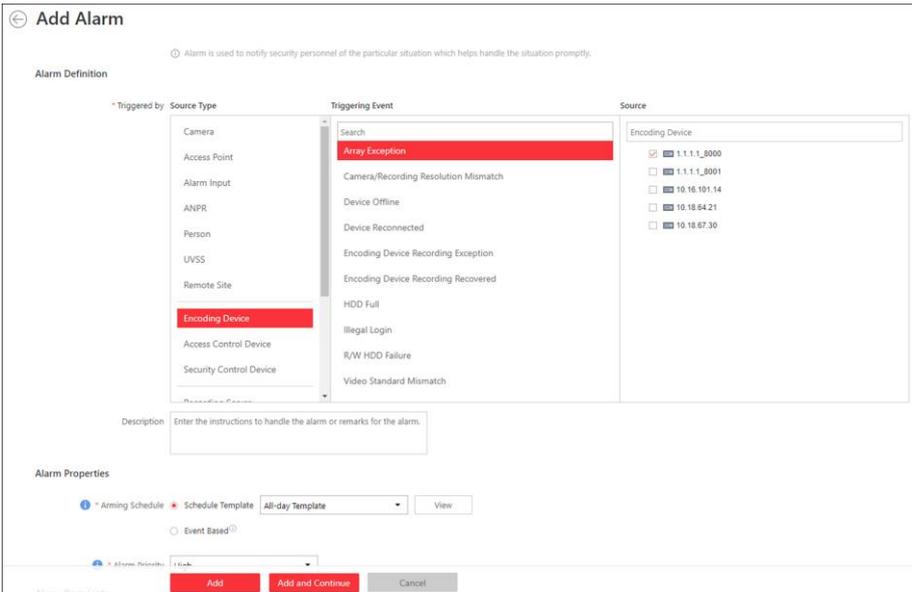


Figura 13-31 Adicionar alarme para dispositivo de codificação

2. Defina o tipo de origem como **Dispositivo de codificação** no campo **Acionado por**.
3. Selecione o evento de disparo e um dispositivo de codificação específico como a origem para acionar o alarme.
4. Opcional: Configure a definição de alarme, incluindo nome e descrição do alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O dispositivo é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos

dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione um usuário para enviar as informações de alarme e o usuário pode receber as informações de alarme quando ele/ela faz login no HikCentral através do Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.



Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Exiba a janela de alarme no Control Client para mostrar os detalhes do alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.10 Adicionar alarme para o dispositivo de controle de acesso

Você pode definir alarmes para dispositivos de controle de acesso adicionais, como dispositivo on-line/off-line, alarme de adulteração, bateria fraca etc., e configurar uma série de ações de vinculação (por exemplo, acionando janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando precisar adicionar um alarme para um dispositivo de controle de acesso adicionado.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

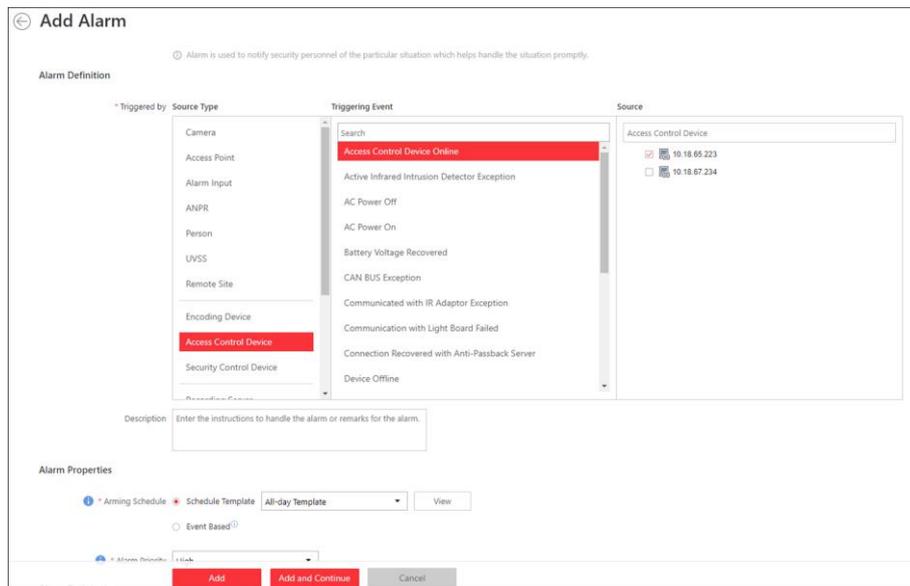


Figura 13-32 Adicionar alarme para dispositivo de controle de acesso

2. Defina o **dispositivo de controle de acesso** como o tipo de origem no campo **Acionado por**.
3. Selecione um evento de acionamento e um dispositivo específico como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O dispositivo é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

Modelo de cronograma

Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.

Baseado em evento

Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione um usuário para enviar as informações de alarme e o usuário pode receber as informações de alarme quando ele/ela faz logon no HikCentral através do Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.

Pós-gravação

Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.

Exibir vídeo de pré-alarme:

Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.

Bloqueio de arquivos de vídeo por

Defina os dias para proteger o arquivo de vídeo de ser substituído.

Exibir vídeo por padrão

Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os

vídeos ao vivo das câmeras relacionadas ao alarme e arquivos de vídeo gravados quando o alarme ocorrer.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

 **Observação**

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.11 Adicionar alarme dispositivo de controle de segurança

Você pode definir alarmes para os dispositivos de controle de segurança adicionados, como dispositivo on-line/off-line, alarme de adulteração, bateria fraca etc., e configurar uma série de ações de vinculação (por exemplo, acionando janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando precisar adicionar um alarme para um dispositivo de controle de segurança adicional.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

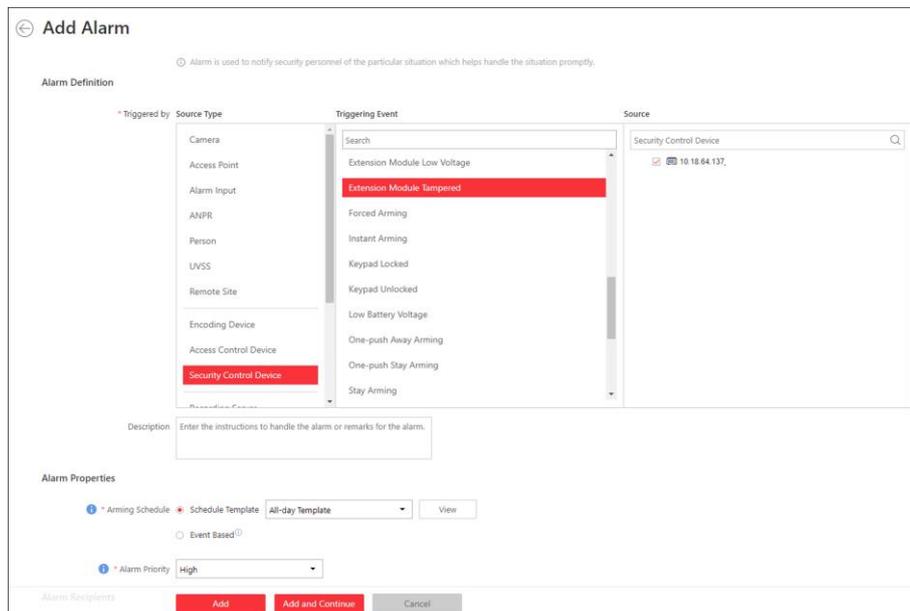


Figura 13-33 Adicionar alarme para dispositivo de controle de segurança

2. Defina o **Dispositivo de Controle de Segurança** como o tipo de origem no campo **Acionado por**.
3. Selecione um evento de acionamento e um dispositivo específico como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O dispositivo é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido

pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte *Definições de alarme*.

Destinatários do alarme

Selecione um usuário para enviar as informações de alarme e o usuário pode receber as informações de alarme quando ele/ela faz login no HikCentral através do Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.



Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e arquivos de vídeo gravados quando o alarme ocorrer.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na

parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.

- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.4.12 Adicionar alarme para servidor de transmissão e servidor de gravação

Você pode definir alarmes de exceção de servidor para servidores adicionados (Servidor de transmissão e Servidor de Gravação) e configurar uma série de ações de vinculação (p. ex., acionando janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando precisar adicionar alarmes para Servidor de transmissão e Servidor de gravação adicionados.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

The screenshot shows the 'Add Alarm' configuration interface. It is divided into two main sections: 'Alarm Definition' and 'Alarm Properties'.
In the 'Alarm Definition' section, there are three columns:

- Triggered by: Source Type:** A list of source types including Remote Site, Encoding Device, Access Control Device, Security Control Device, Recording Server (highlighted), Streaming Server, HikCentral Server, User, User-Defined Event, and Generic Event.
- Triggering Event:** A list of events including Array Degradation (highlighted), Array Detection, Array Expansion, Array Initialization, Array Rebuilding, Array Repair, Array Unavailable, Bad Disk, Chip Temperature Too High, and CPU Temperature Too High.
- Source:** A search box and a list containing Recording Server.

Below these columns is a 'Description' field with the placeholder text 'Enter the instructions to handle the alarm or remarks for the alarm.'

In the 'Alarm Properties' section, there are two radio buttons: 'Arming Schedule' (selected) and 'Schedule Template'. Below them is a checked option for 'Event Based'. At the bottom, there are three buttons: 'Add', 'Add and Continue', and 'Cancel'.

Figura 13-34 Adicionar alarme para servidor de transmissão e servidor de gravação

2. Definir o **Servidor de gravação** ou **Servidor de transmissão** como o tipo de origem no campo **Acionado por**.
3. Selecione um evento de acionamento específico e um servidor específico como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O servidor é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.



Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Exiba a janela de alarme no Control Client para mostrar os detalhes do alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é

acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

Depois de adicionar o alarme, ele é exibido na lista de alarmes e você pode visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme

Clique em  na coluna operação para editar o alarme.

Copiar para outros alarmes

Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote.

Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em **Copiar para**.

Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em **OK**.

Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.4.13 Adicionar alarme para servidor HikCentral

Você pode definir o alarme para a exceção (incluindo exceção de hardware e serviço) dos servidores que foram instalados com os serviços HikCentral (como serviço VSM, porta de acesso a dispositivos de terceiros, serviço NGINX, serviço proxy de teclado, serviço de gerenciamento de smart wall, etc.) e configurar uma série de ações de vinculação (por exemplo, acionando janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando precisar adicionar um novo alarme para a exceção do servidor HikCentral.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.
2. Defina **Servidor HikCentral** como o tipo de origem no campo **Acionado por**.

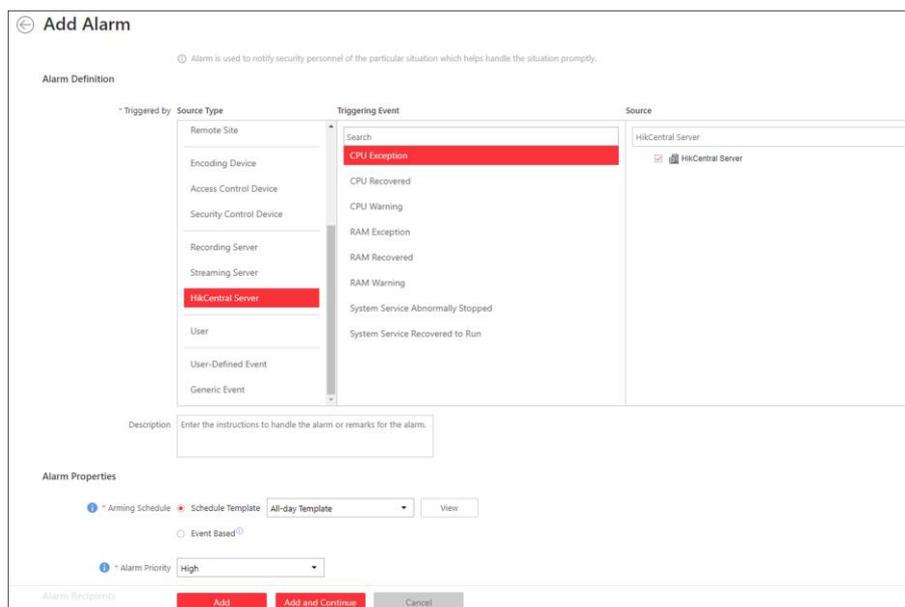


Figura 13-35 Adicionar alarme para servidor HikCentral

3. Selecione um evento de acionamento específico e selecione **Servidor HikCentral** na lista **Origem** como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O servidor é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para detalhes sobre como configurar um modelo personalizado, consulte **Configure Arming Schedule Template (Configurar o modelo de programação de arme)**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para detalhes sobre como definir a prioridade do alarme, consulte **Configurações de Alarme**.

Destinatários do alarme

Selecione um usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o login no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.



Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e arquivos de vídeo gravados quando o alarme ocorrer.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede

inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para detalhes sobre como configurar o evento definido pelo usuário, consulte **Configurar evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

Depois de adicionar o alarme, ele é exibido na lista de alarmes e você pode visualizar o nome do alarme e o status do alarme.

8. Realize as seguintes operações depois de adicionar o alarme.

Editar alarme

Clique em  na coluna operação para editar as informações do alarme.

Copiar para outros alarmes

Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote.

Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em **Copiar para**.

	Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique em habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique em Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.4.14 Adicionar alarme para usuário

Você pode definir alarmes para os usuários, incluindo o login do usuário e o logout do usuário, e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando você precisar adicionar um novo alarme para os usuários do sistema.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.
2. Defina **Usuário** como o tipo de origem no campo **Acionado por**.

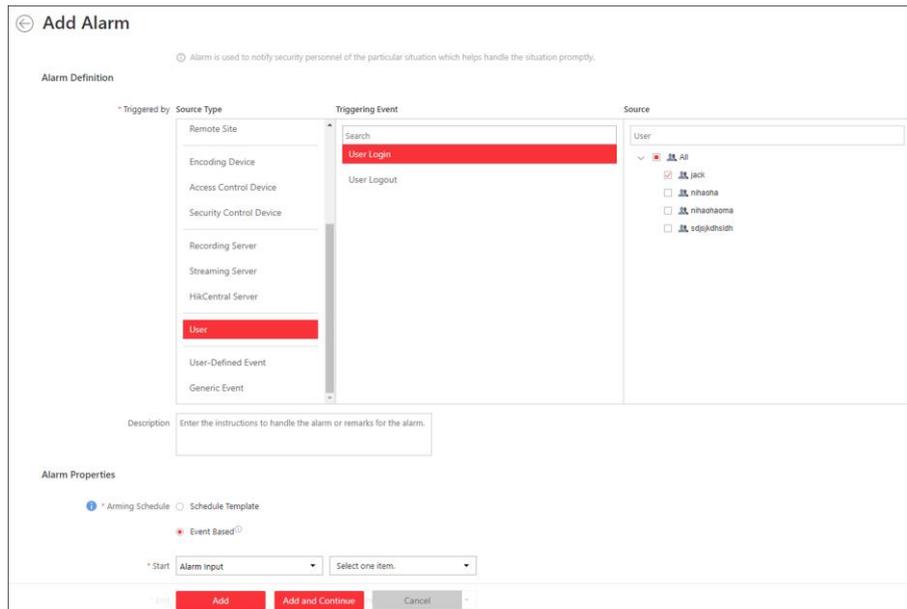


Figura 13-36 Adicionar alarme para usuário

3. Selecione um evento de acionamento específico e um usuário específico como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

O usuário é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar outro usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione o usuário para o qual serão enviadas as informações de alarme e o usuário poderá receber as informações de alarme quando ele/ela fizer o logon no HikCentral via Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Ele exibe a janela de alarme no Control Client para mostrar os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e a reprodução quando ocorrer um alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar as informações do alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .

Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique em habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique em Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.4.15 Adicionar alarme para evento definido pelo usuário

Você pode definir alarmes para o evento adicionado definido pelo usuário e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme for acionado.

Antes de começar

Você deve criar pelo menos um evento definido pelo usuário. Para detalhes, consulte **Configurar evento definido pelo usuário**.

Execute esta tarefa quando precisar adicionar um novo alarme para o evento definido pelo usuário.

Etapas

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.
2. Defina **Evento definido pelo usuário** como o tipo de origem no campo **Acionado por**.

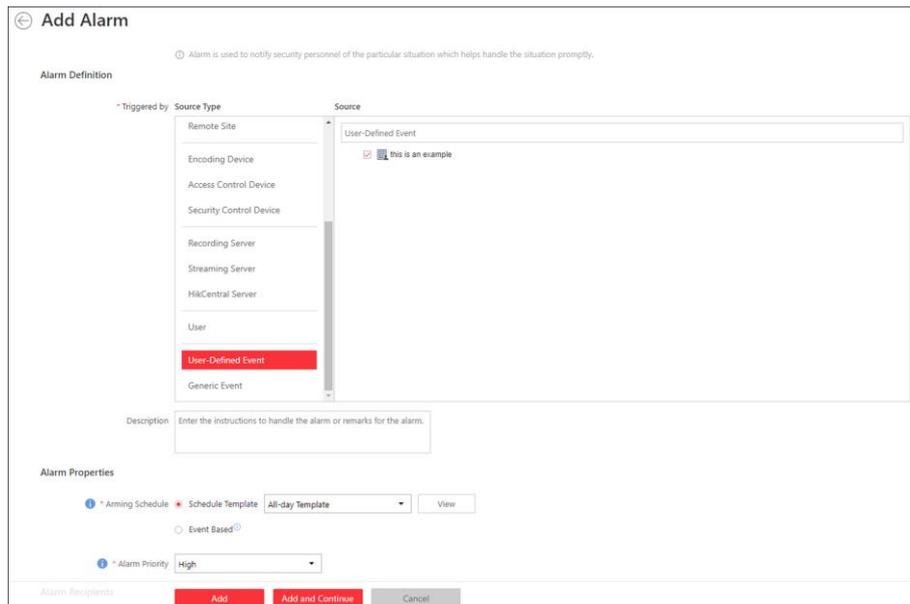


Figura 13-37 Adicionar alarme para evento definido pelo usuário

3. Selecione um evento específico definido pelo usuário como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Configure os parâmetros necessários.

Agendamento de armação

O evento é armado durante a programação de armar e o evento ocorrido durante a programação de armar será acionado como alarme e notificará o usuário. Ele fornece dois tipos de programação de arme:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione um usuário para enviar as informações de alarme e o usuário pode receber as informações de alarme quando ele/ela faz logon no HikCentral através do Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Ele mostra a janela de alarme no Control Client para exibir os detalhes do alarme e todos os vídeos ao vivo das câmeras relacionadas ao alarme e a reprodução quando ocorrer um alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista de alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme	Clique em  na coluna operação para editar o alarme.
Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.

Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em ☑ na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em ☒ na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em ☑ para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.16 Adicionar alarme para evento genérico

Você pode definir alarmes para o evento genérico adicionado e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme for acionado.

Antes de começar

Você deve criar pelo menos um evento genérico. Consulte **Configurar evento genérico** para detalhes sobre a criação do evento genérico.

Execute esta tarefa quando precisar adicionar um alarme para o evento genérico adicionado.

Etapas

1. Clique em **Evento e Alarme → Alarme → Adicionar** na página inicial.

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Alarm Definition

Triggered by: Source Type

Source

Generic Event Name

3423

4400

Generic Event

Description: Enter the instructions to handle the alarm or remarks for the alarm.

Alarm Properties

Arming Schedule: Schedule Template (All-day Template) View

Event Based

Alarm Priority: High

Alarm Recipients: Add Add and Continue Cancel

Figura 13-38 Adicionar alarme para evento genérico

2. Selecione **Evento genérico** como o tipo de fonte no campo **Acionado por**.
3. Selecione um evento genérico específico como a fonte para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Configure os parâmetros necessários.

Agendamento de armação

O evento é armado durante a programação de armar e quando ocorre um evento durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de arme para o alarme para definir quando o alarme será acionado. Para detalhes sobre como configurar um modelo personalizado, consulte **Configure Arming Schedule Template (Configurar o modelo de programação de arme)**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para detalhes sobre como definir a prioridade do alarme, consulte **Configurações de Alarme**.

Destinatários do alarme

Selecione um usuário para enviar as informações de alarme e o usuário pode receber as informações de alarme quando ele/ela faz logon no HikCentral através do Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.



Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Janela Pop-up de acionamento

Selecione para exibir a janela de alarme no Control Client para mostrar os detalhes do alarme quando o alarme ocorrer.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.
- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou

substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para detalhes sobre como configurar o evento definido pelo usuário, consulte **Configurar evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme

Clique em  na coluna operação para editar o alarme.

Copiar para outros alarmes

Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote.

Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em **Copiar para**.

Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em **OK**.

Excluir alarme	Clique em ✕ na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em ☑ na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique em habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em ☐ na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em 📢 para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente como você deseja.

13.4.17 Adicionar alarme para local remoto

Se o sistema for um Sistema Central com módulo de Gerenciamento Remoto de Local (com base em licença adquirida), você pode definir o alarme offline do site para Local Remoto adicionado e configurar uma série de ações de vinculação (por exemplo, acionando a janela pop-up no Control Client) para notificação quando o alarme é acionado.

Execute esta tarefa quando precisar adicionar o alarme para local remoto.

Etapas

Observação

Você pode definir alarmes para o Local Remoto adicionado somente quando o sistema tiver o módulo Gerenciamento Remoto de Local.

1. Clique em **Evento & Alarme** → **Alarme** → **Adicionar** para entrar na página Adicionar alarme.

Alarm Definition

Alarm is used to notify security personnel of the particular situation which helps handle the situation promptly.

Triggered by: Source Type: Camera, Access Point, Alarm Input, ANPR, Person, UVSS, Remote Site, Encoding Device, Access Control Device, Security Control Device

Triggering Event: Site Offline

Source: Remote Site, 127.0.0.1_80

Description: Enter the instructions to handle the alarm or remarks for the alarm.

Alarm Properties

Arming Schedule: Schedule Template, All-day Template, View

Event Based

Alarm Priority: High

Alarm Recipients: Add, Add and Continue, Cancel

Figura 13-39 Adicionar alarme no Local Remoto

2. Defina **Local Remoto** como o tipo de origem no campo **Acionado por**.
3. Selecione um evento de acionamento e um local remoto específico como a origem para acionar o alarme.
4. Opcional: Insira a instrução de como lidar com o alarme ou insira as observações para o alarme.
5. Preencha as informações solicitadas.

Agendamento de armar

Os recursos no local remoto estão armados durante o agendamento de armar e quando um evento ocorre durante a programação de armar, um alarme será acionado para notificar o usuário. São fornecidos dois tipos de programação de armar:

- **Modelo de cronograma:** Selecione um modelo de programação de armar para o alarme para definir quando o alarme será acionado. Para definir o modelo personalizado, consulte **Configurar modelo de agendamento de armar**.
- **Evento baseado:** Especifique um evento definido pelo usuário ou uma entrada de alarme como o evento de início ou término do agendamento de armar. Quando o evento definido pelo usuário ou a entrada de alarme é acionada, a programação de armar iniciará ou terminará.

Prioridade de alarme

Define a prioridade para o alarme. A prioridade pode ser usada para filtrar alarmes no Control Client. Para definir a prioridade do alarme, consulte **Definições de alarme**.

Destinatários do alarme

Selecione um usuário para enviar as informações de alarme e o usuário pode receber as informações de alarme quando ele/ela faz login no HikCentral através do Control Client ou Mobile Client.

6. Opcional: Defina as configurações adicionais do alarme, tais como câmeras relacionadas ao alarme e mapa, e ações de ligação de alarme

Câmera relacionada

Você pode ver o vídeo ao vivo e reproduzir os arquivos de vídeo gravados quando o alarme ocorre na central de alarmes do Control Client.

- Selecione as câmeras para gravar o vídeo do alarme quando o alarme é acionado.
- **Pós-gravação:** Gravar vídeo a partir de períodos após alarmes detectados. Especifique o número de segundos que você deseja gravar vídeo para depois que o alarme parar.
- **Ver vídeo de pré-alarme:** Se a câmara tiver gravado ficheiros de vídeo antes do alarme, pode ver o vídeo gravado a partir de períodos anteriores ao alarme. Especifique o número de segundos que você deseja exibir o vídeo gravado antes do início do alarme. Por exemplo, quando alguém abre uma porta, você pode ver o vídeo gravado para ver o que acontece logo antes da porta ser aberta.
- **Bloqueio de arquivos de vídeo por:** Defina os dias para proteger o arquivo de vídeo de ser substituído.
- **Exibir vídeo por padrão:** Defina o vídeo padrão a ser exibido no Control Client ao verificar as informações de alarme acionadas.

Observação

- Certifique-se de que as câmaras relacionadas foram configuradas com a programação de gravação.
 - Até 16 câmeras podem ser definidas como câmera relacionada.
-

Mapa relacionado

Exiba a localização do local remoto no mapa GIS ou quando você verificar os detalhes do alarme na central de alarmes e na pesquisa de alarmes e eventos do Control Client.

Observação

Você deve localizar o mapa no mapa GIS primeiro. Para obter detalhes, consulte **Localizar locais no mapa**.

Janela Pop-up de acionamento

Exiba a janela de alarme no Control Client para mostrar os detalhes do alarme.

Visualização no Smart Wall

Exiba o vídeo de alarme da câmera relacionada do alarme ou exiba a visão pública especificada na parede inteligente. Você pode selecionar a parede inteligente adicionada e selecionar que janela para indicar o alarme.

- **Câmeras relacionadas do alarme:** Exiba o vídeo das câmeras relacionadas do alarme na parede inteligente. Você pode selecionar para exibir o vídeo em que parede inteligente e qual janela. Selecione o tipo de transmissão para o vídeo de alarme exibido na parede inteligente.
- **Exibição pública:** Um modo de exibição permite que você salve a divisão de janela e a

correspondência entre câmeras e janelas como favoritos para acessar rapidamente as câmeras relacionadas mais tarde. Se você selecionar **Exibição pública**, quando o alarme for acionado, o sistema poderá exibir a exibição pública selecionada na parede inteligente especificada e os usuários poderão visualizar o vídeo das câmeras pré-definidas na exibição.

- **Parar a exibição do alarme:** Defina quando o sistema parará de exibir o alarme na parede inteligente. O sistema pode parar de exibir o alarme dentro de segundos especificados, ou substituir o alarme original quando outro alarme com maior prioridade de alarme é acionado.

Restringir o tempo de manipulação do alarme

Quando o alarme é acionado, você precisa de segurar o alarme no Control Client. Ative esta função para acionar eventos definidos pelo usuário ou saída (s) de alarme se o alarme não for manipulado dentro do tempo de manuseio do alarme configurado.

Observação

- Até 16 eventos definidos pelo usuário e saídas de alarme podem ser definidos como o evento acionado ao manipular o alarme esgotado.
 - Para configurar o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

Aviso audível de acionamento

Defina o texto de voz para reproduzir no PC quando o alarme for acionado.

Observação

Você deve definir o mecanismo de voz como som de alarme na página de Configurações de sistema do Control Client.

Acionar Eventos de Movimento

Acionar o evento definido pelo usuário (s) quando o alarme é acionado.

Observação

- Até 16 eventos definidos pelo usuário podem ser selecionados como ligação de alarme.
 - Para definir o evento definido pelo usuário, consulte **Configurar o evento definido pelo usuário**.
-

7. Termine de adicionar o alarme.

- Clique em **Adicionar** para adicionar o alarme e retornar à página de lista dos alarmes.
- Clique em **Adicionar e continuar** para adicionar o alarme e continuar adicionando outros alarmes.

O alarme será exibido na lista de alarmes e você poderá visualizar o nome do alarme e o status do alarme.

8. Opcional: Realize as seguintes operações depois de adicionar o alarme.

Editar alarme

Clique em  na coluna operação para editar o alarme.

Copiar para outros alarmes	Você pode copiar os parâmetros especificados do alarme atual para outros alarmes adicionados para a configuração em lote. Clique em  na coluna operação para entrar na página de detalhes do alarme e clique em Copiar para . Especifique as configurações do alarme de origem, selecione alarme (s) de destino e clique em OK .
Excluir alarme	Clique em  na coluna Operação para excluir o alarme.
Excluir todos os alarmes	Clique Deletar Tudo para deletar todos os alarmes adicionados.
Excluir todos os alarmes inválidos	Clique Deletar todos os itens inválidos para deletar todos os alarmes inválidos em um lote.
Habilitar alarme	Clique em  na coluna operação para ativar o alarme.
Habilitar todos os alarmes	Clique habilitar tudo para habilitar todos os alarmes adicionados.
Desativar alarme	Clique em  na coluna operação para desabilitar o alarme.
Desabilitar todos os alarmes	Clique Desabilitar Tudo para desabilitar todos os alarmes adicionados.
Alarme de teste	Clique em  para acionar este alarme automaticamente. Você pode testar se as ações de vinculação funcionam corretamente.

13.5 Configurar modelo de agendamento de armar

Ao definir o evento e o alarme, você pode selecionar o modelo de agendamento de armar predefinida para definir quando o evento ou alarme será acionado. O sistema predefine três modelos de agendamento de armar padrão: Modelo de dia inteiro, modelo da semana e modelo de fim de semana. Você também pode adicionar um modelo personalizado de acordo com as necessidades reais.

Etapas

1. Clique em **Sistema** na página inicial.
2. Clique em **agendamento** → **armar do modelo de agendamento** à esquerda.
3. Clique em **Adicionar** para inserir a página de agendamento de armar de adição.

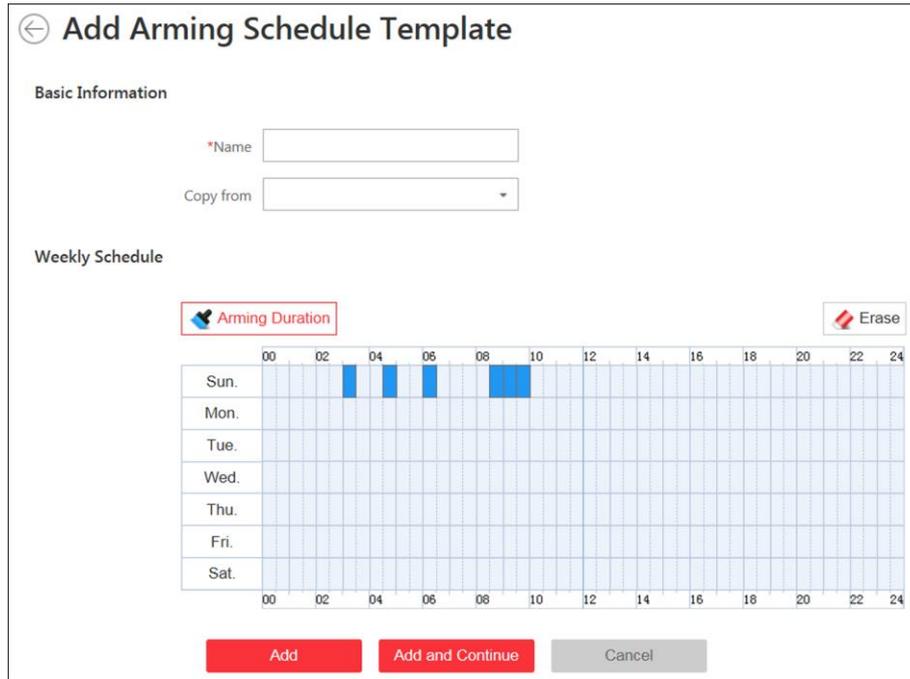


Figura 13-40 Adicionar página de modelo de agendamento de armar

4. Preencha as informações solicitadas.

Nome

Defina um nome para o modelo.

Copiar de

Opcionalmente, selecione copiar as configurações de outros modelos definidos.

5. Clique em **duração de armar** e arraste na barra de tempo para definir os períodos de tempo.

 **Observação**

Até 4 períodos de tempo podem ser definidos para cada dia.

6. Opcional: Clique em **Apagar** e clique no período de tempo desenhado para limpar o período de tempo correspondente.

7. Termine de adicionar o modelo de programação de armar.

- Clique em **Adicionar** para adicionar o modelo e volte para a página de listagem do modelo de agendamento de armar.
- Clique em **Adicionar e continuar** para adicionar o modelo de alarme e continuar adicionando outros alarmes.

O modelo de agendamento de armar será exibido na lista de modelos de agendamento de armar.

8. Opcional: Execute as seguintes operações depois de adicionar o modelo de programação de armar.

Exibir Detalhes do Modelo Clique no modelo para exibir seus detalhes.

- Edição do modelo** Clique em  na coluna operação para editar os detalhes do modelo.
- Excluir o modelo** Clique em  na coluna de operação para excluir o modelo.
- Exclusão de todos os modelos** Clique em **Excluir tudo** para excluir todos os modelos adicionados (exceto os modelos padrão). Se os modelos adicionados tiverem sido utilizados por eventos ou alarmes, ser-lhe-á perguntado se pretende ou não substituir a agenda.

Capítulo 14 Gerenciar mapa

Dois tipos de mapas estão disponíveis: Mapa GIS e E-map. No mapa GIS, você pode definir e exibir o site atual, o site remoto e a localização geográfica do elemento. No e-MAP, que é um mapa estático, você pode definir e visualizar as localizações geográficas das câmeras instaladas, entradas de alarme, e saídas de alarme, etc. Depois de configurar o mapa via Web Client, você pode visualizar o vídeo ao vivo e a reprodução dos recursos adicionados ao mapa via Control Client e receber uma mensagem de notificação do mapa via Control Client quando um alarme é acionado. Com o mapa GIS, você pode ver as localizações geográficas do seu sistema de vigilância. Este tipo de mapa usa um sistema de informação geográfica para mostrar com precisão todos os pontos quentes' (recursos (por exemplo, câmera, entrada de alarme) colocados no mapa são chamados de pontos quentes) localizações geográficas no mundo real. O mapa GIS permite visualizar e acessar câmeras em vários locais ao redor do mundo de forma geograficamente correta. Se os recursos localizarem em vários locais (por exemplo, cidades diferentes, países diferentes), o mapa GIS pode dar a você uma visão única para mostrar a todos eles e ajudá-lo a ir rapidamente para cada local para ver o vídeo das câmeras. Com a região quente, você pode vincular ao e-MAP para exibir o cenário de monitoramento detalhado, por exemplo, o cenário de monitoramento de um edifício.

E-mapa é uma imagem estática (não tem que ser mapas geográficos, embora muitas vezes sejam. Dependendo das necessidades da sua organização, fotos e outros tipos de arquivos de imagem também podem ser usados como e-mapas) que lhe dá uma visão geral dos locais e distribuições dos pontos quentes (recursos (por exemplo, câmera, entrada de alarme) colocados no mapa são chamados de pontos quentes). Você pode ver os locais físicos das câmeras, entradas de alarme, e saídas de alarme, etc, e em que direção as câmeras estão apontando. Com a função da região quente, os e-mapas podem ser organizados em hierarquias para navegar de grandes perspectivas para perspectivas detalhadas, por exemplo, do nível do piso ao nível da sala.

Depois de configurar o e-mapa através do Web Client, você pode ver o vídeo ao vivo e a reprodução dos elementos através do Control Client, e receber uma mensagem de notificação do mapa via Control Client quando um alarme é acionado.

14.1 Definir Mapa GIS e Ícones

Esta página permite que você habilite a função de mapa GIS (sistema de informações geográficas) para exibir o mapa de GIS no Web Client e no Control Client, para que a localização geográfica dos recursos (como site atual, sites remotos, câmeras) possa ser mostrada no mapa.

Execute esta tarefa para definir a URL da API do mapa GIS e ícones personalizados.

Etapas

1. Clique em **Sistema** → **Normal** → **Mapa** para acessar à página de definições do mapa.
2. Definir o mapa GSI
 - 1) Definir o seletor **Mapa GIS** como ON para ativar a função de mapa GIS.

2) Insira o URL da API do mapa GIS.

 **Observação**

- A API do Google Map é suportada atualmente.
 - O Google Maps é fornecido pela Google Inc. (doravante denominado "Google"). Nós só fornecemos as URLs para usar o Google Maps. Você deve aplicar por si mesmo para o uso do Google Maps a partir do Google. Você deve cumprir com os termos do Google e fornecer determinadas informações ao Google, se necessário.
-

3. Defina os ícones personalizados.

Selecione a região quente ou o ponto de acesso como o tipo de ícone no campo **Tipo**.

2) defina o tamanho do ícone, incluindo a largura (px) e a altura (px).

3) Opcional: Clique no ícone  para cancelar a proporção.

 **Observação**

Por padrão, a taxa de proporção é mantida.

4) Clique em **Adicionar** no campo imagem para selecionar um arquivo de imagem do caminho local.

 **Observação**

O formato de imagem de ícone só pode ser BMP, PNG, JPG ou JPEG.

As imagens adicionadas são exibidas como visualização em miniatura no campo imagem.

4. Clique em **Salvar**.

Resultado

Você pode visualizar o mapa GIS na página exibição lógica e executar as seguintes operações na área do mapa.

Filtro	Clique em  e selecione o tipo de objeto que você deseja mostrar no mapa.
Tela inteira	Clique em  para mostrar o mapa no modo de tela inteira.
Aumentar/reduzir o zoom	Desloque a roda do mouse ou clique em  /  para aumentar o zoom ou diminuir o zoom do mapa.
Ajustar a área do mapa	Clique e arraste o mapa para ajustar a área do mapa para visualização.

14.2 Vincular e-map para a área

Você pode adicionar e vincular mapas eletrônicos à área para que os elementos atribuídos à área possam ser adicionados ao e-MAP.

Execute a tarefa quando desejar vincular e-MAP à área.

Etapas

1. Clique em **exibição Lógica**.
2. Estão disponíveis três maneiras para adicionar o e-mapa.

Adicionar e-map ao adicionar área

1. Clique em **+** no painel de lista de áreas.
2. Defina os parâmetros para adicionar a área.
3. Defina o seletor de **mapa relacionado** para ON.
4. Passe o mouse sobre o campo mapa e vincule um mapa para a área.

Você pode clicar em **carregar imagem** e selecionar uma imagem do PC local como o e-map. Ou clicar em **mapa existente** e selecione um mapa existente para vincular à área atual

5. **Opcional:** Repita a etapa anterior para adicionar mais e-maps para a área.

Adicionar e-map ao editar área

1. Selecione um mapa e clique em  no painel de lista de área para entrar na página de edição da área.
2. Edite as configurações de área conforme desejado.
3. Defina o seletor **mapa relacionado** como ON se estiver desativada.
4. Passe o mouse sobre o campo mapa vazio e vincule um mapa para a área.

Você pode clicar em **carregar imagem** e selecionar uma imagem do PC local como o e-map. Ou clicar em **mapa existente** e selecione um mapa existente para vincular à área atual

5. **Opcional:** Repita a etapa anterior para adicionar mais e-maps para a área.

Vincular diretamente mapa para a área existente

Observação

Você pode adotar essa maneira quando o mapa GIS não estiver habilitado.

1. Clique em  para mostrar a área do mapa.
2. Clique em **Relacionar mapa** para adicionar e vincular o mapa.
3. Selecione as áreas para vincular e-maps.
4. Passe o mouse sobre o campo mapa e vincule um mapa para a

área.

Você pode clicar em **carregar imagem** e selecionar uma imagem do PC local como o e-map. Ou clicar em **mapa existente** e selecione um mapa existente para vincular à área atual

5. **Opcional:** Repita a etapa anterior para adicionar mais e-maps para a área.

3. Opcional: Passe o mouse sobre a área de e-map adicionada para executar as operações a seguir.

Editar Imagem	Clique e altere uma imagem.
Editar o nome do mapa	Clique e defina um nome personalizado para o mapa.
Desvincular mapa	Clique para remover o mapa ou cancelar a ligação entre o mapa e a área.

4. Clique em **Salvar** para confirmar as configurações.

5. Opcional: Execute as seguintes operações após adicionar o mapa na área do mapa.

Filtro	Clique em  e selecione o tipo de objeto que você deseja mostrar no mapa.
Tela inteira	Clique em  para mostrar o mapa no modo de tela inteira.
Aumentar/reduzir o zoom	Desloque a roda do mouse ou clique em  /  para aumentar o zoom ou diminuir o zoom do mapa.
Ajustar a área do mapa	Arraste o mapa ou a janela vermelha na parte inferior para ajustar a área do mapa para visualização.

14.3 Pesquisa de Localização

Você pode pesquisar os locais no mapa GIS.

Antes de começar

Você deve ativar a função de mapa GIS e definir a URL da API de mapa GIS corretamente. Para detalhes, consulte **Ajuste o mapa e os ícones do GIS**.

Realize esta tarefa quando precisar pesquisar os locais no mapa GIS.

Etapas

1. Clique em **exibição lógica** na página inicial.
2. Clique em  para mostrar a área do mapa.
3. Insira um nome de local que você deseja pesquisar no  campo.

Os locais relacionados são exibidos no campo de pesquisa.

4. Clique para selecionar a localização que pretende localizar a partir das localizações relacionadas.

Resultado

O local será localizado no mapa.

14.4 Localizar locais no mapa

Você pode definir o site atual e adicionar local do site remoto para o mapa GIS.

Antes de começar

Você deve ativar a função de mapa GIS e definir a URL da API de mapa GIS corretamente. Para detalhes, consulte *Ajuste o mapa e os ícones do GIS*.

Execute esta tarefa quando você precisa de ajustar a posição dos locais ao mapa do GIS.

Etapas

1. Clique em **exibição lógica** na página inicial.
2. Clique em  para mostrar a área do mapa.
3. Selecione o local atual ou o local remoto na lista suspensa no painel de lista de áreas.

Observação

O ícone  indica que o local é o local atual, e  indica locais remotos.

4. Clique em **Localizar** na área do mapa GIS.

Observação

O botão **Localizar** só está disponível quando o local não está localizado no mapa GIS.

5. Opere o mapa GIS para encontrar a localização do local e clique no mapa para localizar o local no mapa.

Observação

Você pode usar o mouse para arrastar, ampliar e diminuir o zoom do mapa.

Depois de localizado com êxito, o ícone do local será exibido no local selecionado.

6. Opcional: Execute as seguintes operações depois de adicionar o site ao mapa GIS.

Exibir detalhes do local

Clique no ícone do local para visualizar os detalhes do local, incluindo o endereço do local, localização e informações de observação

Editar

Clique no ícone do local e clique em **editar** para editar a informação do local.

Excluir

Clique no ícone do local e clique em **excluir** para remover o local do

mapa.

Exibir os recursos do local

Clique no ícone do local e clique em **exibir recursos do local** para visualizar os recursos do site.

14.5 Adicionar área de destaque

Você pode adicionar elementos como a área de destaque e colocar o ponto de acesso no e-map ou mapa GIS.

Antes de começar

Um mapa deve ter sido adicionado. Refira o *e-map de vinculação à área* ou *definir mapa GIS e ícones* para detalhes sobre a adição do e-mapa ou do mapa do GIS.

Execute esta tarefa quando você precisa obter a visualização ao vivo e informações de alarme dos cenários de vigilância através da área de destaque no mapa.

Etapas

1. Clique em **Exibição Lógica** na página inicial.
2. Selecione o local atual na lista suspensa no painel de lista de áreas.

Observação

O ícone  indica que o local é o local atual, você só pode adicionar elementos do local atual como as áreas de destaque.

3. Estão disponíveis três maneiras para adicionar a área de destaque.

Adicionar a área de destaque ao adicionar elemento à área

1. Clique na guia para inserir a página de elemento correspondente.
2. Clique em + na área do elemento.
3. Defina os parâmetros necessários para adicionar o elemento à área.

Observação

Para obter detalhes, consulte *Adicionar elemento à área*.

4. Marque a caixa de seleção **Adicionar ao mapa** e a área do mapa será exibida.
5. Na área do mapa, clique para selecionar um mapa para adicionar a área de destaque.
6. Clique **Adicionar** e você pode ver o resultado do elemento de adição na caixa de diálogo pop-up.

Arrastar elemento para o mapa

 **Observação**

Você pode adotar essa maneira quando o elemento é adicionado à área, mas não adicionado ao mapa.

1. Clique na guia para inserir a página de elemento correspondente.
2. **Opcional: Opcional:** Clique para selecionar uma área para que os elementos desta área sejam exibidos.
3. Clique em  para mostrar a área do mapa.
4. Na área do mapa, clique para selecionar um mapa para adicionar a área de destaque.
5. Arraste um elemento com adicionado ao mapa como não ao mapa.

Adicionar ponto de acesso ao editar o elemento

 **Observação**

Você pode adotar essa maneira quando o elemento é adicionado à área, mas não adicionado ao mapa.

1. Clique na guia para inserir a página de elemento correspondente.
2. **Opcional: Opcional:** Clique para selecionar uma área para que os elementos desta área sejam exibidos.
3. Clique no campo nome do elemento com adicionado ao mapa como não.
4. Defina o seletor de **mapa relacionado** para ON.
5. Na área do mapa, clique para selecionar um mapa para adicionar a área de destaque.
6. Configure as configurações necessárias para a área de destaque.
7. Clique em **Salvar**.

4. Opcional: Execute as seguintes operações depois de adicionar a área de destaque.

Ajuste a localização da área de destaque

Arraste a área de destaque adicionado no mapa para os locais desejados.

Adicionar ponto de acesso

Clique no ícone de ponto de acesso adicionado no mapa e clique em **Editar** para edit as informações detalhadas (como a definição da localização GPS (disponível apenas quando o mapa principal é o mapa GIS e consulte **Pesquisa de localização** para detalhes), e selecionando o estilo de ícone).

Para o ponto de acesso da câmera, você também pode editar a área de detecção, incluindo raio, direção e ângulo, ou arrastar o setor exibido no mapa para ajustar diretamente a área de detecção.

Excluir ponto de acesso

Clique no ícone do ponto de acesso e clique em **excluir** para remover o local do mapa.

14.6 Região da área de destaque

A função da área de destaque vincula um mapa a outro mapa. Ao adicionar um mapa a outro mapa como uma região de destaque, um ícone do link para o mapa adicionado será exibido no mapa principal. O mapa adicionado é chamado submapa e o mapa a que se acrescenta a área de destaque é o mapa principal.

Antes de começar

Pelo menos 2 mapas devem ter sido adicionados. Refira o ***e-map de vinculação à área*** ou ***definir mapa GIS e ícones*** para detalhes sobre a adição dos mapas.

Realize essa tarefa quando desejar vincular um mapa a outro mapa para acesso conveniente.

Etapas

1. Clique em **Exibição Lógica** na página inicial.
2. Selecione o local atual na lista suspensa no painel de lista de áreas.

Observação

O ícone  indica que o local é o local atual, você só pode adicionar região da área de destaque para o local atual.

3. Clique em  para mostrar a área do mapa.
4. Selecione um e-map adicionado ou mapa GIS como mapa principal.
5. Clique em  na área do mapa e clique no local onde você deseja colocar a região de destaque. Aparece uma caixa de diálogo para definir o submapa.
6. Selecione um mapa menor no painel para defini-lo como a região de destaque do mapa atual.
7. Clique em **Salvar** na caixa de diálogo para adicionar a região de destaque. O ícone de região de destaque adicionado será exibido no mapa principal.
8. Opcional: Execute as seguintes operações depois de adicionar a região de destaque.

Ajuste a localização da área de destaque

Arraste a área de destaque adicionada no mapa para os locais desejados.

Editar áreas de destaque

Clique no ícone de região de destaque adicionado no mapa para visualizar e editar as informações detalhadas, incluindo a localização GPS (disponível apenas quando o mapa principal é o mapa SIG e consulte ***Pesquisa de localização*** para detalhes), nome de região de destaque, estilo de ícone, cor de nome e observações na caixa de diálogo aparecendo.

Excluir região de

Clique no ícone de região quente no mapa e clique em **excluir** na

destaque

caixa de diálogo que aparece para excluir a região de destaque.

14.7 Adicionar etiquetas

Você pode adicionar etiquetas com a descrição no mapa.

Antes de começar

Pelo menos um mapa deve ter sido adicionado. Refira o ***e-map de vinculação à área*** ou ***definir mapa GIS e ícones*** para detalhes sobre a adição do e-mapa ou do mapa do GIS.

Execute essa tarefa quando precisar adicionar etiqueta no mapa.

Etapas

1. Clique em **Exibição Lógica** na página inicial.
2. Selecione o local atual na lista suspensa no painel de lista de áreas.

Observação

O ícone  indica que o local é o local atual, você só pode adicionar etiqueta para o local atual.

3. Clique em  para mostrar a área do mapa.
4. Selecione um mapa para adicionar etiqueta para.
5. Clique em  na área do mapa e clique no local onde você deseja colocar a etiqueta.
6. Personalize um nome para a etiqueta e você pode inserir o conteúdo para a etiqueta conforme desejado.
7. Clique em **Salvar**.
O ícone de etiqueta adicionado será exibido no mapa.
8. Opcional: Realize as seguintes operação (es) depois de adicionar a etiqueta.

Ajustar a localização da etiqueta Arraste a etiqueta adicionada no mapa para os locais desejados.

Editar etiqueta Clique no ícone da etiqueta adicionada no mapa para visualizar e editar as informações detalhadas, incluindo o nome e o conteúdo na caixa de diálogo que aparece.

Excluir etiqueta Clique no ícone da etiqueta no mapa e clique em **excluir** na caixa de diálogo que aparece para excluir a etiqueta.

Capítulo 15 Gerenciar veículo

Você pode importar as informações do veículo de acordo com o modelo pré-definido e você pode adicionar as informações do veículo manualmente. As informações dos veículos adicionados podem ser usadas para alarme ANPR ao adicionar o alarme.

Observação

Consulte **Adicionar alarme para câmera ANPR** para obter informações detalhadas sobre como adicionar alarme.

15.1 Adicionar lista de veículos

Antes de adicionar as informações do veículo ao sistema, você deve criar a lista de veículos.

Execute as seguintes etapas para adicionar a lista de veículos.

Etapas

Observação

Até 100 listas de veículos podem ser adicionadas ao sistema.

1. Clique em **Veículo** para entrar na página de gerenciamento de veículos.
2. Clique em **+** à esquerda para abrir a janela de lista de veículos.

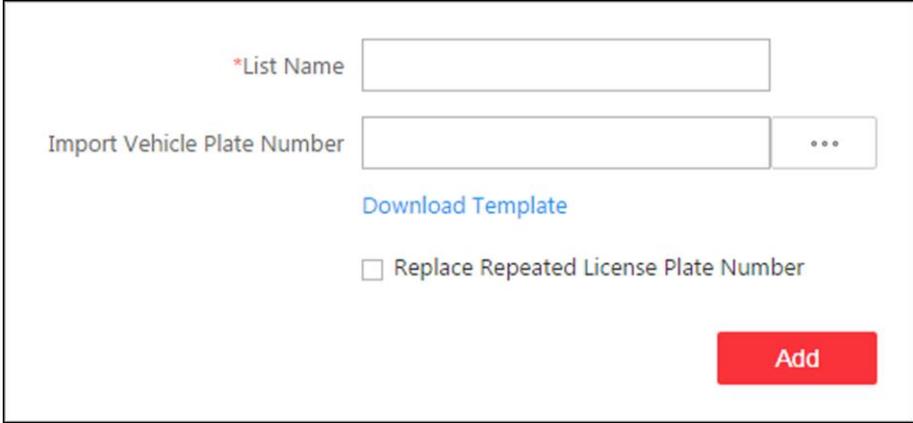


Figura 15-1 Adicionando a janela da lista do veículo

3. Defina um nome descritivo para a lista de veículos.
4. Opcional: Clique em **modelo de download** e importar informações do veículo em um lote, ou você pode importar informações do veículo ao verificar detalhes da lista de veículos. Consulte **Adicionar informações do veículo** para detalhes.

5. Opcional: Verifique **substitua o número repetido da matrícula** para substituir o existente com as novas informações do veículo se o número da matrícula para importação já existir em outra lista de veículos. Caso contrário, as informações originais do veículo serão reservadas.

6. Clique em **Adicionar**.

A lista de veículos adicionados será exibida à esquerda da página do veículo.

7. Opcional: Realize as seguintes operações na área de lista de veículos.

Editar lista de veículos

Clique  na área da lista de veículos para editar o nome da lista de veículos.

Excluir lista de veículos

Clique em  na área da lista de veículos para excluir a lista.

15.2 Adicionar informação do Veículo

Depois de adicionar a lista de veículos, você pode verificar as informações do veículo na lista de veículos ou você pode adicionar as informações do veículo para a lista.

As informações dos veículos adicionados podem ser usadas para alarme ANPR ao adicionar o alarme.

Você pode importar as informações do veículo em lote ou você pode adicionar as informações do veículo manualmente.

Observação

Cada lista de veículos pode conter até 5.000 veículos.

15.2.1 Importar informações do veículo em um lote

Você pode importar várias informações de veículos ao mesmo tempo.

Antes de começar

Você deve adicionar a lista do veículo antes que você possa adicionar a informação do veículo. Consulte **Adicionar lista de veículo** para detalhes.

Execute a tarefa a seguir quando precisar importar informações do veículo em um lote.

Etapas

Observação

Cada lista de veículos pode conter até 5.000 veículos.

1. Clique em **Veículo** para entrar na página de gerenciamento de veículos.
2. Selecione a lista de veículo.
3. Clique em Importar para abrir a janela de importação.

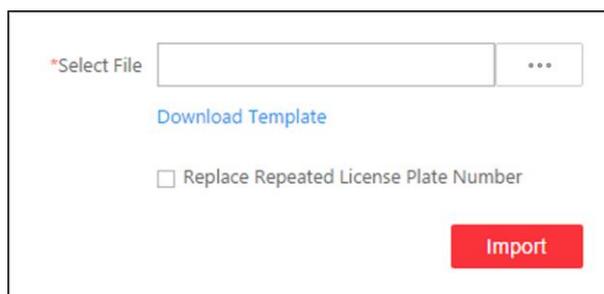


Figura 15-2 Janela de importação

4. Clique em **modelo de download** na janela importar para salvar o arquivo de modelo (formato CSV) no seu PC.
5. Abra o arquivo de modelo baixado.
6. Insira as informações exigidas do veículo na coluna correspondente.
7. Clique em e selecione o arquivo de modelo.
8. Opcional: Verifique **substituir número de placa de veículo repetida** para substituir a existente pelas informações do novo veículo, se o modelo tiver o número da placa que já existe na lista de veículos atuais ou outros. Caso contrário, as informações originais do veículo serão reservadas.
9. Clicar em **Importar**.
10. Opcional: Realize as seguintes operações depois de importar as informações do veículo.

Editar informações de veículo

Clique no número da placa na coluna número da placa do veículo para editar as informações do veículo

Editar período efetivo

Selecione o (s) veículo (s) e clique em **Editar período efetivo** para editar o período efetivo dos veículos selecionados em um lote. Se o número da placa expirou, ele não pode acionar um evento ou alarme quando houver correspondência do número da placa se o evento/alarme do número da placa correspondido estiver configurado.

Delete informações de veículo

Verifique a informação do veículo e clique em **excluir** para excluir a informação do veículo.

Exportar informações de veículo

Clique em **Exportar tudo** para salvar as informações de veículos da lista (arquivo CSV) no seu PC, as quais podem ser importadas para outra lista de veículos.

15.2.2 Adição manual de informações de veículo

Você pode adicionar informações de veículo único manualmente.

Antes de começar

Você deve adicionar a lista do veículo antes que você possa adicionar a informação do veículo. Consulte **Adicionar lista de veículo** para detalhes.

Execute essa tarefa quando precisar adicionar uma etiqueta no mapa.

Etapas

1. Clique em **Veículo** para entrar na página de gerenciamento de veículos.
2. Selecione a lista de veículo.
3. Clique em **Adicionar** para entrar na página de adição de veículo.

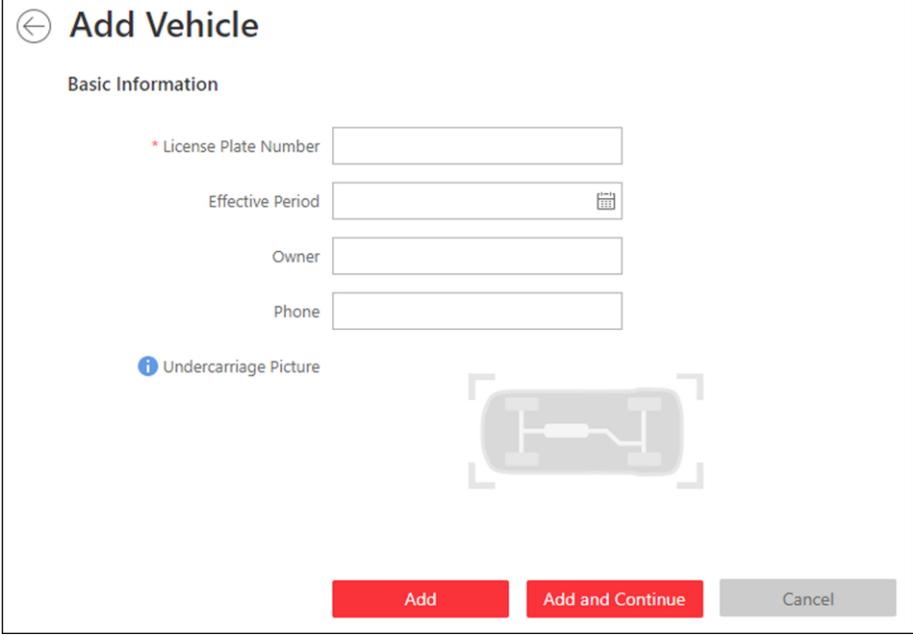


Figura 15-3 Adicionar Veículo

4. Insira o número da placa do veículo.
5. Opcional: Defina um período efetivo para este veículo.
Se o número da placa expirou, ele não pode acionar um evento ou alarme quando houver correspondência do número da placa se o evento/alarme do número da placa correspondido estiver configurado.
6. Opcional: Insira as informações do proprietário do veículo, incluindo nome e número de telefone.
7. Opcional: Carregue uma imagem de material rodante para este veículo.
 - 1) Mova o cursor para a área da imagem e clique em **carregar**.
 - 2) Na janela pop-up, selecione a imagem de material rodante para carregá-la.Depois de carregar uma imagem de material rodante, você pode ver a imagem do material rodante capturado do veículo atual e esta imagem carregada para comparação no Control Client.
8. Termine de adicionar a informação do veículo.
 - Clique em **Adicionar** para adicionar as informações do veículo e retornar à página de lista de veículos.
 - Você também pode clicar em **Adicionar e continuar** para salvar as configurações e continuar adicionando outros veículos.

Observação

Se o número da matrícula já existir (na lista de veículos atual ou em outras listas de veículos), será exibida uma caixa de prompt e você poderá selecionar se deseja substituir o veículo existente por um novo.

9. Opcional: Realize as seguintes operações depois de importar as informações do veículo.

Editar informações de veículo	Clique no número da placa na coluna número da placa do veículo para editar as informações do veículo
Editar período efetivo	Selecione o (s) veículo (s) e clique em Editar período efetivo para editar o período efetivo dos veículos selecionados em um lote. Se o número da placa expirou, ele não pode acionar um evento ou alarme quando houver correspondência do número da placa se o evento/alarme do número da placa correspondido estiver configurado.
Delete informações de veículo	Verifique a informação do veículo e clique em excluir para excluir a informação do veículo.
Exportar informações de veículo	Clique em Exportar tudo para salvar as informações de veículos da lista (arquivo CSV) no seu PC, as quais podem ser importadas para outra lista de veículos.

Capítulo 16 Gerenciar lista de pessoas

Você pode adicionar informações de pessoa ao sistema para outras operações, como controle de acesso (adicionando a pessoa ao grupo de acesso), comparação de face (adicionando o grupo de comparação de pessoa a face), tempo e presença (adicionando a pessoa ao grupo de atendimento), etc. Depois de adicionar as pessoas, você pode editar e excluir as informações da pessoa, se necessário.

16.1 Adicionar pessoa

Você pode adicionar as informações da pessoa ao sistema, uma a uma.

Execute esta tarefa se você quiser adicionar as informações da pessoa uma a uma.

Etapas

1. Clique **Pessoa** → **Lista de pessoa** → **Adicionar** para inserir a página de adição de pessoa.

Add Person

Basic Information

* ID

* First Name

* Last Name

Gender Male
 Female
 Unknown

Email

Phone

Remark

Additional Information

No available additional information item. [Configuration](#)

Face Comparison

Face Comparison Group

Search

All
 222
 Iiu
 Iiu22

Add **Add and Continue** Cancel

Figura 16-1 Adicionar uma pessoa

2. Defina as informações básicas da pessoa.

ID

A ID padrão é gerada pelo sistema. Você pode editá-lo se necessário.

Observação

Ele deve conter 1 a 16 caracteres e o primeiro caractere não pode ser 0.

Retrato da pessoa

Carregue a imagem do rosto de uma pessoa. Você pode clicar em **tirar uma foto** para usar a webcam do PC para tirar uma foto. Ou clique em **carregar imagem** para selecionar uma imagem do seu PC.

Observação

Recomenda-se que o rosto na imagem deve estar em full-face vista diretamente voltada para a câmera, sem um chapéu ou cobertura de cabeça.

3. Opcional: Defina as informações adicionais da pessoa.

Observação

Você pode personalizar esses itens de acordo com as necessidades reais como informações adicionais da pessoa. Para obter detalhes, consulte **Informações adicionais personalizadas**.

4. Opcional: Adicione a pessoa aos grupos de comparação de faces existentes que serão usados para reconhecimento facial e comparação.

Observação

Depois de adicionar a pessoa ao grupo de comparação de faces, você deve aplicar o grupo de comparação de faces a um dispositivo para tornar as configurações efetivas. Para obter detalhes sobre como aplicar o grupo de comparação de faces ao dispositivo, consulte **Aplicar grupo de comparação de face ao dispositivo**.

5. Opcional: Defina as informações de controle de acesso e tempo e frequência.

Período efetivo

Defina o período efetivo para a pessoa no aplicativo de controle de acesso e a aplicação hora & presença. Por exemplo, se a pessoa é um visitante, seu período efetivo pode ser curto e temporário.

Grupo de acesso

Adicione a pessoa aos grupos de acesso existentes que podem ser vinculados com nível de acesso (s). A ligação do nível de acesso e do grupo de acesso define a permissão de acesso que a pessoa (s) pode acessar quais pontos de acesso no período autorizado.

Você pode clicar no nome do grupo de acesso para exibir seus níveis de acesso vinculados. Mova o cursor para o nível de acesso para visualizar seus pontos de acesso e agendamento

de acesso.

 **Observação**

Você pode clicar em **Adicionar novo** para adicionar um novo grupo de acesso. Para detalhes, consulte **Adicionar grupo de acesso**.

Superusuário

Se a pessoa for definida como um superusuário, ele/ela será isento de restrições bloqueadas (credencial falhou), todas as regras de retorno do anti-retorno e autorização de primeiro cartão.

 **Observação**

Para obter detalhes sobre como definir essas funções, consulte **Editar ponto de acesso para o site atual**.

Acesso estendido

Quando a pessoa que acessa a porta, conceda a esta pessoa mais tempo para passar através das portas que foram configuradas com duração aberta prolongada. Utilize esta função para as pessoas com mobilidade reduzida.

 **Observação**

Você deve definir a duração de abertura estendida da porta no modo de exibição lógico. Para obter detalhes, consulte **Editar ponto de acesso para o local atual**.

Grupo de acesso

Adicione a pessoa ao grupo de atendimento existente se sua necessidade de monitorar as horas de trabalho e o absentismo da pessoa.

 **Observação**

Você pode clicar em **Adicionar novo** para adicionar um novo grupo de acesso. Para detalhes, consulte **Adicionar grupo de acesso**.

 **Observação**

As funções de acesso estendido e superusuário não podem ser ativadas simultaneamente.

6. Defina as informações de credencial da pessoa, incluindo PIN, credencial de face, número do cartão, impressão digital e credenciais de coação.

 **Observação**

Até 50.000 credenciais são permitidas no total.

PIN

O PIN deve ser usado após o cartão ou a impressão digital ao acessar. Ele não pode ser usado de forma independente.

Observação

Deve conter 1 a 8 dígitos.

Definir perfil como credencial de face

Se você quiser usar catraca com função de reconhecimento facial, você precisa definir a imagem do perfil da pessoa como herhis face credencial para que a pessoa pode digitalizar herhis face no terminal de reconhecimento facial quando ele/ela quer acessar a catraca. Certifique-se de ter carregado uma imagem como o perfil da pessoa.

Cartão

Emita um cartão a pessoa para atribuir o número do cartão à pessoa. Você pode inserir o número do cartão manualmente ou deslizar um cartão na estação de registro do cartão ou no leitor de cartão para obter o número do cartão e, em seguida, emití-lo para a pessoa.

1. Clique em + na campo do cartão.
2. Coloque o cartão que pretende emitir a esta pessoa na estação de matrícula do cartão ou no leitor de cartões e o número do cartão será lido automaticamente. Ou você pode digitar o número do cartão manualmente

Observação

Se a estação de registro de cartão não for detectada ou a configuração de emissão estiver incorreta, você poderá clicar em **Configuração** para definir o modo de emissão. Para detalhes, consulte *Definir parâmetros de emissão de cartão*.

3. Defina o período efetivo do cartão se o cartão for usado para fins temporários. Se o cartão estiver definida com um período efetivo, outras cartões vinculadas a essa pessoa estarão inativos, e as impressões digitais e o perfil vinculados a essas cartões inativos serão vinculados a este cartão com um período efetivo. Depois de apagar o cartão com período efetivo, estes cartões inativos irão recuperar a ativação, e suas impressões digitais e perfil previamente ligados irão ser recuperados, também.

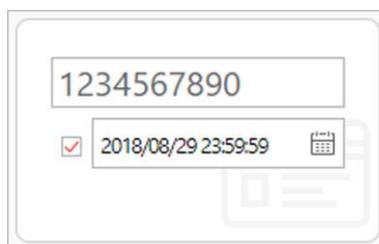


Figura 16-2 Número do cartão lido

Observação

Até 5 cartões podem ser exibidas de uma só vez.

Impressão digital

Depois de conectar o gravador de impressão digital ao seu PC, clique em +, coloque e levante sua impressão digital no gravador após as instruções e ele coletará sua impressão digital automaticamente.

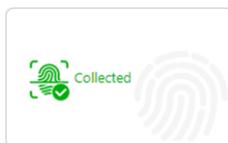


Figura 16-3 Gravador de impressão digital

Observação

Até 10 impressões digitais podem ser adicionadas a uma pessoa.

Credencial sob coação

Defina as credenciais (número do cartão e impressão digital) para que quando você estiver pressionando, você pode deslizar o cartão ou digitalizar a impressão digital configurada aqui. A porta será destravada e o cliente do controle receberá um alarme da pressão (se configurado) para notificar o pessoal de segurança.

Observação

Quando a pessoa acessa com credenciais sob coação, ele/ela não pode ser isento de restrições bloqueadas (credencial falhou) restantes, todas as regras de retorno do anti-retorno da autorização de primeiro cartão. O acesso estendido também não é permitido.

7. Termine de adicionar a pessoa.

- Clique em **Adicionar** para adicionar uma pessoa e retornar à página de lista de pessoa.
- Clique em **Adicionar e continuar** para adicionar uma pessoa e continuar adicionando outras pessoas.

A pessoa será exibida na lista de pessoas e você pode ver os detalhes.

8. Opcional: Depois de adicionar a pessoa, você pode fazer um ou mais dos seguintes itens:

Editar pessoa	Clique no nome da pessoa para editar os detalhes da pessoa.
Excluir pessoa	Selecione a pessoa e clique em Excluir para deletar .
Exportar informações de pessoa adicionada	Clique em exportar tudo para exportar todas as informações da pessoa adicionada e você pode salvar o arquivo em seu PC. Para segurança de dados, é necessário definir uma senha antes de exportar o que é necessário ao descompactar o arquivo ZIP baixado.

16.2 Adicionar pessoas em lote

Você pode adicionar as informações de várias pessoas ao sistema importando um modelo com informações de pessoa.

Execute esta tarefa quando você precisa adicionar informações em lote de várias pessoas.

Etapas

1. Clique **Pessoa** → **Lista de pessoa** → para entrar na página da lista de pessoas.
2. Clique em **Importar** → **Importar pessoas**.

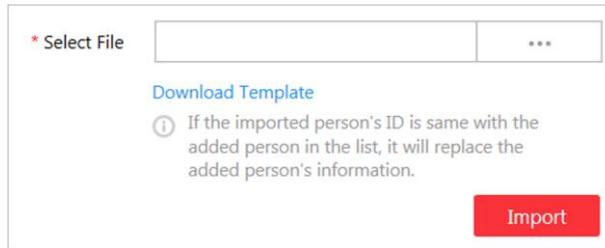


Figura 16-4 Importar pessoas

3. Clique em **modelo de download** para baixar o arquivo de modelo e você pode salvá-lo em seu PC.
4. No modelo baixado, insira as informações da pessoa seguindo as regras no modelo.
5. Clique em **Importar** → **Importar pessoas**.
6. Selecione o modelo com as informações da pessoa
7. Clique em **Importar** para iniciar a importação.

Observação

Se o ID da pessoa exportada for o mesmo com a pessoa adicionada na lista, ele substituirá as informações da pessoa adicionada.

O progresso de importação mostra e você pode verificar os resultados.

8. Opcional: Depois de adicionar a pessoa, você pode fazer um ou mais dos seguintes itens:

Editar pessoa	Clique no nome da pessoa para editar os detalhes da pessoa.
Excluir pessoa	Selecione a (s) pessoa (s) e clique em excluir para excluir a (s) pessoa (s).
Exportar informações de pessoa adicionada	Clique em exportar tudo para exportar todas as informações da pessoa adicionada e você pode salvar o arquivo em seu PC. Para segurança de dados, é necessário definir uma senha antes de exportar o que é necessário ao descompactar o arquivo ZIP baixado.

16.3 Importar pessoas do domínio

Você pode importar os usuários no domínio do AD em um lote para o sistema como pessoas. Depois de importar as informações da pessoa (incluindo nome da pessoa e nome da conta) no domínio do AD, você pode definir outras informações para as pessoas, como credenciais.

Antes de começar

Você deve configurar as configurações do Active Directory. Veja **Definir o Active Directory** para detalhes.

Etapas

1. Clique **Pessoa** → **Lista de pessoa** para entrar na página de gerenciamento da lista de pessoas.
2. Clique em **Importar** → **Importar pessoas do domínio** para entrar na página seguinte.

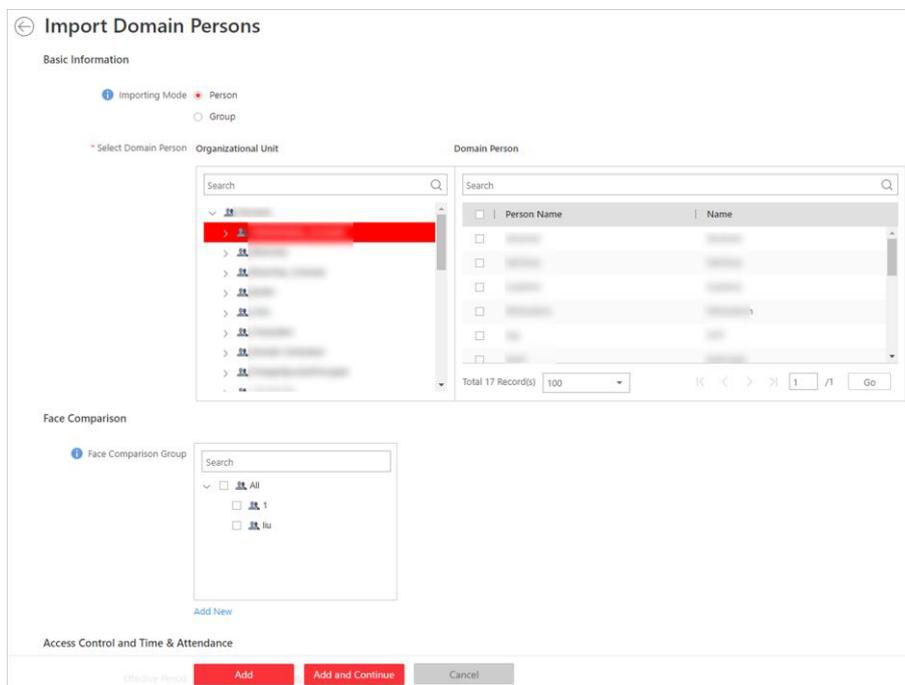


Figura 16-5 Importar pessoas

3. Selecione o modo de importação.

Pessoa

Importar pessoas específicas. Selecione a unidade organizacional e selecione as pessoas a unidade organizacional que são exibidas na lista pessoa do domínio à direita. Ele sincronizará as informações da pessoa com base em cada pessoa.

Grupo

Importe todas as pessoas da unidade organizacional. Ele sincronizará as informações da pessoa com base em cada grupo.

4. Adicionar as pessoas para o (s) grupo (s) de comparação de face existente (s) que será usado para reconhecimento facial e comparação.

 **Observação**

Depois de adicionar a pessoa ao grupo de comparação de faces, você deve aplicar o grupo de comparação de faces a um dispositivo para tornar as configurações efetivas. Para obter detalhes sobre como aplicar o grupo de comparação de faces ao dispositivo, consulte ***Aplicar grupo de comparação de face ao dispositivo***.

5. Defina as informações de controle de acesso e tempo e frequência.

Período efetivo

Defina o período efetivo para a pessoa no aplicativo de controle de acesso e a aplicação hora & presença. Por exemplo, se a pessoa é um visitante, seu período efetivo pode ser curto e temporário.

Grupo de acesso

Adicione a pessoa aos grupos de acesso existentes que podem ser vinculados com nível de acesso (s). A ligação do nível de acesso e do grupo de acesso define a permissão de acesso que a pessoa (s) pode acessar quais pontos de acesso no período autorizado. Você pode clicar no nome do grupo de acesso para exibir seus níveis de acesso vinculados. Mova o cursor para o nível de acesso para visualizar seus pontos de acesso e agendamento de acesso.

 **Observação**

Você pode clicar em **Adicionar novo** para adicionar um novo grupo de acesso. Para detalhes, consulte ***Adicionar grupo de acesso***.

Superusuário

Se as pessoas forem definidas como um superusuários, eles/elas serão isentas de restrições bloqueadas (credencial falhou), todas as regras de retorno do anti-retorno e autorização de primeiro cartão.

 **Observação**

Para obter detalhes sobre como definir essas funções, consulte ***Editar ponto de acesso para o site atual***.

Acesso estendido

Quando as pessoas que acessam o ponto de acesso, conceda a estas pessoas mais tempo para passar através das portas que foram configuradas com duração aberta prolongada. Utilize esta função para as pessoas com mobilidade reduzida.

 **Observação**

Você deve definir a duração de abertura estendida do ponto de acesso no modo de exibição lógico. Para obter detalhes, consulte ***Editar ponto de acesso para o local atual***.

Grupo de acesso

Adicione a pessoa ao grupo de atendimento existente se sua necessidade de monitorar as horas de trabalho e o absentismo das pessoas.

Observação

Você pode clicar em **Adicionar novo** para adicionar um novo grupo de acesso. Para detalhes, consulte **Adicionar grupo de acesso**.

Observação

As funções de acesso estendido e superusuário não podem ser ativadas simultaneamente.

6. Conclua a importação das pessoas do domínio.
 - Clique em **adicionar** para adicionar a pessoa.
 - Clique em **adicionar e continuar** para salvar as configurações e continuar adicionando outras pessoas.
7. Opcional: Depois de importar as informações da pessoa no domínio para o sistema, se as informações de pessoa no domínio forem alteradas, clique em **sincronizar pessoas de domínio** para obter as informações mais recentes das pessoas importadas para o sistema. Se as pessoas forem importadas por grupo, ele sincronizará as informações mais recentes da pessoa do grupo de domínio (incluindo pessoas adicionadas, pessoas excluídas, pessoas editadas, etc., no grupo).

16.4 Adicionar perfil em lote

Você pode adicionar imagens de várias pessoas ao sistema importando um arquivo ZIP contendo imagens de pessoa.

Antes de começar

Nomeie a imagem da pessoa após a identificação da pessoa e pacote as imagens da pessoa a um arquivo em ZIP.

Observação

- Atualmente ele suporta imagens em formato JPG, JPEG e PNG.
 - Recomendação para cada imagem: Dimensões: 295×412. Tamanho: 60 KB para 100 KB.
 - O arquivo ZIP deve ser menor do que 100 MB, ou o carregamento falhará.
-

Execute essa tarefa quando precisar adicionar perfis de pessoa ao sistema.

Etapas

1. Clique **Pessoa** → **Lista de pessoa** → para entrar na página da lista de pessoas.
2. Clique em **Importar** → **Importar perfis**.

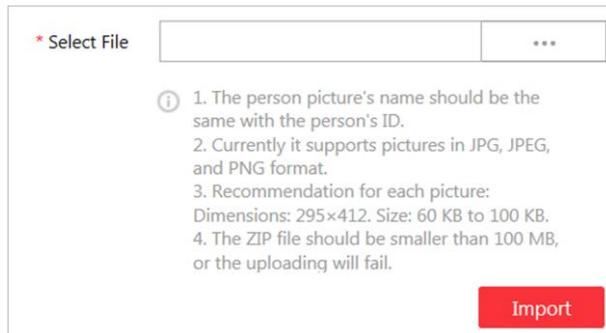


Figura 16-6 Importar perfis

3. Selecione o arquivo ZIP que contém as fotos da pessoa
4. Clique em **Importar** para iniciar a importação.
O progresso de importação mostra e você pode verificar os resultados.

16.5 Cartões de emissão de lote para pessoas

O sistema fornece uma maneira conveniente de emitir cartão para várias pessoas em um lote. Realize essa tarefa quando precisar emitir as cartas para várias pessoas em um lote.

Etapas

Observação

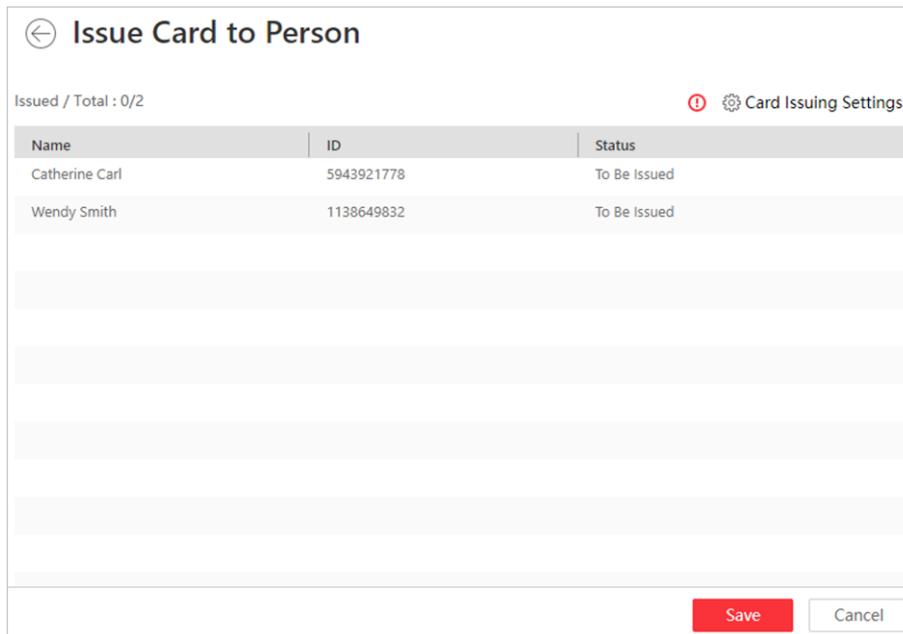
- Até 5 cartões podem ser exibidas de uma só vez.
- Você não pode emitir cartões para pessoas que têm cartões com período efetivo.

-
1. Clique **Pessoa** → **Lista de pessoa** → para entrar na página da lista de pessoas.

Observação

As pessoas selecionadas que têm menos de 5 cartões serão exibidas.

-
2. Selecione as pessoas para as quais emitir o cartão.
 3. Clique em **gerenciamento de credenciais** → **cartões de emissão de lote** para pessoas para entrar na página a seguir.



The screenshot shows a web interface titled "Issue Card to Person". At the top left is a back arrow icon. Below the title, it says "Issued / Total : 0/2". To the right, there is a red warning icon, a gear icon, and the text "Card Issuing Settings". Below this is a table with three columns: "Name", "ID", and "Status". The table contains two rows of data. At the bottom right of the interface are two buttons: "Save" (in red) and "Cancel".

Name	ID	Status
Catherine Carl	5943921778	To Be Issued
Wendy Smith	1138649832	To Be Issued

Figura 16-7 Emitir cartão para pessoas em lote

4. Clique em **configurações de emissão de cartão** para selecionar o modo de emissão e definir os parâmetros.

 **Observação**

Para obter detalhes sobre como definir o modo de emissão e os parâmetros do cartão, consulte ***Definir parâmetros de emissão de cartão.***

5. Coloque o cartão estação de matrícula do cartão ou deslize o cartão no leitor de cartões de acordo com o modo de emissão selecionado.
O número do cartão será lido automaticamente e o cartão será emitida para a primeira pessoa na lista.
6. Repita a etapa acima para emitir os cartões para as pessoas na lista em sequência.
7. Clique em **Salvar**.

16.6 Definir parâmetros de emissão de cartão

A HikCentral fornece dois modos para ler o número de um cartão: através da estação de matrícula do cartão ou através do leitor de cartão do dispositivo de controle de acesso. Se uma estação de registro de cartão estiver disponível, conecte-a ao computador que executa o Web Client e coloque o cartão no registro do cartão para ler o número do cartão. Se não, você também pode deslizar o cartão no leitor de cartão do dispositivo de controle de acesso adicionado para obter o número do cartão. Como resultado, antes de emitir um cartão para uma pessoa, você precisa definir os parâmetros de emissão do cartão, incluindo o modo de emissão e parâmetros relacionados.

Etapas

1. Clique em **Pessoa** na página inicial e insira a página **lista de pessoas**.
2. Você pode inserir a página de configurações de parâmetros de emissão do cartão ao adicionar uma única pessoa ou emitir cartões para pessoas em um lote.
 - Para inserir a página de configurações dos parâmetros de emissão do cartão ao adicionar uma única pessoa, consulte **Adicionar uma pessoa**.
 - Para inserir a página de configurações dos parâmetros de emissão do cartão ao emitir cartões para pessoas em um lote, consulte **Cartões de emissão de lote para pessoas**.
3. Defina o modo de emissão e defina os parâmetros relacionados.

Estação de registro de cartão

Conecte uma estação de registro de cartão ao computador que executa o Web Client. Você pode colocar o cartão na estação de matrícula do cartão para obter o número do cartão. Se selecionar este modo, deve definir o formato do cartão e a função de encriptação do cartão.

Formato dos cartões

Se o cartão for cartão Wiegand, selecione **Wiegand**. Caso contrário, selecione **Normal**.

Criptografia do Cartão

Se você definir o formato do cartão como **Normal**, você pode ativar a função de criptografia de cartão para fins de segurança. Depois de ativada, você deve habilitar a criptografia de cartão na página de configuração do dispositivo de controle de acesso para entrar em vigor.

Leitor de Cartões

Selecione um leitor de cartão de um dispositivo de controle de acesso adicionado ao sistema. Você pode deslizar o cartão no leitor de cartão para obter o número do cartão.



Observação

- Um leitor de cartão pode ser ajustado para emitir o cartão por até um usuário ao mesmo tempo.
- Se você definir um leitor de cartão de terceiros para ler o número do cartão, você deve definir o protocolo personalizado do dispositivo Wiegand para configurar a regra de

comunicação primeiro.

4. Clique em **Salvar**.

16.7 Informações adicionais personalizadas

Você pode personalizar os itens de informações adicionais que não são pré-definidos nas informações básicas de acordo com as necessidades reais.

Execute esta tarefa se pretender personalizar as informações adicionais.

Etapas

Observação

Até 20 informações adicionais podem ser personalizadas.

1. Clique em **pessoa** → **Lista de pessoa** → **Informação adicional personalizada** para entrar na página de informações de adição personalizada.
 2. Clique em **Adicionar**.
 3. Criar um nome para este item.
-

Observação

Até 32 caracteres são permitidos no nome.

4. Clique em **Salvar**.
5. Opcional: Depois de adicionar uma informação adicional, você pode fazer um ou mais dos seguintes itens:

Editar nome

Clique em  para editar seu nome.

Excluir

Clique em  para excluir a informação adicional.

Observação

As informações adicionais que estão vinculadas com informações de pessoa no domínio não podem ser excluídas.

Capítulo 17 Gerenciar controle de acesso

Após ter adicionado as pessoas à lista da pessoa, você pode atribuir a permissão de acesso às pessoas para definir quando podem começar o acesso a que porta (s). Para definir a permissão de acesso, você deve criar um nível de acesso para agrupar as portas e um grupo de acesso para agrupar as pessoas. Depois de atribuir o nível de acesso ao grupo de acesso, as pessoas no grupo de acesso serão autorizadas a acessar as portas no nível de acesso com suas credenciais durante o período de tempo autorizado.

17.1 Adicionar grupo de acesso

O grupo de acesso é um grupo de pessoas que têm a mesma permissão de acesso. As pessoas do grupo de acesso podem acessar as mesmas portas (as portas no nível de acesso vinculado) durante o mesmo período de tempo autorizado. Você precisa de atribuir o nível de acesso ao (a) grupo de acesso de modo que estas pessoas no grupo de acesso possam alcançar a porta (s) no nível de acesso.

Antes de começar

Adicionar pessoa ao sistema, para obter detalhes, consulte *Gerenciar lista de pessoas*.

Execute esta tarefa para adicionar um grupo de acesso.

Etapas

Observação

Até 64 grupos de acesso podem ser adicionados.

1. Clique **Pessoa** → **Lista de pessoa** → **Adicionar** para entrar na página do grupo de acesso de adição.

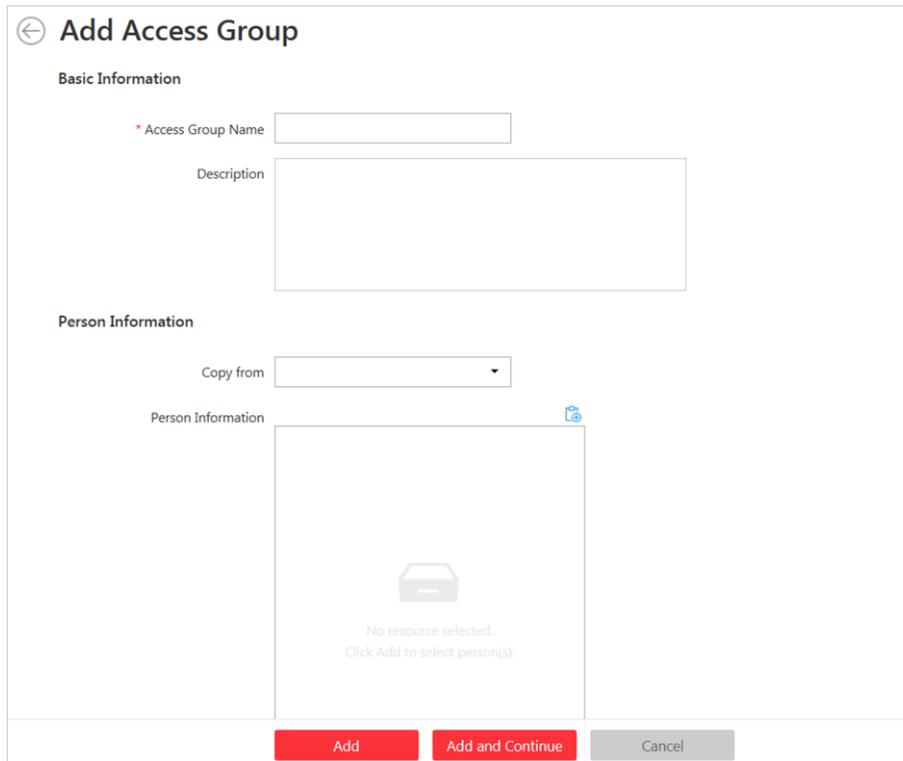


Figura 17-1 Adicionar grupo de acesso

2. Defina as informações básicas da pessoa.

Nome do grupo de acesso

Crie um nome para o grupo de acesso.

3. Opcional: Definir a pessoa (s) para adicionar ao grupo de acesso.

1) Clique em .

Todas as pessoas adicionadas à exibição do sistema. Você pode visualizar o nome da pessoa, imagem, ID da pessoa e informações de observação.

2) Selecione a pessoa (s) para adicionar ao grupo de acesso.

3) Opcional: Você também pode selecionar o grupo de acesso ou o grupo de atendimento existente na lista suspensa copiar de para copiar informações de pessoa de outro grupo.

Observação

Para definir o grupo de atendimento, consulte **Adicionar grupo de atendimento**.

Observação

Até 1.000 pessoas podem ser adicionadas a um grupo de acesso.

4. Opcional: Selecione o (s) nível (eis) de acesso para vincular o grupo de acesso ao (s) nível (eis) de acesso para que as pessoas selecionadas na etapa 3 possam acessar as portas vinculadas ao nível de acesso durante o período de tempo autorizado.

 **Observação**

- Até 8 níveis de acesso podem ser atribuídos a um grupo de acesso.
 - Você pode clicar em **adicionar novo** para adicionar um novo nível de acesso. Para detalhes, consulte **Adicionar nível de acesso**.
 - Mova o cursor para o nível de acesso e você pode ver sua porta (s) e cronograma de acesso.
-

5. Termine de adicionar o grupo de acesso.

- Clique em **adicionar** para adicionar o grupo de acesso e retornar à página de gerenciamento do grupo de acesso.
- Clique em **adicionar e continuar** para adicionar nível de acesso e continuar adicionando outros grupos de acesso.

6. Opcional: Depois de adicionar o grupo de acesso, você pode fazer um ou mais como segue:

Editar grupo de acesso Clique em  na coluna para editar estes detalhes.

Excluir grupo de acesso Clique em  na coluna operação para excluir isto.

Excluir todos os grupos de acesso Clique **Deletar tudo** para deletar todos os grupos de acesso.

17.2 Gerenciar nível de acesso

No controle de acesso, o nível de acesso é um grupo de porta (s). Depois de atribuir o nível de acesso a determinados grupos de acesso, ele define a permissão de acesso que a pessoa (s) pode obter acesso a que porta (s) durante o período de tempo autorizado.

17.2.1 Gerenciar nível de acesso

Para definir a permissão de acesso, você precisa adicionar um nível de acesso primeiro e agrupar as portas.

Execute esta tarefa se você precisar adicionar um nível de acesso.

Etapas

 **Observação**

Até 128 níveis de acesso podem ser adicionados ao sistema.

1. Clique em **nível de acesso** na página inicial para entrar na página de gerenciamento de nível de acesso.
 2. Clique em **Adicionar**.
-

The screenshot shows the 'Add Access Level' form. It has a back arrow in the top left. The form contains the following elements:

- *Access Level Name**: A text input field.
- Description**: A larger text input field.
- *Door**: A dropdown menu with a search bar. The dropdown is open, showing a list of doors with checkboxes:
 - Door 01 (checked)
 - 10.18.139.121 (checked)
 - Door 01 (checked)
 - Door 02 (checked)
 - Door 03 (unchecked)
 - Door 04 (unchecked)
- *Access Schedule**: A dropdown menu with 'All-day Template' selected and a 'View' button next to it.
- At the bottom: Three buttons: 'Add' (red), 'Add and Assign' (red), and 'Cancel' (grey).

Figura 17-2 Adicionar nível de acesso

3. Crie um nome para o nível de acesso.
4. Opcional: Insira a descrição para o nível de acesso.
5. Selecione a porta (s) para adicionar a (s) porta (s) ao nível de acesso.
6. Selecione o agendamento de acesso para definir em que período de tempo, as pessoas estão autorizadas a acessar as portas (selecionado na etapa 5).

Observação

As agendas de acesso padrão e personalizadas são exibidas na lista suspensa. Você pode clicar em **adicionar novo** para personalizar uma nova agenda. Para detalhes, consulte **Definir modelo de agendamento de acesso**.

7. Termine de adicionar o nível de acesso.
 - Clique em **adicionar** para adicionar o nível de acesso e retornar à página de gerenciamento do nível de acesso.
 - Clique em **adicionar e atribuir** para atribuir o nível de acesso a alguns grupos de acesso para que a pessoa (s) nos grupos de acesso terá a permissão de acesso para acessar as portas selecionadas na etapa 5.

Observação

- Para obter detalhes sobre como atribuir o nível de acesso ao grupo de acesso, consulte **Atribuir nível de acesso ao grupo de acesso**.
- Para definir o grupo de acesso, consulte.

8. Opcional: Depois de adicionar o nível de acesso, você pode fazer um ou mais como segue:

Editar nível de Clique em  na coluna para editar estes detalhes. Se pretender

acesso	alterar os grupos de acesso atribuídos ou atribuí-lo a outro grupo de acesso, clique em configuração .
Atribuir ao grupo de acesso	Clique em  na coluna operação para atribuir o nível de acesso ao(s) grupo(s) de acesso adicionado(s). Para obter detalhes, consulte Atribuir nível de acesso ao grupo de acesso .
Excluir nível de acesso	Clique em  na coluna Operação para excluir o nível de acesso.
Excluir todos os níveis de acesso	Clique Deletar tudo para deletar todos os níveis de acesso.

17.2.2 Atribuir nível de acesso ao grupo de acesso

Depois de adicionar o nível de acesso, você precisa atribuí-lo para acessar grupo (s). Depois disso, as pessoas no (s) grupo (es) de acesso terão permissão para acessar as portas vinculadas ao nível de acesso.

Antes de começar

Adicione o (s) grupo (s) de acesso Para obter detalhes, consulte.

Execute esta tarefa se você precisa de atribuir o nível de acesso aos grupos de acesso.

Etapas

Observação

Você também pode vincular o grupo de acesso a nível (s) de acesso ao adicionar ou editar o grupo de acesso. A ligação configurada a mais atrasada tomará o efeito. Para detalhes, consulte **Adicionar grupo de acesso**.

1. Clique em **nível de acesso** na página inicial para entrar na página de gerenciamento de nível de acesso.
2. Insira a página atribuir ao grupo de acesso.
 - Depois de definir os parâmetros de nível de acesso ao adicionar, clique em **adicionar e atribuir**.
 - Ao editar o nível de acesso, clique em **configuração** na página de detalhes do nível de acesso.
 - Clique em  na coluna operação.
3. No campo atribuir ao grupo de acesso, selecione os grupos de acesso aos quais você deseja atribuir o nível de acesso.
4. Opcional: Clique em **adicionar novo** para adicionar um novo grupo de acesso.
5. Clique em **Salvar**.

17.3 Aplicar os níveis de acesso das pessoas ao dispositivo

Depois de definir a ligação entre o grupo de acesso e os níveis de acesso, ou se as configurações do nível de acesso e do grupo de acesso da pessoa forem alteradas, você precisará aplicar as configurações de nível de acesso da pessoa ao dispositivo de controle de acesso do ponto de acesso vinculado ao nível de acesso para ter efeito. Depois disso, as pessoas no grupo de acesso podem acessar os pontos de acesso durante o período de tempo autorizado definido pelo nível de acesso relacionado.

17.3.1 Aplicar manualmente os níveis de acesso das pessoas ao dispositivo

Depois de definir os níveis de acesso e atribuir níveis de acesso ao grupo de acesso, você deve aplicar a relação entre pessoas e pontos de acesso ao dispositivo de controle de acesso. Em outras palavras, depois de definir ou alterar os grupos de acesso e os níveis de acesso, você precisa aplicar essas configurações ao dispositivo de controle de acesso para entrar em vigor.

Antes de começar

Vincule o grupo de acesso ao nível de acesso para definir a permissão de acesso. Para obter detalhes, consulte *Atribuir nível de acesso ao grupo de acesso* ou *Adicionar grupo de acesso*.

Etapas

1. Clique **Pessoa** → **Grupo de acesso** para entrar na página de gerenciamento do grupo de acesso.
2. Clique em **aplicar ao dispositivo** para abrir a janela aplicar.

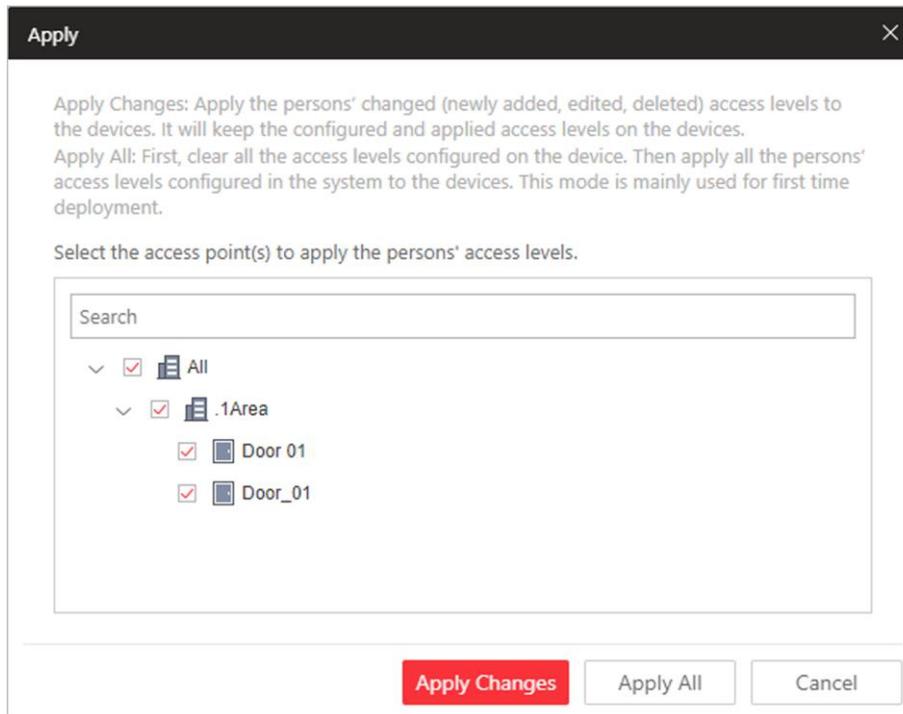


Figura 17-3 Aplicar ao dispositivo manual

3. Selecione os pontos de acesso para aplicar os níveis de acesso das pessoas.
4. Selecione o modo de aplicabilidade.

Aplicar Alterações

Aplique os níveis de acesso alterados (recém-adicionados, editados, excluídos) das pessoas aos dispositivos. Manterá os níveis de acesso configurados e aplicados nos dispositivos.

Aplicar a todos

Primeiro, limpe todos os níveis de acesso configurados no dispositivo. Em seguida, aplique todos os níveis de acesso das pessoas configurados no sistema para os dispositivos. Este modo é usado principalmente para implantação de primeira vez.

Durante este processo, os dispositivos estarão off-line por um tempo, e as pessoas não podem acessar através desses pontos de acesso.

5. Opcional: Se as configurações de permissão de acesso da pessoa forem alteradas (como alterações no nível de acesso vinculado, credenciais de pessoa, etc.), o ícone ⓘ será exibido próximo ao ícone **Aplicar ao dispositivo**, indicando que essas novas configurações de permissão de acesso devem ser aplicadas ao dispositivo. Você pode passar o cursor para ele para ver que os níveis de acesso de quantas pessoas devem ser aplicadas ao dispositivo.

17.3.2 Aplicar regularmente os níveis de acesso da pessoa a dispositivos

Além de aplicar manualmente ao dispositivo, você também pode definir um cronograma e o sistema pode aplicar os níveis de acesso atribuídos a pessoas configuradas no sistema para o dispositivo automaticamente todos os dias.

Antes de começar

Vincule o grupo de acesso ao nível de acesso para definir a permissão de acesso. Para obter detalhes, consulte **Atribuir nível de acesso ao grupo de acesso** ou **Adicionar grupo de acesso**.

Etapas

Observação

Por predefinição, o sistema aplicará automaticamente os níveis de acesso das pessoas ao dispositivo em 01:00 todos os dias.

1. Clique **Pessoa** → **Grupo de acesso** para entrar na página de gerenciamento do grupo de acesso.
2. Clique em **aplicar ao dispositivo (agendado)** para abrir a janela seguinte.

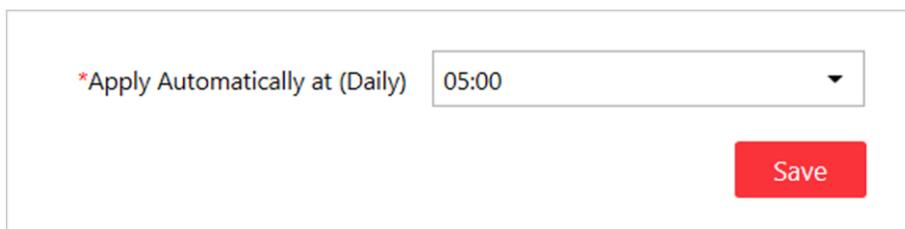


Figura 17-4 aplicar ao dispositivo regularmente

3. Defina uma hora e o sistema aplicará os níveis de acesso alterados vinculados a pessoas, bem como a aplicação de níveis de acesso com falha, ao dispositivo no momento configurado automaticamente.

Observação

O tempo aqui é o tempo do servidor VSM.

4. Clique em **Salvar**.

17.4 Definir modelo de agendamento de acesso

O agendamento de acesso define quando a pessoa pode abrir o ponto de acesso com credenciais ou quando o ponto de acesso permanece desbloqueado para que a pessoa possa abrir o ponto de acesso com acesso livre. O sistema predefine três modelos de agendamento de controle de acesso padrão: Modelo de dia inteiro, modelo da semana e modelo de fim de semana. Você também pode adicionar um modelo personalizado de acordo com as necessidades reais.

Etapas

1. Clique em **Sistema** na página inicial.
2. Clique em **agendamento** → **modelo de agendamento de acesso** na tabela à esquerda.
3. Clique em **adicionar** na página agendamento de acesso para inserir a página de modelo de agendamento de acesso de adição.

← Add Access Control Schedule Template

Basic Information

* Name

Copy from

Weekly Schedule

Authorized Erase

Sun.	00	02	04	06	08	10	12	14	16	18	20	22	24
Mon.													
Tue.													
Wed.													
Thu.													
Fri.													
Sat.													

Holiday Schedule

+ Add Holiday

Add Add and Continue Cancel

Figura 17-5 Definir modelo de agendamento de controle de acesso

4. Preencha as informações solicitadas.

Nome

Criar um nome para o modelo.

Copiar de

Opcionalmente, selecione copiar as configurações de outros modelos definidos.

5. Desenhe um período de tempo na barra de tempo.

 **Observação**

Podem ser configurados até 8 períodos de tempo a cada dia.

6. Opcional: Clique em **Apagar** e clique no período de tempo desenhado para limpar o período de tempo correspondente ao desenho.
 7. Opcional: Defina a agenda de feriados se desejar definir agendas diferentes para alguns dias especiais. A prioridade da programação do feriado é mais elevada do que a programação semanal que significa que os feriados predefinidos adotarão a programação do feriado um pouco do que a programação semanal.
 - 1) Clique em **adicionar feriado**.
 - 2) Selecione as férias predefinidas ou clique em **adicionar novo** para criar um novo feriado (veja **definir feriado** para obter detalhes).
 - 3) Clique em **Adicionar**.
 - 4) Desenhe um período de tempo na barra de tempo.
-

 **Observação**

Podem ser configurados até 8 períodos de tempo a cada dia.

- 5) Opcional: Clique em **Apagar** e clique no período de tempo desenhado para limpar o período de tempo correspondente ao desenho.
8. Termine de adicionar o modelo de agendamento de acesso.
 - Clique em **Adicionar** para adicionar o modelo e retornar à página de lista de modelos de agendamento de acesso.
 - Clique em **Adicionar e continuar** para adicionar o modelo de alarme e continuar adicionando outros alarmes.

O modelo de agendamento de acesso será exibido na lista de modelos de agendamento de acesso.

9. Opcional: Execute as seguintes operações depois de adicionar o modelo.

Exibir Detalhes do Modelo	Clique no modelo para exibir seus detalhes.
Edição do modelo	Clique em  na coluna operação para editar os detalhes do modelo.
Excluir o modelo	Clique em  na coluna de operação para excluir o modelo.
Exclusão de todos os modelos	Clique em Excluir todos para excluir todos os modelos de agendamento (exceto os modelos padrão e os modelos em uso).

17.5 Configurar regras de retorno do anti-retorno

O retorno de anti-retorno foi projetado para minimizar o uso indevido ou fraudulento de credenciais de acesso, como a passagem de cartão de volta para uma pessoa não autorizada, ou

acesso atado. A função retorno de anti-retorno estabelece uma sequência específica na qual os cartões devem ser usados para conceder acesso. A pessoa deve sair através do ponto de acesso no retorno de anti-retorno se ele/ela entra através do ponto de acesso no retorno de anti-retorno.

Etapas

1. Clique em **Exibição Lógica** na página inicial.
2. Selecione uma área que contenha o ponto de acesso para o qual você deseja configurar uma regra de retorno de anti-retorno.
3. Clique em  para entrar na página da área de edição.
4. No campo retorno de anti-retorno, clique em **adicionar** para adicionar uma regra de retorno de anti-retorno.

Na página adicionar retorno de anti-retorno, todas as áreas com pontos de acesso são exibidas.

5. Selecione os pontos de acesso a serem adicionados à regra de retorno de anti-retorno.



Observação

- Até 16 pontos de acesso podem ser adicionados a uma regra de retorno de anti-retorno.
- Selecione pelo menos um ponto de acesso na área atual.

-
6. Clique em **Adicionar**.

A regra de retorno de anti-retorno é adicionada na tabela e você pode exibir os pontos de acesso na regra.

Capítulo 18 gerenciar tempo e atendimento

Após ter adicionado as pessoas à lista da pessoa, se você quer controlar e monitorar quando as pessoas começam/param o trabalho e monitoram suas horas de trabalho e chegadas atrasadas, partidas adiantadas, tempo tomado em rupturas, e ABSENTEEISM, você pode adicionar a pessoa ao grupo do atendimento e atribuir uma agenda de turno (uma regra para a frequência que define como a agenda se repete, o tipo de turno, as configurações de quebra e a regra de passando do cartão.) ao grupo de atendimento para definir os parâmetros de atendimento para as pessoas no grupo de atendimento.

18.1 Adicionar grupo de acesso

Depois de adicionar as pessoas, você pode agrupar as pessoas em diferentes grupos de atendimento. As pessoas no mesmo grupo de atendimento são atribuídas com o mesmo cronograma de turno.

Realize esta tarefa se precisar agrupar as pessoas em um grupo de atendimento diferente.

Etapas

Observação

- Até 64 grupos de atendimento podem ser adicionados.
 - Para cada pessoa, ele/ela pode ser adicionado a até um grupo de atendimento.
-

1. Clique **Pessoa** → **Grupo de atendimento** → **Adicionar** para entrar na página do grupo de atendimento.

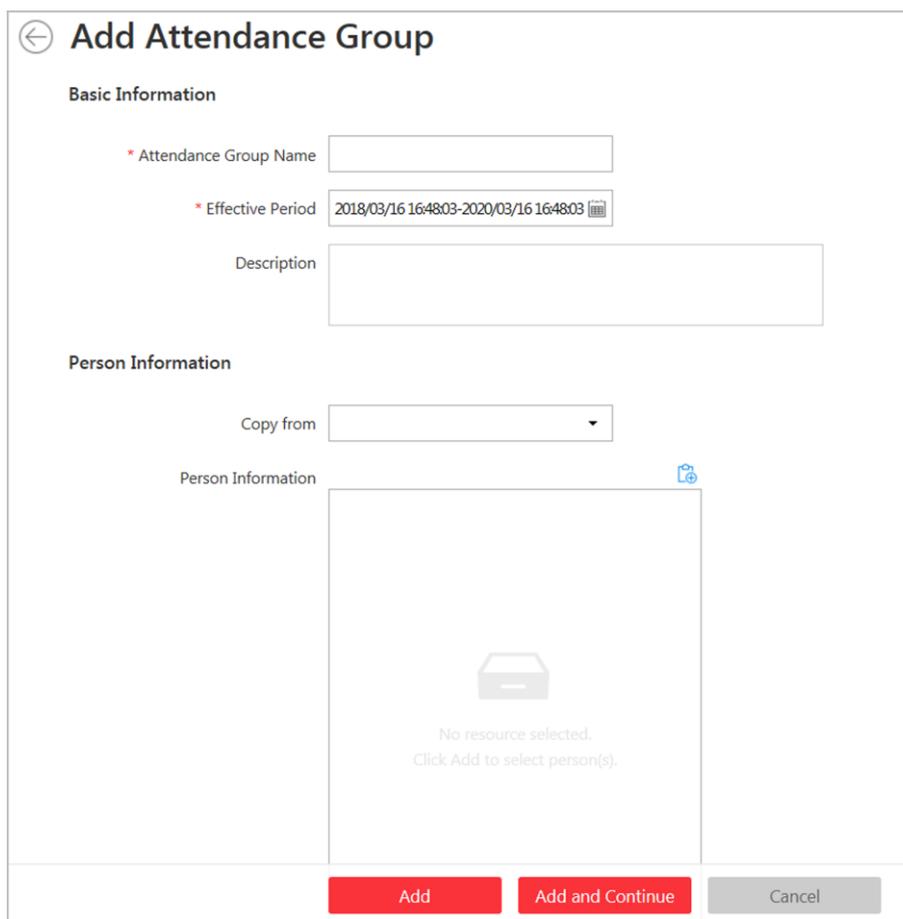


Figura 18-1 Adicionar grupo de atendimento

2. Defina as informações básicas do grupo.

Nome do grupo de atendimento

Crie um nome para o grupo de atendimento.

Período efetivo

Defina o período efetivo para o grupo. Uma vez expirado, os registros de atendimento das pessoas do grupo não serão registrados.

3. Defina a pessoa (s) a adicionar ao grupo de atendimento.

1) Clique em .

Todas as pessoas adicionadas à exibição do sistema. Você pode visualizar o nome da pessoa, a imagem e a ID da pessoa.

2) Selecione a pessoa (s) para adicionar ao grupo de atendimento.

3) Opcional: Você também pode selecionar o grupo de acesso existente na lista suspensa **copiar de** para copiar as informações da pessoa de outros grupos.

Observação

Para definir o grupo de acesso, consulte **Adicionar grupo de acesso**.

 **Observação**

Até 1.000 pessoas podem ser adicionadas a um grupo de atendimento.

4. Opcional: Definir o cronograma de turno para as pessoas no grupo para que eles precisam para atender de acordo com este cronograma de turno.
-

 **Observação**

Clique em **adicionar novo** para adicionar uma nova agenda de turno. Para detalhes, consulte **Adicionar agendamento de turno**.

5. Termine de adicionar o grupo de atendimento.
- Clique em **adicionar** para adicionar o grupo de atendimento e retornar à página de listagem do grupo de atendimento.
 - Clique em **adicionar e continuar** para adicionar grupo de atendimento e continuar adicionando outros grupos de atendimento.
6. Depois de adicionar o grupo de atendimento, você pode fazer um ou mais como segue:

Editar o grupo de atendimento

Clique em  na coluna para editar estes detalhes.

Excluir um grupo de atendimento

Clique em  na coluna operação para excluir isto.

Excluir todos os grupos de atendimento

Clique **Deletar tudo** para deletar todos os grupos de atendimento.

18.2 Adicionar agendamento de turno

Uma agenda de turno é uma agenda de atendimento que define o tempo de trabalho agendado e como ele se repete. Você pode criar um cronograma de turno para comparar a atendimento dos funcionários com ele, de modo a identificar aqueles que são Tardy, sair cedo, fazer uma longa pausa, ou estão ausentes, etc.

Execute esta tarefa para adicionar uma agenda de turno.

Etapas

1. Clique em **tempo & atendimento** → **agendamento de turno** → **adicionar** para inserir a página de agendamento de turno de adição.
2. Defina as informações básicas da agenda de turno, incluindo um nome personalizado e a descrição.

3. Opcional: Selecione outra agenda de turno na lista suspensa do campo **copiar de** para copiar as informações de agendamento para a agenda atual. Você pode editar as configurações de agendamento nesta base.
4. Defina o modo de repetição do agendamento.

Semana

A programação será repetida a cada 7 dias com base na semana.

Dia(s)

Você pode personalizar o número de dias em um período. Você deve definir uma data de início de um período para referência que pode definir como a agenda se repete.

Observação

O número de dias deve ser entre 1 a 14.

5. Desenhe o tempo de trabalho agendado na linha do tempo.
 - 1) arraste na linha do tempo para definir o intervalo do horário de trabalho agendado. Os parâmetros detalhados da regra de agendamento serão exibidos.

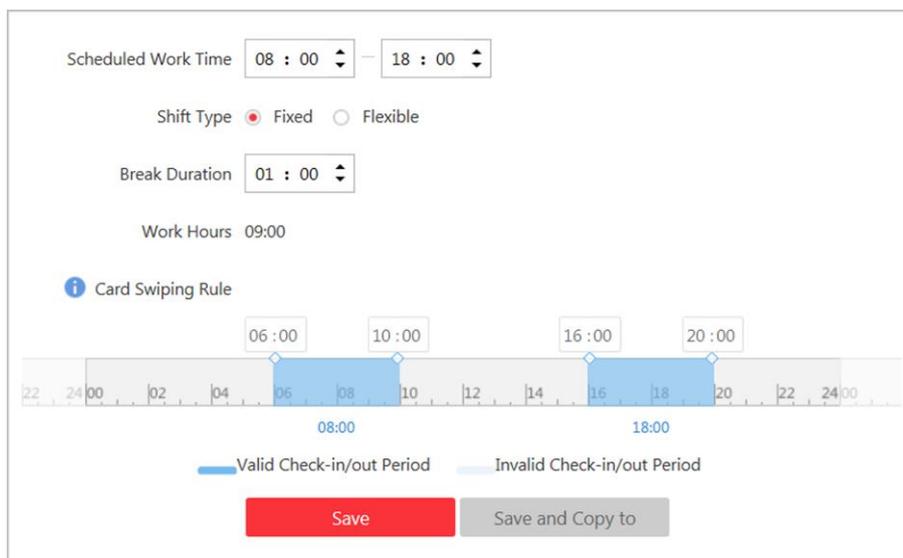


Figura 18-2 definir regra de agendamento detalhado

- 2) Opcional: Edite o tempo de trabalho necessário para torná-lo mais preciso, se necessário.
- 3) Selecione o tipo de turno.

Fixado

O tempo de início de trabalho agendado e o tempo de trabalho final são corrigidos. Somente quando o funcionário faz check-in antes do tempo de início e do check-out após o horário de trabalho final, o status de atendimento é normal. Ou pode ser tarde, sair cedo, ou ausente.

Flexível

O cronograma de trabalho flexível é uma alternativa ao cronograma fixo. Ele permite que

os funcionários estendam seu tempo de trabalho inicial e o tempo de trabalho final e você pode definir a duração prolongada permitida para o tempo de início e trabalho final.

- 4) Opcional: Para agendar flexível, defina a duração flexível, que define a duração estendida para o tempo de início e de trabalho final. Durante este horário flexível, o check-in/out será gravado e o status será **normal**.

Exemplo

Se o tempo de trabalho exigido é ajustado como 09:00 a 18:00, e a duração flexível é 30 minutos, se o empregado check-in em 09:15, e check-in para fora em 18:15, o status do comparecimento nesse dia será **Normal**.

- 5) Ajuste a duração da ruptura tal como o tempo do almoço.
Para agendamento fixo, as horas de trabalho necessárias serão calculadas automaticamente de acordo com as configurações acima (exceto a duração flexível).
- 6) Opcional: Para uma programação flexível, defina as horas de trabalho mínimas.
- 7) Defina o período de check-in/out válido na linha do tempo. Se o funcionário fizer check-in/out durante o período de entrada/saída válido, o check-in/out será gravado e o status de atendimento não estará ausente.

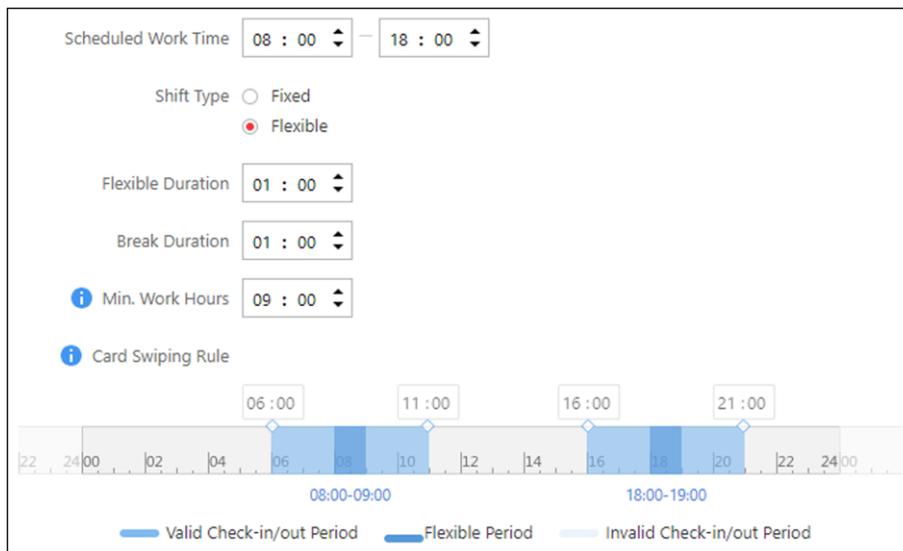


Figura 18-3 Cronograma de turno flexível

Exemplo

Na imagem acima, se você definir os parâmetros como acima, se o funcionário verifica durante 08:00 para 09:00, o check-in será normal. Se o funcionário verifica durante 09:00 para 11:00, o check-in será atrasado.

Se o funcionário fizer check-out durante o 18:00 para 19:00, a saída será normal. Se o funcionário fizer check-out durante o 16:00 para 18:00, a saída será antecipada.

Se o funcionário fizer check-in depois de 11:00, a entrada será inválida e será marcada como ausente.

Se o funcionário verificar antes de 16:00, o check-out será inválido e ele/ela será marcado como ausente.

- 8) Clique em **Salvar**. Você pode clicar em **salvar e copiar para** copiar a agenda para outros dias.
6. Selecione os feriados em que dias a agenda de turno não será efetiva.

 **Observação**

Para definir o feriado, consulte *Definir o feriado*.

7. Termine de adicionar a agenda de turno.
- Clique em **adicionar** para adicionar a agenda de turno e retornar à página de gerenciamento de agendamento de turno.
 - Clique em **adicionar e atribuir** para adicionar a agenda de turno e atribuí-la ao grupo de atendimento. Para obter detalhes, consulte *Atribuir agendamento de turno ao grupo de atendimento*.

18.3 Atribuir agendamento de turno ao grupo de atendimento

Depois de definir o cronograma de turno, é necessário atribuí-lo ao grupo de atendimento para que ele calcule os registros de atendimento para pessoas no grupo de atendimento de acordo com este cronograma de turno.

Antes de começar

- Adicione uma agenda de turno e defina a regra. Para detalhes, consulte *Adicionar agendamento de turno*.
- Adicione um grupo de atendimento. Para detalhes, consulte *Adicionar grupo de atendimento*.

Execute esta tarefa para atribuir uma agenda de turno ao (s) grupo (s) de atendimento.

Etapas

1. Clique em **tempo & atendimento → agendamento de turno** para entrar na página de gerenciamento de agendamento de turno.
2. Insira a página atribuir ao grupo de atendimento.
 - Depois de definir os parâmetros de agendamento de turno ao adicionar, clique em **adicionar e atribuir**.
 - Ao editar a agenda de turno, clique em **configuração** na página de detalhes da agenda de turno.
 - Clique em  na coluna operação.
3. No campo atribuir ao grupo de atendimento, selecione o (s) grupo (s) de atendimento para os quais você deseja atribuir a agenda de turno.

 **Observação**

Somente os grupos de atendimento que não foram vinculados a uma agenda de turno serão exibidos.

4. Opcional: Clique em **adicionar novo** para adicionar um novo grupo de atendimento.
5. Clique em **Salvar**.

18.4 Adicionar ponto de verificação de atendimento

Você deve definir uma porta como um ponto de verificação de atendimento, de modo que o check-in/out por credenciais (como passando cartão no leitor de cartão da porta) será válido e será gravado.

Execute esta tarefa para adicionar um ponto de verificação de atendimento.

Etapas

1. Clique em **tempo & atendimento** → **agendamento de turno** para entrar na página de gerenciamento de agendamento de turno.
2. Clique em **Adicionar**.

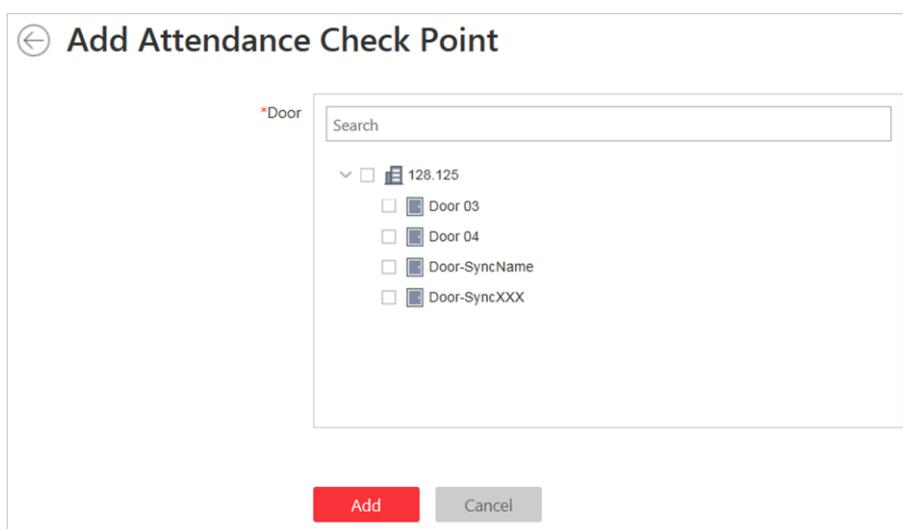


Figura 18-4 Adicionar ponto de verificação de atendimento

Todas as portas que não foram ajustadas como o ponto de verificação do comparecimento serão indicadas.

3. Selecione a (s) porta (s)
4. Clique em **Adicionar**.
As portas selecionadas serão exibidas na lista de pontos de verificação de atendimento.
5. Para excluir o ponto de verificação de atendimento adicionado, selecione a porta (s) e clique em **excluir**.

Observação

Se o ponto de verificação de atendimento for excluído, os registros de atendimento nesse ponto de verificação de atendimento também serão excluídos e afetarão os resultados de participação das pessoas nos dias em que os dados de atendimento não foram calculados.

18.5 Gerenciar registro de atendimento

Os registros de atendimento das pessoas serão gravados e armazenados no sistema. Você pode pesquisar os registros definindo as condições de pesquisa para exibir os detalhes de atendimento e exibir o relatório de atendimento da pessoa. Você também pode corrigir o tempo de check-in/out para os registros excepcionais de acordo com as necessidades reais.

18.5.1 Pesquisa registro de atendimento

Você pode pesquisar os registros de atendimento para exibir o status de atendimento da pessoa definindo as condições de pesquisa.

Antes de começar

- Certifique-se de que a pessoa não expirou.
- Certifique-se de que o grupo de atendimento da pessoa não expirou. Ou os registros de assiduidade não serão gravados. Para definir o período efetivo do grupo de atendimento, vide **Adicionar grupo de atendimento**.

Etapas

1. Clique em **tempo & atendimento** → **registro de atendimento** para entrar na página de registro de atendimento.
2. No painel de filtro, defina as condições de pesquisa.

Tempo

Defina o intervalo de tempo dos registros de atendimento que você deseja pesquisar. Você pode pesquisar os registros de atendimento das pessoas registradas dentro de três anos.

3. Clique em **filtrar** para filtrar os registros de atendimento de acordo com as condições de pesquisa.
Se você pesquisar os registros de atendimento em um dia, poderá visualizar o status de atendimento das pessoas e o tempo de trabalho Detalhado (incluindo tempo de trabalho agendado e tempo de trabalho real).
Se você Pesquisar os registros de atendimento em vários dias, poderá visualizar o relatório de atendimento das pessoas, incluindo os horários de licença normal, tardia, antecipada, status ausente durante o período de tempo e o total de horas de trabalho.
4. Opcional: Se você pesquisar os registros de atendimento em vários dias, passe o cursor sobre o número de horas de licença tardia, antecipada ou ausente para visualizar a data específica.
5. Opcional: Clique no nome da pessoa para ver os registros de atendimento da pessoa.

Observação

Passa o cursor sobre a data para ver o tempo de trabalho detalhado, incluindo tempo de trabalho agendado e tempo de trabalho real.

6. Opcional: Você também pode corrigir o check-in/out para o status de atendimento excepcional, se necessário. Para obter detalhes, consulte **registro de atendimento correto para uma única pessoa..**
7. Opcional: Clique em **exportar** e selecione os itens para exportar os registros de atendimento filtrados e salvar em seu PC.

 **Observação**

O arquivo exportado está no formato CSV. Se o arquivo for maior do que 50 MB, o arquivo será compactado para um pacote ZIP.

18.5.2 Registro de atendimento correto para pessoa singular

Depois de pesquisar o registro de atendimento da pessoa, você pode corrigir o tempo de entrada/saída de uma pessoa de acordo com as necessidades reais se o status de atendimento não for normal.

Execute esta tarefa se precisar corrigir a hora de check-in/check-out da pessoa.

Etapas

1. Clique em **tempo & atendimento** → **registro de atendimento** para entrar na página de registro de atendimento.
2. Pesquise os registros de atendimento.

 **Observação**

Para detalhes, consulte **Registro de atendimento de pesquisa.**

3. Opcional: Se você pesquisar os registros de atendimento em um único dia, você pode executar as seguintes etapas para corrigir o tempo de check-in/out.
 - 1) Clique em  na coluna operação.
 - 2) Defina o tempo de check-in/out correto.
 - 3) Opcional: Insira o motivo da correção.
 - 4) Clique em **OK**.

O status de atendimento da pessoa nesse dia muda de acordo com a correção.
4. Opcional: Se você pesquisar os registros de atendimento em vários dias, você pode executar as seguintes etapas para corrigir o tempo de check-in/out.
 - 1) Clique no nome da pessoa para entrar na página de registro de atendimento detalhada.

Attendance Record

< 2018/01 2018/02 2018/03 • 2018/04 2018/05 2018/06 >

Total: Late: 0. Early Leave: 1. Absent: 4.

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1	2	3
4	5	6	7	8 Normal	9 Early Leave	10 Normal
11 Absent	12 Normal	13 Normal	14 Normal	15 Normal	16 Normal	17 Absent
18 Normal	19 Absent	20 Normal	21 Absent	22	23	24
25	26	27	28	29	30	31

Figura 18-5 Página detalhada de atendimento

Os status de atendimento da pessoa são exibidos no calendário.

- 2) Passe o cursor para a data em que o status de atendimento não é normal e clique em **check-in/out correto**.
- 3) Defina o tempo de check-in/out correto.
- 4) Opcional: Insira o motivo da correção.
- 5) Clique em **OK**.

O status de presença da pessoa nesse dia muda de acordo com a correção e o ícone  será exibido, indicando que o status foi corrigido.

18.5.3 Registros de atendimento corretos para várias pessoas

Você pode corrigir o tempo de check-in/out de várias pessoas em um lote de acordo com as necessidades reais se o status de atendimento não for normal.

Execute esta tarefa se necessitar de corrigir o tempo de check-in/out de várias pessoas.

Etapas

Observação

Até 50.000 registros de assiduidade podem ser corrigidos por vez.

1. Clique em **tempo & atendimento** → **registro de atendimento** para entrar na página de registro de atendimento.
2. Clique em **lote correto check-in/out** para abrir a janela seguinte.

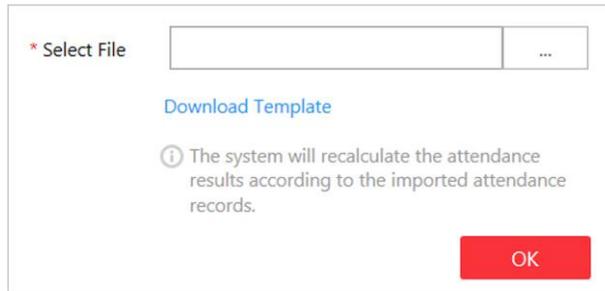


Figura 18-6 Registros de atendimento corretos em lote

3. Clique em **baixar modelo** para baixar o arquivo de modelo e você pode salvá-lo no seu PC.
4. No modelo baixado, insira o tempo de início de trabalho real ou/e o tempo de trabalho final seguindo as regras no modelo.
5. Clique em **lote correto check-in/out** e carregue o modelo com os registros de atendimento corrigidos.
6. Clique em **OK** e o progresso será exibido.

 **Observação**

O sistema recalculará os resultados de atendimento de acordo com os registros de atendimento importados.

Capítulo 19 Gerenciar grupo de comparação de face

Depois de adicionar as pessoas à lista de pessoa, você deve criar um grupo de comparação de faces e, em seguida, adicionar pessoas (selecionadas da lista de pessoas) ao grupo antes de poder realizar a comparação de faces. Finalmente, você precisa aplicar o grupo de comparação de face com informações de pessoa para o dispositivo de reconhecimento de face para ter efeito. Quando o rosto de uma pessoa é detectado e corresponde ou não coincide com as informações da pessoa no grupo de comparação de faces, um evento/alarme (se configurado) será acionado para notificar o pessoal de segurança e você poderá visualizar as informações de comparação de face durante a visualização ao vivo no o cliente de controle.

19.1 Adicionar grupo de comparação de faces

Depois de adicionar a pessoa (s), você pode adicionar um grupo de comparação de faces e adicionar pessoa (s) ao grupo para comparação de faces.

Execute essa tarefa se desejar adicionar um grupo de comparação de faces.

Etapas

Observação

Até 64 grupos de comparação de faces podem ser adicionados.

1. Clique em **pessoa** → **grupo de comparação de faces** para entrar na página de gerenciamento de grupo de comparação de faces.

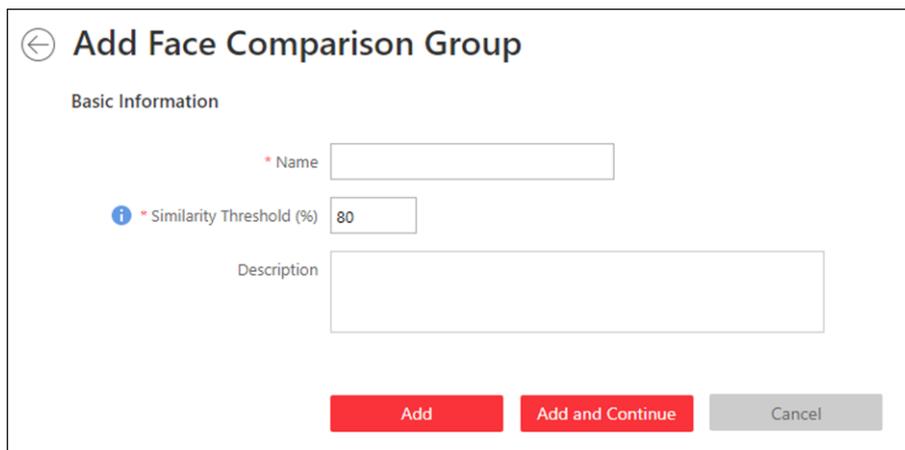


Figura 19-1 Adicionar grupo de comparação de faces

2. Adicione um novo grupo de comparação de faces.
 - 1) Clique em **Adicionar**.
 - 2) Crie um nome para o grupo de comparação de faces.

- 3) Defina o limiar de similaridade de comparação de faces que afeta a frequência e a precisão do alarme de comparação de imagens faciais. Quando a similaridade de comparação de face é maior do que o limite configurado, a câmera considerará a pessoa como correspondida.
 - 4) Opcional: Insira as informações de descrição, se necessário.
 - 5) Clique em **adicionar** para adicionar o grupo e voltar para a lista de grupos de comparação de faces. Você também pode clicar em **adicionar e continuar** para adicionar outros grupos.
3. Adicionar pessoa (s) ao grupo.
- 1) Na página de lista de grupos de comparação facial, clique em > para mostrar as pessoas adicionadas ao grupo.
 - 2) clique em + para abrir a janela seguinte.

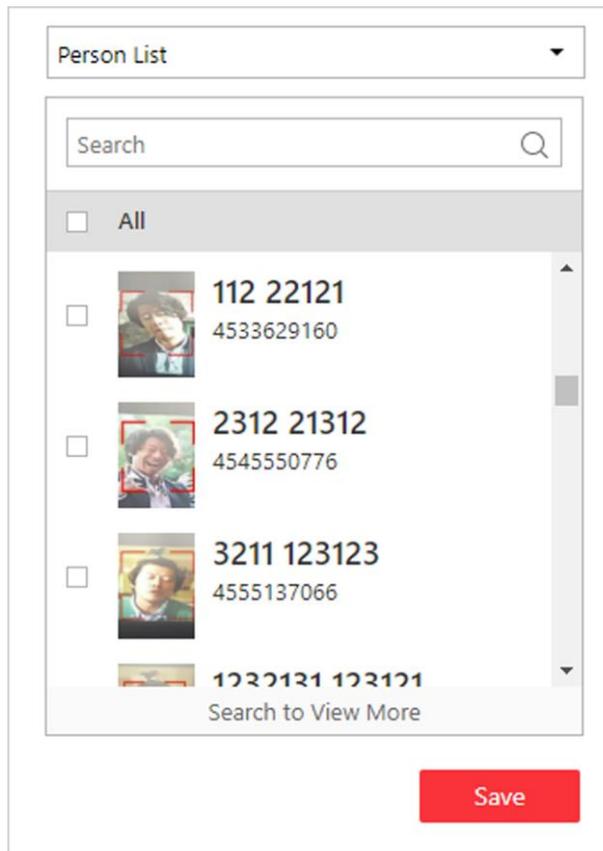


Figura 19-2 Adicionar pessoa ao grupo de comparação de face

- 3) Selecione o modo de adição como **lista de pessoas**.
Todas as pessoas na lista de pessoa que não foram adicionadas ao grupo atual serão exibidas.
- 4) Selecione a pessoa (s) para adicionar ao grupo.
- 5) Clique em **Salvar**.
- 6) Opcional: Você também pode definir o modo de **adição como grupo de comparação de face adicionado** ou **grupo de domínio importado** para adicionar as pessoas em outros grupos existentes ao grupo atual.

 **Observação**

As pessoas originais no grupo atual não serão substituídas depois de adicionar a pessoa do grupo existente.

 **Observação**

Até 10.000 pessoas podem ser adicionadas a um grupo de comparação de faces.

4. Opcional: Depois de adicionar as pessoas ao grupo de comparação de faces, você pode fazer uma ou mais das seguintes ações.

Remover pessoa do grupo de comparação de faces

Passa o cursor na imagem do rosto e clique em .

Editar grupo de comparação de faces

Clique em  na coluna operação para editá-la e exibir as câmeras às quais ela é aplicada.

Excluir comparação de face

Clique em  na coluna operação para excluir isto.

Excluir todos os grupos de comparação de face

Clique em **excluir tudo** para excluir todos os grupos de comparação de face adicionados.

O que fazer a seguir

Depois de adicionar o grupo de comparação de faces e configurar as pessoas no grupo, aplique o grupo à câmera que suporta a comparação de imagens faciais para entrar em vigor. Para detalhes, consulte *Aplicar grupo de comparação de face ao dispositivo*.

19.2 Aplicar grupo de comparação de face ao dispositivo

Depois de definir o grupo de comparação de faces e adicionar pessoa (s) ao grupo, você precisa aplicar as configurações de grupo à câmera que suporta a comparação de imagens faciais para que a câmera possa comparar as faces detectadas com as imagens de face no grupo de comparação de face e acionar alarmes (se configurados). Depois de aplicar o grupo de comparação de faces ao dispositivo, se os dados no grupo forem alterados (como adicionar uma pessoa ao grupo, remover a pessoa do grupo, etc.), o sistema aplicará automaticamente os dados no grupo ao dispositivo para entrar em vigor.

Antes de começar

Adicione a câmera que suporta a comparação do retrato da cara ao sistema.

Execute essa tarefa se você precisar aplicar as informações de pessoa no grupo de comparação de

face à câmera para entrar em vigor.

Etapas

Observação

- Atualmente, ele só suporta a aplicação de câmera que suporta face comparação de imagens.
- O número máximo de grupos que podem ser aplicados à câmera depende da capacidade da câmera.

1. Clique em **pessoa** → **grupo de comparação de faces** para entrar na página de gerenciamento de grupo de comparação de faces.
2. Clique em **aplicar ao dispositivo**

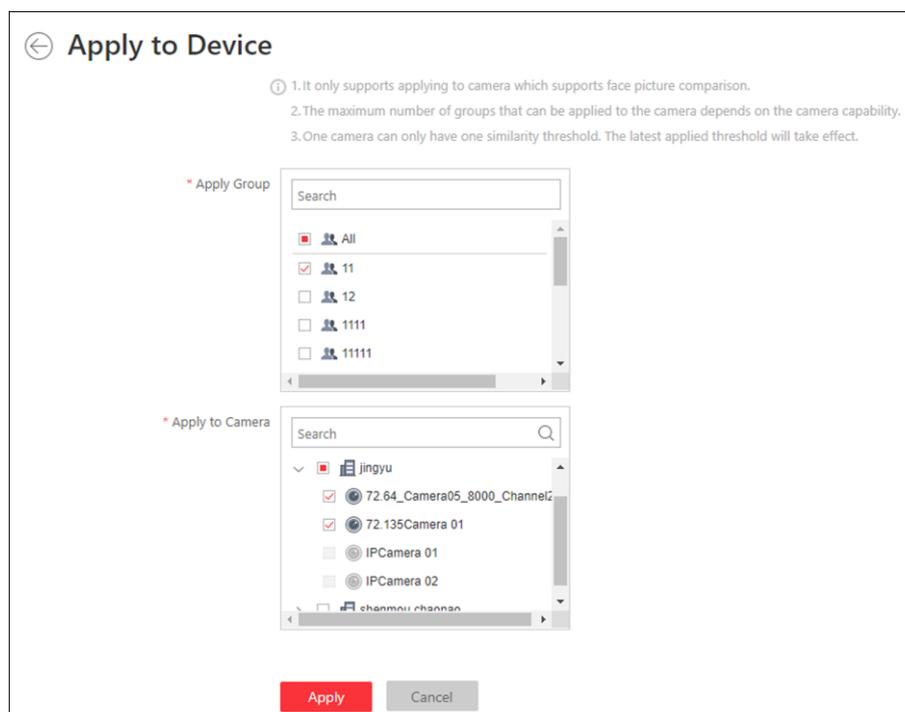


Figura 19-3 Aplicar grupo de comparação de face ao dispositivo

3. Selecione os grupos de comparação de faces a serem aplicados.
4. Selecione a (s) câmera (s) para aplicar os grupos de comparação de faces selecionados.
5. Clique em **aplicar** para iniciar a aplicação.
O andamento da aplicação será exibido na coluna operação.
6. Opcional: Se houver falha no grupo de aplicação de comparação facial, o ícone  será exibido próximo ao nome do grupo. Passe o cursor para o ícone para verificar o prompt.

Observação

Você pode clicar em **repetir** para aplicar esse grupo às câmeras vinculadas novamente. Clique em **detalhes** para exibir os detalhes da exceção.

Capítulo 20 Gerenciar função e usuário

O sistema permite que você adicione usuários e atribua permissões do usuário para acessar e gerenciar o sistema. Antes de adicionar usuários no sistema, você deve criar funções para definir os direitos de acesso de usuário aos recursos do sistema e, a seguir, atribuir a função ao usuário para conceder as permissões ao usuário. Um usuário pode ter várias funções diferentes.

20.1 Adicionar função

Você pode atribuir as permissões às funções conforme necessário e os usuários podem ser atribuídos com funções diferentes para obter permissões diferentes.

Execute essa tarefa quando você adicionar a função.

Etapas

1. Clique em **segurança** → **funções** para entrar na página Gerenciamento de função.

Observação

O sistema pré-define duas funções padrão: administrador e operador. Você pode clicar no nome da função para visualizar os detalhes e as operações. Mas você não pode editar ou excluir as duas funções padrão.

Administrador

A função que tem toda a permissão do sistema.

Operador

A função que tem toda a permissão para operar o cliente de controle e tem a permissão para operar os aplicativos (exibição ao vivo, reprodução e configuração local) no cliente da Web.

2. Clique em **Adicionar** para entrar na página de Adição de função.

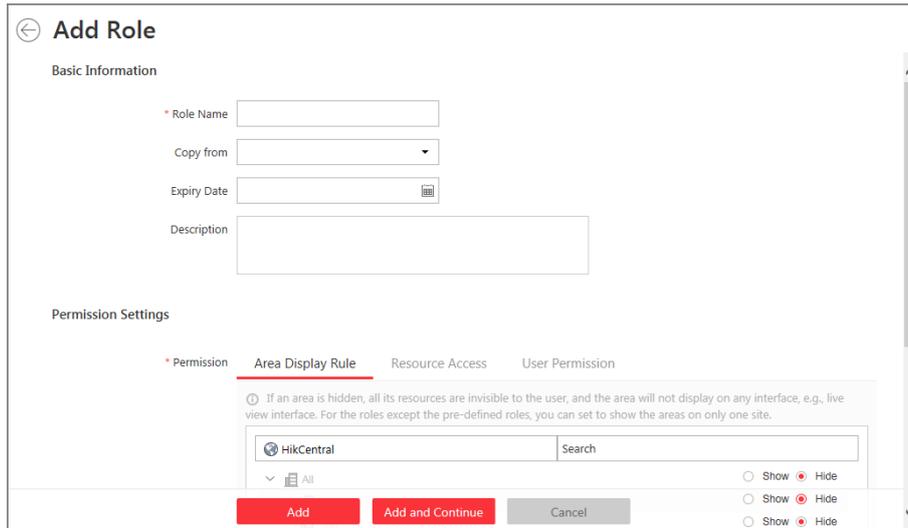


Figura 20-1 Adicionar página de funções

3. Defina o nome da função, a data de expiração e a descrição conforme desejado.

Data de validade

A data em que essa função se torna inválida.

4. Defina a permissão para a função.

- Selecione a função padrão ou pré-definida na lista suspensa **copiar formulário** para copiar as configurações de permissão da função selecionada.
- Atribua as permissões à função.

Regra de exibição de área

Mostre ou oculte a (s) área (s) específica para a função. Se a área estiver oculta, o usuário com a função não poderá exibir e acessar a área e seus recursos em qualquer interface.

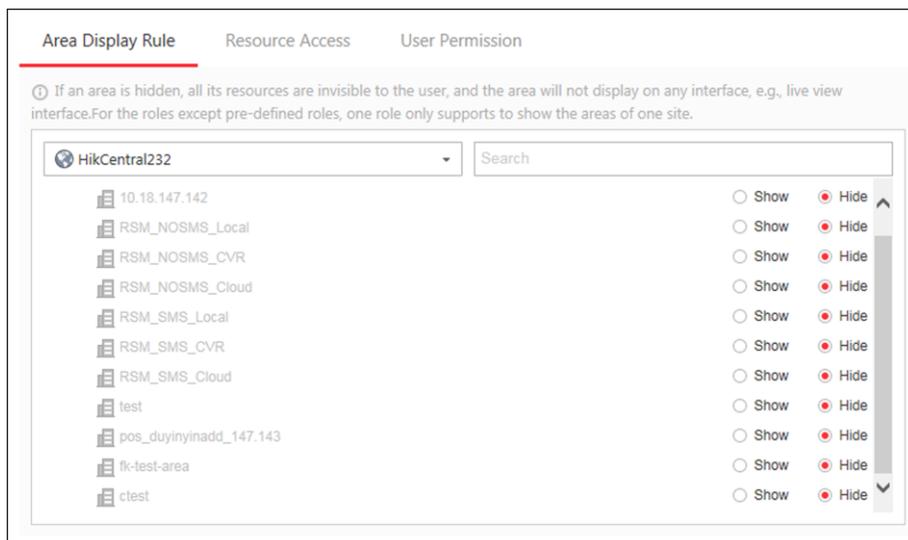


Figura 20-2 regra de exibição de área

Permissão de acesso a recursos

Selecione as funções no painel esquerdo e selecione os recursos do painel direito para atribuir as permissões dos recursos selecionados à função.

Observação

Se você não verificar os recursos, a permissão de recurso não pode ser aplicada à função.

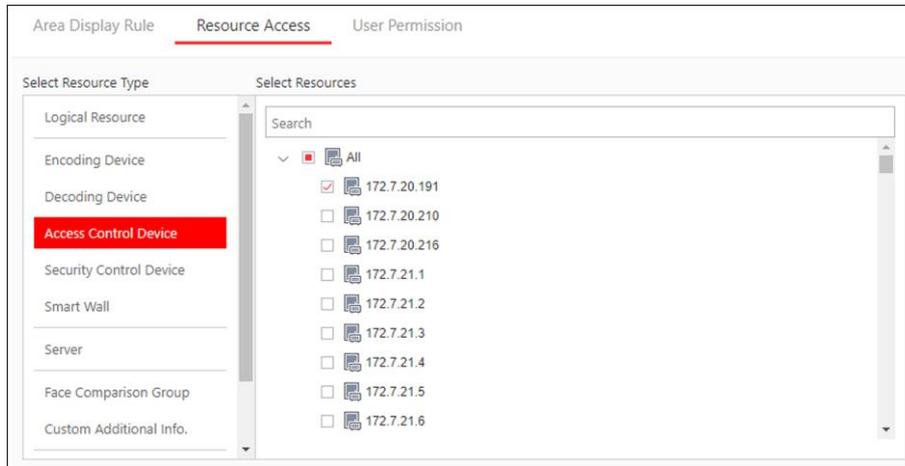


Figura 20-3 permissão de acesso a recursos

Permissão do usuário

Atribua as permissões de recurso, permissões de configuração no cliente da Web e as permissões de Control Client de controle para a função.

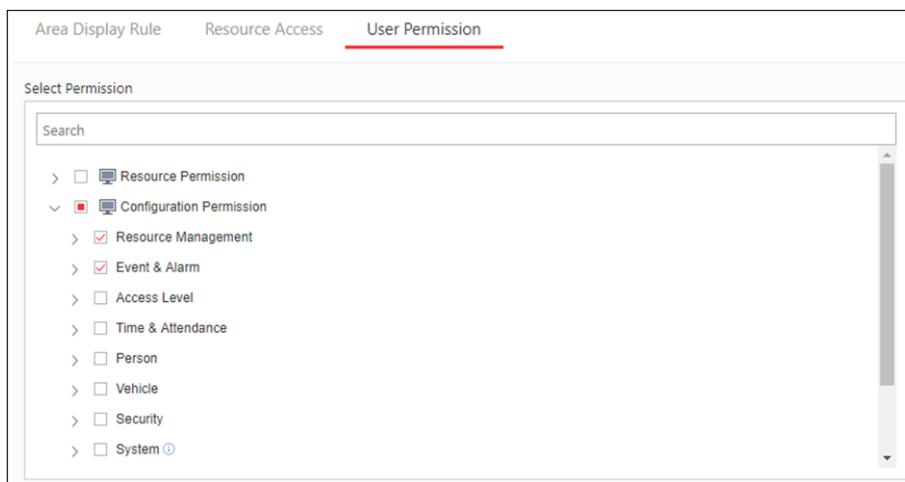


Figura 20-4 permissão do usuário

5. Complete a adição da função.
 - Clique em **Adicionar** para adicionar a função.
 - Clique em **adicionar e continuar** para salvar as configurações e continuar adicionando funções.

6. Opcional: Depois de adicionar a função, você pode fazer um ou mais dos seguintes procedimentos:

Editar função	Clique no campo nome para editar as configurações da função.
Atualizar função	Clique em atualizar tudo para obter o status mais recente das funções.
Excluir função	Clique em excluir para excluir a função.
Filtrar função	Clique em  para expandir as condições de filtro. Defina as condições e clique em filtrar para filtrar as funções de acordo com as condições do conjunto.

20.2 Adicionar usuário normal

Você pode adicionar usuários normais para acessar o sistema e atribuir a função ao usuário normal. Usuários normais referem-se a todos os usuários, exceto o usuário administrador.

Execute esta tarefa quando você precisa adicionar o usuário normal.

Etapas

1. Clique em **segurança** → **usuários** para entrar na página Gerenciamento de usuários.
2. Clique em **Adicionar** para entrar na página de Adição de usuário.

Add User

* User Name

i Password

Expiry Date

i Email

* User Status Active Inactive

Restrict Concurrent Logins

Description

Permission

i * PTZ Control Permission

* Assign Role

Role Name	Description
<input type="checkbox"/> All	
<input type="checkbox"/> Administrator	
<input type="checkbox"/> Operator	
<input type="checkbox"/> 1213	
<input type="checkbox"/> 121-door01,door02	
<input type="checkbox"/> 121-door01,door03	
<input type="checkbox"/> 123	
<input type="checkbox"/> 123456	

[Add New Role](#)

Add **Add and Continue** **Cancel**

Figura 20-5 Adicionar página de usuário

3. Configure os parâmetros necessários.

Nome de usuário

Para o nome de usuário, somente letras (a-z, A-Z), dígitos (0-9), e - podem ser contidas.

Senha

O sistema fornece uma senha padrão (Abc123). Você pode usá-lo ou personalizar uma senha mais forte. No entanto, você deve alterar a senha inicial para login pela primeira vez.

Data de validade

A data em que essa conta de usuário se torna inválida.

E-mail

O sistema pode notificar o usuário enviando um e-mail para o endereço de e-mail. Se o usuário normal esquecer sua senha, ele/ela pode redefinir a senha via e-mail.

i Observação

O endereço de e-mail do usuário administrador pode ser editado pelo usuário com a função de administrador.

Restringir logon's simultâneos

Se necessário, defina **restringir logon's simultâneos** alterne para ON e insira o número máximo de logons simultâneos.

Status de usuário

Há dois tipos de status disponíveis. Se você selecionar congelar, a conta de usuário estará inativa até que você defina o status do usuário como ativo.

4. Defina o nível de permissão (1-100) para o controle PTZ na permissão de controle PTZ.
-

Observação

Quanto maior o valor for, o nível de permissão mais alto que o usuário tem. O usuário com nível de permissão mais alto tem a prioridade para controlar a unidade PTZ.

Exemplo

Quando o usuário1 e o usuário1 controlam a unidade PTZ ao mesmo tempo, o usuário que tem o nível de permissão de controle PTZ mais alto tomará o controle do movimento PTZ.

5. Verifique as funções existentes para atribuir a função (s) para o usuário.
-

Observação

- Se não for adicionada nenhuma função, duas funções padrão são selecionáveis: administrador e operador.

Administrador

A função que tem todas as permissões do sistema.

Operador

A função que tem todas as permissões do cliente de controle do sistema.

- Se você quiser adicionar funções personalizadas, poderá clicar em **adicionar nova função** para inserir rapidamente a página Adicionar função. Veja **Adicionar função** para detalhes.
-

6. Complete adicionando o usuário.
 - Clique em **adicionar** para adicionar o usuário.
 - Clique em **adicionar e continuar** para salvar as configurações e continuar a adicionar usuários.
-

Observação

Você será solicitado a alterar a senha ao fazer login pela primeira vez. Veja **Logon pela primeira vez para o usuário normal** para detalhes.

7. Opcional: Execute as seguintes operações depois de adicionar o usuário normal.

Editar usuário Clique no campo **nome** do usuário para editar as informações

Redefinir senha Na página Editar usuário, clique em Redefinir para redefinir a senha

do usuário.

 **Observação**

- Se você redefinir a senha, a senha do usuário será redefinida para sua senha inicial Abc123. O usuário deve fazer o login com senha inicial e, a seguir, troque a senha.
 - O usuário administrador pode redefinir as senhas de todos os outros usuários (exceto o usuário do domínio). Outros usuários com permissão de segurança (em configuração e permissão de controle) podem redefinir as senhas dos usuários sem permissão de segurança. Para alterar a senha, consulte ***Alterar senha para redefinir usuário***.
-

Excluir usuário	Clique em OK para excluir o usuário.
Forçar logout	Você também pode selecionar o usuário online e clicar em Forçar saída para desconectar do usuário online.
Atualizar tudo	Clique em atualizar tudo para obter o status mais recente dos usuários.
Filtrar usuário	Clique em  para expandir as condições de filtro. Defina as condições e clique em filtrar para filtrar os usuários de acordo com as condições definidas.

 **Observação**

O usuário administrador chamado admin foi pré-definido por padrão. Ele não pode ser editado, excluído ou forçado a fazer logoff.

20.3 Importar usuários do domínio

Você pode importar os usuários no domínio do AD em um lote para o sistema (incluindo nome de usuário, nome real e email) e atribuir funções aos usuários do domínio.

Antes de começar

Você deve configurar as configurações do Active Directory. Veja ***Definir o Active Directory*** para detalhes.

Etapas

1. Clique em **segurança** → **usuários** para entrar na página Gerenciamento de usuários.
2. Clique em **importar usuários do domínio** para entrar na página importar usuários do domínio.

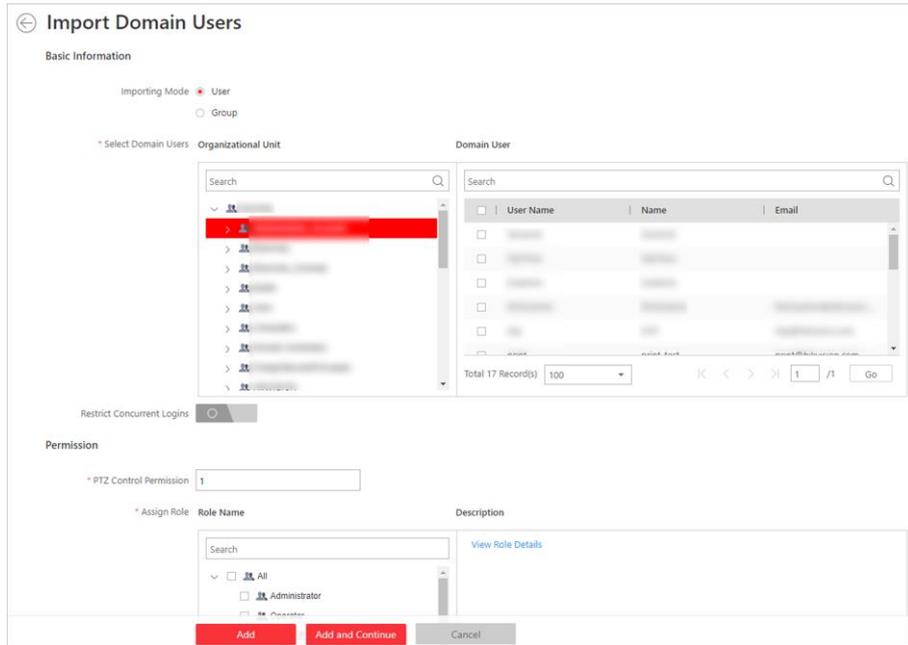


Figura 20-6 importar usuários do domínio

3. Selecione o modo de importação.

Usuário

Importe os usuários especificados. Selecione a unidade organizacional e selecione as contas de usuário na unidade organizacional que são exibidas na lista usuário do domínio à direita.

grupo

Importe todos os usuários do grupo.

4. Opcional: Defina **restringir logon's simultâneos** alterne para ON e insira o número máximo de logons simultâneos.
5. Defina o nível de permissão (1-100) para o controle PTZ na permissão de controle PTZ.

Observação

Quanto maior o valor for, o nível de permissão mais alto que o usuário tem. O usuário com nível de permissão mais alto tem a prioridade para controlar a unidade PTZ.

Exemplo

Quando o usuário1 e o usuário1 controlam a unidade PTZ ao mesmo tempo, o usuário que tem o nível de permissão de controle PTZ mais alto tomará o controle do movimento PTZ.

6. Verifique as funções existentes para atribuir a função (s) para o usuário de domínio selecionado.
-

Observação

- Se não for adicionada nenhuma função, duas funções padrão são selecionáveis: administrador e operador.

Administrador

A função que tem todas as permissões do HikCentral.

Operador

A função que tem todas as permissões do Control Client HikCentral.

Se você quiser adicionar funções personalizadas, poderá clicar em **adicionar nova função** para inserir rapidamente a página Adicionar função. Veja **Adicionar função** para detalhes.

7. Conclua a importação do usuário do domínio.
 - Clique em **adicionar** para adicionar o usuário.
 - Clique em **adicionar e continuar** para salvar as configurações e continuar a adicionar usuários.
8. Opcional: Depois de importar as informações do usuário no domínio para o sistema, se as informações do usuário no domínio forem alteradas, clique em **sincronizar usuários do domínio** para obter as informações mais recentes dos usuários importados para o sistema. Se os usuários forem importados por grupo, ele sincronizará as informações mais recentes do usuário do grupo de domínio (incluindo usuários adicionados, usuários excluídos, usuários editados, etc., no grupo).

Resultado

Depois de adicionar com êxito os utilizadores do domínio, os utilizadores podem iniciar sessão no HikCentral através do Web Client, Control Client e Mobile Client pela respectiva conta de domínio e palavra-passe.

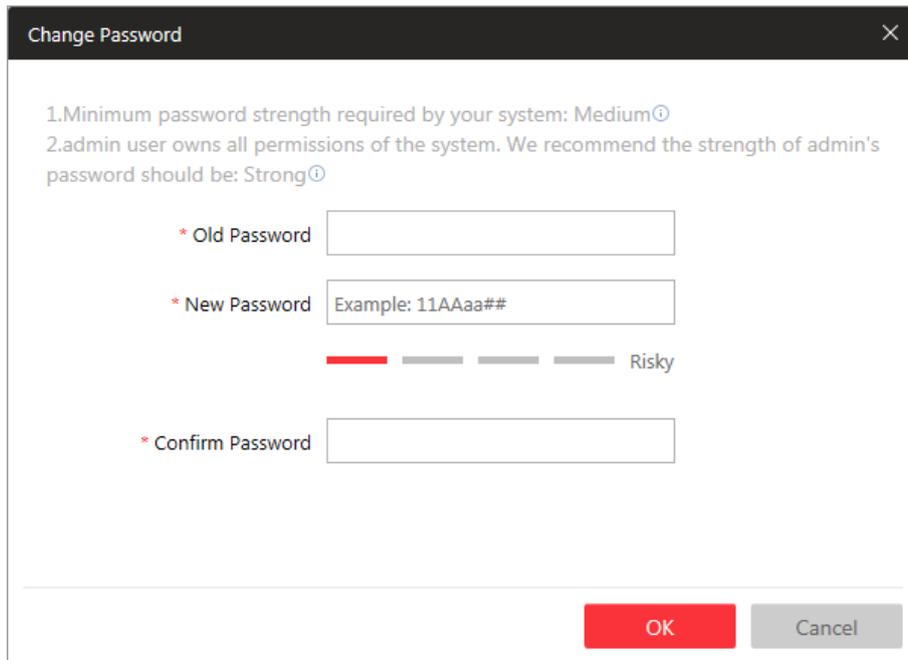
20.4 Alterar senha do usuário atual

Quando você faz logon via Web Client, você pode alterar sua senha conforme desejado.

Realize esta tarefa quando precisar pesquisar os locais no mapa GIS.

Etapas

1. Mova o cursor sobre o nome do usuário atual no canto superior direito do sistema e.
2. Na lista suspensa, selecione Alterar senha para abrir a caixa de diálogo Alterar senha.



The image shows a 'Change Password' dialog box with the following elements:

- Header: 'Change Password' with a close button (X).
- Instructions:
 - 1. Minimum password strength required by your system: Medium ⓘ
 - 2. admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong ⓘ
- Fields:
 - * Old Password: An empty text input field.
 - * New Password: A text input field containing 'Example: 11AAaa##'.
 - * Confirm Password: An empty text input field.
- Strength Indicator: A progress bar below the 'New Password' field. The first segment is red, and the rest are grey. The label 'Risky' is positioned to the right of the bar.
- Buttons: 'OK' (red) and 'Cancel' (grey) buttons at the bottom right.

Figura 20-7 caixa de diálogo Alterar senha

3. Introduza a palavra-passe antiga, a nova palavra-passe e confirme a palavra-passe.

Cuidado

A força da senha do dispositivo pode ser verificada pelo sistema. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

4. Clique em **OK** para alterar a senha.

20.5 Redefinir senha para usuário admin

Quando você esqueceu a senha do usuário administrador, você pode redefinir a senha e definir uma nova senha para o usuário admin.

Etapas

1. Na barra de endereço do navegador da Web, digite o endereço do PC executando o serviço VSM e pressione **Enter**.

Exemplo:

Se o endereço IP do PC executando o VSM for 172.6.21.96, você deverá inserir

http://172.6.21.96 na barra de endereços.

 **Observação**

Você deve configurar o endereço IP do VSM em **Sistema → Rede → Acesso WAN** antes de acessar o VSM via WAN. Para detalhes, consulte **Definir Acesso WAN**.

Uma página de login aparecerá.

2. Opcional: Quando você faz logon via navegador Internet Explorer atual pela primeira vez, você deve instalar o plug-in antes de poder acessar as funções.
-

 **Observação**

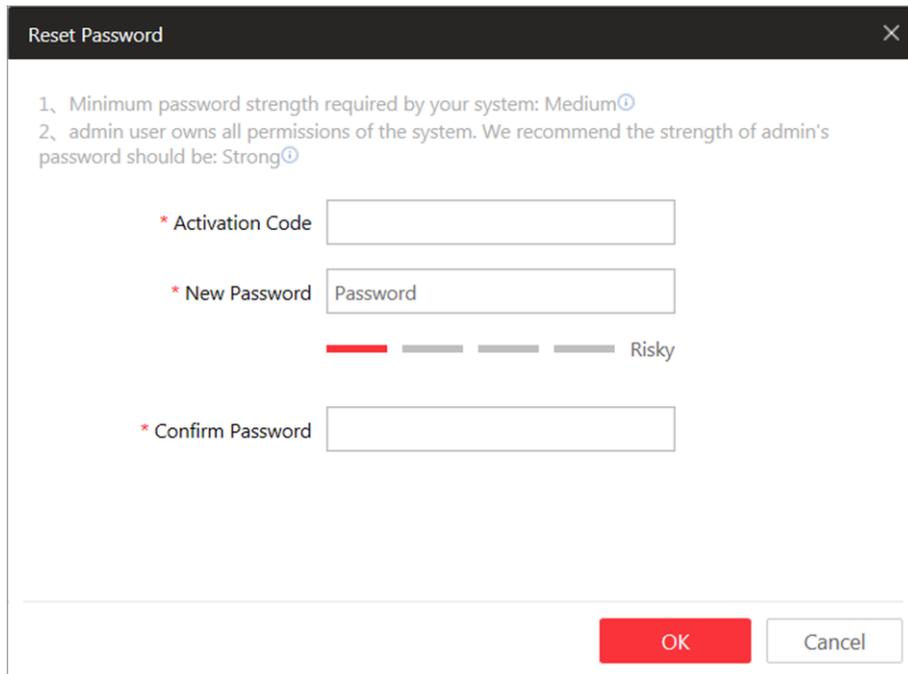
Se uma nova versão do plug-in é detectada, você deve atualizá-lo para garantir o uso adequado e melhor experiência do usuário.

- 1) Clique em **OK** na caixa de diálogo pop-up para instalar o plug-in. Ou clique em **baixar plug-in** para baixá-lo.
 - 2) Salve o arquivo de plug-in no seu PC e feche o navegador da Web.
 - 3) Encontre o plug-in que armazena em seu PC e instale o plug-in de acordo com o prompt.
 - 4) Reabra o navegador da Web e efetue login no VSM (etapa 1).
-

 **Observação**

Por favor, permita que o navegador execute o plug-in no prompt pop-up.

3. Entrar como **admin** de entrada no campo nome de usuário.
4. Clique em **esqueceu a senha** para abrir a caixa de diálogo Redefinir senha.



The image shows a 'Reset Password' dialog box with the following content:

- 1、 Minimum password strength required by your system: Medium ⓘ
- 2、 admin user owns all permissions of the system. We recommend the strength of admin's password should be: Strong ⓘ
- * Activation Code
- * New Password
A progress bar below the 'New Password' field shows a red segment followed by three grey segments, with the word 'Risky' to its right.
- * Confirm Password

At the bottom right, there are two buttons: 'OK' (red) and 'Cancel' (white).

Figura 20-8 Redefinir senha

5. Insira os parâmetros necessários na caixa de diálogo pop-up, incluindo o código de ativação, a nova senha e confirme a senha.

 **Observação**

A força da senha pode ser verificada pelo sistema e deve atender aos requisitos dele. Se a força da senha for inferior à força mínima exigida, será solicitado que você a altere. Para ajustes detalhados da força mínima da senha, consulte **Gerenciar a segurança do sistema** Segurança.

 **Cuidado**

A força da senha do dispositivo pode ser verificada pelo sistema. Recomenda-se alterar a senha de sua escolha (utilizando no mínimo 8 caracteres, incluindo pelo menos três tipos de categorias a seguir: letras maiúsculas, letras minúsculas, números e caracteres especiais) para aumentar a segurança do seu produto. Recomendamos que você redefina sua senha regularmente, especialmente no sistema de alta segurança. Redefinir a senha mensal ou semanalmente pode proteger melhor seu produto.

A configuração apropriada de todas as senhas e outras configurações de segurança são responsabilidade do instalador e/ou usuário final.

6. Clique em **OK** para redefinir a senha de admin.

 **Observação**

Se você esqueceu a senha de outros usuários, entre em contato com o usuário administrador para redefinir a senha e, em seguida, alterar a senha para logon.

20.6 Redefinir senha para usuário normal

Se o usuário esqueceu a senha, ele/ela pode entrar em contato com os usuários com função de administrador para redefinir a senha.

Execute esta tarefa para redefinir a senha para o usuário normal.

Etapas

 **Observação**

O usuário admin pode redefinir as senhas de todos os outros usuários. Outros usuários com função de administrador podem redefinir as senhas dos usuários sem função de administrador. Veja **Adicionar usuário normal** para obter detalhes sobre as configurações de função do usuário.

1. Clique em **segurança** para entrar na página Gerenciamento de segurança.
2. Clique em **usuários** à esquerda.
3. Selecione um usuário e clique no campo **nome** para entrar na página de detalhes do usuário.
4. Clique em **redefinir** para redefinir a senha do usuário selecionado.
Depois de redefinir a senha, a senha do usuário será redefinida para sua senha inicial Abc123.

Capítulo 21 Manutenção

A HikCentral fornece backup do banco de dados, para que seus dados podem ser bem protegidos e recuperados quando ocorre uma exceção.

Você também pode exportar os dados de configuração do sistema e salvá-los no PC local.

21.1 Definir backup de dados do sistema

Para a finalidade de restaurar os dados do sistema original após um evento de perda de dados ou recuperar dados de um tempo anterior, você pode manualmente fazer backup dos dados no sistema, ou configurar uma agenda para executar a tarefa de backup regularmente. Os dados do sistema incluem dados configurados no sistema, imagens configuradas no sistema, eventos recebidos e alarmes, dados de comparação de face, dados de passando do cartão, logs do servidor, etc.

Execute essa tarefa quando você precisar configurar a agenda para executar a tarefa de backup de dados do sistema regularmente ou fazer backup manualmente dos dados.

Etapas

Observação

Os backups são armazenados no servidor VSM e o caminho de salvamento padrão é C:Arquivos de programas (x86) HikCentral\VSM Servers\VSMBBackup. Se pretender editar o caminho de poupança predefinido, deve introduzir a página de backup e restaurar dados do sistema através do Web Client em execução no servidor VSM.

1. Clique em **fazer backup e restaurar dados do sistema** na página inicial.
2. Clique em **backup** na caixa de diálogo pop-up para entrar na página de backup.

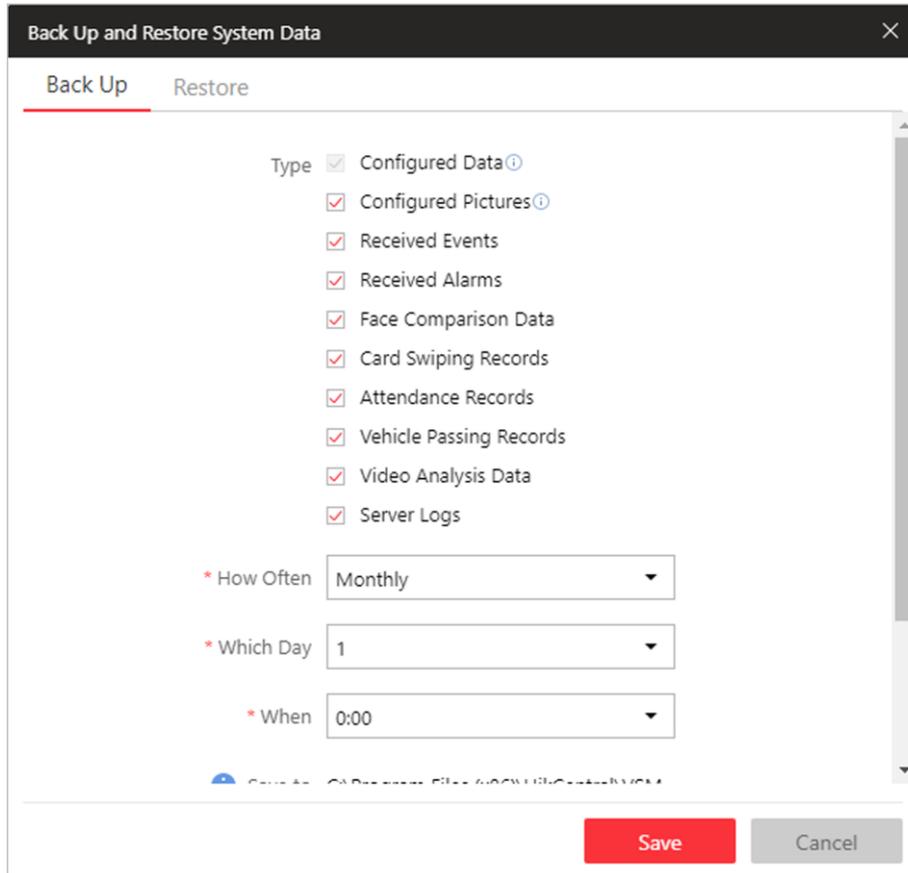


Figura 21-1 Definir backup de dados do sistema

3. Selecione o tipo de dados do sistema para backup.

Dados configurados

Os dados configurados por meio do Web Client, incluindo recursos físicos, recursos lógicos, permissões de usuário, etc. Ele é selecionado por padrão.

Imagens configuradas

Os retratos carregados ao ajustar mapas, pessoas, veículos, etc.

4. Defina a agenda de backup para executar o backup regularmente.

1) Selecione a frequência para fazer backup dos dados do sistema.

Observação

- Se você selecionar o tipo de dados além dos dados configurados, não será possível definir a frequência como **diária**.
 - Se selecionar **Semanalmente** ou **Mensalmente** para realizar a tarefa de cópia de segurança, selecione em qual dia executar.
-

2) Selecione uma hora do dia para iniciar o cópia de segurança.

3) Defina o **número máx. de backup's** para definir o número máximo de arquivos de backup disponíveis no sistema.

 **Observação**

O valor varia de 1 a 5.

5. Opcional: Clique em **Backup agora** e clique em **OK** na caixa de diálogo pop-up se você precisar executar o backup imediatamente.
6. Clique em **Salvar**.

21.2 Restaurar banco de dados

Quando ocorrer uma situação de exceção, você poderá recuperar o banco de dados se tiver feito o backup do banco de dados.

Antes de começar

Você deve ter feito backup do banco de dados. Consulte *Definir backup de dados do sistema* para detalhes.

Execute essa tarefa quando você precisar restaurar o banco de dados.

Etapas

 **Observação**

A recuperação do banco de dados recuperará o banco de dados em um estado anterior. Assim, os dados adicionados após esse Estado serão perdidos.

1. Clique em **fazer backup e restaurar banco de dados** na página inicial.
2. Clique em **restaurar** na caixa de diálogo pop-up para entrar na página de restauração do banco de dados.
3. Selecione um arquivo de backup para recuperar o banco de dados a um estado anterior.

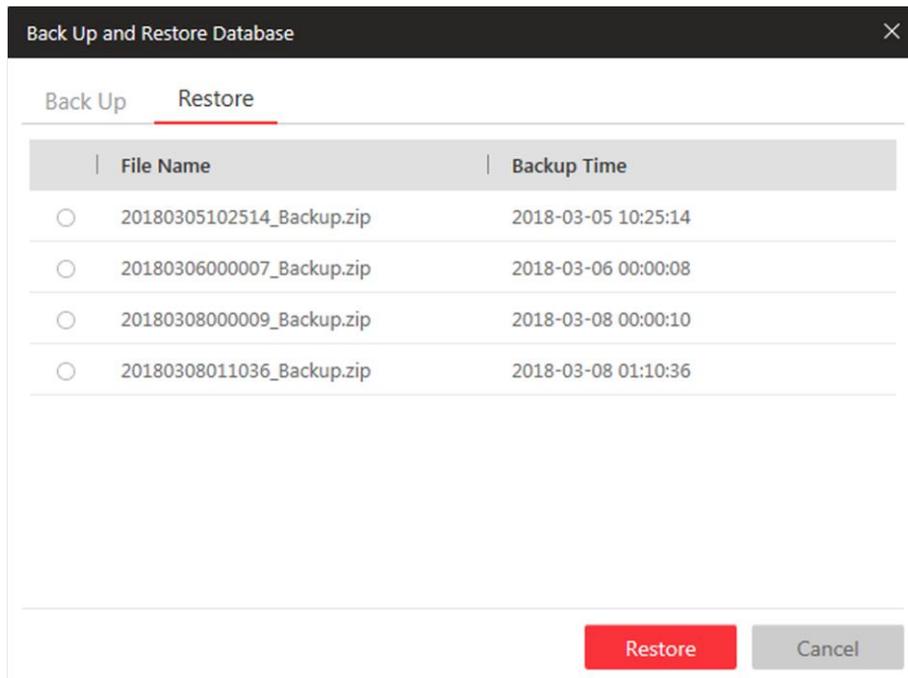


Figura 21-2 Restauração de banco de dados

4. Clique em **Recuperar** para confirmar a recuperação do banco de dados.

O que fazer em seguida

Depois de restaurar a base de dados, tem de reiniciar o serviço VSM através do Service Manager e iniciar sessão novamente através do Web Client.

21.3 Exportar arquivo de configuração

Você pode exportar e salvar dados de configuração para o PC local, incluindo o local remoto, configurações de gravação e etc.

Execute essa tarefa quando precisar exportar dados de configuração.

Etapas

1. Clique em **exportar dados de configuração** na página inicial para abrir a caixa de diálogo Exportar dados de configuração.
2. Selecione o tipo de dados de configuração a ser exportado.
3. Clique em **exportar** para salvar os dados no seu PC local.

Observação

- Você pode definir o caminho de salvamento seguindo o prompt do navegador.
 - O arquivo de dados de configuração está no formato CSV.
-

Capítulo 22 Gerenciar a segurança do sistema

A segurança do sistema é crucial para o seu sistema e propriedade, você pode definir a força da senha e bloquear o endereço IP para evitar ataques maliciosos, e definir outras políticas de segurança para aumentar a segurança do sistema.

Execute esta tarefa para definir a força de senha mínima, o bloqueio de endereço IP e outras configurações de diretiva de segurança para evitar ataques mal-intencionados.

Etapas

1. Clique em **segurança** → **configurações de segurança** para abrir a página Configurações de segurança.
2. Defina o **comutador de endereço IP** de bloqueio para ON e o número de tentativas de logon com falha é limitado.
 - 1) selecione as tentativas de logon permitidas para acessar o HikCentral.

Observação

Falha na tentativa de logon inclui tentativa de senha falhou e tentativa de código de verificação falhou.

- 2) Defina a duração de bloqueio para este endereço IP. Durante o prazo do bloqueio, as tentativas de fazer login a partir desse endereço de IP não são permitidas.
O número de tentativas de logon é limitado.
3. Selecione a **força mínima da senha** para definir os requisitos mínimos de complexidade que a senha deve atender.
4. Defina a idade máxima da senha.
 - 1) definir **ativar o interruptor de idade máxima de senha** como ON para forçar o usuário a alterar a senha quando a senha expira.
 - 2) Defina o número máximo de dias que a senha é válida.

Observação

Depois desse número de dias, você terá que trocar a senha. Você pode selecionar o intervalo de tempo pré-definido ou personalizar o intervalo de tempo.

5. Configure as configurações para bloquear automaticamente o control client após um período de inatividade no Control Client.
 - 1) Definir o **interruptor automático do Control Client** do fechamento a sobre para travar o cliente do controle após um período de tempo da inatividade no cliente do controle.
Selecione o período de tempo para inatividade do usuário. Você pode selecionar o período de tempo pré-definido ou personalizar o período de tempo.
6. Clique em **Salvar**.

Capítulo 23 Configuração do sistema

A página sistema permite que você defina parâmetros básicos para o sistema, como definir um nome personalizado para o seu local, definindo o endereço IP da WAN para permitir o acesso ao seu sistema via WAN (Wide Area Network) e configurando as configurações NTP (Network Time Protocol) para sincronizando o tempo entre o sistema e o servidor NTP.

- Para o sistema com o módulo de gerenciamento de local remoto, você pode habilitá-lo para receber o registro do local remoto.
- Para o sistema sem módulo de gerenciamento de local remoto, você pode definir para registrá-lo no sistema central como um local remoto.

23.1 Definir nome do local

Você pode definir um nome para o sistema atual.

Etapas

1. Clique em **sistema** → **normal** → **nome do local** na página inicial.
2. Edite o nome do local para o sistema atual.
3. Clique em **Salvar**.

23.2 Definir limite de aviso para uso do servidor

Você pode ativar o sistema para acionar um alarme se o uso da CPU do servidor VSM e o uso de RAM atingirem um limite de aviso predefinido e durará um tempo predefinido. O valor de limiar relacionado pode ser verificado através do Control Client.

Etapas

1. Clique em **sistema** → **normal** → **limites de uso do servidor** na página inicial.
2. Arraste o \triangle para ajustar o valor de limiar de CPU e RAM.
3. Defina a duração no campo **notificar se o valor excede para (s)** para uso da CPU e uso de RAM.

Exemplo:

- Se você definir o limite de aviso como 60% e definir 20 no campo **notificar se o valor exceder para (s)** do uso da CPU, você poderá exibir as alterações de status da CPU para atenção no monitoramento de integridade no control client quando o uso da CPU atingir o limite de aviso e durar 20 segundos.
- Se você definir 60% como o limite de aviso e definir 20 no campo **notificar se o valor exceder para (s)** do uso da CPU e definir um alarme para aviso de CPU (consulte **Adicionar alarme para o servidor HikCentral**), o alarme será acionado quando o uso da CPU atingir o limite de aviso e durar 20 segundos.

23.3 Definir NTP

Você pode ajustar o servidor de NTP para sincronizar o tempo entre o VSM e o servidor de NTP.

Etapas

1. Clique em **sistema** → **rede** → **configurações de NTP**.
2. Defina o botão **Sincronização de tempo** como LIGADO para ativar a função NTP.
3. Defina o endereço do servidor NTP e a porta NTP.
4. Insira o intervalo para a sincronização automática de tempo.
5. Opcional: Clique em **teste** para testar a comunicação entre o VSM e o servidor NTP.
6. Clique em **Salvar**.

23.4 Definir o Active Directory

Se você tiver o controlador de domínio AD (Active Directory) que contém as informações (por exemplo, dados do usuário, informações do computador), você pode configurar as configurações para obter as informações relacionadas. Desta forma, você pode adicionar os usuários que pertencem a uma unidade organizacional (UO) (por exemplo, um departamento de sua empresa) para HikCentral convenientemente.

Execute essa tarefa quando precisar definir o diretório ativo.

Etapas

1. Clique em **sistema** → **rede** → **diretório ativo** na página inicial.
2. Configure os parâmetros de informações básicas para se conectar ao controlador de domínio do AD.

Nome de domínio

O nome de domínio do controlador de domínio do AD.

Observação

- A HikCentral suporta apenas o formato NetBIOS: por exemplo, TESTE\usuário e não o formato de nome de domínio DNS.
- Para obter o nome de domínio NetBIOS, abra a janela CMD e digite **nbtstat - n**.
O nome de domínio NetBIOS é aquele no tipo de **GRUPO**.

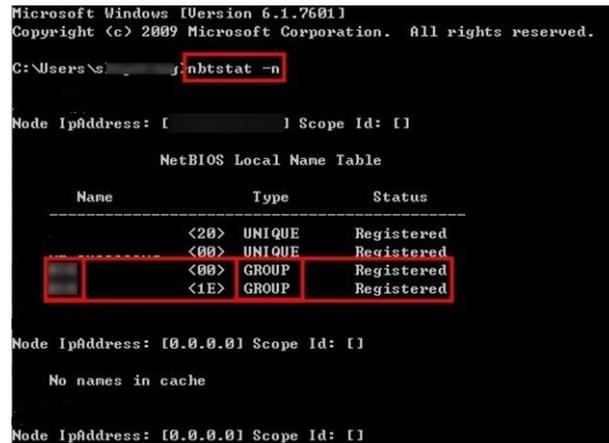


Figura 23-1 Como obter o nome de domínio NetBIOS

Nome do Host

O endereço IP do servidor DNS. Você pode obtê-lo em detalhes da conexão de rede.

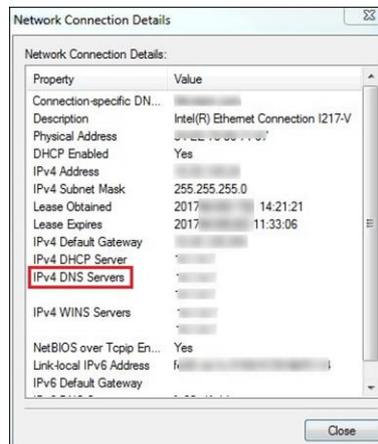


Figura 23-2 Como obter o nome do host

Nº da porta

A porta nº. do controlador de domínio AD. Por padrão, é 389.

Ativar SSL (opcional):

Habilite o SSL se exigido pelo controlador de domínio do AD.

Nome de usuário

O nome de usuário do controlador de domínio do AD. Isso precisa ser o administrador de domínio.

Senha

A senha do controlador de domínio do AD.

Base DN (nome distinto)

Insira a condição de filtro no texto arquivado se você estiver familiarizado com o formato. Ou

você pode clicar em **buscar DN** para obter a condição de filtro inserida automaticamente.

Observação

- Somente os usuários encontrados em uma unidade organizacional (UO) no domínio podem ser importados. Clique em **buscar DN** para que a condição de filtro seja inserida automaticamente.
 - Se você incorpora manualmente o DN da base, você precisa de definir o nó de raiz como desejado. Se você clicar em **buscar DN**, a estrutura inteira armazenada no controlador de domínio do AD será obtida.
-

3. Opcional: Vincule as informações da pessoa em questão armazenadas no domínio às informações da pessoa no sistema.

1) Ajuste o **interruptor da informação da pessoa** da ligação a lig.

Os itens de informações adicionais padrão e personalizados (consulte **Informações adicionais personalizadas**) são exibidas na área de informações da pessoa por padrão. Você pode definir a relação de vínculo para aqueles ou adicionar novos itens de informações de pessoa como você desejou.

2) Opcional: Clique em **adicionar novo** para adicionar um item de informações de pessoa em questão.

Observação

- Você não precisa adicionar os itens de informações de pessoa básica, incluindo ID, nome, sobrenome, telefone e observação) manualmente, que tem a relação de vínculo padrão com o domínio.
 - O item de informações de nova pessoa também é exibido na página informações adicionais personalizadas, onde você pode editar ou excluir os itens. Consulte **Informações adicionais personalizadas** para detalhes.
 - O item de informações de pessoa diferencia maiúsculas de minúsculas.
-

3) Opcional: Clique em + para mostrar os itens de informações pessoais armazenados no domínio.

4) Marque a caixa de seleção no domínio para vinculá-la aos itens de informações da pessoa adicionada ao importar as pessoas do domínio.

5) Opcional: Passe o mouse sobre as informações da pessoa vinculada no domínio e clique em x para remover o relacionamento. Você também pode alterar a relação de vínculo entre si clicando e arrastando o item para outro.

4. Clique em **Salvar**.

Após a configuração, a unidade organizacional e as informações do usuário de domínio serão exibidas quando você clicar em **Importar usuário do domínio** na página gerenciamento de usuários.

Se a função vincular informações de pessoa estiver habilitada, as informações da pessoa correspondente no sistema corresponderá às informações da pessoa vinculada no domínio e não poderão ser editadas.

23.5 Ativar evento genérico de recebimento

Depois de criar um evento genérico para analisar os pacotes de dados TCP e/ou UDP recebidos de uma ampla gama de sistemas externos, você pode habilitar a função de evento genérico de recebimento para que o sistema possa receber os eventos genéricos configurados.

Execute essa tarefa quando você precisar habilitar a função de evento genérico de recebimento.

Etapas

1. Clique em **sistema** → **rede** → **recebendo eventos genéricos**.
2. Verifique **receber evento genérico** para habilitar essa função.
3. Clique em **Salvar**.

Observação

Você pode configurar a porta do sistema não. para o evento genérico: Abra o Gerenciar serviço (instalado no PC executando o serviço VSM) e clique em **Serviço de gerenciamento de videovigilância HikCentral** para editar.

23.6 Permitir registro de local remoto

Para o sistema com o módulo de gerenciamento de local remoto, você pode ativá-lo para receber o registro do local remoto. Local remoto é o sistema que não tem módulo de gerenciamento de local remoto e pode se registrar para o sistema central para formar uma União de grande escala. O objetivo de ingressar no sistema central e nos locais remotos é permitir que os usuários do sistema central visualizem e gerenciem os recursos pertencentes a vários locais remotos simultaneamente como se estivessem no mesmo sistema.

Antes de começar

Se um local remoto precisar se registrar no sistema central, ele deverá abrir o Web Client do local remoto e entrar **registrando no sistema central** para configurar os parâmetros do sistema central. Veja **Registre-se no sistema central** para detalhes.

Etapas

Observação

Permitir o registro do local remoto só está disponível para o sistema com o módulo de gerenciamento de local remoto.

1. Clique em **sistema** → **rede** → **registro do local de recebimento**.
2. Verifique o **registro do local de recebimento** para habilitar essa função.
3. Clique em **Salvar**.

23.7 Registre-se no sistema central

Para o sistema sem módulo de gerenciamento de local remoto (como chamamos de local remoto), ele pode se registrar no sistema central depois de ativar essa função e definir os parâmetros do sistema central.

Antes de começar

Para o sistema central, ele deve habilitar a função de registro de site de recebimento para que ele possa receber o registro do site remoto. Veja **Permitir registro de site remoto** para detalhes.

Execute essa tarefa quando precisar registrar o site remoto no sistema central.

Etapas

Observação

O registro no sistema central só está disponível para o sistema sem o módulo gerenciamento de local remoto

1. Clique em **sistema → rede → registrando no sistema central**.
 2. Defina a opção **registrando no sistema central** como ON para habilitar essa função.
 3. Digite o endereço IP e a porta nº. do sistema central.
-

Observação

Abra o Service Manager (instalado no PC executando o serviço VSM do sistema central) e clique em **Serviço de gerenciamento de videovigilância HikCentral** se você precisar visualizar ou editar a porta do sistema central.

4. Clique em **Salvar**.

23.8 Definir acesso WAN

Em ambientes de rede complicados, você precisa definir um endereço IP estático e portas para HikCentral para ativá-lo para acessar o servidor VSM via WAN (Wide Area Network). Por exemplo, se o servidor VSM estiver em uma rede de área local e você precisar visitar o sistema por meio do cliente da Web ou do control client em execução na WAN, você deve habilitar o acesso WAN e definir um endereço IP estático e portas para HikCentral.

Etapas

1. Clique em **sistema → rede → acesso WAN**.
2. Defina o comutador de **acesso WAN** como ON para ativar a função de acesso WAN.
3. Insira um endereço IP estático para acesso WAN.
4. Defina a porta para HikCentral, incluindo HTTP, HTTPS, RTSP (porta de transmissão em tempo real), porta de transmissão de ficheiros de vídeo e porta WebSocket.

5. Opcional: Se você adota o evento genérico para integrar o HikCentral com fontes externas, você precisa definir a porta TCP e a porta UDP para receber os pacotes de dados TCP e/ou UDP.

 **Observação**

Para definir o evento genérico, consulte *Configurar o evento genérico*.

6. Opcional: Para o sistema com módulo de gerenciamento de site remoto, defina a porta para receber o registro de um site remoto.

 **Observação**

Este item de configuração só está disponível para o sistema central com um módulo de gerenciamento de site remoto baseado na licença que você adquiriu.

7. Clique em **Salvar**.

23.9 Definir tempo limite de rede

Duração de tempo limite de rede refere-se ao tempo de espera predefinido para as configurações no Web Client. A configuração será considerada como falha se nenhuma resposta dentro do tempo de espera configurado.

O tempo de espera padrão mínimo das interações entre as configurações e o servidor VSM é 60s, o tempo mínimo entre o servidor e os dispositivos VSM é 5s, e o tempo mínimo entre as configurações e os dispositivos é 5s.

 **Observação**

Esse parâmetro afeta todos os clientes Web que acessam o servidor VSM atual.

23.10 Definir modo de acesso a dispositivos

A página modo de acesso ao dispositivo permite que você defina como o sistema acessa todos os dispositivos de codificação e dispositivos de decodificação adicionados.

Execute esta tarefa para definir como o sistema acessa todos os dispositivos de codificação adicionados e dispositivos de decodificação.

Etapas

1. Clique em **sistema** → **rede** → **modo de acesso ao dispositivo**.
2. Defina o modo de acesso do dispositivo como julgar automaticamente ou modo de proxy.

Julgue automaticamente

O sistema julgará automaticamente a condição da conexão de rede e, em seguida, definirá o modo de acesso ao dispositivo de acordo com o acesso direto ou acesso por meio da

transmissão Gateway e do Serviço de Gerenciamento.

Proxy

O sistema acessará o dispositivo por meio da transmissão Gateway e do Serviço de Gerenciamento. É menos eficaz e menos eficiente do que acessar diretamente.

3. Clique em **Salvar** para confirmar as configurações.

O sistema acessa todos os dispositivos de codificação adicionados e dispositivos de decodificação através do modo selecionado.

23.11 Definir NIC do servidor

Você pode selecionar o NIC do servidor atual de VSM de modo que o sistema possa receber a informação do alarme do dispositivo conectado através do protocolo de ONVIF.

Etapas

1. Clique em **sistema → rede → servidor NIC**.

2. Selecione o nome de NIC usado atualmente do VSM na lista suspensa.

As informações de NIC incluindo descrição, endereço MAC e endereço IP serão exibidas.

3. Clique em **Salvar**.

23.12 Definir período de retenção de dados

O período de retenção de dados especifica por quanto tempo você pode manter os eventos, logs e alguns registros do servidor VSM, como marcas de gravação, dados de comparação de face.

Etapas

1. Clique em **sistema → armazenamento → dados gravados no sistema**.

2. Defina o período de dados gravados na lista suspensa para os tipos de dados necessários.

Data Recorded in System

*Received Events	One Year	▼
*Recording Tags	Two Years	▼
*Face Comparison Data	Two Years	▼
*Card Swiping Records	Two Years	▼
*Attendance Records	Two Years	▼
*Vehicle Passing Records	Two Years	▼
*Video Analysis Data	Two Years	▼
*Service Error Logs	Two Years	▼
*Service Warning Logs	Six Months	▼
*Service Information Logs	Two Years	▼

Save

Figura 23-3 definir período gravado de dados

Observação

Os registros de passando do cartão são salvos como o período configurado. O usuário com a permissão pode pesquisar os registros de passando das pessoas e exibir informações relacionadas durante esse período, mesmo se as pessoas pesquisadas tiverem sido excluídas do servidor VSM.

3. Clique em **Salvar**.

23.13 Definir feriado

Você pode adicionar o feriado para definir os dias especiais que podem adotar agenda de turno diferente ou cronograma de controle de acesso.

Realize esta tarefa para adicionar alguns dias especiais como feriado.

Etapas

1. Clique em **sistema** → **rede** → **configurações de NTP**.
2. Clique em **adicionar** para abrir a caixa de diálogo Adicionar feriado.

Observação

Você pode adicionar até 16 feriados.

3. Defina um nome personalizado.
4. Clique no campo hora e defina a data de início e a data de término para o período de feriados.
5. Clique em **adicionar** para salvar o feriado.
6. Opcional: Execute as seguintes operações depois de adicionar o feriado.

Editar férias.	Clique em  na coluna operação para editar o feriado (incluindo o(s) feriado(s) em uso).
Excluir feriado	Clique em  na coluna operação para excluir o feriado.
Excluir todos os feriados	Clique em excluir tudo para excluir todos os feriados (exceto o feriado (s) em uso).

23.14 Definir modelo de email

Você deve definir o modelo de email corretamente antes de enviar a mensagem de evento para a conta de email designada como vinculação de email.

23.14.1 Configurar conta de email

Você deve configurar os parâmetros da conta de email do remetente antes que o sistema possa enviar a mensagem para a (s) conta (s) de email designada como vinculação de email.

Execute essa tarefa quando precisar configurar a conta de email do remetente.

Etapas

1. Clique em **sistema** → **email** para entrar na página de email.
2. Clique em **configurações de email** para entrar na página Configurações de email.

← Email Settings

Email Settings

Server Authentication

Cryptographic Protocol None ▾

* Sender Email Address

* Sender Name

* SMTP Server Address

* SMTP Server Port 25

* User Name

* Password

Email Test

Save Cancel

Figura 23-4 Configuração de email

3. Configure os parâmetros de acordo com as necessidades reais.

Autenticação de servidor (opcional)

Se o servidor de email exigir autenticação, marque esta caixa de seleção para usar a autenticação para fazer logon neste servidor.

Protocolo criptográfico

Selecione o protocolo criptográfico do e-mail para proteger o conteúdo do e-mail se for exigido pelo servidor SMTP.

Endereço do servidor SMTP

O endereço de IP do servidor SMTP ou nome do host (p.ex., smtp.263xmail.com)

Porta do servidor SMTP

A porta TCP/IP padrão usada para SMTP é 25.

4. Clique em **teste de email** para testar se as configurações de email funcionam ou não. A caixa de mensagens de atenção correspondente aparecerá.

5. Clique em **Salvar**.

23.14.2 Adicionar modelo de email

Você pode definir modelos de email, incluindo a especificação do destinatário, assunto do email e conteúdo, para que o sistema possa enviar as informações para o destinatário designado de acordo com o modelo de email predefinido.

Antes de começar

Antes de adicionar o modelo de email, você deve definir a conta de email do remetente primeiro. Veja **Configurar conta de email** para detalhes.

Execute essa tarefa quando precisar adicionar um novo modelo de email.

Etapas

1. Digite o **sistema → email** para entrar na página de email.
2. Clique em **adicionar** para entrar na página Adicionar modelo de email.
3. Insira os parâmetros necessários.

Nome

Criar um nome para o modelo.

Destinatários

Clique em **adicionar usuário** e selecione o email da pessoa como o destinatário, que é configurado ao adicionar a pessoa.

Clique em adicionar email e digite o endereço de email do destinatário (s) para enviar o email.

Observação

Você pode inserir vários destinatários e separá-los por ";".

Indivíduo

Digite o assunto do email como desejado. Você também pode clicar no botão na parte inferior da janela para adicionar as informações relacionadas com o assunto.

Índice

Defina as informações do evento a serem enviadas. Você também pode clicar no botão na parte inferior da janela para adicionar as informações relacionadas com o conteúdo.

Observação

Se você selecionar para adicionar o tempo do evento ao assunto ou ao conteúdo do email, e o aplicativo de email (como o Outlook) e o sistema estiverem em fusos horários diferentes, o tempo de evento exibido poderá ter alguns desvios.

4. Opcional: Marque **anexar imagem** para enviar email com anexo de imagem.
5. Termine de adicionar o modelo de email.

- Clique em **adicionar** para adicionar o modelo e voltar para a página de lista de modelos de email.
- Clique em **adicionar e continuar** para adicionar o modelo e continuar a adicionar outros modelos.

O modelo de email será exibido na lista de modelos de email.

6. Execute as seguintes operações depois de adicionar o modelo de email:

- Edição do modelo** Clique em  na coluna operação para editar os detalhes do modelo.
- Excluir o modelo** Clique em  na coluna de operação para excluir o modelo.
- Exclusão de todos os modelos** Clique em **excluir tudo** para excluir todos os modelos adicionados.

23.15 Enviar relatório regularmente

Os relatórios são documentos essenciais, a fim de submeter o desempenho aos usuários para fazer negócios funcionar sem problemas e eficazmente. Os usuários podem usar relatórios como base na criação de decisões, abordando problemas, verificando a tendência e comparação, etc. HikCentral fornece funções de relatório que o sistema pode enviar relatórios automaticamente e regularmente para direcionar os usuários por email's, mostrando os eventos ocorridos e alarmes, número de veículos que passam, contagem de pessoas, gerenciamento de filas e status de temperatura durante período de tempo especificado.

23.15.1 Enviar relatório de eventos regularmente

Você pode definir uma regra de relatório regular para eventos monitorados pelo sistema especificados e o sistema pode enviar um email com um relatório anexado aos destinatários de destino diariamente ou semanalmente, mostrando os detalhes de eventos monitorados pelo sistema especificados acionados no dia ou na semana.

Antes de começar

- Defina o modelo de email com informações do destinatário, assunto e conteúdo. Para obter mais detalhes, consulte **Definir modelo de e-mail**.
- Defina as configurações de email, como endereço do remetente, endereço do servidor SMTP e porta, etc. Para obter detalhes, consulte **Configurar conta de email**.

Etapas

Observação

Um relatório pode conter até 10.000 registros de eventos no total.

1. Clique em **sistema** na página inicial e insira a página **relatório**.
2. Selecione a categoria de relatório como **evento**.

3. Crie um nome para o relatório.
4. Defina os evento (s) monitorados pelo sistema contidos no relatório.
 - 1) no campo de destino do relatório, clique em **adicionar**.
Todos os eventos adicionais monitorados pelo sistema são exibidos.
 - 2) (opcional) filtrar os eventos por tipo de origem do evento e acionando evento.
Selecione o (s) evento (s).

Observação

Até 32 eventos podem ser adicionados em uma regra de relatório.

- 4) Clique em **Adicionar**.
5. Defina o tipo de relatório como **diário** ou **semanal** e defina o tempo de envio.

Relatório diário

Relatório diário mostra dados em base diária. O sistema enviará um relatório na hora de envio todos os dias, que contém informações dos eventos acionados no dia (24 horas) antes do dia atual.

Por exemplo, se você definir o tempo de envio como 20:00, o sistema enviará um relatório em 20:00. todos os dias, contendo detalhes de todos os eventos desencadeados entre 00:00. e 24:00. antes do dia atual.

Relatório semanal

Em comparação com o relatório diário, o relatório semanal pode ser menos demorado, uma vez que não deve ser submetido todos os dias. O sistema enviará um relatório na hora de envio a cada semana, que contém informações dos eventos acionados nos últimos 7 dias antes da data de envio.

Por exemplo, se você definir o tempo de envio como 6:00 na segunda-feira, o sistema enviará um relatório em 6:00 pela manhã em todas as segundas-feiras, contendo detalhes de todos os eventos desencadeados entre a última segunda-feira e domingo.

6. Selecione o modelo de email na lista suspensa para definir as informações do destinatário e o formato de email.

Observação

Você pode clicar em **adicionar novo** para adicionar um novo modelo de email Para definir o modelo de email, consulte **Definir modelo de email**.

7. Selecione Excel ou PDF como o formato do relatório.
8. Termine de adicionar o relatório.
 - Clique em **adicionar** para adicionar o relatório e voltar para a página de lista de relatórios.
 - Clique em **adicionar e continuar** para adicionar o relatório e continuar a adicionar outros relatórios.

23.15.2 Enviar relatório de alarme regularmente

Você pode definir uma regra de relatório regular para alarmes especificados, e o sistema pode enviar um email com um relatório anexado aos destinatários de destino diariamente ou semanalmente, mostrando os detalhes dos alarmes especificados acionados no dia ou na semana.

Antes de começar

- Defina o modelo de email com informações do destinatário, assunto e conteúdo. Para obter mais detalhes, consulte *Definir modelo de e-mail*.
- Defina as configurações de email, como endereço do remetente, endereço do servidor SMTP e porta, etc. Para obter detalhes, consulte *Configurar conta de email*.

Etapas

Observação

Um relatório pode conter até 10.000 registros de alarmes no total.

1. Clique em **sistema** na página inicial e insira a página **relatório**.
2. Selecione a categoria de relatório como **alarme**.
3. Crie um nome para o relatório.
4. Defina o alarme (s) contido no relatório.
 - 1) no campo de destino do relatório, clique em **adicionar**.
Todos os alarmes adicionados são exibidos.
 - 2) (opcional) filtre os alarmes por tipo de fonte de alarme, evento desencadeante e prioridade de alarme.
 - 3) Selecione o (s) alarme (s).

Observação

Até 32 alarmes podem ser adicionados em uma regra de relatório.

- 4) Clique em **Adicionar**.
5. Defina o tipo de relatório como **diário** ou **semanal** e defina o tempo de envio.

Relatório Diário

Relatório diário mostra dados em base diária. O sistema enviará um relatório na hora de envio todos os dias, que contém informações dos alarmes acionados no dia (24 horas) antes do dia atual.

Por exemplo, se você definir o tempo de envio como 20:00, o sistema enviará um relatório em 20:00 todos os dias, contendo detalhes de todos os alarmes acionados entre 00:00 e 24:00 antes do dia atual.

Relatório semanal

Em comparação com o relatório diário, o relatório semanal pode ser menos demorado, uma vez que não deve ser submetido todos os dias. O sistema enviará um relatório na hora de envio todas as semanas, que contém informações dos alarmes acionados nos últimos 7 dias

antes da data de envio.

Por exemplo, se você definir o tempo de envio como 6:00 na segunda-feira, o sistema enviará um relatório em 6:00 pela manhã em todas as segundas-feiras, contendo detalhes de todos os eventos desencadeados entre a última segunda-feira e domingo.

6. Selecione o modelo de email na lista suspensa para definir as informações do destinatário e o formato de email.

Observação

Você pode clicar em **adicionar novo** para adicionar um novo modelo de email. Para definir o modelo de email, consulte *Definir modelo de email*.

7. Selecione Excel ou PDF como o formato do relatório.
8. Termine de adicionar o relatório.
 - Clique em **adicionar** para adicionar o relatório e voltar para a página de lista de relatórios.
 - Clique em **adicionar e continuar** para adicionar o relatório e continuar a adicionar outros relatórios.

23.15.3 Enviar relatório de passagem de veículo regularmente

Você pode definir uma regra de relatório regular para câmeras ANPR especificadas, e o sistema pode enviar um email com um relatório anexado aos destinatários de destino diariamente, semanalmente ou mensalmente, mostrando o número de veículos que passam detectados por essas câmeras ANPR durante o tempo especificado. Períodos.

Antes de começar

- Defina o modelo de email com informações do destinatário, assunto e conteúdo. Para obter mais detalhes, consulte *Definir modelo de e-mail*.
- Defina as configurações de email, como endereço do remetente, endereço do servidor SMTP e porta, etc. Para obter detalhes, consulte *Configurar conta de email*.

Etapas

Observação

- Um relatório pode conter até 10.000 registros no total.
 - O relatório será um arquivo do Excel.
-

1. Clique em **sistema** na página inicial e insira a página **relatório**.
2. Selecione a categoria de relatório como **veículo**.
3. Crie um nome para o relatório.
4. Defina a (s) câmera (s) ANPR contidas no relatório.
 - 1) no campo de destino do relatório, clique em **adicionar**.
Todas as câmeras ANPR adicionadas ao site atual são exibidas.
 - 2) Selecione a câmera (s) ANPR.
 - 3) Clique em **Adicionar**.

5. Defina o tipo de relatório como **diário**, **semanal** ou **mensal** e defina o tempo de envio.

Relatório Diário

Relatório diário mostra dados em base diária. O sistema enviará um relatório na hora de envio todos os dias, que contém informações dos alarmes acionados no dia (24 horas) antes do dia atual.

Por exemplo, se você definir o tempo de envio como 20:00, o sistema enviará um relatório em 20:00 todos os dias, contendo o número de veículos que passam detectados entre 00:00 e 24:00 antes do dia atual.

Relatório semanal e relatório mensal

Em comparação com o relatório diário, o relatório semanal e o relatório mensal podem ser menos demorados, uma vez que não devem ser submetidos todos os dias. O sistema enviará um relatório na hora de envio a cada semana ou a cada mês, que contém o número de veículos que passam detectados nos últimos 7 dias ou no mês passado antes da data de envio.

Por exemplo, para o relatório semanal, se você definir o tempo de envio como 6:00 na segunda-feira, o sistema enviará um relatório em 6:00 da manhã em cada segunda-feira, contendo o número de veículos que passam detectado entre a última segunda-feira e domingo.

6. Depois de definir o tempo do relatório, defina como o relatório apresentará os dados detectados no período de tempo especificado.

Exemplo:

Por exemplo, se você selecionar o tipo de relatório como **Diário**, poderá selecionar **Calcular por hora** ou **Calcular por minuto**. Haverá 24 ou 24×60 registros para cada câmera, respectivamente, no relatório, mostrando o número de veículos que passam detectados em cada hora ou cada minuto para uma câmera.

7. Selecione o modelo de email na lista suspensa para definir as informações do destinatário e o formato de email.

Observação

Você pode clicar em **adicionar novo** para adicionar um novo modelo de email. Para definir o modelo de email, consulte *Definir modelo de email*.

8. Termine de adicionar o relatório.
- Clique em **adicionar** para adicionar o relatório e voltar para a página de lista de relatórios.
 - Clique em **adicionar e continuar** para adicionar o relatório e continuar a adicionar outros relatórios.

23.15.4 Enviar relatório de contagem de pessoas regularmente

Você pode definir uma regra de relatório regular para pessoas especificadas que contam câmeras, e o sistema pode enviar um email com um relatório anexado aos destinatários de destino diariamente, semanalmente ou mensalmente, mostrando o número de pessoas inseridas ou

Exited, detectadas por essas pessoas contando câmaras durante os períodos de tempo especificados.

Antes de começar

- Defina o modelo de email com informações do destinatário, assunto e conteúdo. Para obter mais detalhes, consulte **Definir modelo de e-mail**.
- Defina as configurações de email, como endereço do remetente, endereço do servidor SMTP e porta, etc. Para obter detalhes, consulte **Configurar conta de email**.

Etapas

Observação

- Um relatório pode conter até 10.000 registros no total.
 - O relatório será um arquivo do Excel.
-

1. Clique em **sistema** na página inicial e insira a página **relatório**.
2. Selecione a categoria de relatório como **contagem de pessoas**.
3. Crie um nome para o relatório.
4. Defina as pessoas que contam a câmera (s) contida no relatório.
 - 1) no campo de destino do relatório, clique em **adicionar**.
Todas as pessoas que contam a câmera (s) adicionadas ao site atual são exibidas.
 - 2) Selecione as pessoas que contam a câmera (s).
 - 3) Clique em **Adicionar**.
5. Defina o tipo de relatório como **diário, semanal** ou **mensal** e defina o tempo de envio.

Relatório Diário

Relatório diário mostra dados em base diária. O sistema enviará um relatório na hora de envio todos os dias, que contém informações dos alarmes acionados no dia (24 horas) antes do dia atual.

Por exemplo, se você definir o tempo de envio como 20:00, o sistema enviará um relatório em 20:00 todos os dias, contendo o número de pessoas inseridas e saiu detectadas entre 00:00 e 24:00 antes do dia atual.

Relatório semanal e relatório mensal

Em comparação com o relatório diário, o relatório semanal e o relatório mensal podem ser menos demorados, uma vez que não devem ser submetidos todos os dias. O sistema enviará um relatório na hora de envio a cada semana ou a cada mês, que contém o número de pessoas inseridas e saiu detectado nos últimos 7 dias ou no mês anterior à data de envio.

Por exemplo, para o relatório semanal, se você definir o tempo de envio como 6:00 na segunda-feira, o sistema enviará um relatório em 6:00 da manhã em todas as segundas-feiras, contendo o número de pessoas inseridas e saiu detectado entre a última segunda-feira e domingo.

6. Depois de definir o tipo de relatório, defina como o relatório apresentará os dados detectados no período de tempo especificado.

Exemplo:

Por exemplo, se você selecionar o tipo de relatório como **Diário**, poderá selecionar **Calcular por hora** ou **Calcular por minuto**. Haverá 24 ou 24 × 60 registros para cada câmera, respectivamente, no relatório, mostrando o número existente de pessoas detectadas em cada hora ou cada minuto para uma câmera.

7. Defina o tempo de envio de acordo com o tipo de relatório.
8. Selecione o modelo de email na lista suspensa para definir as informações do destinatário e o formato de email.

 **Observação**

Você pode clicar em **adicionar novo** para adicionar um novo modelo de email. Para definir o modelo de email, consulte *Definir modelo de email*.

9. Termine de adicionar o relatório.
 - Clique em **adicionar** para adicionar o relatório e voltar para a página de lista de relatórios.
 - Clique em **adicionar e continuar** para adicionar o relatório e continuar a adicionar outros relatórios.

23.15.5 Enviar relatório de análise de filas regularmente

Você pode definir uma regra de relatório regular para câmeras especificadas que suportam o gerenciamento de filas, e o sistema pode enviar um email com um relatório anexado aos destinatários de destino diariamente, semanalmente ou mensalmente, mostrando exceções de fila, número de pessoas na fila e fila Estado, detectado por essas pessoas contando câmeras durante os períodos de tempo especificados.

Antes de começar

- Defina o modelo de email com informações do destinatário, assunto e conteúdo. Para obter mais detalhes, consulte *Definir modelo de e-mail*.
- Defina as configurações de email, como endereço do remetente, endereço do servidor SMTP e porta, etc. Para obter detalhes, consulte *Configurar conta de email*.

Etapas

 **Observação**

- Um relatório pode conter até 10.000 registros no total.
 - O relatório será um arquivo do Excel.
-

1. Clique em **sistema** na página inicial e insira a página **relatório**.
2. Selecione a categoria de relatório como **fila**.
3. Crie um nome para o relatório.
4. Defina as câmeras que suportam a gestão de filas contida no relatório.
 - 1) no campo de destino do relatório, clique em **adicionar**.

Todas as câmeras que suportam o gerenciamento de filas adicionadas ao site atual são

exibidas.

2) Selecione a câmera.

3) Clique em **Adicionar**.

O relatório mostrará os dados de todas as filas configuradas nas câmeras.

Observação

Para configurar a fila, consulte o manual do usuário da câmera.

5. Defina o tipo de relatório como **diário, semanal** ou **mensal**.

Relatório diário

Relatório diário mostra dados em base diária. O sistema enviará um relatório na hora de envio todos os dias, que contém informações dos alarmes acionados no dia (24 horas) antes do dia atual.

Por exemplo, se você definir o tempo de envio como 20:00, o sistema enviará um relatório em 20:00 todos os dias, contendo dados de fila detectados entre 00:00 e 24:00 antes do dia atual.

Relatório semanal e relatório mensal

Em comparação com o relatório diário, o relatório semanal e o relatório mensal podem ser menos demorados, uma vez que não devem ser submetidos todos os dias. O sistema enviará um relatório na hora de envio a cada semana ou a cada mês, que contém os dados da fila detectados nos últimos 7 dias ou no mês anterior à data de envio.

Por exemplo, para relatório semanal, se você definir o tempo de envio como 6:00 na segunda-feira, o sistema enviará um relatório em 6:00 da manhã em todas as segundas-feiras, contendo dados de fila detectados entre a última segunda-feira e domingo.

6. Defina o conteúdo no relatório.

Exceção de Fila

É o número de exceções (quantidade de pessoas excedendo e tempo limite de espera) de cada fila.

Quantidade de Pessoas Excedendo

É quando o número de pessoas na fila excede o limite pré-estabelecido.

Timeout de Espera

É quando a duração de espera das pessoas na fila excede o limite pré-estabelecido.

Quantidade de Pessoas em Fila

O número de pessoas em cada fila.

Status da Fila

O status de cada fila, incluindo a duração de espera das pessoas e o número de pessoas na fila.

Se você selecionar **status da fila**, deverá selecionar o **tipo de análise** como duração de espera ou comprimento da fila e definir o intervalo.

Duração da Espera

O relatório mostrará o número de pessoas em cada fila que esperou a duração especificada.

Por exemplo, se você definir o intervalo de relatório como **intervalo 1 < 300 ≤ intervalo 2 ≤ 600 < intervalo 3**, o relatório mostrará que, em cada fila, quantas pessoas esperaram menos de 300s, quantas pessoas esperaram por 300 a 600s, e quantas pessoas esperaram por mais de 300s.

Comprimento da Fila

O relatório mostrará quantos segundos cada status da fila (número de pessoas em intervalos diferentes) dura.

Por exemplo, se você definir o intervalo de relatório como **intervalo 1 < 5 ≤ intervalo 2 ≤ 10 < intervalo 3**, o relatório mostrará que, em cada fila, quantos segundos o status dura quando há menos de 5 pessoas, quantos segundos o status dura quando há 5 a 10 pessoas, e quantos segundos o status dura quando há mais de 10 pessoas.

7. Defina o tempo de envio de acordo com o tipo de relatório.
8. Selecione o modelo de email na lista suspensa para definir as informações do destinatário e o formato de email.

Observação

Você pode clicar em **adicionar novo** para adicionar um novo modelo de email Para definir o modelo de email, consulte *Definir modelo de email*.

9. Termine de adicionar o relatório.
 - Clique em **adicionar** para adicionar o relatório e voltar para a página de lista de relatórios.
 - Clique em **adicionar e continuar** para adicionar o relatório e continuar a adicionar outros relatórios.

23.15.6 Enviar relatório de temperatura regularmente

Você pode definir uma regra de relatório regular para câmeras térmicas especificadas, e o sistema pode enviar um email com um relatório anexado aos destinatários de destino diariamente, semanalmente ou mensalmente, mostrando exceções de temperatura ou mín./Max. temperatura, detectada por estas câmaras térmicas durante os períodos de tempo especificados.

Antes de começar

- Defina o modelo de email com informações do destinatário, assunto e conteúdo. Para obter mais detalhes, consulte *Definir modelo de e-mail*.
- Defina as configurações de email, como endereço do remetente, endereço do servidor SMTP e porta, etc. Para obter detalhes, consulte *Configurar conta de email*.

Etapas

Observação

- Um relatório pode conter até 10.000 registros no total.
 - O relatório será um arquivo do Excel.
-

1. Clique em **sistema** na página inicial e insira a página **relatório**.
2. Selecione a categoria de relatório como **temperatura**.
3. Crie um nome para o relatório.
4. Defina as câmaras térmicas e as predefinições contidas no relatório.
 - 1) no campo de destino do relatório, clique em **adicionar**.
Todas as câmeras térmicas adicionadas ao site atual são exibidas.
 - 2) selecione as câmaras térmicas e a predefinição.
 - 3) Clique em **Adicionar**.O relatório mostrará as exceções da temperatura (que incluem a temperatura demasiado elevada ou demasiado baixa) ou a temperatura máxima e mínima de pontos diferentes da termometria nestes presets.
5. Defina o tipo de relatório como **diário**, **semanal** ou **mensal** e defina o tempo de envio.

Relatório diário

Relatório diário mostra dados em base diária. O sistema enviará um relatório na hora de envio todos os dias, que contém informações dos alarmes acionados no dia (24 horas) antes do dia atual.

Por exemplo, se você definir o tempo de envio como 20:00, o sistema enviará um relatório em 20:00 todos os dias, contendo as exceções de temperatura ou min./Max. temperatura detectada entre 00:00 e 24:00 antes do dia atual.

Relatório semanal e relatório mensal

Em comparação com o relatório diário, o relatório semanal e o relatório mensal podem ser menos demorados, uma vez que não devem ser submetidos todos os dias. O sistema enviará um relatório na hora de envio a cada semana ou a cada mês, que contém as exceções de temperatura ou min./Max. temperatura detectada nos últimos 7 dias ou no mês anterior à data de envio.

Por exemplo, para o relatório semanal, se você definir o tempo de envio como 6:00 na segunda-feira, o sistema enviará um relatório em 6:00 da manhã em cada segunda-feira, contendo exceções de temperatura ou min./Max. temperatura detectada entre a última segunda-feira e domingo.

6. Depois de definir o tempo do relatório, defina como o relatório apresentará os dados detectados no período de tempo especificado.

Exemplo

Por exemplo, se você selecionar o tipo de relatório como **Diário**, poderá selecionar **Calcular por hora** ou **Calcular por minuto**. Haverá 24 ou 24 × 60 registros para cada ponto de termometria, respectivamente, no relatório, mostrando as exceções de temperatura ou min./Max. temperatura detectada a cada hora ou a cada minuto.

7. Defina o conteúdo no relatório.

Exceção de Temperatura

O número de exceções na temperatura (temperatura muito alta ou muito baixa) de cada ponto de termometria.

Status de Temperatura

A temperatura máxima e temperatura mínima de cada ponto de termometria.

8. Selecione o modelo de email na lista suspensa para definir as informações do destinatário e o formato de email.

Observação

Você pode clicar em **adicionar novo** para adicionar um novo modelo de email. Para definir o modelo de email, consulte *Definir modelo de email*.

9. Termine de adicionar o relatório.

- Clique em **adicionar** para adicionar o relatório e voltar para a página de lista de relatórios.
- Clique em **adicionar e continuar** para adicionar o relatório e continuar a adicionar outros relatórios.

23.16 Definir protocolo de transferência

Você pode ajustar o protocolo de transferência do servidor VSM para definir o modo de acesso para o VSM (através do Web Client, do cliente do controle, ou do cliente móvel) como o HTTP ou o HTTPS. O protocolo HTTPS fornece maior segurança de dados.

Execute esta tarefa quando você precisa de ajustar o protocolo de transferência do servidor VSM.

Etapas

Observação

O protocolo de transferência de configuração está disponível somente ao acessar o Web Client no servidor VSM localmente.

1. Clique em sistema → avançado → protocolo de transferência.
 2. Selecione **HTTP** ou **HTTPS** como o protocolo de transferência.
 3. Se você selecionar **HTTPS**, será necessário definir o certificado. Você pode usar o certificado fornecido pelo sistema ou selecionar **Novo certificado** e clicar em para selecionar um novo arquivo de certificado.
-

Observação

- O novo certificado deve estar no formato PEM.
 - A chave pública e a chave privada devem estar no mesmo arquivo de certificado.
-

4. Clique em **Salvar**.

- O servidor VSM será reiniciado automaticamente depois de alterar o protocolo de transferência ou o certificado.
- Os usuários dos control clients e dos mobile clients que conectam a este servidor VSM serão forçado logout, e não são permitidos ao início de uma sessão até que reinicializar terminado.

Resultado

Você pode acessar o VSM via cliente Web, control client ou cliente móvel pelo protocolo de transferência selecionado.

23.17 Definir ID da câmera

Ao exibir a visualização ao vivo na parede inteligente, você pode usar um teclado para operações de conveniência, como iniciar a visualização ao vivo na parede inteligente, controle PTZ, etc. Se você quiser exibir a exibição ao vivo de determinada câmera na parede inteligente, você deve pressionar o número do identificador da câmera no teclado, que é chamado de **ID da câmera**. Como resultado, HikCentral fornece este módulo para você definir um ID exclusivo para cada câmera.

Clique em **sistema** → **avançado** → **ID da câmera** para entrar na página de configurações da ID da câmera.

Você pode filtrar as câmeras definindo o site e a área, ou inserindo palavras-chave do nome da câmera ou da ID da câmera.

O sistema fornece uma ID padrão para cada câmera. Você pode editar o valor padrão para as câmeras, se necessário.



Observação

O ID da câmera deve ser exclusivo no sistema.

23.18 Configuração do modo de funcionamento

No controle de acesso, se você adotar a série de reconhecimento de face DS-K5600 (como o DS-K5603-Z) na aplicação real, você precisa definir o modo de trabalho para esses dispositivos depois de adicioná-los ao sistema de acordo com as necessidades reais.

Se o dispositivo da série DS-K5600 for aplicado com a nossa catraca, selecione modo de **terminal de reconhecimento facial** para formar uma catraca com função de reconhecimento facial. As pessoas podem acessar a catraca escaneando suas faces com o dispositivo da série DS-K5600 depois de definir as credenciais do rosto e os níveis de acesso.

Se o dispositivo da série DS-K5600 for aplicado com outros catraca de terceiros, selecione modo **terminal de controle de acesso** e você poderá definir os níveis de acesso no sistema para definir as permissões de acesso.

23.19 Certificado de componente de serviço de exportação

Para segurança de dados, antes de adicionar o servidor de streaming ou o servidor de armazenamento em nuvem ao sistema, você deve exportar o certificado de componente de serviço armazenado no servidor VSM e importá-lo para o servidor de streaming ou o servidor de armazenamento em nuvem que deseja adicionar para que o certificados do servidor de streaming ou servidor de armazenamento em nuvem e servidor VSM são os mesmos.

Etapas

Observação

A exportação do certificado de componente de serviço do servidor VSM só está disponível quando você acessa o web client no servidor VSM localmente.

1. Clique em **sistema** → **avançado** → **certificado de componente de serviço**.
2. Clique em **exportar** para exportar o certificado de componente de serviço e salvá-lo no PC local.

O que fazer a seguir

Importe o arquivo de certificado exportado para o servidor de armazenamento em nuvem e o servidor de streaming que você deseja adicionar. Para as operações a seguir, consulte **Adicionar servidor de armazenamento em nuvem** e **Adicionar servidor de streaming** para detalhes.

23.20 Configurar o sistema de reposição qte

Se você constrói o sistema de reposição quente ao instalar o serviço VSM, você pode permitir a função de reposição quente e configurar a propriedade de reposição quente do servidor atual VSM como o servidor do host ou o servidor de reposição. Quando o servidor host falha, o servidor de reposição alterna para a operação, garantindo assim a estabilidade do sistema.

Antes de começar

Você deve construir o sistema de reposição quente ao instalar o serviço VSM. Ver **Módulo de instalação** para detalhes.

Execute esta tarefa quando você precisa de ajustar o sistema sobressalente quente.

Etapas

1. Clique em **sistema** → **avançado** → **reposição de destaque**.
2. Defina o interruptor de **configuração de reposição de destaque** para ON para ativar a função hot spare.
O nome do servidor do servidor VSM atual e o endereço IP disponível serão exibidos.
3. Defina o servidor como servidor host ou servidor de reposição da propriedade de destaque.
4. Clique em **Salvar**.

23.21 Redefinir informações de rede do dispositivo

Quando o domínio de rede do sistema é alterado (como a migração do servidor), você deve redefinir as informações de rede do dispositivo adicionado para se adaptar ao novo ambiente de rede. Caso contrário, a visualização ao vivo do dispositivo, a reprodução e outras funções serão afetadas.

Execute esta tarefa quando você precisar redefinir as informações de rede do dispositivo adicionado.

Etapas

1. Clique em **sistema** → **avançado** → **redefinir informações de rede**.
2. Clique em **redefinir** para redefinir um toque as informações de rede do dispositivo.

Capítulo 24 Aplicações

O HikCentral também fornece funcionalidades de visualização ao vivo, reprodução e configuração local através do navegador da Web.

Observação

- Se o protocolo de transferência do VSM for HTTPS, o módulo aplicativos (incluindo visualização ao vivo, reprodução e configuração local) estará disponível somente ao acessar o Web Client via Internet Explorer.
 - Se o protocolo de transferência do VSM for HTTP, os módulos de visualização e reprodução ao vivo estão disponíveis para o Internet Explorer, Google Chrome e Firefox. Mas o módulo de configuração local está disponível apenas para o Internet Explorer.
-

24.1 Exibição ao vivo

No módulo exibição ao vivo do Web Client, você pode visualizar o vídeo ao vivo das câmeras adicionadas e fazer algumas operações básicas, incluindo captura de imagens, gravação, controle PTZ e assim por diante.

24.1.1 Iniciar exibição ao vivo

Depois de adicionar as câmeras em áreas, você pode começar a visualização ao vivo para ver o vídeo ao vivo da câmera, e realizar algumas operações básicas através do Web Client.

Antes de começar

É necessário definir uma área com câmeras atribuídas para exibição ao vivo.

Realize esta tarefa quando precisar exibir o vídeo ao vivo da câmera via Web Client.

Etapas

1. Clique em **Exibição ao vivo** na página inicial para entrar na página da exibição ao vivo.
2. Selecione um local na lista suspensa.
A área e as câmeras do site selecionado são exibidas.
3. Opcional: Digite uma palavra-chave do nome da câmera ou nome da área no campo de pesquisa e clique em **pesquisar em todos os locais** ou **pesquisar no site atual** para pesquisar as câmeras ou áreas.
Todos os resultados da pesquisa são exibidos.

 **Observação**

Você pode mover o cursor para o nome da câmera para visualizar a miniatura da imagem.

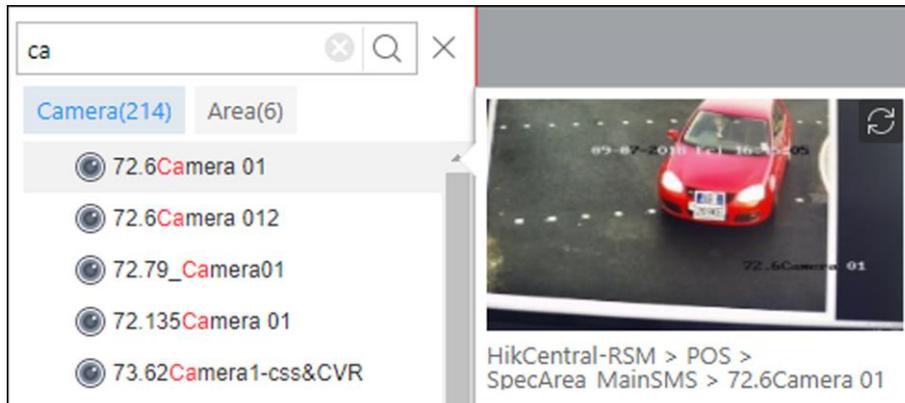


Figura 24-1 Miniatura

-
4. Opcional: Clique em  na barra de ferramentas visualização ao vivo e selecione um modo de divisão de janela.

 **Observação**

Até 16-modo de janela está disponível quando você acessa o Web Client através do Google Chrome, Firefox ou Internet Explorer.

-
5. Arraste a câmera para a janela de exibição ou clique duas vezes no nome da câmera depois de selecionar a janela de exibição para iniciar a visualização ao vivo.. A janela selecionada é descrita em vermelho.

 **Observação**

- Se o sistema é o sistema central com módulo de gerenciamento de local remoto, você também pode ver o vídeo ao vivo das câmeras importadas do local remoto. Para gerenciar as câmeras do site remoto em áreas, consulte **Adicionar câmera à área do local remoto**.
- Você também pode clicar duas vezes no nome da área para iniciar a visualização ao vivo das câmeras na área. As janelas de exibição se adaptam ao número de câmeras na área.

-
6. Opcional: Mova o mouse sobre a janela de exibição durante a exibição ao vivo e você pode executar algumas operações, como zoom digital, reprodução instantânea, áudio bidirecional e assim por diante.

24.1.2 Controle PTZ

Câmeras com a funcionalidade de rotação horizontal, rotação vertical e zoom podem ser controlada por meio do navegador da internet. Você também pode configurar predefinição, patrulha e padrão para as câmeras.

Configurar predefinição

Uma predefinição é uma posição de imagem predefinida que contém informações de panorâmica, inclinação, zoom, foco e outros parâmetros. Você também pode definir uma predefinição virtual depois de ativar o zoom digital.

Realize essa tarefa quando precisar adicionar uma predefinição para a câmera.

Etapas

1. Clique em **exibição ao vivo** na página inicial para entrar na página de visualização ao vivo.
2. Iniciar exibição ao vivo da câmera.

Observação

Veja **Iniciar exibição ao vivo** para obter detalhes sobre como iniciar a exibição ao vivo.

3. Clique em  na barra de ferramentas de visualização ao vivo para abrir o painel de controle PTZ.
4. Clique em  para entrar no painel de configuração da predefinição PTZ.

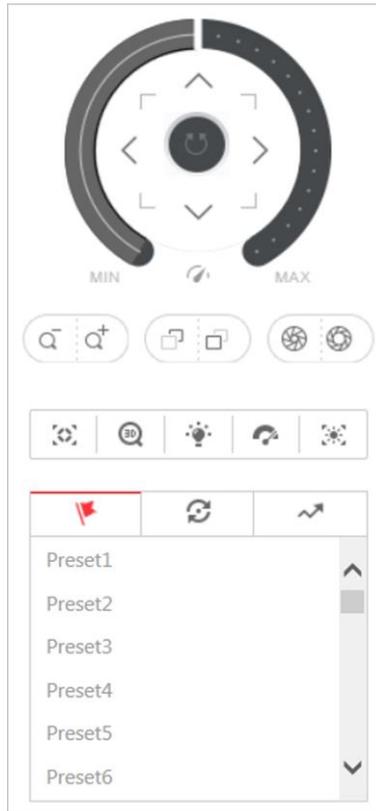


Figura 24-2 Configurar predefinição

5. Clique nos botões de direção para mover a câmera para a vista desejada ou ampliar/reduzir o modo de exibição.

Observação

Você também pode rolar a roda do mouse para ampliar ou reduzir o modo de exibição.

6. Selecione um número de preset PTZ na lista de presets e clique em .
7. Crie um nome para a predefinição.
8. Clique em **OK** para salvar as configurações.

Observação

Até 256 predefinições podem ser adicionadas.

9. Opcional: Depois de definir a predefinição, você pode fazer um ou mais dos seguintes itens:

Predefinição de chamada	Clique duas vezes na predefinição configurada na lista ou selecione a predefinição e clique em  para chamar a predefinição.
Editar Predefinições	Selecione a predefinição configurada na lista e clique em  para editar.
Excluir Predefinição	Selecione a predefinição configurada na lista e clique em  para

excluir.

Configurar patrulha

Um rastreamento é uma trilha de varredura especificada por um grupo de predefinições definida por usuários (incluindo predefinições virtuais) com uma velocidade de varredura entre duas predefinições e tempo de espera na predefinição programáveis separadamente.

Antes de começar

É necessário adicionar duas ou mais predefinições para uma câmera PTZ.

Observação

Veja **Configurar predefinição** para detalhes.

Realize essa tarefa quando precisar adicionar uma patrulha para a câmera.

Etapas

1. Clique em **exibir ao vivo** na página inicial.
2. Iniciar exibição ao vivo da câmera.

Observação

Veja **Iniciar exibição ao vivo** para obter detalhes sobre como iniciar a exibição ao vivo.

3. Clique em  na barra de ferramentas de visualização ao vivo para abrir o painel de controle PTZ.
4. Clique em  para entrar no painel de configuração da patrulha.

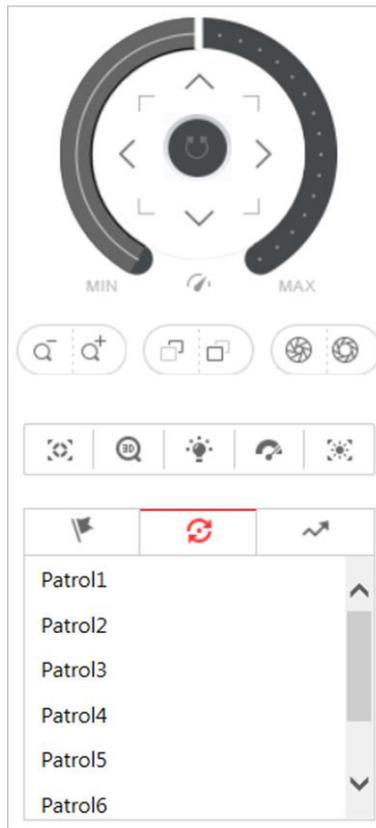


Figura 24-3 Configurar patrulha

5. Selecione uma patrulha e clique em .
6. Clique em  para adicionar uma predefinição configurada e definir o tempo de permanência e a velocidade de patrulha.

 **Observação**

- O tempo de permanência predefinido varia de 15 a 30s.
- A velocidade de rastreamento varia de 0 a 40.

-
7. Repita o passo acima para adicionar outras predefinições para a patrulha.

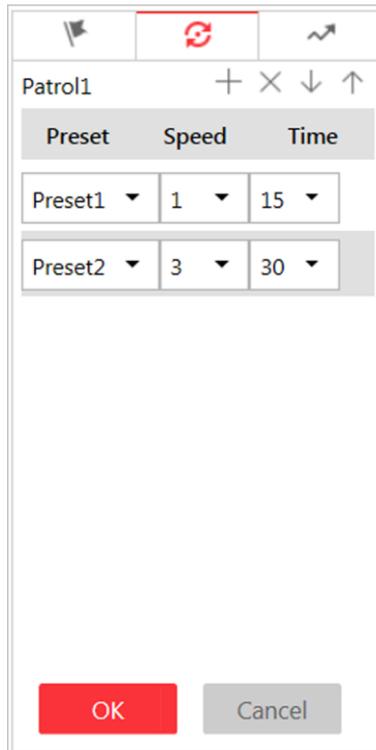


Figura 24-4 Adicionar predefinição para patrulha

8. Opcional: Execute as seguintes operações depois de adicionar a predefinição.

Remover Predefinição do Rastreamento Selecione a predefinição adicionada e clique em para remover a predefinição da patrulha.

Ajustar o Sequenciamento da Predefinição Selecione a predefinição adicionada e clique em para ajustar a sequência predefinida.

9. Clique em **OK** para salvar as configurações de rastreamento.

Observação

Podem ser configurados até oito rastreamentos.

10. Opcional: Realize as seguintes operações depois de definir a patrulha.

Ativação de rastreamentos Clique em para iniciar o rastreamento.

Parar de Ativar os Rastreamentos Clique em para parar o rastreamento.

Configurar padrão

Você pode definir padrões para gravar o movimento do PTZ.

Execute essa tarefa quando precisar adicionar um padrão para a câmera.

Etapas

1. Clique em **exibição ao vivo** na página inicial para entrar na página de visualização ao vivo.
2. Iniciar exibição ao vivo da câmera.

Observação

Veja **Iniciar exibição ao vivo** para obter detalhes sobre como iniciar a exibição ao vivo.

3. Clique em  na barra de ferramentas de visualização ao vivo para abrir o painel de controle PTZ.
4. Clique em  para entrar no painel de configuração de padrão PTZ.

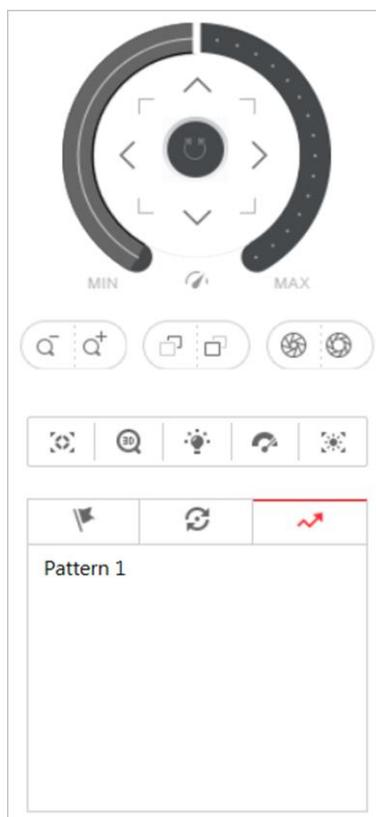


Figura 24-5 Configurar padrão

5. Clique em  para iniciar a gravação do caminho do padrão de movimento.
6. Clique nos botões de direção e outros botões para controlar o movimento PTZ.
7. Clique em  para parar e salvar a gravação do padrão.

Observação

Somente um padrão pode ser configurado cada vez, e o padrão recém-definido substituirá o padrão anterior.

8. Opcional: Execute as seguintes operações depois de definir o padrão.

Ativação de Padrões Clique em  para ativar o padrão.

Parar de Ativar o Padrão Clique em  para parar de ativar o padrão.

Deletar Padrão Clique em  para excluir o padrão.

24.2 Reprodução

Os arquivos de vídeo armazenados nos dispositivos de armazenamento local, como HDDs, HDDs net e cartões SD/SDHC ou o servidor de gravação podem ser pesquisados e reproduzidos remotamente através do navegador da Web.

24.2.1 Pesquisar Arquivo de Vídeo

Você pode pesquisar os arquivos de vídeo de câmeras e filtrar os arquivos de vídeo pesquisados por tipo de vídeo ou pelo local de armazenamento.

Realize essa tarefa quando precisar pesquisar os arquivos de vídeo específicos.

Etapas

1. Clique em **reprodução** na página inicial para abrir a página reprodução.
2. Opcional: Digite uma palavra-chave do nome da câmera ou nome da área no campo de pesquisa e clique em **pesquisar em todos os locais** ou **pesquisar no site atual** para pesquisar as câmeras ou áreas.

Todos os resultados da pesquisa são exibidos.

Observação

Você pode mover o cursor para o nome da câmera para visualizar a miniatura da imagem.

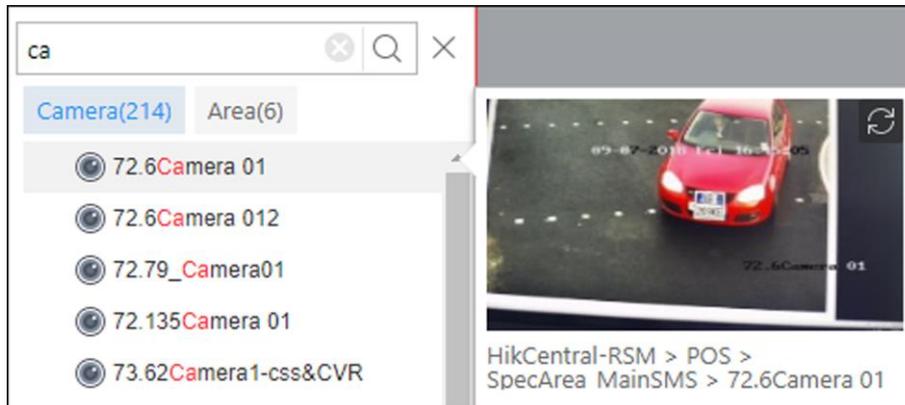


Figura 24-6 Miniatura

3. Arraste a câmera para a janela de exibição ou clique duas vezes na câmera para iniciar a reprodução.

Observação

Se o sistema é sistema central com módulo de gerenciamento remoto do local, você pode igualmente jogar para trás o vídeo gravado das câmeras importadas do local remoto. Para gerenciar as câmeras do site remoto em áreas, consulte **Gerenciar área**.

4. Opcional: Clique na data e hora na barra de ferramentas para selecionar a data e a hora para pesquisar os arquivos de vídeo.

Observação

- No painel de calendário, a data com os arquivos de vídeo será marcada com um triângulo.
- O calendário não é suportado por câmaras no local remoto.

5. Opcional: Clique em na barra de ferramentas de reprodução para selecionar o tipo de arquivo de vídeo para reprodução.
6. Opcional: Selecione o local de armazenamento e o tipo de fluxo dos arquivos de vídeo para reprodução.

Para câmera configurada com armazenamento auxiliar:

Selecione o local de armazenamento dos arquivos de vídeo para reprodução.

Para câmera configurada com gravação de fluxo

Selecione o tipo de fluxo dos arquivos de vídeo para reprodução.

duplo:

 **Observação**

Para definir o local de armazenamento da gravação, consulte **Configurar reprodução**.

24.2.2 Reproduzir Arquivo de Vídeo

Depois de Pesquisar os arquivos de vídeo, a reprodução é iniciada. Você pode controlar a reprodução de vídeo através da linha do tempo. A linha do tempo indica o tempo de duração do arquivo de vídeo.

Execute essa tarefa quando precisar controlar a reprodução.

Etapas

1. Clique em **reprodução** na página inicial para abrir a página reprodução.
2. Pesquise o arquivo de vídeo das câmeras para reprodução. Para obter detalhes, consulte **Pesquisar arquivo de vídeo**.
A reprodução é iniciada.
3. Clique nos ícones na barra de ferramentas para controlar a reprodução.
4. Clique na linha do tempo ou arraste a linha do tempo para reproduzir o vídeo da hora específica.
5. Opcional: Clique  ou  ou use a rolagem do mouse para ampliar verticalmente ou reduzir a barra da linha do tempo.
6. Opcional: Mova o cursor para a janela de exibição na reprodução para acessar outras funções, incluindo captura, recorte e outras funções.

Abrir o Zoom Digital Clique em  para ativar a função de zoom digital e desenhar um retângulo no vídeo. Clique novamente para desativar a função.

 **Observação**

Quando no modo de decodificação de software, você também pode capturar a imagem ampliada depois de ativar a função de zoom digital.

Status da Câmera Clique em  para mostrar o status da gravação da câmera, o status do sinal, o número da conexão, etc.

Alternância de Transmissão Clique em , , ou  (se suportado) para alternar a transmissão da exibição ao vivo para o transmissão principal, transmissão secundária ou transmissão suave (se suportado).

 **Observação**

A transmissão suave será exibida se o dispositivo suportar a função de suavização. Você pode alternar para transmissão suave se estiver em situação de baixa largura de banda a fim de tornar a exibição ao vivo mais fluente.

Controle de áudio

Clique em  ou  para desligar/ligar o som.

 **Observação**

Pode ajustar o volume ao mover o cursor para .

24.3 Configuração Local

O HikCentral fornece funções de visualização e reprodução ao vivo através do Web Client. Você pode definir os parâmetros de transmissão de rede relacionados (como decodificação de hardware, tipo de fluxo, etc.) para o desempenho da exibição ao vivo e a reprodução por meio do cliente Web atual. Você também pode visualizar o caminho de salvamento de arquivos de vídeo e imagens capturadas no seu PC atual.

Etapas

 **Observação**

Os parâmetros na configuração local afetam somente o cliente da Web atual.

1. Clique em **configuração local** na página inicial para entrar na página configuração local.
2. Clique na **rede transmissão** de rede à esquerda.
3. Defina os seguintes parâmetros conforme desejado.

Decodificação de Hardware da GPU

Ative a decodificação da GPU para visualização ao vivo e reprodução para economizar recursos da CPU.

 **Observação**

- O PC tem de suportar a decodificação de hardware GPU.
- Depois de habilitar a decodificação de hardware GPU, reinicie a exibição ao vivo e a reprodução para ter efeito.
- Se o cliente mostrar uma tela desfocada após habilitar a decodificação de hardware da

GPU, desabilite-a.

Transmissão global

O tipo de fluxo padrão para uso global no web client atual.

Se o dispositivo não suportar transmissão suave, ele usará transmissão secundária. Se o dispositivo não suportar transmissão secundária, ele usará transmissão principal.

Se a rede estiver em boas condições, selecione transmissão principal ou secundária. Se a rede estiver em más condições, selecione transmissão suave.

Limites para transmissão principal/secundária

Se a proporção de uma janela da área de exibição for maior que o limite configurado, o tipo de transmissão será transmissão principal. Se a proporção for menor que o limite, ele será alternado para transmissão secundária.

Por exemplo, se você definir o limite como $\frac{1}{4}$, quando a divisão da janela mudar para 5 janelas, o tipo de transmissão da câmera será alternado de transmissão principal para secundária.



Observação

Este parâmetro só está disponível quando o fluxo global é definido como fluxo principal.

Tempo limite de rede

O tempo de espera padrão para as operações em aplicativos na Web client atual. As operações serão consideradas como falhas se não houver resposta dentro do tempo configurado.

O tempo de espera padrão mínimo das interações entre os aplicativos e o servidor VSM é 60s, o tempo mínimo entre o servidor VSM e os dispositivos é 5s, e o tempo mínimo entre os aplicativos e os dispositivos é 5s.

Cache de vídeo

O cache de vídeo deve ser determinado com base no desempenho da rede, no desempenho do computador e na taxa de bits. Você pode definir é como **pequeno (1 quadro)**, **médio (6 quadros)**, ou **grande (15 quadro)**. O cache de quadro maior resultará em melhor desempenho de vídeo.

Formato de Imagem

Define o formato de arquivo para as imagens capturadas durante a exibição ao vivo ou reprodução. Atualmente ele suporta formatos **BMP** e **JPEG**.

Modo de acesso do dispositivo

Restaurar padrão

Restaure o modo de acesso do dispositivo como configurado no **sistema** → **modo de acesso a dispositivos** no Web Client.

Julgue automaticamente

Julgue o modo de acesso ao dispositivo de acordo com a rede atual.

Acesso direto

Acessa o dispositivo diretamente, não por meio do HikCentral Streaming Service.

Proxy

Acesse o dispositivo através do HikCentral Streaming Gateway e do HikCentral Management Service.



Observação

Por padrão, o sistema julgará o modo de acesso do dispositivo de acordo com a rede atual. Se você mudar para outro modo, ele afeta apenas o cliente conectado no momento.

4. Opcional: Clique em **valor padrão** para restaurar os padrões das configurações.
5. Clique em **Salvar**.
6. Opcional: Clique em **salvar caminho** à esquerda para visualizar o caminho de salvamento dos arquivos de vídeo gravados ou cortados e imagens capturadas durante a visualização ao vivo ou a reprodução em seu PC local.

Capítulo 25 Entradas importantes

HikCentral usa portas específicas ao se comunicar com outros servidores, dispositivos e assim por diante.

Certifique-se de que as seguintes portas não são ocupadas para o tráfego de dados em sua rede e você deve reencaminhar estas portas no roteador para o acesso de WAN ou abrir estas portas no firewall caso que você pode precisar de alcançar o sistema através de outras redes.

Nº da porta	Description (Descrição)
Porta NGINX	
80 (TCP)	Usado para o acesso do navegador da Web no protocolo HTTP.
443 (TCP)	Usado para o acesso do navegador da Web no protocolo HTTPS.
Porta VSM	
14200 (TCP)	Usado para o registro do local remoto ao sistema central.
15300 (TCP e UDP)	Usado para receber o evento genérico.
Gateway de transmissão	
554 (TCP)	Usado para obter fluxo (porta de transmissão em tempo real).
559 (TCP)	Usado para obter fluxo para o Google Chrome ou Firefox (porta WebSocket).
10000 (TCP)	Usado para obter fluxo para reprodução (porta de streaming de arquivo de vídeo).
Porta de serviço de proxy de teclado	
8910 (TCP)	Usado para o teclado de rede para acessar o serviço de proxy de teclado.
Porta de serviço NTP	
123 (UDP)	Porta NTP usada para sincronização de tempo.
Porta de serviço de streaming	
554 (TCP)	Usado para o serviço de streaming para obter fluxo (porta de streaming em tempo real).
559 (TCP)	Usado para obter fluxo para o Google Chrome ou Firefox (porta WebSocket).
10000 (TCP)	Usado para o serviço de streaming para obter fluxo para reprodução (porta de streaming de arquivo de vídeo).

Nº da porta	Description (Descrição)
6001 (UDP)	Porta de gerenciamento de rede.



Veja longe, Vá além