



Сетевая камера Web 5.0

Руководство по эксплуатации







Предисловие

Общие сведения

В данном руководстве представлено описание функций, настроек, общей эксплуатации и системного обслуживания сетевой камеры.

Указания по технике безопасности

В руководстве могут появляться следующие разбитые на категории сигнальные слова с определенным значением.

Сигнальные слова	Значение
 ПРЕДУПРЕЖДЕНИЕ!	Указывает на потенциально опасную ситуацию со средней и низкой степенью риска, которая, если ее не предотвратить, может привести к травме легкой или средней степени тяжести.
 ВНИМАНИЕ!	Указывает на наличие потенциального риска, который при несоблюдении соответствующих мер безопасности может привести к повреждению имущества, потере данных, снижению производительности или нештатным ситуациям.
 СОВЕТЫ	Предоставляет способы решения проблемы или позволяет сэкономить ваше время.
 ПРИМЕЧАНИЕ	Предоставляет дополнительную информацию для выделения и дополнения основного текста.

История изменений

Версия	Содержание изменения	Дата выпуска
V1.0.0	Первый выпуск.	Октябрь 2020 г.

О данном руководстве

- Настоящее руководство носит исключительно информативный характер. В случае несоответствия между руководством и реальным изделием, преимущественную силу имеет реальное изделие.
- Мы не несем ответственности за любые убытки, понесенные в результате проведения операций, которые не соответствуют руководству.
- Руководство будет обновляться в соответствии с последними законодательными и нормативно-правовыми актами соответствующих компетентных органов. Более подробная информация приведена в бумажных копиях руководства, на CD-ROM, либо можно воспользоваться QR-кодом или зайти на наш официальный сайт. В случае несоответствия между бумажной копией и электронной версией руководства преимущественную силу имеет электронная версия.
- Все варианты конструкции и программное обеспечение могут быть изменены без предварительного письменного уведомления. Обновления изделия могут привести к

некоторым различиям между реальным изделием и руководством. Для получения последней версии программы и дополнительной документации обратитесь в службу по работе с заказчиками.

- При этом не исключаются отклонения в технических характеристиках, функциях и описании операций, а также ошибки при печати. В случае возникновения каких-либо сомнений или разногласий мы оставляем за собой право на окончательное разъяснение.
- Обновите программу чтения или попробуйте другую широко распространенную программу чтения, если не можете открыть руководство (в формате PDF).
- Все товарные знаки, зарегистрированные товарные знаки и названия компаний, упомянутые в руководстве, являются собственностью соответствующих владельцев.
- Посетите наш сайт, свяжитесь с поставщиком или службой по работе с заказчиками, если при использовании устройства возникнут какие-либо проблемы.
- В случае какой-либо неопределенности или противоречия мы оставляем за собой право на окончательное разъяснение.

Важные меры предосторожности и предупреждения

Электробезопасность

- Все монтажные работы и операции должны соответствовать местным правилам безопасной эксплуатации электрооборудования.
- Источник питания должен соответствовать стандарту безопасного сверхнизкого напряжения (SELV), а подача питания должна осуществляться при номинальном напряжении, отвечающем требованию к ограниченному источнику питания согласно IEC60950-1. Обратите внимание, что требования к электропитанию указаны на бирке изделия.
- Перед началом эксплуатации устройства проверьте, отвечает ли электропитание требованиям.
- В электропроводке здания должно быть предусмотрено легкодоступное устройство отключения.
- Не допускайте смятие или сжатие силового кабеля, особенно вилки, розетки и места соединения с устройством.

Системные требования

- Не направляйте устройство в целях фокусировки на источники сильного света, такие как солнце или лампа. В противном случае это может привести к чрезмерной яркости или световым помехам, что не является неисправностью устройства, но влияет на срок службы комплементарного металлоксидного полупроводника (CMOS).
- Не подвергайте устройство воздействию влаги, пыли, чрезмерно высоких и низких температур, а также не размещайте устройство в местах с сильным электромагнитным излучением или нестабильным освещением.
- Во избежание повреждений внутренних элементов не размещайте устройство рядом с какими-либо жидкостями.
- Во избежание возгорания или удара молнии не подвергайте устройство воздействию дождя или влаги.
- Обеспечьте подходящую вентиляцию, чтобы предотвратить накопление тепла.
- Транспортировка, хранение и эксплуатация устройства должны происходить только в допустимом диапазоне температур и влажности.
- Удары, интенсивная вибрация и брызги воды недопустимы при транспортировке, хранении и установке.
- При транспортировке устройства упаковывайте его в стандартную заводскую упаковку или другой подходящий материал.
- Доступом к месту установки устройства должен обладать только квалифицированный персонал, обладающий соответствующими знаниями о предупредительных знаках и средствах обеспечения безопасности. Появление неквалифицированных лиц в зоне установки устройства может привести к случайному получению травм при нормальной эксплуатации устройства.

Эксплуатация и ежедневное техническое обслуживание

- Во избежание ожогов не прикасайтесь к теплоотводу устройства.
- При любой разборке устройства внимательно следуйте инструкциям, приведенным в руководстве. В противном случае, непрофессиональная разборка может привести к попаданию внутрь влаги или плохому качеству изображения. Если после распаковки на объективе появился конденсат или если влагопоглотитель стал зеленым, свяжитесь с отделом послепродажного обслуживания для замены влагопоглотителя. (Не все модели поставляются с влагопоглотителем).
- В целях более эффективной молниезащиты рекомендуется использовать устройство вместе с молниеотводом.
- В целях повышения надежности работы рекомендуется заземлить устройство.
- Не прикасайтесь непосредственно к датчику изображений (CMOS). Пыль и грязь можно удалить воздуходувкой, либо можно аккуратно протереть объектив мягкой тканью, смоченной спиртом.
- Для очищения корпуса устройства используйте мягкую сухую ткань, для удаления стойких пятен — ткань с мягким моющим средством. Во избежание возможных повреждений покрытия корпуса устройства, которые могут привести к снижению производительности, не используйте для очистки корпуса устройства летучий растворитель, например, спирт, бензол, разбавитель и т. п., а также не используйте концентрированное абразивное чистящее средство.
- Крышка купола является оптическим элементом. Не прикасайтесь непосредственно к крышке и не протирайте ее руками во время установки или эксплуатации. Для удаления пыли, жира или отпечатков пальцев аккуратно удалите их смоченной в диэтиле обезжиренной ватой или влажной мягкой тканью. Пыль также можно удалить при помощи воздуходувки.



ПРЕДУПРЕЖДЕНИЕ!

- Повысьте степень защиты сети, данных устройств и личной информации путем принятия мер, включающих в том числе использование надежного пароля, регулярную смену пароля, обновление встроенного ПО до последней версии и изоляцию компьютерной сети. У некоторых устройств со старыми версиями встроенного ПО пароль ONVIF не меняется автоматически при смене системного пароля, поэтому вам необходимо обновить встроенное ПО или вручную обновить пароль ONVIF.
- Используйте стандартные компоненты или аксессуары, поставляемые изготовителем; убедитесь, что монтаж и обслуживание устройства выполняются квалифицированными инженерами.
- Поверхность матрицы не должна подвергаться воздействию лазерного излучения в среде, где используется лазерное устройство.
- Не подключайте устройство к двум или более источникам электропитания, если не указано иное. Несоблюдение данного указания может привести к повреждению устройства.

Содержание

Предисловие	I
Важные меры предосторожности и предупреждения.....	III
1 Краткий обзор	1
1.1 Введение	1
1.2 Сетевое подключение	1
1.3 Порядок настройки	1
2 Инициализация устройства	3
3 Вход	7
3.1 Вход устройства в систему.....	7
3.2 Сброс пароля	8
4 Реальное время.....	10
4.1 Интерфейс просмотра в реальном времени.....	10
4.2 Настройка кодирования.....	11
5 Настройка.....	12
5.1 Сеть	12
5.1.1 TCP/IP.....	12
5.1.2 Порт.....	15
5.1.3 Адрес эл. почты.....	17
5.1.4 Основные службы	19
5.2 Событие	21
5.2.1 Настройка тревожного входа	21
5.2.2 Настройка привязки сигналов тревоги	22
5.2.2.1 Добавление расписания.....	23
5.2.2.2 Привязка расписания.....	24
5.2.2.3 Привязка снимков.....	25
5.2.2.4 Привязка тревожного выхода	25
5.2.2.5 Привязка эл. почты	26
5.3 Система	26
5.3.1 Общие сведения.....	26
5.3.1.1 Основные параметры	26
5.3.1.2 Дата и время	27
5.3.2 Учетная запись	28
5.3.2.1 Пользователь	29
5.3.2.1.1 Добавление пользователя.....	29
5.3.2.1.2 Сброс пароля.....	31
5.3.2.2 Пользователь ONVIF	32
5.3.3 Диспетчер	33

5.3.3.1 Требования.....	33
5.3.3.2 Техническое обслуживание	34
5.3.3.3 Импорт/экспорт	35
5.3.3.4 По умолч.	35
5.3.4 Обновление	36
Приложение 1 Рекомендации о кибербезопасности.....	37

1 Краткий обзор

1.1 Введение

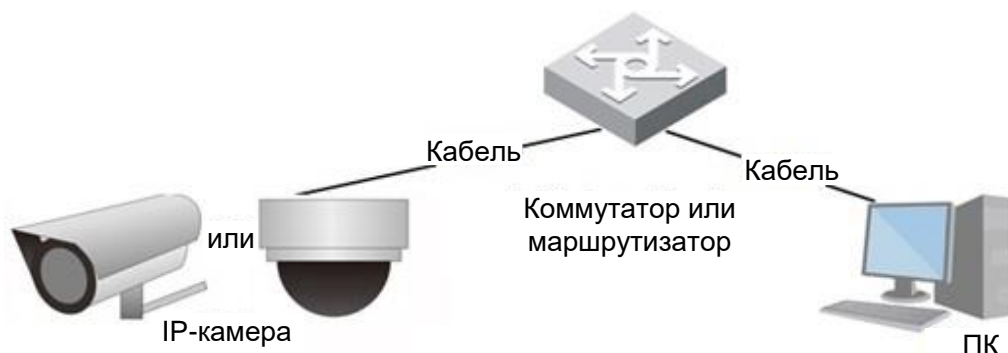
IP-камера — тип цифровой видеокамеры, которая получает контрольные данные и отправляет графические данные через сеть Интернет. Как правило, она используется для наблюдения, при этом не требует наличия локального записывающего устройства, а лишь подключения к локальной сети.

В зависимости от количества каналов IP-камеры подразделяются на одноканальные и многоканальные. У многоканальной камеры можно задать параметры для каждого канала.

1.2 Сетевое подключение

В общей топологии сети IP-камеры подключение IP-камеры к ПК осуществляется через сетевой коммутатор или маршрутизатор.

Рис. 1–1 Общая сеть IP-камеры

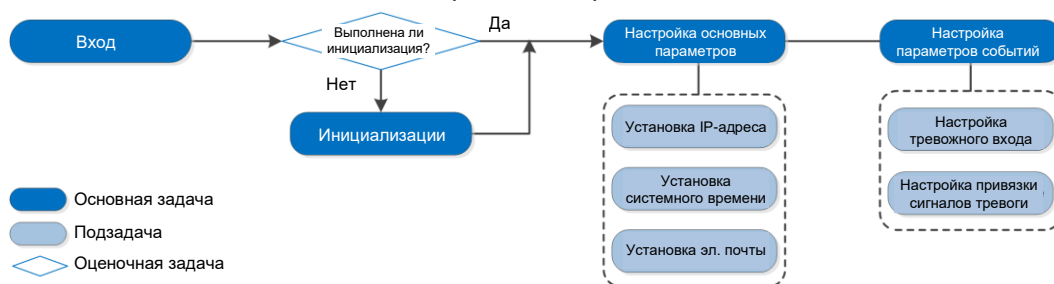


Для доступа к IP-камере через сеть необходимо получить ее IP-адрес, выполнив поиск при помощи ConfigTool.

1.3 Порядок настройки

Сведения о порядке настройки устройства см. в Рис. 1–2. Подробнее см. Таб. 1–1. Выполните конфигурацию устройства с учетом фактической ситуации.

Рис. 1–2 Порядок настройки



Таб. 1–1 Описание порядка

Конфигурация		Описание	Справка
Вход		Откройте браузер IE и введите IP-адрес для входа в веб-интерфейс. IP-адрес камеры по умолчанию — 192.168.1.108.	«3 Вход».
Инициализация		Выполните инициализацию камеры при первом использовании.	«2 Инициализация устройства»
Основные параметры	IP-адрес	Измените IP-адрес в соответствии с планом сети при первом использовании устройства или настройке сети.	«5.1.1 TCP/IP»
	Дата и время	Установите дату и время, чтобы обеспечить верность времени записи.	«5.3.1.2 Дата и время»

2 Инициализация устройства

При первом использовании устройства необходимо выполнить его инициализацию. Данное руководство описывает работу с веб-интерфейсом. Вы также можете выполнить инициализацию устройства через ConfigTool или сетевой видеорегистратор (NVR).



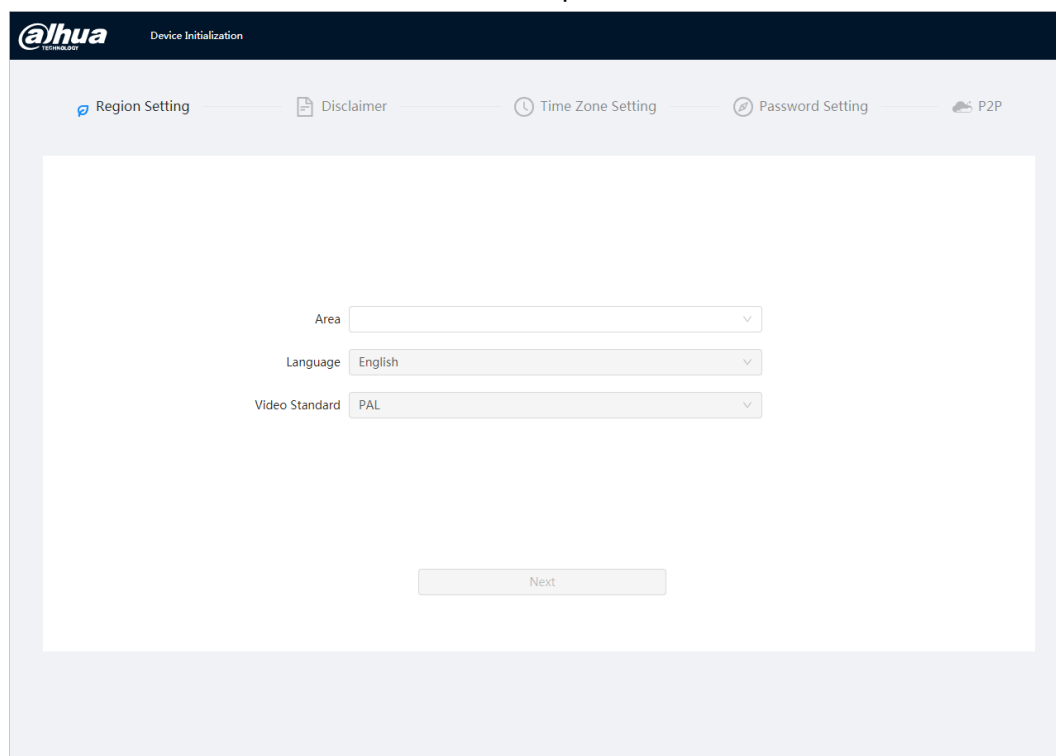
- Чтобы обеспечить безопасность устройства, должным образом храните пароль после инициализации и регулярно меняйте его.
- При инициализации устройства IP-адрес ПК и IP-адрес устройства должны принадлежать к одной сети.

Шаг 1: Откройте браузер Chrome, введите IP-адрес устройства в адресной строке и нажмите клавишу Enter.



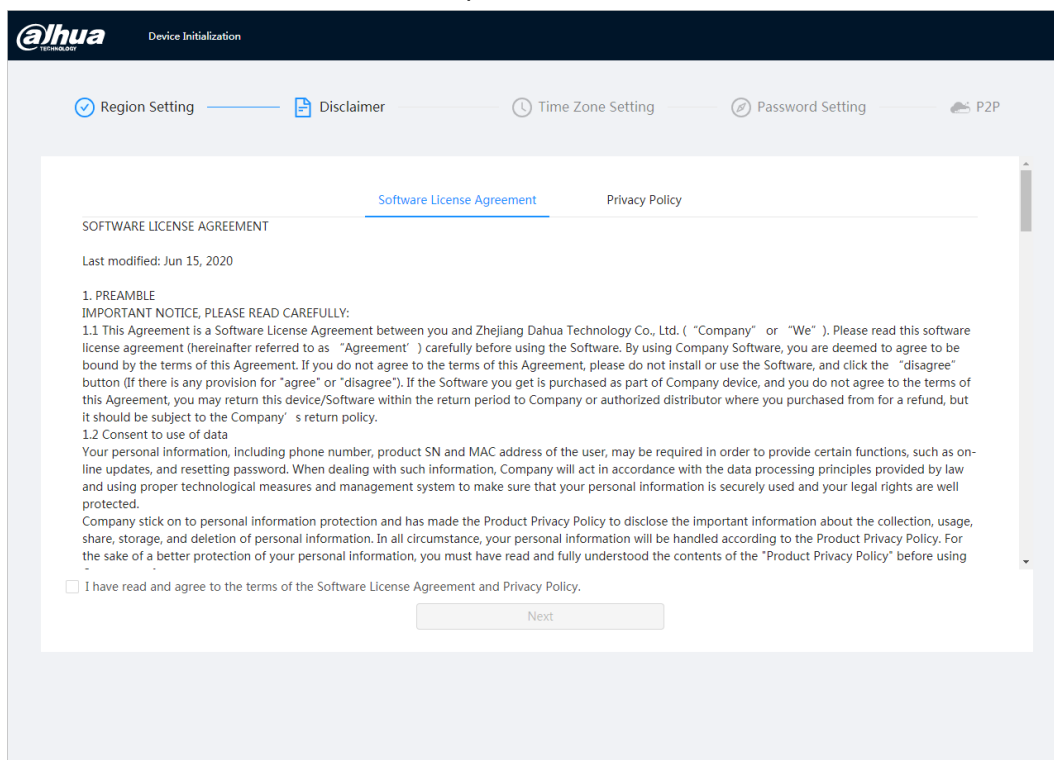
IP-адрес по умолчанию — 192.168.1.108.

Рис. 2–1 Установка региона



Шаг 2: Выберите регион, язык и стандарт видео с учетом фактической ситуации, а затем нажмите **Далее** (Next).

Рис. 2–2 Заявление об ограничении ответственности



Device Initialization

Region Setting — Disclaimer — Time Zone Setting — Password Setting — P2P

Software License Agreement Privacy Policy

SOFTWARE LICENSE AGREEMENT

Last modified: Jun 15, 2020

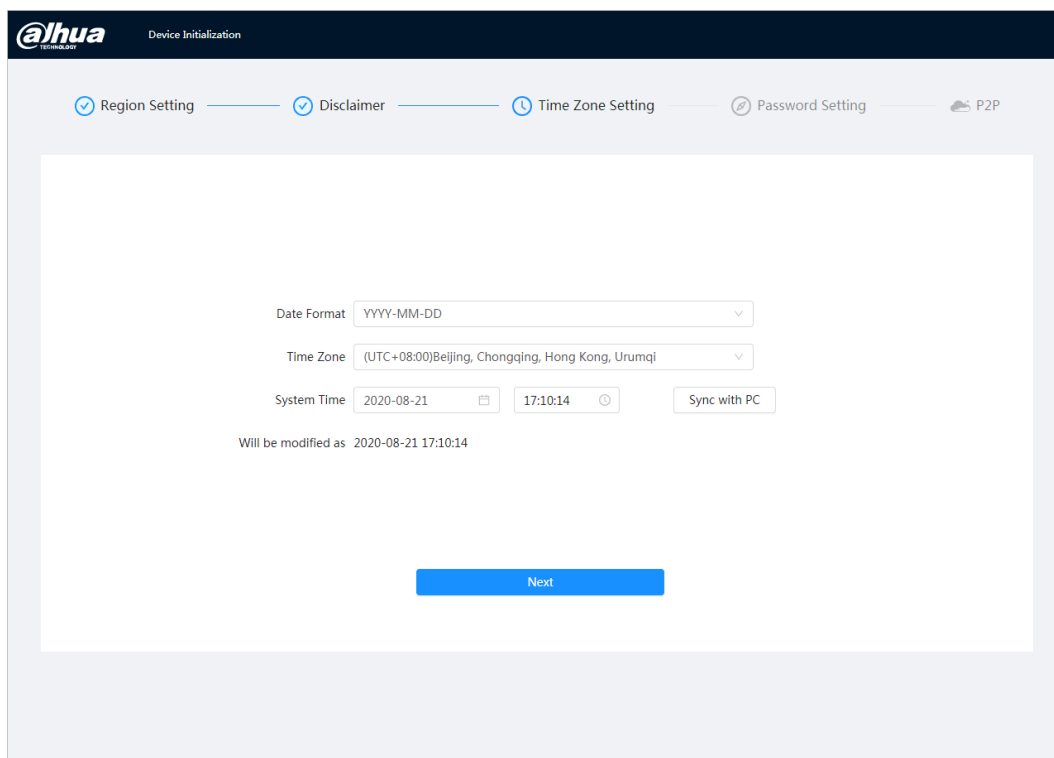
1. PREAMBLE
IMPORTANT NOTICE, PLEASE READ CAREFULLY:
1.1 This Agreement is a Software License Agreement between you and Zhejiang Dahua Technology Co., Ltd. ("Company" or "We"). Please read this software license agreement (hereinafter referred to as "Agreement") carefully before using the Software. By using Company Software, you are deemed to agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, please do not install or use the Software, and click the "disagree" button (If there is any provision for "agree" or "disagree"). If the Software you get is purchased as part of Company device, and you do not agree to the terms of this Agreement, you may return this device/Software within the return period to Company or authorized distributor where you purchased from for a refund, but it should be subject to the Company' s return policy.
1.2 Consent to use of data
Your personal information, including phone number, product SN and MAC address of the user, may be required in order to provide certain functions, such as on-line updates, and resetting password. When dealing with such information, Company will act in accordance with the data processing principles provided by law and using proper technological measures and management system to make sure that your personal information is securely used and your legal rights are well protected.
Company stick on to personal information protection and has made the Product Privacy Policy to disclose the important information about the collection, usage, share, storage, and deletion of personal information. In all circumstance, your personal information will be handled according to the Product Privacy Policy. For the sake of a better protection of your personal information, you must have read and fully understood the contents of the "Product Privacy Policy" before using

☐ I have read and agree to the terms of the Software License Agreement and Privacy Policy.

Next

Шаг 3: Установите флажок **Я прочитал(-а) и согласен(-на) с условиями Лицензионного соглашения на программное обеспечение и Политики конфиденциальности** (I have read and agree to the terms of the Software License Agreement and Privacy Policy), а затем нажмите **Далее** (Next).

Рис. 2–3 Установка часового пояса



Device Initialization

Region Setting — Disclaimer — Time Zone Setting — Password Setting — P2P

Date Format YYYY-MM-DD

Time Zone (UTC+08:00)Beijing, Chongqing, Hong Kong, Urumqi

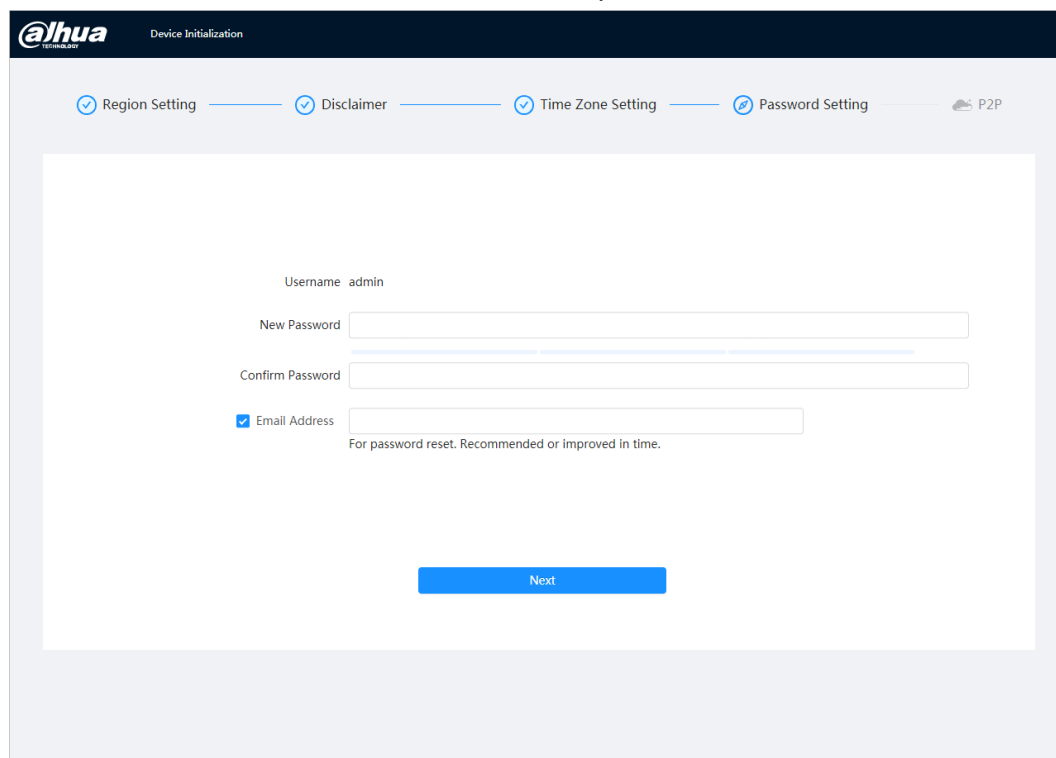
System Time 2020-08-21 17:10:14 Sync with PC

Will be modified as 2020-08-21 17:10:14

Next

Шаг 4: Выполните конфигурацию параметров времени, а затем нажмите **Далее** (Next).

Рис. 2–4 Установка пароля



alhua TECHNOLOGY Device Initialization

Region Setting — Disclaimer — Time Zone Setting — Password Setting — P2P

Username admin

New Password

Confirm Password

☒ Email Address

For password reset. Recommended or improved in time.

Next

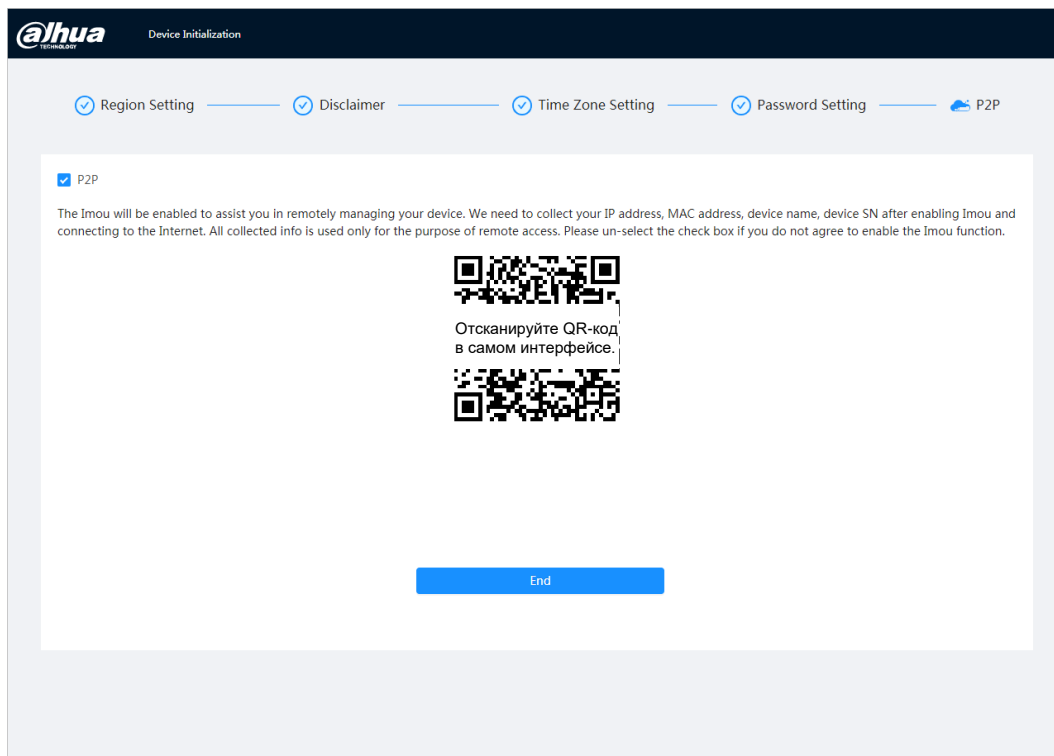
Шаг 5: Установите пароль для учетной записи администратора.

Таб. 2–1 Описание настройки пароля

Параметр	Описание
Имя пользователя	Имя пользователя по умолчанию — admin.
Пароль	Пароль должен состоять из 8-32 непустых символов и содержать не менее двух следующих типов символов: прописные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &). Установите пароль высокого уровня безопасности с учетом уведомления о безопасности пароля.
Подтверждение пароля	
Зарезервированный адрес эл. почты	Введите адрес эл. почты для сброса пароля, и он будет выбран по умолчанию. При необходимости сбросить пароль учетной записи администратора на зарезервированный адрес эл. почты будет отправлен код безопасности для сброса пароля.

Шаг 6: Нажмите **Далее** (Next), после чего появится интерфейс **P2P** (P2P).

Рис. 2–5 P2P



3 Вход

3.1 Вход устройства в систему

В данном разделе описано, как войти в веб-интерфейс и выйти из него. В данном разделе в качестве примера используется Chrome.



- Перед входом в веб-интерфейс необходимо выполнить инициализацию камеры. Подробнее см. «2 Инициализация устройства».
- При инициализации камеры IP-адрес ПК и IP-адрес устройства должны находиться в одной сети.
- При первом входе в систему следуйте инструкциям по загрузке и установке плагина.

Шаг 1: Откройте браузер Chrome, введите IP-адрес камеры (по умолчанию 192.168.1.108) в адресную строку и нажмите Enter.

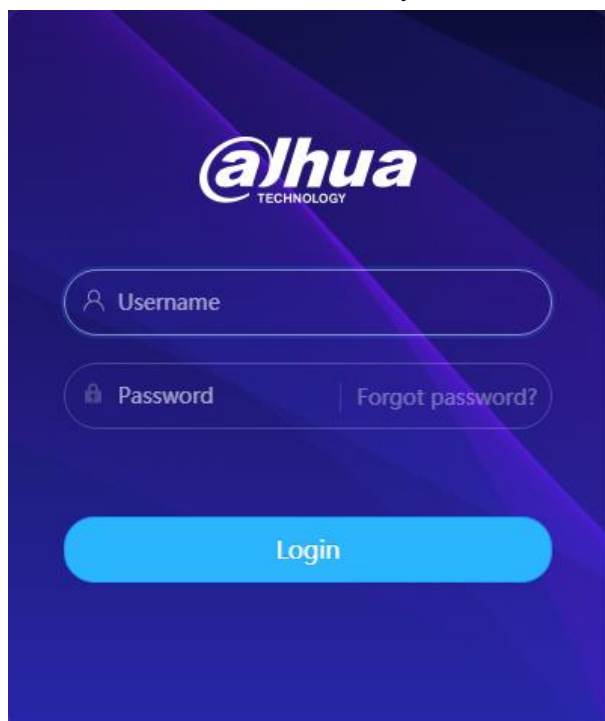
Шаг 2: Введите имя пользователя и пароль.

Имя пользователя по умолчанию — admin.




Чтобы сбросить пароль через адрес эл. почты, установленный во время инициализации, нажмите **Забыли пароль?** (Forgot password?). Подробнее см. «3.2 Сброс пароля».

Рис. 3–1 Вход в систему



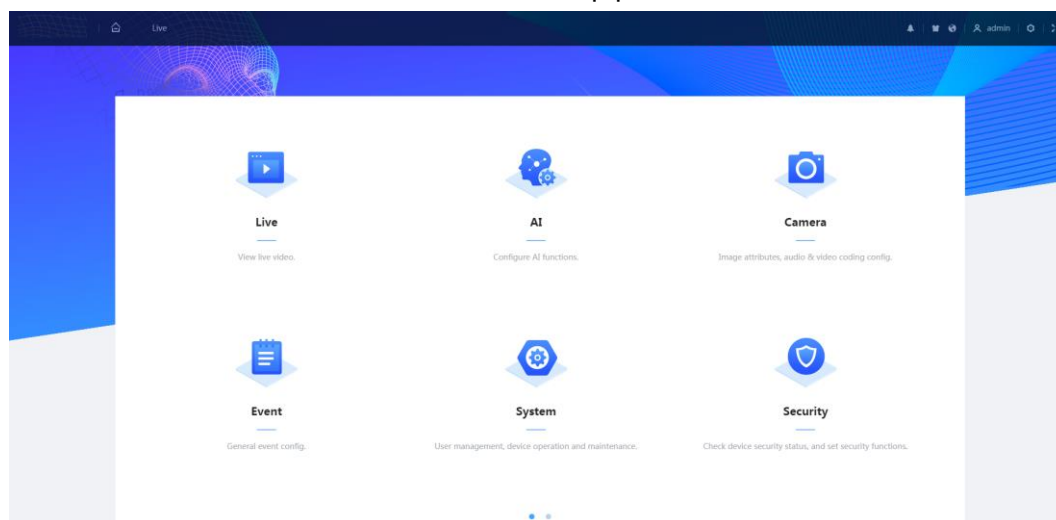
Шаг 3: Нажмите **Войти в систему** (Login).

Отобразится интерфейс **Реальное время** (Live). Для отображения главного интерфейса нажмите  в левом верхнем углу интерфейса.



При первом входе в систему установите плагин в соответствии с инструкциями на экране.

Рис. 3–2 Главный интерфейс




- Реальное время: мониторинг изображения в реальном времени.
- ИИ: настройка функции ИИ камеры.
- Камера: настройка параметров камеры, включая параметры изображения, параметры кодирующего устройства и параметры звука.
- Событие: настройка общих событий, включая сбои привязки сигналов тревоги, обнаружение видео и обнаружение звука.
- Система: настройка системных параметров, включая общие параметры, дату и время, учетную запись, безопасность, настройки PTZ, настройки по умолчанию, импорт/экспорт, удаленный режим, автоматическое обслуживание и обновление.
- Безопасность: проверка состояния безопасности устройства и настройка функций безопасности.
- Запись: воспроизведение или загрузка записанного видео.
- Изображение: воспроизведение или загрузка файлов изображений.
- Отчет: поиск интеллектуального отчета о событиях и системного отчета.

3.2 Сброс пароля

В случае необходимости сбросить пароль учетной записи администратора на введенный адрес эл. почты будет отправлен код безопасности, который можно использовать для сброса пароля.

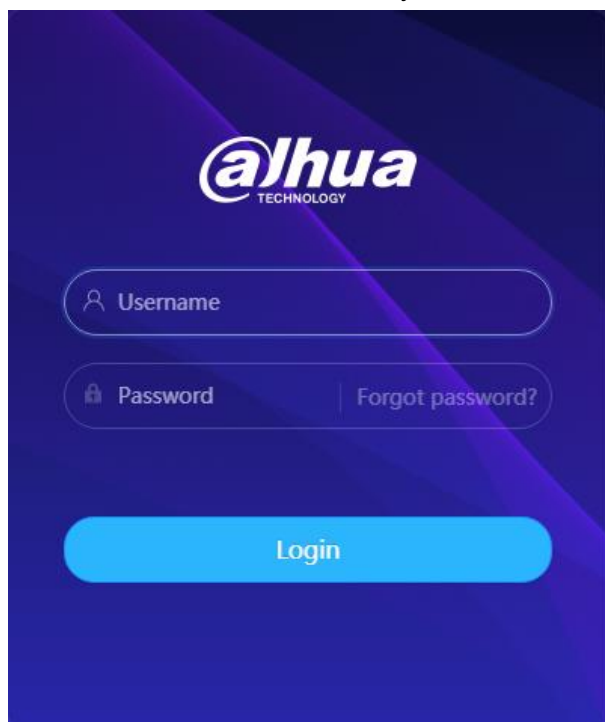
Предварительные требования

Служба сброса пароля включена во вкладке  > Система (System) > Учетная запись (Account) > Пользователь (User).

Процедура

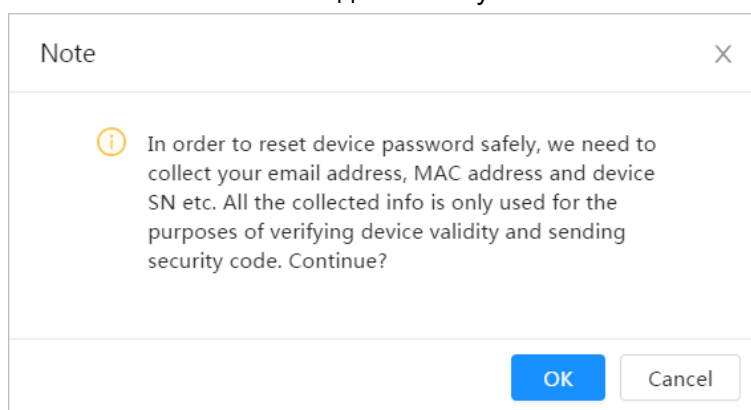
Шаг 1: Откройте браузер Chrome, введите IP-адрес устройства в адресную строку и нажмите Enter.

Рис. 3–3 Вход в систему



Шаг 2: Чтобы сбросить пароль через адрес эл. почты, установленный во время инициализации, нажмите **Забыли пароль?** (Forgot password?).

Рис. 3–4 Вход в систему



4 Реальное время

В данном разделе описана структура интерфейса и настройка функций.

4.1 Интерфейс просмотра в реальном времени

Войдите в систему или нажмите на вкладку **Реальное время** (Live).



Интерфейс может отличаться в зависимости от модели, и преимущественную силу имеет фактический интерфейс.

Рис. 4–1 Реальное время (одноканальный режим)

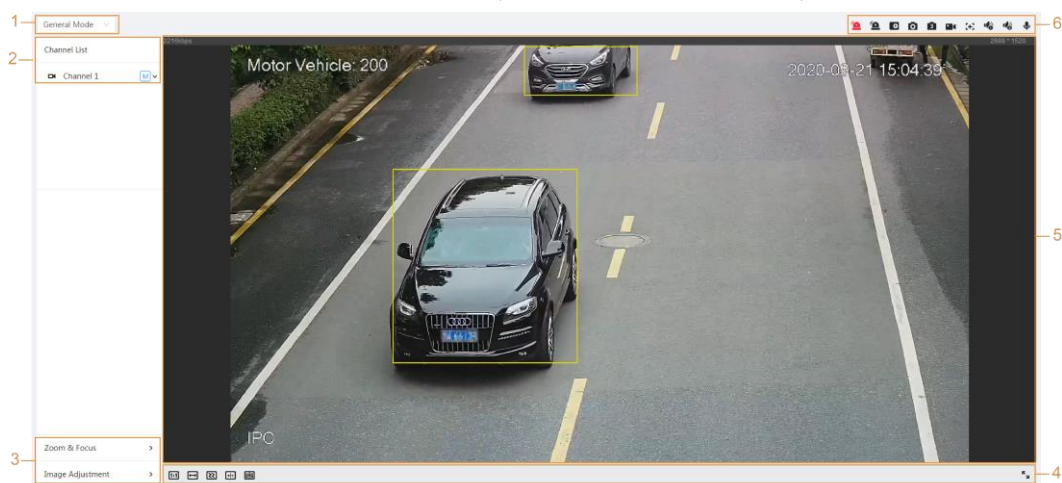
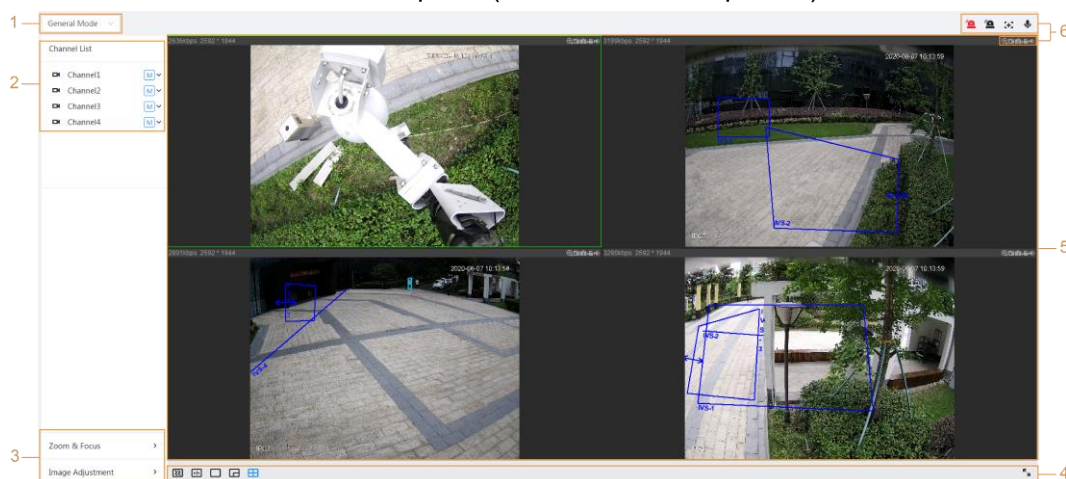


Рис. 4–2 Реальное время (многоканальный режим)



Таб. 4–1 Описание строки функций

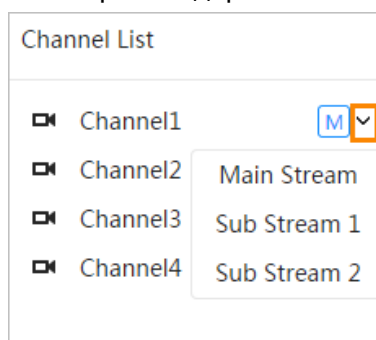
№	Функция	Описание
1	Режим отображения	Вы можете выбрать один из следующих режимов отображения: Общий режим (General Mode) или Режим лиц (Face Mode).




№	Функция	Описание
2	Список каналов	Отображение всех каналов. Вы можете выбрать необходимый канал и настроить тип потока.
3	Регулировка изображения	Регулировка операций при просмотре в реальном времени.
4		
5	Реальное время	Мониторинг изображения в реальном времени.
6	Строка функций просмотра в реальном времени	Функции и операции при просмотре в реальном времени.

4.2 Настройка кодирования

Нажмите , а затем выберите необходимый поток.

Рис. 4–3 Строка кодирования



- **Основной поток:** для него характерны большой битовый поток и высокое разрешение изображений, но при этом он требует большой пропускной способности. Данный параметр можно использовать для хранения и мониторинга.
- **Дополнительный поток:** для него характерны небольшой битовый поток и менее высокое разрешение изображений, но при этом он требует меньшей пропускной способности. Данный параметр обычно используется для замены основного потока при недостаточной пропускной способности.
-  означает, что текущий поток является основным потоком.  означает, что текущий поток является дополнительным потоком 1.  означает, что текущий поток является дополнительным потоком 2.

5 Настройка

В данном разделе описаны основные настройки камеры, включая конфигурацию сети, событий и системы.

5.1 Сеть

В данном разделе описана конфигурация сети.

5.1.1 TCP/IP

Вы можете настроить IP-адрес, сервер DNS и пр. в соответствии с планом сети.

Предварительные требования

Камера подключена к сети.

Процедура


Шаг 1: Выберите  > **Сеть** (Network) > **TCP/IP**.

Рис. 5–1 TCP/IP

Host Name

IPC

ARP/Ping

☒

NIC

Wired(Default) ▾

Mode

☒ Static ☐ DHCP

MAC Address

IP Version

IPv4 ▾

IP Address

Subnet Mask

Default Gateway

Preferred DNS

Alternate DNS

Apply


Refresh


Default

Шаг 2: Выполните конфигурацию параметров TCP/IP.

Таб. 5–1 Описание параметров TCP/IP

Параметр	Описание
Имя хоста	Введите имя хоста, при этом его длина не должна превышать 15 символов.

Параметр	Описание
ARP/Ping	<p>Нажмите , чтобы включить ARP/Ping для настройки службы IP-адресов. Для смены и настройки IP-адреса устройства при помощи команды ARP/ping необходимо получить MAC-адрес камеры.</p> <p>Данный параметр включен по умолчанию. Во время перезагрузки у вас будет не более 2 минут на настройку IP-адреса устройства при помощи пакета ping определенной длины. Сервер отключится через 2 минуты или сразу после успешной настройки IP-адреса. Если данный параметр не включен, настройка IP-адреса при помощи пакета ping невозможна.</p> <p>Порядок настройки IP-адреса при помощи ARP/Ping.</p> <ol style="list-style-type: none"> Для получения пригодного для использования IP-адреса ПК и камера, которую необходимо настроить, должны находиться в одной локальной сети. Узнайте MAC-адрес камеры на бирке изделия. Откройте редактор команд на ПК и введите следующую команду. <div data-bbox="676 898 1351 1464"> <pre>Windows syntax> arp -s <IP Address> <MAC> ^ ping -l 480 -t <IP Address> ^ Windows example> arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -l 480 -t 192.168.0.125^ UNIX/Linux/Mac syntax> arp -s <IP Address> <MAC> ^ ping -s 480 <IP Address> ^ UNIX/Linux/Mac example> arp -s 192.168.0.125 11-40-8c-18-10-11^ ping -s 480 192.168.0.125^</pre> </div> <ol style="list-style-type: none"> Перезагрузите камеру. Проверьте, отображается ли в командной строке ПК информация Ответ от 192.168.0.125... (Reply from 192.168.0.125...). В таком случае конфигурация выполнена успешно, и вы можете закрыть командную строку. Для входа в систему введите http://(IP-адрес) в адресной строке браузера.
Сетевая плата	<p>Выберите карту Ethernet, которую необходимо настроить, при этом параметр по умолчанию — Проводной (Wired).</p>

Параметр	Описание
Режим	<p>Режим, в котором камера получает IP-адрес:</p> <ul style="list-style-type: none"> Статический (Static) Вручную настройте IP-адрес (IP Address), Маска подсети (Subnet Mask) и Шлюз по умолчанию (Default Gateway), а затем нажмите Сохранить (Save). Отобразится интерфейс входа в систему с настроенным IP-адресом. DHCP При наличии сервера DHCP в сети выберите DHCP, и камера автоматически получит IP-адрес.
MAC-адрес	Отображение MAC-адреса хоста.
Версия IP	Выберите IPv4 или IPv6 .
IP-адрес	<p>При выборе параметра Статический (Static) в разделе Режим (Mode) введите необходимые IP-адрес и маску подсети.</p> <p></p> <ul style="list-style-type: none"> IPv6 не имеет маски подсети. Шлюз по умолчанию должен находиться в том же сегменте сети, что и IP-адрес.
Маска подсети	
Шлюз по умолчанию	
Предпочтительный DNS	IP-адрес предпочтительного DNS
Альтернативный DNS	IP-адрес альтернативного DNS

Шаг 3: Нажмите кнопку **Применить (Apply)**.

5.1.2 Порт

Настройте номера портов и максимальное количество пользователей (включая веб-клиент, клиент платформы и клиент мобильного телефона), которые могут одновременно подключаться к устройству.

Шаг 1: Выберите  > **Сеть (Network)** > **ТСР/IP**.

Рис. 5–2 Порт

Max Connection	<input type="text" value="10"/>	(1-20)
TCP Port	<input type="text" value="37777"/>	(1025-65534)
UDP Port	<input type="text" value="37778"/>	(1025-65534)
HTTP Port	<input type="text" value="80"/>	
RTSP Port	<input type="text" value="554"/>	
RTMP Port	<input type="text" value="1935"/>	(1025-65534)
HTTPS Port	<input type="text" value="443"/>	
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>		

Шаг 2: Настройте параметры порта.



- Порты 0–1024, 1900, 3800, 5000, 5050, 9999, 37776, 37780–37880, 39999, 42323 отведены для определенных целей.
- При настройке порта не указывайте значение любого другого порта.

Таб. 5–2 Описание параметров порта

Параметр	Описание
Максимальное число соединений	Максимальное число пользователей (включая веб-клиент, клиент платформы и клиент мобильного телефона), которые могут одновременно подключаться к устройству. Значение по умолчанию — 10.
Порт TCP	Порт протокола управления передачей. Значение по умолчанию — 37777.
Порт UDP	Порт протокола пользовательских датаграмм. Значение по умолчанию — 37778.
Порт HTTP	Порт протокола передачи гипертекста. Значение по умолчанию — 80.

Параметр	Описание
Порт RTSP	<ul style="list-style-type: none"> Порт протокола потоковой передачи в реальном времени. Значение по умолчанию — 554. Следующий формат адреса URL доступен при просмотре в реальном времени на смартфоне QuickTime, VLC или Blackberry. Когда формат адреса URL требует RTSP, укажите номер канала и тип битового потока в адресе URL, а также при необходимости имя пользователя и пароль. <p>Пример формата адреса URL: rtsp://username:password@ip:port/cam/realmonitor?channel=1&subtype=0</p> <p>Расшифровка:</p> <ul style="list-style-type: none"> Имя пользователя: имя пользователя, например admin. Пароль: пароль, например admin. IP: IP-адрес устройства, например 192.168.1.112. Порт: оставьте неизменным, если значение по умолчанию равно 554. Канал: номер канала, который начинается с 1. Например, если вы используете канал 2, то канал=2. Подтип (subtype): тип битового потока. 0 означает основной поток (подтип=0), а 1 — дополнительный поток (подтип=1). <p>Пример: если вам требуется дополнительный поток канала 2 на определенном устройстве, адрес URL должен иметь следующий формат: rtsp://admin:admin@10.12.4.84:554/cam/realmonitor?channel=21&=1</p> <p>Если имя пользователя и пароль не нужны, URL-адрес может иметь следующий формат: rtsp://ip:port/cam/realmonitor?channel=11&=0</p>
Порт RTMP	Протокол обмена сообщениями в реальном времени. Порт, который RTMP предоставляет сервису. Значение по умолчанию – 1935.
Порт HTTPS	Коммуникационный порт HTTPS. Значение по умолчанию – 443.

Шаг 3: Нажмите кнопку **Применить** (Apply).



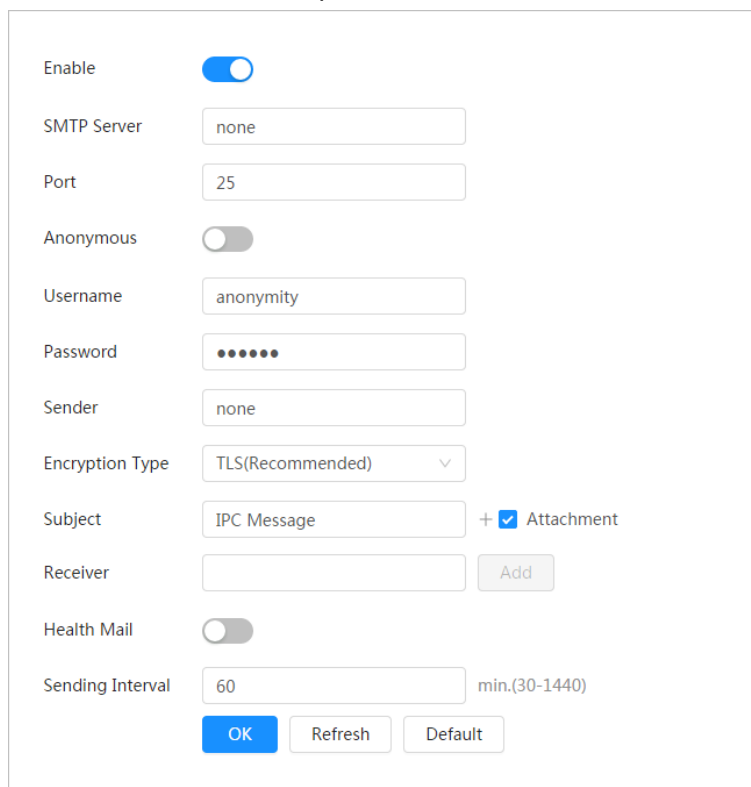
Конфигурация **Максимальное число соединений** (Max Connection) мгновенно вступает в силу, а остальные параметры вступят в силу после перезагрузки.


5.1.3 Адрес эл. почты

Выполните конфигурацию параметра эл. почты и включите привязку эл. почты. При срабатывании соответствующего сигнала тревоги система безопасности отправляет эл. письмо на указанный адрес.

Шаг 1: Выберите  > **Сеть** (Network) > **Адрес эл. почты** (Email).





Рис. 5–3 Адрес эл. почты




Шаг 2: Нажмите  для включения функции.

Шаг 3: Настройте параметры адреса эл. почты.


Таб. 5–3 Описание параметров адреса эл. почты

Параметр	Описание	
Сервер SMTP	Адрес сервера SMTP	 Подробнее см. Таб. 5–4.
Порт	Номер порта сервера SMTP.	
Имя пользователя	Учетная запись сервера SMTP.	
Пароль	Пароль сервера SMTP.	
Анонимность	Чтобы информация об отправителе не отображалась в сообщении эл. почты, нажмите  .	
Отправитель	Адрес эл. почты отправителя.	
Тип шифрования	Выберите один из следующих параметров: Никакой (None), SSL или TLS .  Подробнее см. Таб. 5–4.	
Тема	Вводите не более 63 символов (типы символов: китайские иероглифы, буквы английского алфавита и арабские цифры). Нажмите  для выбора типа заголовка, включая Имя устройства (Device Name), Идентификатор устройства (Device ID) и Тип события (Event Type). Вы можете указать не более 2 заголовков.	
Приложения	Установите флажок для поддержки отправки приложений в сообщениях эл. почты.	

Параметр	Описание
Получатель	<ul style="list-style-type: none"> Адрес эл. почты получателя. Поддерживает не более 3 адресов. После ввода адреса эл. почты получателя отображается кнопка Проверить (Test). Нажмите Проверить (Test), чтобы проверить, можно ли успешно отправлять и получать эл. письма.
Тестовое эл. письмо	Система отправляет тестовое эл. письмо, чтобы проверить успешную настройку соединения. Нажмите  и настройте Интервал отправки (Sending Interval), а затем система будет отправлять тестовое эл. письмо с заданным интервалом.

Сведения о конфигурации основных почтовых ящиков см. в Таб. 5–4.

Таб. 5–4 Описание настройки почтового ящика

Почтовый ящик	Сервер SMTP	Аутентификация	Порт	Описание
gmail	smtp.gmail.com	SSL	465	<ul style="list-style-type: none"> Вам необходимо включить службу SMTP в почтовом ящике. Требуется код аутентификации. Пароль эл. почты не применим.  <div>Код аутентификации: код, получаемый при включении службы SMTP.</div>
		TLS	587	

Шаг 4: Нажмите кнопку **Применить** (Apply).

5.1.4 Основные службы

Настройте основные службы для повышения безопасности сети и данных.


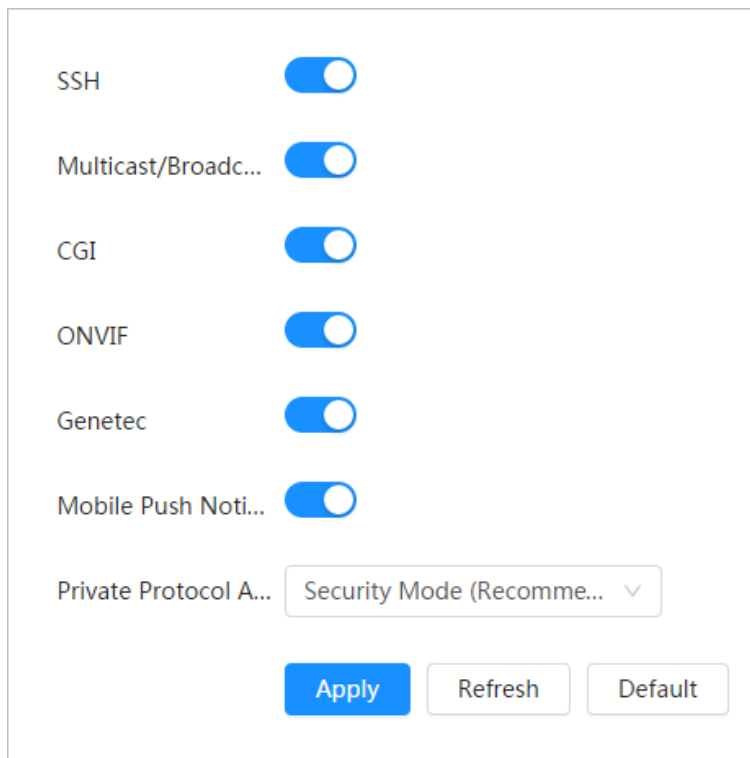
Шаг 1: Выберите  > **Сеть** (Network) > **Основные службы** (Basic Service).

Рис. 5–4 Основные службы



Шаг 2: Включите основные службы согласно фактическим потребностям.

Таб. 5–5 Описание параметров основных служб

Функция	Описание
SSH	Вы можете включить аутентификацию SSH в целях управления безопасностью.
Поиск многоадресной рассылки/трансляции	Если данная функция включена, несколько пользователей при одновременном просмотре видеоизображений устройства через сеть могут найти ваше устройство при помощи протокола многоадресной рассылки/трансляции.
CGI	Если данная функция включена, другие устройства могут получить доступ через данную службу. Данная функция включена по умолчанию.
Onvif	
Genetec	
Мобильные push-уведомления	Если данная функция включена, система отправит снимок, который был сделан при срабатывании сигнала тревоги, на ваш телефон. Данная функция включена по умолчанию.
Режим аутентификации частного протокола	Выберите один из следующих режимов аутентификации: Режим безопасности (Security Mode) и Режим совместимости (Compatible Mode). Рекомендован режим безопасности.

Шаг 3: Нажмите кнопку **Применить** (Apply).

5.2 Событие


В данном разделе в качестве примера используется тревожный вход, например для конфигурации привязки сигналов тревоги.

Рис. 5–5 Настройка событий тревоги



5.2.1 Настройка тревожного входа

При срабатывании сигнала тревоги из-за устройства, подключенного к порту тревожного входа, система выполняет заданную привязку сигнала тревоги.

Шаг 1: Выберите  > **Событие** (Event) > **Сигнал тревоги** (Alarm).


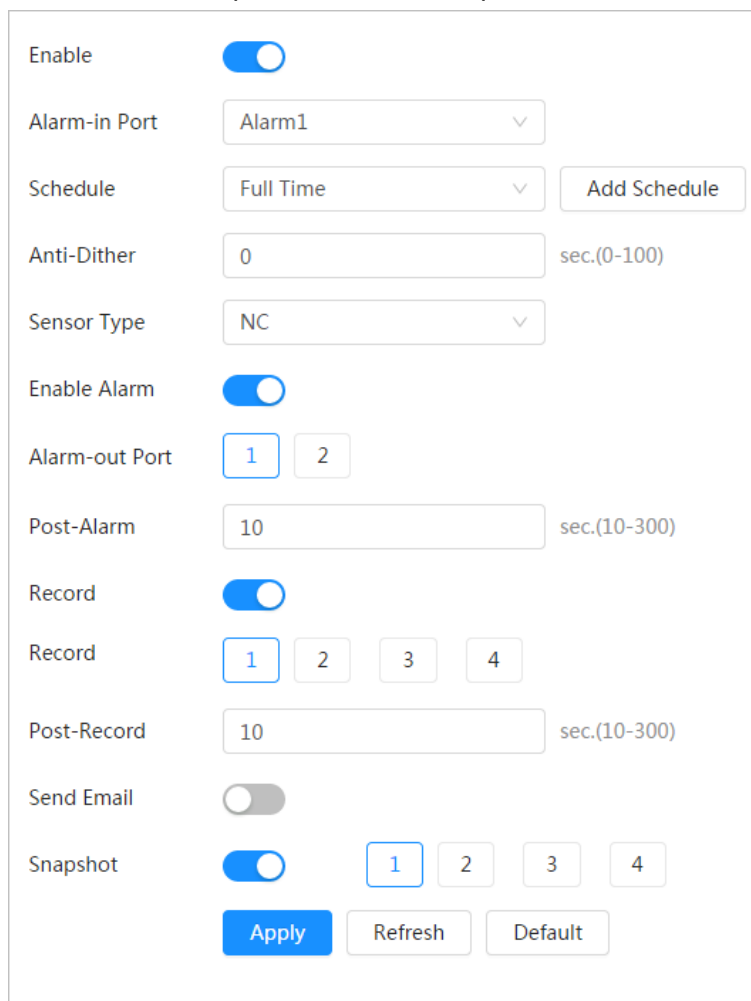
Шаг 2: Нажмите  рядом с **Включить** (Enable) для включения привязки сигналов тревоги.

Рис. 5–6 Привязка сигналов тревоги



Enable ☒

Alarm-in Port Alarm1

Schedule Full Time Add Schedule

Anti-Dither 0 sec.(0-100)

Sensor Type NC

Enable Alarm ☒

Alarm-out Port 1 2

Post-Alarm 10 sec.(10-300)

Record ☒

Record 1 2 3 4

Post-Record 10 sec.(10-300)

Send Email ☐

Snapshot ☒ 1 2 3 4

Apply Refresh Default

Шаг 3: Выберите порт тревожного входа и тип датчика.

- Тип датчика: НО или НЗ.
- Антидизеринг: запись только одного события тревоги в рамках периода антидизеринга.

Шаг 4: Выберите расписание, периоды постановки на охрану и действие привязки сигналов тревоги. Подробнее см. «5.2.2 Настройка привязки сигналов тревоги». Если существующие расписания не отвечают требованиям сцены, для добавления нового расписания нажмите **Добавить расписание** (Add Schedule). Подробнее см. «5.2.2.1 Добавление расписания».

Шаг 5: Нажмите кнопку **Применить** (Apply).

5.2.2 Настройка привязки сигналов тревоги

При настройке событий тревоги выберите привязки сигналов тревоги (например запись, снимок). При срабатывании соответствующего сигнала тревоги в рамках указанного периода постановки на охрану система подает сигнал тревоги.


Выберите  > **Событие** (Event) > **Сигнал тревоги** (Alarm), а затем нажмите ☐ рядом с **Включить** (Enable) для включения привязки сигналов тревоги.

Рис. 5–7 Привязка сигналов тревоги

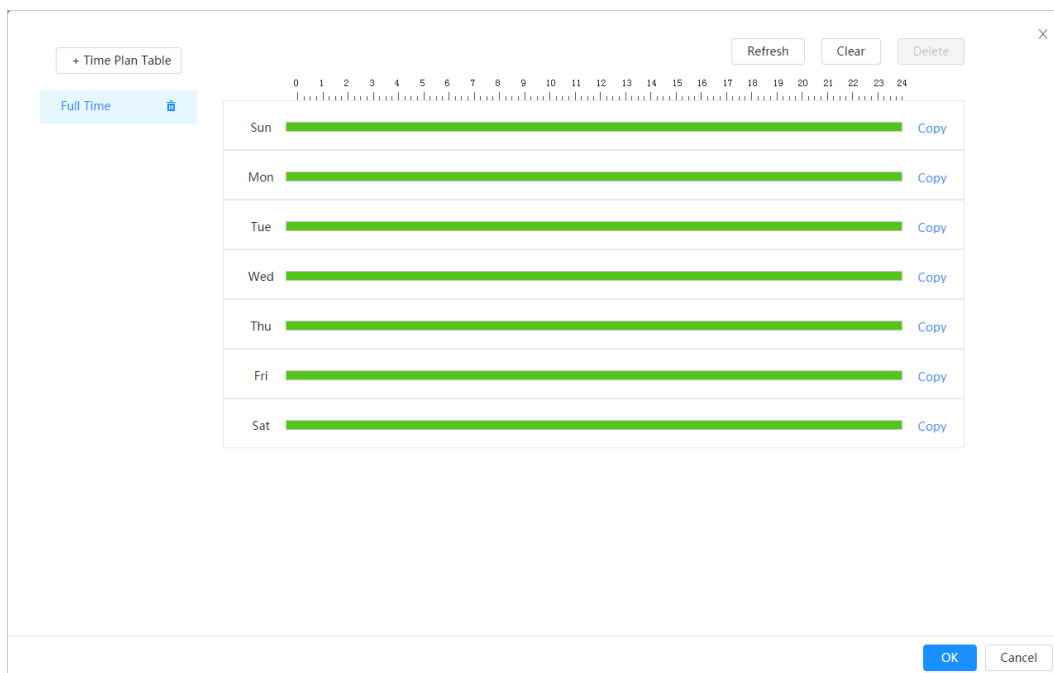
Enable	<input checked="" type="checkbox"/>
Alarm-in Port	Alarm1 <input type="button" value="v"/>
Schedule	Full Time <input type="button" value="v"/> <input type="button" value="Add Schedule"/>
Anti-Dither	0 sec.(0-100)
Sensor Type	NC <input type="button" value="v"/>
Enable Alarm	<input checked="" type="checkbox"/>
Alarm-out Port	<input type="button" value="1"/> <input type="button" value="2"/>
Post-Alarm	10 sec.(10-300)
Record	<input checked="" type="checkbox"/>
Record	<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
Post-Record	10 sec.(10-300)
Send Email	<input type="checkbox"/>
Snapshot	<input checked="" type="checkbox"/> <input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/>
<input type="button" value="Apply"/> <input type="button" value="Refresh"/> <input type="button" value="Default"/>	

5.2.2.1Добавление расписания

Задайте периоды постановки на охрану. Система выполняет только соответствующее действие привязки в рамках настроенного периода.

Шаг 1: Нажмите **Добавить расписание** (Add Schedule) рядом с **Расписание** (Schedule).

Рис. 5–8 Расписание




Шаг 2: Чтобы задать периоды постановки на охрану, нажмите на левую кнопку мыши и выделите период на временной шкале. Сигналы тревоги будут срабатывать в период времени, выделенный зеленым цветом на временной шкале.

- Нажмите **Копировать** (Copy) рядом с днем и выберите дни, для которых вы хотите выполнить копирование в интерфейсе подсказки. Возможно скопировать конфигурацию для выбранных дней. Чтобы выбрать все дни для копирования конфигурации, установите флажок **Выбрать все** (Select All).
- Вы можете задать 6 временных периодов в день.

Шаг 3: Нажмите кнопку **Применить** (Apply).

Шаг 4: (Дополнительно) Чтобы добавить новую таблицу плана времени, нажмите **Таблица плана времени** (Time Plan Table).

Возможные действия:

- Дважды нажмите имя таблицы, чтобы отредактировать его.
- Нажмите , чтобы удалить необходимый элемент.


5.2.2.2Привязка расписания

Система может связать канал записи при возникновении события тревоги. После срабатывания сигнала тревоги система прекращает запись через определенный период времени согласно настройкам в разделе **Продлить запись** (Post-Record).

Предварительные требования

- После включения соответствующего типа сигнала тревоги (**Нормальный** (Normal), **Движение** (Motion) или **Тревога** (Alarm)) канал записи выполняет привязку записи.
- Включите режим автоматической записи, и привязка записи вступит в силу.

Настройка привязки записи

В интерфейсе **Сигнал тревоги** (Alarm) нажмите , чтобы включить привязку записи, выберите необходимый канал и нажмите **Продлить запись** (Post-Record) для настройки привязки сигналов тревоги и задержки записи.

После настройки параметра **Продлить запись** (Post-Record) запись по сигналу тревоги продлится в течение определенного периода времени после окончания сигнала тревоги.

Рис. 5–9 Привязка записи



5.2.2.3Привязка снимков

Настройка привязки снимков обеспечивает автоматическое срабатывание сигналов тревоги в системе и выполнение снимков.

Предварительные требования

При включении соответствующего типа сигнала тревоги (**Нормальный** (Normal), **Движение** (Motion) или **Тревога** (Alarm)) выполняется привязка между каналом снимка и выполнением снимка.

Настройка привязки записи



В интерфейсе **Сигнал тревоги** (Alarm) нажмите , чтобы включить привязку снимков, и выберите необходимый канал.

Рис. 5–10 Привязка снимков



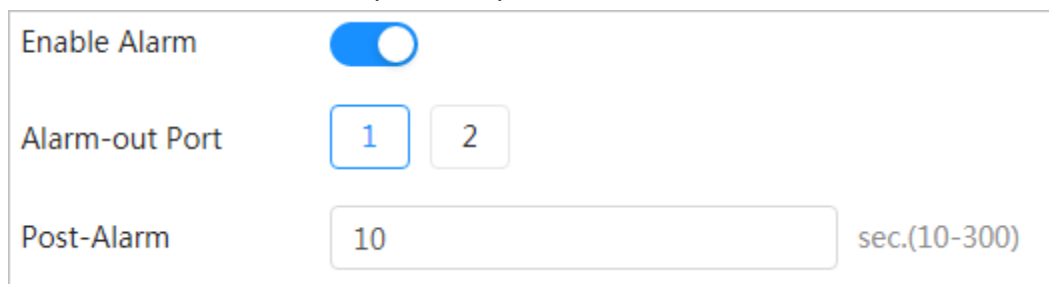
5.2.2.4Привязка тревожного выхода

При срабатывании сигнала тревоги система может автоматически связываться с устройством тревожного выхода.

В интерфейсе **Сигнал тревоги** (Alarm) нажмите , чтобы включить привязку тревожного выхода, выберите необходимый канал, а затем настройте **Задержка сигнала тревоги** (Post alarm).

После настройки задержки сигнала тревоги сигнал тревоги продолжит работу в течение определенного периода после окончания сигнала тревоги.

Рис. 5–11 Привязка тревожного выхода



5.2.2.5 Привязка эл. почты

При срабатывании сигнала тревоги система автоматически отправляет пользователям эл. письмо.

Привязка адреса эл. почты вступает в силу только при выборе SMTP. Подробнее см. «5.1.3 Адрес эл. почты».

Рис. 5–12 Привязка адреса эл. почты



5.3 Система

В данном разделе описана настройка системных параметров, включая общие параметры, дату и время, учетную запись, безопасность, настройки PTZ, настройки по умолчанию, импорт/экспорт, удаленный режим, автоматическое обслуживание и обновление.

5.3.1 Общие сведения

5.3.1.1 Основные параметры

Вы можете настроить имя устройства, язык и стандарт видео.


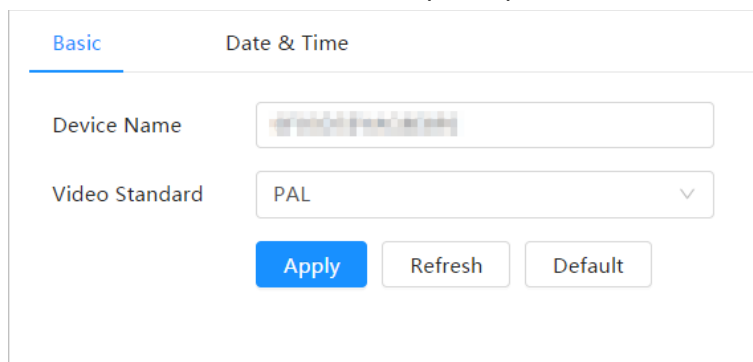
Шаг 1: Выберите  > **Система** (System) > **Общие параметры** (General) > **Основные параметры** (Basic).

Рис. 5–13 Основные параметры



Шаг 2: Выполните конфигурацию общих параметров.

Таб. 5–6 Описание общих параметров

Параметр	Описание
Имя	Введите имя устройства.
Стандарт сжатия видеосигнала	Выберите один из следующих стандартов видео: PAL или NTSC .

Шаг 3: Нажмите кнопку **Применить** (Apply).

5.3.1.2Дата и время

Вы можете настроить формат даты и времени, часовой пояс, текущее время, DST (летнее время) или сервер NTP.


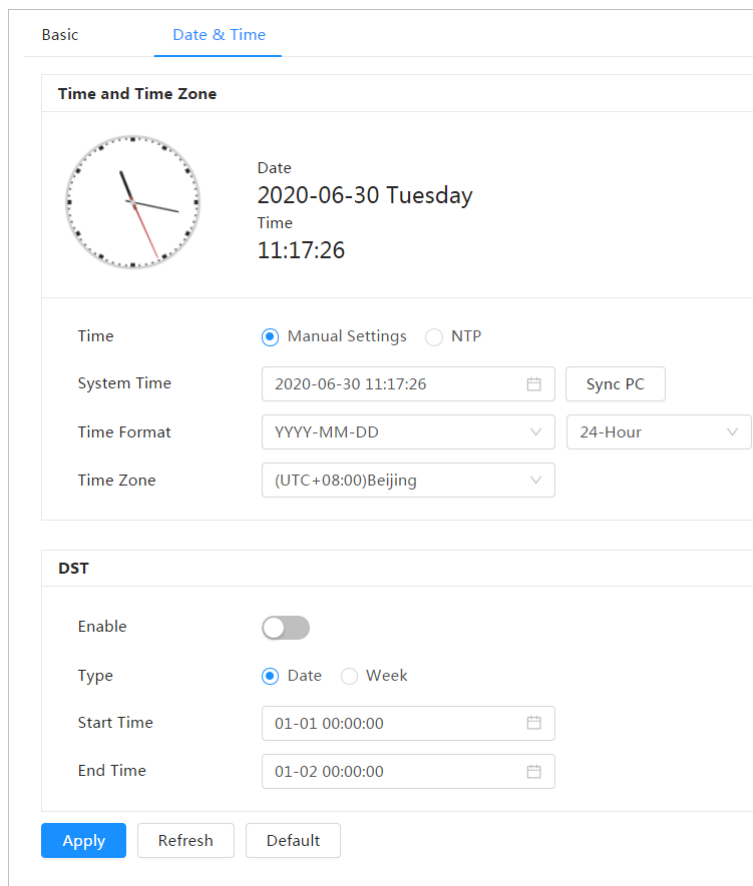
Шаг 1: Выберите  > **Система** (System) > **Общие параметры** (General) > **Дата и время** (Date & Time).


Рис. 5–14 Дата и время



Шаг 2: Выполните конфигурацию параметров даты и времени.

Таб. 5–7 Описание параметров даты и времени

Параметр	Описание
Формат даты	Выполните конфигурацию формата даты.

Параметр	Описание
Время	<ul style="list-style-type: none"> ● Ручная настройка: выполните конфигурацию параметров вручную. ● NTP: при выборе NTP система выполняет синхронизацию времени с интернет-сервером в реальном времени. Вы также можете ввести IP-адрес, часовой пояс, порт и интервал компьютера, на котором установлен сервер NTP для использования NTP.
Формат времени	Выполните конфигурацию формата времени. Вы можете выбрать один из следующих вариантов: 12 часов (12-Hour) или 24 часов (24-Hour).
Часовой пояс	Выполните конфигурацию часового пояса, в котором находится камера.
Текущее время	Выполните конфигурацию системного времени. Нажмите Синхронизация с ПК (Sync PC), и системное время сменится на время ПК.
DST	При необходимости включите DST. Нажмите  и настройте время начала и окончания DST во вкладках Дата (Date) или Неделя (Week).

Шаг 3: Нажмите кнопку **Применить** (Apply).

5.3.2 Учетная запись

Вы можете управлять пользователями, например добавлять, удалять или редактировать их. К категории пользователей относятся администратор, добавленные пользователи и пользователи ONVIF.

Управление пользователями и группами доступно только для пользователей-администраторов.

- Имя пользователя или группы не должно превышать 31 символ и должно включать цифры, буквы, нижнее подчеркивание, дефис, точку и @.
- Пароль должен состоять из 8-32 непустых символов и содержать не менее двух следующих типов символов: прописные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &).
- Максимальное число пользователей — 18, групп — 8.
- Вы можете управлять пользователями индивидуально или в рамках группы, при этом дублирование имен пользователей или групп не допускается. Пользователь может состоять только в одной группе, при этом пользователи группы могут обладать правами в рамках диапазона прав группы.
- Онлайн-пользователи не могут редактировать собственные права.
- По умолчанию существует один администратор, который обладает правами самого высокого уровня.
- Выберите **Анонимный вход** (Anonymous Login), а затем войдите в систему при помощи только IP-адреса, вместо имени пользователя и пароля. Анонимные пользователи обладают только правом предварительного просмотра. Во время анонимного входа в систему нажмите **Выход из системы** (Logout), а затем можно войти в систему под другим именем пользователя.

5.3.2.1 Пользователь

5.3.2.1.1 Добавление пользователя

По умолчанию вы являетесь пользователем-администратором. Вы можете добавлять пользователей и настраивать различные разрешения.


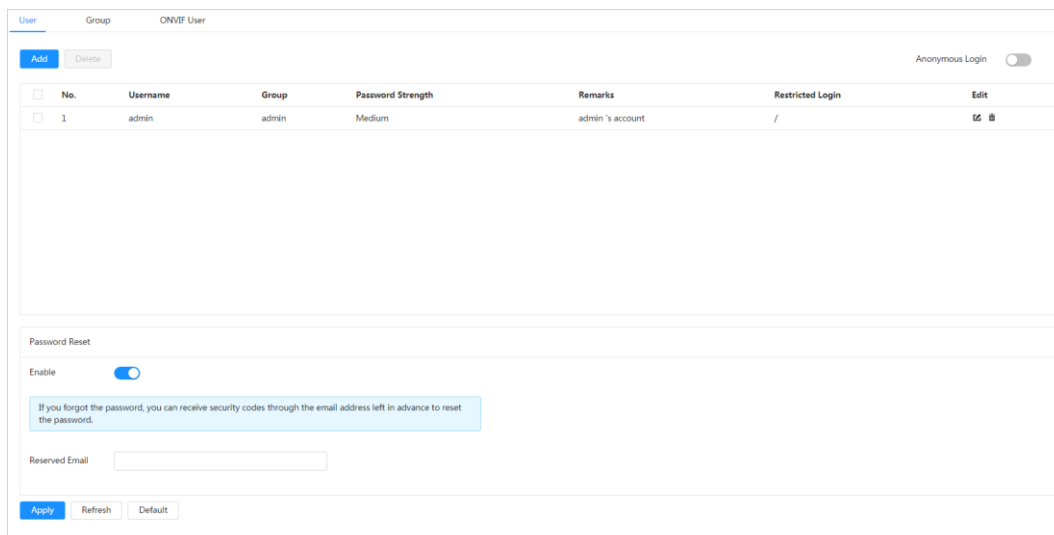


Шаг 1: Выберите  > **Система** (System) > **Учетная запись** (Account) > **Пользователь** (User).

Рис. 5–15 Пользователь



No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
1	admin	admin	Medium	admin's account	/	 

Anonymous Login ☐

Password Reset

Enable ☒

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Reserved Email

Apply Refresh Default

Шаг 2: Нажмите **Добавить** (Add).

Рис. 5–16 Добавить пользователя (система)

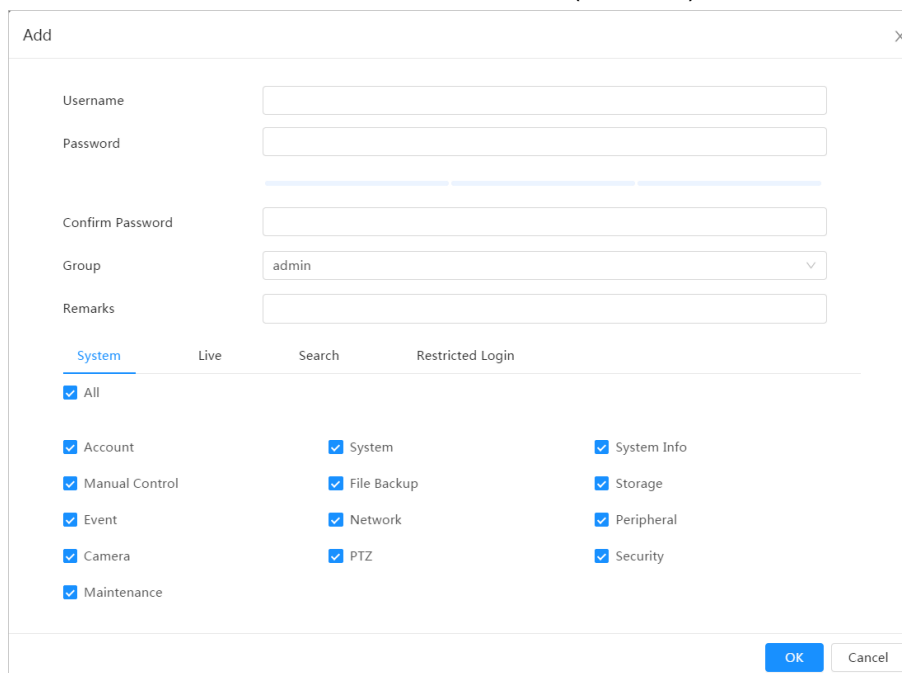
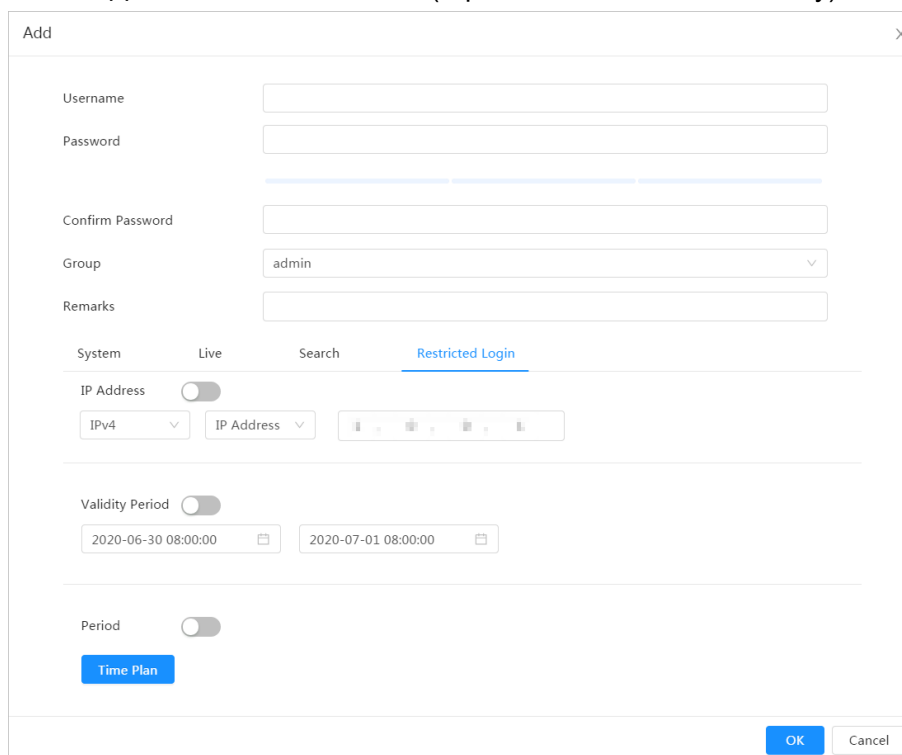



Рис. 5–17 Добавить пользователя (ограниченный вход в систему)



Шаг 3: Выполните конфигурацию параметров пользователя.

Таб. 5–8 Описание параметров пользователя (1)

Параметр	Описание
Имя пользователя	Уникальная идентификация пользователя. Вы не можете использовать существующее имя пользователя.
Пароль	Введите пароль и подтвердите его еще раз.

Параметр	Описание
Подтверждение пароля	Пароль должен состоять из 8-32 непустых символов и содержать не менее двух следующих типов символов: прописные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; : &).
Группа	Группа, в которую входят пользователи. Каждая группа обладает своими правами.
Примечание	Выполните описание пользователя.
Система	<p>Выберите необходимые права.</p>  <p>Рекомендуется предоставлять меньше прав обычным пользователям по сравнению с привилегированными.</p>
Реальное время	Выберите право на просмотр в реальном времени для добавляемого пользователя.
Поиск	Выберите право на поиск для добавляемого пользователя.
Ограниченный вход в систему	<p>Укажите адрес ПК, который позволит определенному пользователю войти в систему камеры, а также срок действия и диапазон времени. Вы можете войти в веб-интерфейс с заданным IP-адресом в заданном диапазоне времени в течение срока действия.</p> <ul style="list-style-type: none"> IP-адрес: вы можете войти в сеть через ПК при помощи заданного IP-адреса. Срок действия: вы можете войти в систему веб-клиента в течение заданного срока действия. Диапазон времени: вы можете войти в систему веб-клиента в рамках заданного диапазона времени. <p>Задайте следующие настройки</p> <ol style="list-style-type: none"> IP-адрес: введите IP-адрес добавляемого хоста. IP-сегмент: введите начальный адрес и конечный адрес добавляемого хоста.

Шаг 4: Нажмите кнопку **Применить** (Apply).


Вновь добавленный пользователь отображается в списке имен пользователей.

Сопутствующие операции

- Нажмите , чтобы изменить пароль, группу, примечания или права.



Для учетной записи администратора возможна только смена пароля.

- Нажмите , чтобы удалить добавленных пользователей. Удаление пользователя-администратора невозможно.



Удаление учетной записи администратора невозможно.

5.3.2.1.2 Сброс пароля

Включите функцию. Для сброса пароля необходимо нажать **Забыли пароль?** (Forget password?) в интерфейсе входа в систему. Подробнее см. «3.2 Сброс пароля».


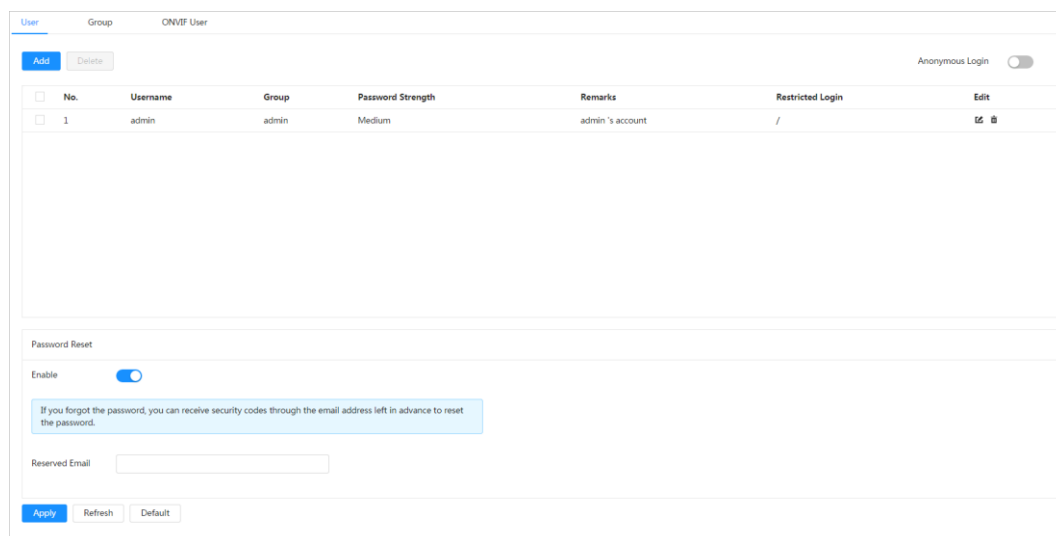


Шаг 1: Выберите  > **Система** (System) > **Учетная запись** (Account) > **Пользователь** (User).

Рис. 5–18 Пользователь



No.	Username	Group	Password Strength	Remarks	Restricted Login	Edit
1	admin	admin	Medium	admin's account	/	 

Password Reset

Enable ☒

If you forgot the password, you can receive security codes through the email address left in advance to reset the password.

Reserved Email

Apply **Refresh** **Default**

Шаг 2: Нажмите ☐ рядом с кнопкой **Включить** (Enable) во вкладке **Сброс пароля** (Password Reset).

Если данная функция не включена, сброс пароля возможен только при сбросе камере.

Шаг 3: Введите зарезервированный адрес эл. почты.

Шаг 4: Нажмите кнопку **Применить** (Apply).

5.3.2.2 Пользователь ONVIF

Вы можете добавить или удалить пользователя ONVIF, а также менять их пароли.


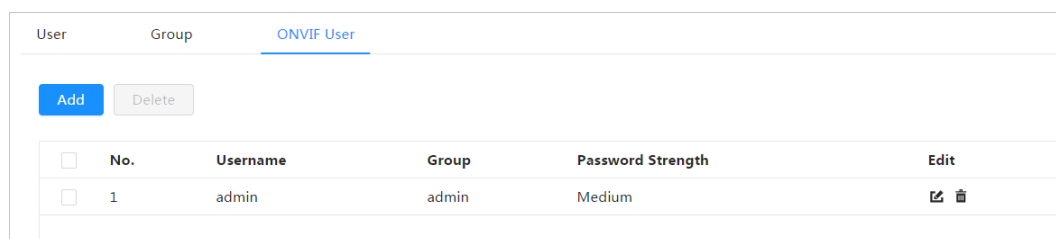


Шаг 1: Выберите  > **Система** (System) > **Учетная запись** (Account) > **Пользователь ONVIF** (ONVIF User).

Рис. 5–19 Пользователь ONVIF



No.	Username	Group	Password Strength	Edit
1	admin	admin	Medium	 

Add **Delete**

Шаг 2: Нажмите **Добавить** (Add).

Рис. 5–20 Добавление пользователя ONVIF



Шаг 3: Выполните конфигурацию параметров пользователя.

Таб. 5–9 Описание параметров пользователя ONVIF

Параметр	Описание
Имя пользователя	Уникальная идентификация пользователя. Вы не можете использовать существующее имя пользователя.
Пароль	Введите пароль и подтвердите его еще раз.
Подтверждение пароля	Пароль должен состоять из 8-32 непустых символов и содержать не менее двух следующих типов символов: прописные буквы, строчные буквы, цифры и специальные символы (за исключением ' " ; &).
Имя группы	Группа, в которую входят пользователи. Каждая группа обладает своими правами.

Шаг 4: Нажмите **ОК**.


Вновь добавленный пользователь отображается в списке имен пользователей.

Сопутствующие операции

- Нажмите , чтобы изменить пароль, группу, примечания или права.



Для учетной записи администратора возможна только смена пароля.

- Нажмите , чтобы удалить добавленных пользователей. Удаление пользователя-администратора невозможно.



Удаление учетной записи администратора невозможно.

5.3.3 Диспетчер

5.3.3.1 Требования

Чтобы обеспечить нормальную работу системы, соблюдайте следующие требования.

- Регулярно проверяйте изображения с камер наблюдения.
- Регулярно очищайте информацию о пользователях и группах пользователей, которые нечасто используются.
- Меняйте пароль каждые три месяца. Подробнее см. «5.3.2 Учетная запись».

- Просматривайте системные журналы и анализируйте их, а также своевременно обрабатывайте сбои.
- Регулярно создавайте резервные копии конфигураций системы.
- Регулярно перезапускайте устройство и удаляйте старые файлы.
- Своевременно обновляйте встроенное ПО.

5.3.3.2 Техническое обслуживание

Вы можете перезапустить систему вручную, а также установить время автоматической перезагрузки и автоматического удаления старых файлов. Данная функция отключена по умолчанию.


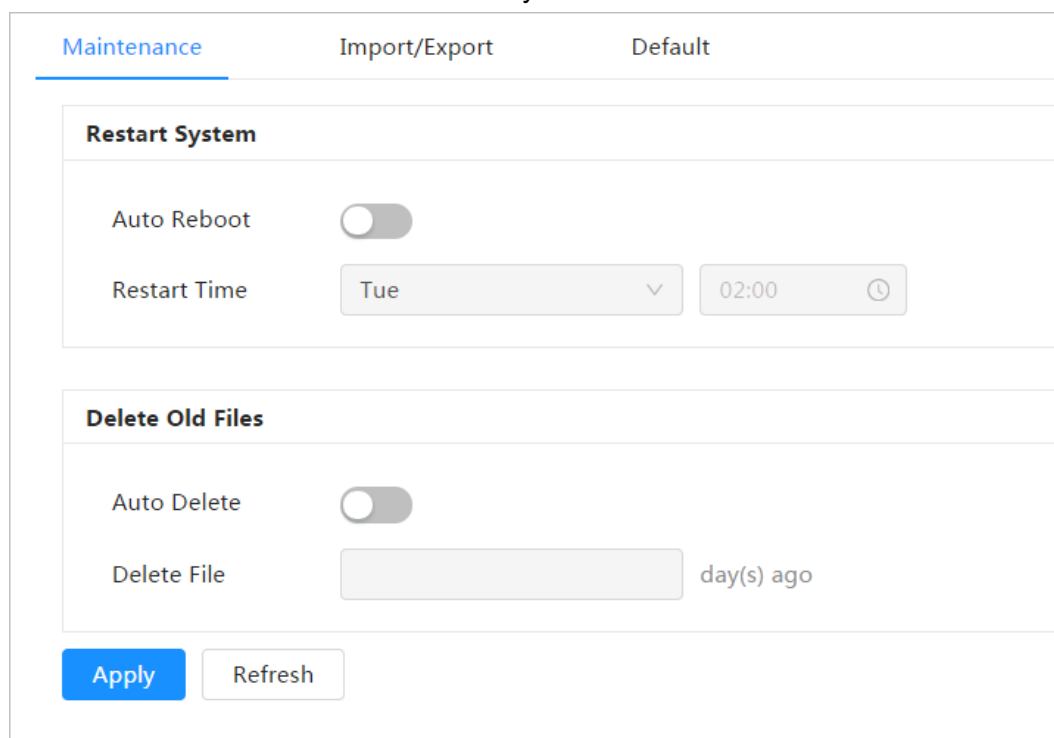


Шаг 1: Выберите  > **Система (System)** > **Диспетчер (Manager)** > **Обслуживание (Maintenance)**.

Рис. 5–21 Обслуживание



Шаг 2: Выполните конфигурацию параметров автоматического обслуживания.

- Нажмите  рядом с кнопкой **Автоматическая перезагрузка (Auto Reboot)** в разделе **Перезагрузка системы (Restart System)** и укажите время перезагрузки. Система автоматически перезагружается в заданное время каждую неделю.
- Нажмите  рядом с кнопкой **Автоматическое удаление (Auto Delete)** в разделе **Удалить старые файлы (Delete Old Files)** и задайте время. Система автоматически выполнит удаление старых файлов в заданное время. Диапазон времени составляет от 1 до 31 дня.



При включении и подтверждении функции **Автоматическое удаление (Auto Delete)** восстановление удаленных файлов невозможно. Используйте эту функцию осторожно.

Шаг 3: Нажмите кнопку **Применить (Apply)**.

5.3.3.3 Импорт/экспорт

- Выполните экспорт файла конфигурации системы для резервного копирования конфигурации системы.
- Импортируйте файл конфигурации системы для быстрой настройки или восстановления конфигурации системы.


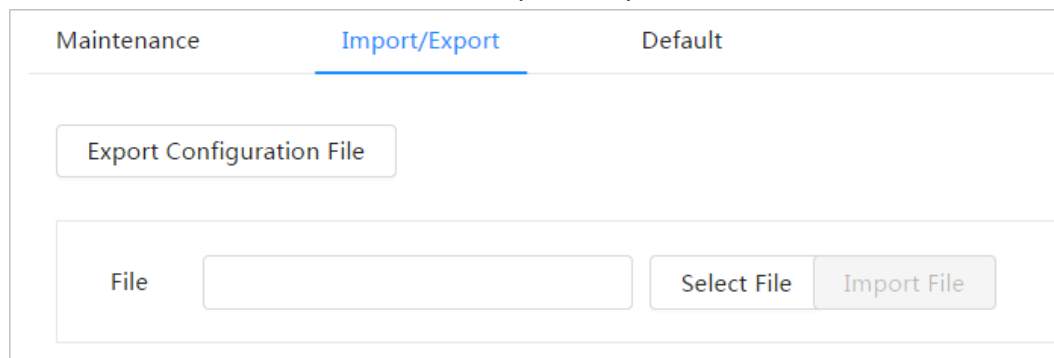
Шаг 1: Выберите  > **Система** (System) > **Диспетчер** (Manager) > **Импорт/экспорт** (Import/Export).

Рис. 5–22 Импорт/экспорт



Шаг 2: Импорт и экспорт.

- Импорт: выберите локальный файл конфигурации и нажмите **Импортировать файл** (Import File), чтобы импортировать файл конфигурации локальной системы в систему.
- Экспорт: нажмите **Экспортировать файл конфигурации** (Export Configuration file), чтобы экспортировать файл конфигурации системы в локальное хранилище.

5.3.3.4 По умолч.

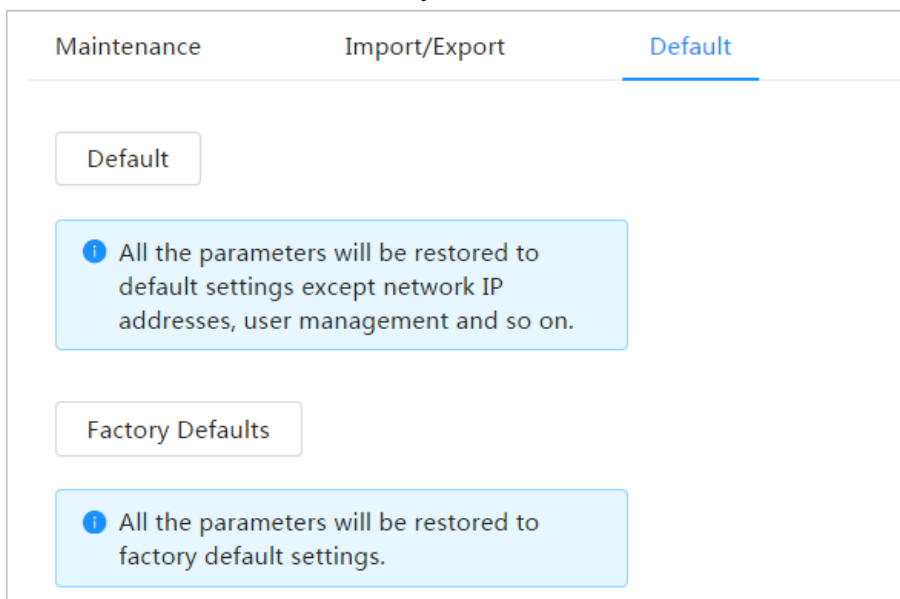
Верните конфигурацию устройства к настройкам по умолчанию или заводским настройкам.

Данная функция позволяет восстановить конфигурацию устройства по умолчанию или вернуться к заводским настройкам.

Выберите  > **Система** (System) > **Диспетчер** (Manager) > **По умолчанию** (Default)

- Нажмите **По умолчанию** (Default). После этого все настройки, за исключением IP-адреса и учетной записи, будут сброшены до настроек по умолчанию.
- Нажмите **Заводские настройки по умолчанию** (Factory Default), и все настройки будут сброшены до заводских.

Рис. 5–23 По умолчанию



5.3.4 Обновление

Обновление до последней версии системы может улучшить работу камеры и повысить стабильность работы.

При использовании неверного файла обновления, перезагрузите устройство. В противном случае некоторые функции не будут работать должным образом.


Шаг 1: Выберите  > **Система** (System) > **Обновить** (Upgrade).

Рис. 5–24 Обновление



Шаг 2: Нажмите **Обзор** (Browse), а затем загрузите файл обновления.

Формат файла обновления — .bin.

Шаг 3: Нажмите **Обновить** (Upgrade).

Начнется обновление.

Приложение 1 Рекомендации о кибербезопасности

Кибербезопасность – это больше, чем просто модное слово: это то, что относится к каждому устройству, подключенному к Интернету. Сетевое видеонаблюдение не застраховано от киберрисков, но принятие основных мер по защите сетей и сетевых устройств делает оборудование менее уязвимыми для атак. Ниже приведены советы и рекомендации по созданию более защищенной системы безопасности.

Обязательные действия, которые необходимо предпринять для обеспечения защиты сети основного оборудования:

1. Используйте надежные пароли

Ознакомьтесь со следующими советами по установке паролей:

- Пароль должен содержать не менее 8 символов.
- Используйте как минимум два типа символов, включая буквы верхнего и нижнего регистра, числа и специальные знаки.
- Не используйте в качестве пароля имя аккаунта в обратном порядке.
- Не используйте последовательные символы, такие как 123, abc и т. д.
- Не используйте одинаковые символы, например 111, aaa и т. д.

2. Своевременно обновляйте прошивку и клиентское программное обеспечение

- В соответствии со стандартной процедурой, принятой в ИТ-индустрии, мы рекомендуем обновлять прошивку вашего оборудования (NVR, DVR, IP-камер и т. д.), чтобы гарантировать, что в системе установлены последние исправления, обеспечивающие безопасность. Когда оборудование подключено к общедоступной сети, рекомендуется включить функцию автоматической проверки обновлений (auto-check for updates), чтобы своевременно получать информацию об обновлениях прошивки, выпущенных производителем.
- Мы предлагаем вам загрузить и использовать последнюю версию клиентского программного обеспечения.

Рекомендации по повышению сетевой безопасности вашего оборудования:

1. Физическая защита

Мы рекомендуем обеспечить физическую защиту оборудования, особенно запоминающих устройств. Например, разместите оборудование в специальном компьютерном зале или в шкафу и обеспечьте хорошо продуманный контроль доступа и управление ключами, чтобы предотвратить несанкционированный доступ персонала к физическому оборудованию с целью его повреждения или подключения съемных устройств (таких как флэш-накопители) через USB порт, последовательный порт и т. д.

2. Регулярно меняйте пароль

Мы рекомендуем регулярно менять пароли, чтобы снизить риск их подбора или взлома.

3. Своевременно вводите и обновляйте информацию для сброса паролей

Оборудование поддерживает функцию сброса пароля. Своевременно укажите необходимую информацию для сброса пароля, включая адрес электронной почты конечного пользователя и контрольные вопросы для защиты пароля. Если информация изменится, обновите ее вовремя. При введении контрольных вопросов для защиты пароля рекомендуется не использовать те, которые легко угадать.

4. Включите блокировку аккаунта

Функция блокировки аккаунта включена по умолчанию, и мы рекомендуем оставить ее включенной, чтобы гарантировать безопасность аккаунта. Если злоумышленник несколько раз попытается войти в систему с неправильным паролем, соответствующий аккаунт и исходный IP-адрес будут заблокированы.

5. Измените порты HTTP и других служб, используемые по умолчанию

Чтобы снизить риск того, что посторонние смогут угадать, какие порты вы используете, мы рекомендуем изменить номера портов HTTP и других служб, используемые по умолчанию, на любые другие из диапазона от 1024 до 65535.

6. Включите HTTPS

Мы предлагаем включить HTTPS, чтобы пользоваться веб-службой через безопасный канал связи.

7. Присоедините MAC-адрес

Мы рекомендуем привязать IP-адрес и MAC-адрес шлюза к оборудованию, чтобы снизить риск спуфинга ARP.

8. Грамотно назначайте аккаунты и полномочия

Грамотно добавляйте пользователей и назначайте им минимальный набор полномочий в соответствии с требованиями бизнеса и администрирования.

9. Отключите ненужные службы и выберите безопасные режимы

Если в этом нет необходимости, рекомендуется отключить некоторые службы, такие как SNMP, SMTP, UPnP и т. д., чтобы снизить риски.

При необходимости настоятельно рекомендуется использовать безопасные режимы, включая нижеследующие:

- SNMP: Выберите SNMP v3 и установите надежные пароли шифрования и аутентификации.
- SMTP: Выберите TLS для доступа к почтовому серверу.
- FTP: Выберите SFTP и установите надежные пароли.
- Точка доступа (AP): Выберите режим шифрования WPA2-PSK и установите надежные пароли.

10. Используйте шифрование для передачи аудио и видео

Если содержимое ваших аудио- и видеоданных очень важно или конфиденциально, рекомендуется использовать функцию зашифрованной передачи, чтобы снизить риск перехвата этих данных во время передачи.

Напоминание: шифрование вызовет некоторое снижение скорости передачи.

11. Выполняйте проверки безопасности

- Проверяйте онлайн-пользователей: мы рекомендуем вам регулярно проверять онлайн-пользователей, чтобы отследить вход устройства в систему без авторизации.
- Проверяйте журнал оборудования: просматривая журналы, вы можете узнать IP-адреса, которые использовались для входа в ваши устройства, и их основные операции.

12. Используйте сетевой журнал

Из-за ограниченного объема памяти оборудования объем данных, сохраняемых в журнале, также ограничен. Если вам нужно хранить журнал в течение длительного времени, рекомендуется включить функцию сетевого журнала, чтобы гарантировать

отслеживание информации путем синхронной передачи критических данных на сервер сетевого журнала.

13. Создайте безопасную сетевую среду

Чтобы повысить уровень безопасности оборудования и снизить потенциальные киберриски, рекомендуется принять перечисленные ниже меры.

- Отключите функцию сопоставления портов маршрутизатора, чтобы избежать прямого доступа к устройствам интрасети из внешней сети.
- Сеть должна быть разделена и изолирована в соответствии с реальными сетевыми потребностями. Если между двумя подсетями не требуется обмениваться данными, рекомендуется использовать VLAN, сетевой стандарт GARP и другие технологии для разделения сети, чтобы добиться эффекта сетевой изоляции.
- Выберите систему аутентификации доступа 802.1x, чтобы снизить риск несанкционированного доступа к частным сетям.
- Включите функцию фильтрации IP/MAC-адресов, чтобы ограничить диапазон хостов, которым разрешен доступ к устройству.

СОДЕЙСТВОВАТЬ БЕЗОПАСНОСТИ ОБЩЕСТВА, РАЗВИВАТЬ УМНЫЕ
ТЕХНОЛОГИИ ДЛЯ ЖИЗНИ

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Адрес: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China (Китайская Народная Республика) |

Сайт: www.dahuasecurity.com | Индекс: 310053

Эл. почта: overseas@dahuatech.com | Факс: +86-571-87688815 | Тел.: +86-571-87688883