BOSCH

BVMS

ru Руководство по конфигурации

Содержание

1 Использование справки

Замечание!
В данном документе описываются некоторые функции, недоступные для BVMS Viewer. Подробные сведения о различных редакциях BVMS см. www.boschsecurity.com и BVMS Руководство по быстрому выбору: Руководство по быстрому выбору BVMS.

Чтобы получить дополнительные сведения о выполнении определенных действий в системе BVMS, откройте интерактивную справку одним из следующих способов.

Для использования вкладок «Содержание», «Указатель» и «Поиск» выполните следующие действия.

- В меню **Справка** нажмите **Показать справку**. Используйте кнопки и ссылки для перехода к соответствующим разделам справки.

Для вызова справки в окне или диалоговом окне выполните следующие действия.

- На панели инструментов щелкните значок  .

ИЛИ

- Нажмите клавишу F1 для вызова справки по окну программы или диалоговому окну.

1.1 Поиск информации

Информацию в справке можно искать несколькими способами.
Для поиска информации в интерактивной справке:

1. В меню **Справка** выберите пункт **Справка**.
2. Если левая часть скрыта, нажмите кнопку **Показать**.
3. В окне "Справка" выполните следующее:

Элемент	Действие
Содержание	Отобразить содержание интерактивной справки. Нажмите по очереди каждый значок книги, чтобы открыть нужный раздел. Затем нажмите ссылку на страницу для отображения соответствующего раздела справа.
Указатель	Начать поиск определенных слов или выражений либо сделать выбор из списка ключевых слов указателя. Дважды нажмите ключевое слово для отображения соответствующего раздела справа.
Поиск	Найти слова или выражения в содержании данного раздела. Введите слово или выражение в текстовое поле, нажмите клавишу ВВОД и выберите нужный раздел из списка.

Текст интерфейса пользователя выделен **жирным шрифтом**.

- Щелкните подчеркнутый текст или элемент приложения, на который указывает стрелка..

Дополнительная информация

- Нажмите для отображения раздела, содержащего сведения об используемом вами окне приложения. В данном разделе содержатся сведения об управляющих элементах окна приложения.

Понятия, Страница 23 предоставляет основные сведения по выбранным вопросам.

Замечание!
Этот символ указывает на потенциальный риск повреждения собственности или потери данных.

1.2 Печать Справки

При использовании интерактивной справки можно распечатать разделы и сведения непосредственно из окна обозревателя.

Чтобы распечатать раздел Справки:

1. Щелкните правой кнопкой мыши в области справа и выберите пункт **Печать**. Откроется диалоговое окно **Печать**.
2. Нажмите кнопку **Печать**.

⇨ Раздел будет распечатан на указанном принтере.

2 Пояснения к предупреждающим сообщениям о соблюдении мер безопасности

В настоящем руководстве для привлечения внимания к отдельным ситуациям используются следующие символы и обозначения.

Опасно!
Высокая степень риска: данный символ указывает на возможность возникновения опасной ситуации, например «Опасное напряжение» внутри изделия. Несоблюдение соответствующих указаний может привести к поражению электрическим током, серьезным травмам или даже к смертельному исходу.

Внимание!
Средняя степень риска: обозначает потенциально опасную ситуацию. Несоблюдение соответствующих указаний может привести к травмам малой или средней тяжести. Обращает внимание пользователя на важные инструкции, касающиеся эксплуатации устройства.

Внимание!
Низкая степень риска: обозначает потенциально опасную ситуацию. Несоблюдение соответствующих указаний может привести к повреждению оборудования или данного устройства.

Замечание!
Данный символ обозначает информацию или корпоративную политику, которая прямо или косвенно относится к безопасности персонала или защите оборудования.

3 Введение

Нажмите ссылку, чтобы посмотреть, какие лицензии на программное обеспечение с открытым исходным кодом используются в BVMS и мобильном приложении: http://www.boschsecurity.com/oss/

Подпадает под действие одного или нескольких патентов, перечисленных на patentlist.hevcadvance.com.

В этой инструкции приводятся основные сведения о настройке с помощью BVMS. Более подробная информация и пошаговые инструкции приведены в руководстве по конфигурации, а также в интерактивной справке.

BVMS

BVMS интегрирует цифровые видео-, аудиопотоки и данные по любой IP-сети. Система состоит из следующих программных модулей:

- Management Server
- VRM (Video Recording Manager)
- Operator Client
- Configuration Client

Для работы системы следует выполнить следующие задачи:

- Установить службы (Management Server и VRM)
- Установить Operator Client и Configuration Client
- Установить подключение к сети
- Подключить устройства к сети
- Базовая конфигурация:
  - Добавить устройства (например, поиском в сети)
  - Построить логическую структуру
  - Настроить расписания, камеры, события и тревоги
  - Настроить группы пользователей

BVMS Export Player

BVMS Export Player отображает экспортированные записи.

BVMS Viewer

BVMS Viewer — это приложение системы IP-видеонаблюдения для просмотра в реальном времени и воспроизведения видео с сетевых камер и видеорегистраторов Bosch. Пакет программного обеспечения состоит из Operator Client для просмотра в реальном времени и воспроизведения видео и Configuration Client. BVMS Viewer поддерживает текущую линейку продуктов видеонаблюдения от Bosch, а также устаревшие видеоустройства Bosch.

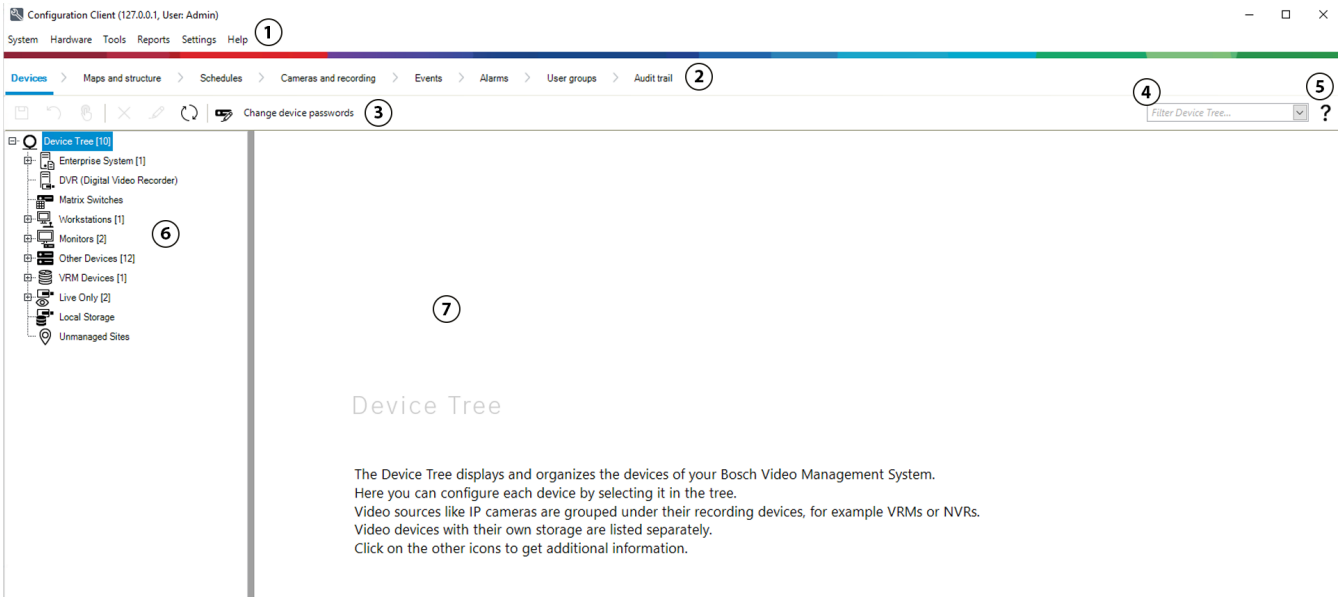
Нажмите ссылку, чтобы посмотреть, какие лицензии на программное обеспечение с открытым исходным кодом используются в BVMS Viewer: http://www.boschsecurity.com/oss.

BVMS Configuration Client

Начать работу с BVMS Configuration Client лучше всего с настройки устройств и логического дерева. Затем на соответствующих страницах можно настроить расписания, записи, события и сигналы тревоги для устройств. Последний этап заключается в настройке групп пользователей на одноименной странице. После настройки всех страниц слева направо оператор может приступить к работе с Operator Client.

После настройки каждой страницы сохраните конфигурацию, нажав  в меню «Инструменты».

Чтобы отобразить изменения в BVMS Operator Client нажмите  .



1	Панель меню	Позволяет выбрать команду меню.
2	Панель вкладок	Позволяет настроить все необходимые действия слева направо.
3	Панель инструментов	Отображает доступные кнопки согласно активной вкладке. Наведите курсор мыши на значок, чтобы отобразить всплывающую подсказку.
4	Панель поиска	Позволяет выполнять поиск определенного устройства и соответствующих родительских элементов в дереве устройств.
5	Значок справки	Отображает интерактивную справку по BVMS Configuration Client.
6	Окно выбора	Иерархический список всех доступных устройств системы.
7	Окно конфигурации	Позволяет настроить выбранное устройство.

BVMS Operator Client

3.1 Версии BVMS

Различные версии BVMS обеспечивают полную масштабируемость и возможность расширения системы в соответствии с вашими потребностями.
Доступны следующие версии BVMS:

- BVMS Professional
- BVMS Enterprise

– BVMS Plus
– BVMS Lite
– BVMS Viewer

BVMS Viewer и BVMS Professional – чисто программные продукты. Их можно использовать их на устройствах Bosch DIVAR IP.
Использовать BVMS Lite и BVMS Plus можно и на устройствах Bosch DIVAR IP либо в качестве исключительно программных продуктов на любом другом аппаратном обеспечении.
Подробные сведения о различных BVMS редакциях: www.boschsecurity.com и в руководстве BVMS по быстрому выбору:
Руководство по быстрому выбору BVMS.

3.2 Обзор активации лицензии BVMS

В данной главе содержится обзор активации лицензии BVMS.

Заказ лицензии

– Заказ через Bosch стол заказов.
– Подтверждение заказа содержит новый ID заказа программного обеспечения, который требуется для активации программного обеспечения в дальнейшем.
– Для BVMS 11.0 BVMSбазовые лицензии и лицензии на расширение больше не зависят от версии программного обеспечения.

Активация лицензии

– Bosch Remote Portal (https://www.remote.boschsecurity.com) заменяет собой Bosch **Диспетчер лицензий**.
– Новым пользователям необходимо зарегистрироваться в Bosch Remote Portal.
– Обязательными данными для ввода при активации лицензии являются файл информации о системе и ID заказа программного обеспечения.
– Выходные данные файла лицензии с Remote Portal содержит все сведения об активации. Добавьте этот файл в установленную BVMS систему.
– В процессе активации определяется дата начала гарантийного периода на программное обеспечение. Дата окончания отображается в **Диспетчер лицензий** для BVMS Configuration Client.

Процесс активации лицензии программного обеспечения

Чтобы активировать лицензии своего программного обеспечения, сделайте следующее:

1. Закажите программные продукты

– Закажите программные продукты по стандартной Bosch процедуре заказа.
– Заказ программного обеспечения может включать один или несколько продуктов одного или нескольких выпусков продукта.

2. Получите ID заказа программного обеспечения
– Результатом заказа является подтверждение заказа программного обеспечения, содержащее ID заказа программного обеспечения.
– ID заказа программного обеспечения позволяет подключить установленное ПО (на операционную систему и аппаратное обеспечение) к заказанным программным продуктам.
3. Активируйте лицензию
– Обязательными данными ввода для активации лицензии является файл информации о системе, описывающий конкретную операционную систему и оборудование, на которое устанавливается ПО.
– При активации ID заказа программного обеспечения объединяется с установленным ПО, и на выходе создается файл лицензии.
– Момент активации определяет свойства системы, например, дату начала и окончания гарантии на ПО.
4. Активируйте программное обеспечение
– Для активации программного обеспечения добавьте файл лицензии в установленное программное обеспечение.
– Файлы лицензии позволяют использовать функции BVMS в соответствии с активированными элементами.

Замечание!
В файле лицензии содержатся следующие сведения об активации:
- BVMS выпуск продукта
- BVMS допустимая версия
- Дата истечения срока действия программного обеспечения
- Число лицензий на расширение и функции

См.
– *Активация лицензии на программное обеспечение, Страница 77*

4 Обзор системы

Замечание!
В данном документе описываются некоторые функции, недоступные для BVMS Viewer. Подробные сведения о различных редакциях BVMS см. www.boschsecurity.com и BVMS Руководство по быстрому выбору: Руководство по быстрому выбору BVMS.

Если вы планируете установить и настроить систему BVMS, примите участие в обучении по системе BVMS.
Поддерживаемые версии аппаратного и микропрограммного обеспечения и другую важную информацию см. в замечаниях к выпуску текущей версии BVMS.
Сведения о компьютерах, на которые можно установить систему BVMS, см. в технических характеристиках рабочих станций и серверов Bosch.
Программные модули BVMS можно устанавливать на один компьютер.

Важные компоненты

Компонент	Описание
Management Server (доступно для выбора при установке)	Управление потоком, обработка тревог, управление приоритетами, журнал Management, управление пользователями, управление состояниями устройств. Дополнительная лицензия Enterprise System: управление группами Enterprise User Groups и учетными записями Enterprise Accounts.
Config Wizard	Простая и быстрая настройка системы записи.
Configuration Client (доступно для выбора при установке)	Конфигурирование системы и администрирование для Operator Client.
Operator Client (доступно для выбора при установке)	Наблюдение в режиме реального времени, поиск сохраненных данных и воспроизведение, тревоги и доступ к нескольким компьютерам Management Server одновременно.
Video Recording Manager (доступно для выбора при установке)	Распределение объема хранилища на устройствах iSCSI по кодерам при одновременном распределении нагрузки между несколькими устройствами iSCSI. Потоковая передача видео- и аудиоданных с iSCSI на клиенты Operator Client.
Mobile Video Service (доступно для выбора при установке)	Предоставление службы транскодирования, которая транскодирует видеопоток в режиме реального времени и записанное видео с камеры, настроенной в системе BVMS в соответствии с доступной пропускной способностью сети. Эта служба позволяет видеоклиентам, таким как клиенты для iPhone или браузера, получать транскодированные потоки, например при ненадежном подключении к сети с низкой пропускной способностью.
Веб-клиент	Может использоваться для доступа к транслируемым видеоданным и воспроизведения видеозаписи через веб-браузер.

Компонент	Описание
Мобильное приложение	Это приложение можно использовать на iPhone или iPad для доступа к транслируемым видеоданным и воспроизведения видеозаписи.
Bosch Video Streaming Gateway (доступно для выбора при установке)	Обеспечивает интеграцию камер сторонних производителей, например в сетях с низкой пропускной способностью.
Cameo SDK (доступно для выбора при установке)	Комплект Cameo SDK используется для встраивания областей изображений BVMS, как получаемых в режиме реального времени, так и записанных, во внешние приложения сторонних производителей. Области изображений используют разрешения пользователя на основе BVMS. Комплект Cameo SDK предоставляет набор функций BVMS Operator Client, позволяющий создавать приложения, сходные с Operator Client.
Client Enterprise SDK	Комплект Client Enterprise SDK используется для управления и мониторинга поведения Operator Client в системе Enterprise System с помощью внешних приложений. Этот комплект разработчика ПО позволяет просматривать устройства, доступные включенному и соединенному с сетью клиенту Operator Client, и управлять некоторыми функциями интерфейса пользователя.
Client SDK / Server SDK	Комплект Server SDK используется для управления и мониторинга сервера Management Server с помощью сценариев и внешних приложений. Эти интерфейсы можно использовать при наличии действующей учетной записи администратора. Комплект Client SDK используется для управления и мониторинга клиента Operator Client с помощью сценариев (часть конфигурации соответствующего сервера) и внешних приложений.

4.1 Требования к аппаратному оборудованию

См. технические характеристики для BVMS. Имеются также технические характеристики для различных платформ ПК.

4.2 Требования к программному обеспечению

Невозможно установить BVMS Viewer туда же, где установлен какой-либо другой компонент системы BVMS.
См. технические характеристики для BVMS.

4.3 Лицензионные требования

Доступные лицензии указаны в технических характеристиках BVMS.

5 Понятия

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

В данном разделе содержится основная информация по данным вопросам.

5.1 Основы проектирования BVMS

Система с одним сервером управления, Страница 23
Одна система BVMS Management Server обеспечивает поддержку, мониторинг и управление до 2000 камер или кодеров.

Enterprise System, Страница 24
Enterprise Management Server обеспечивает одновременный доступ к нескольким Management Servers. Enterprise System позволяет получить полный доступ к событиям и тревогам из нескольких подсистем.

Server Lookup, Страница 25
Функция Server Lookup предоставляет список доступных BVMSManagement Servers для BVMSOperator Client. Оператор может выбрать сервер из списка доступных. При подключении к Management Server клиент имеет полный доступ к Management Server.

Unmanaged site, Страница 27
Устройства могут быть сгруппированы в unmanaged sites. Устройства группы unmanaged sites не контролируются при помощи Management Server. Management Server предоставляет список unmanaged sites для Operator Client. Оператор может по требованию подключаться к объекту и получать доступ к видеоинформации в режиме реального времени и записанным видеоданным. События и обработка тревог недоступны для функции unmanaged site.

5.1.1 Система с одним сервером управления

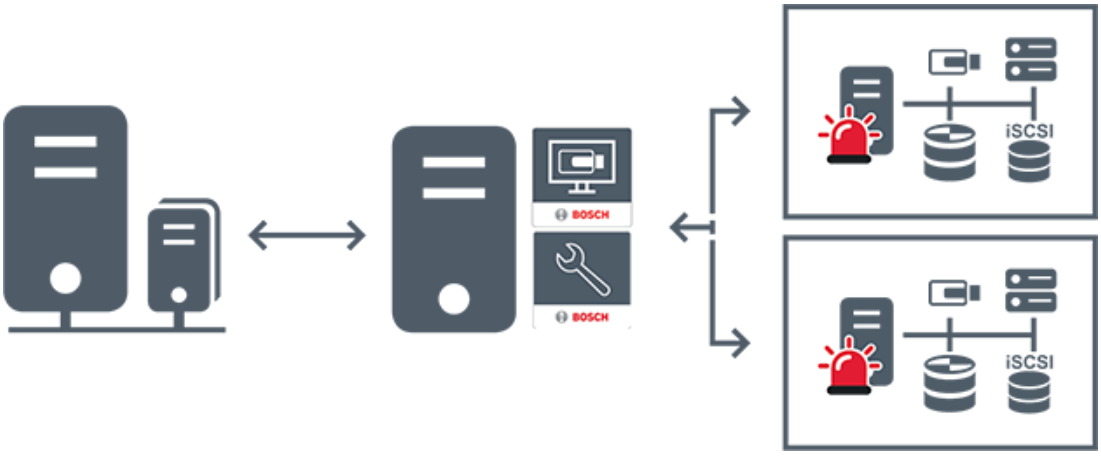
- Один BVMSManagement Server может обслуживать до 2000 каналов.
- BVMS Management Server обеспечивает обслуживание, мониторинг и управление всей системы.
- BVMSOperator Client подключен к Management Server, принимает события и тревоги с BVMSManagement Server и отображает данные в режиме реального времени и воспроизведения записей.
- В большинстве случаев все устройства находятся в одной локальной сети с высокой пропускной способностью и низкой задержкой.

Функции
- Конфигурационные данные
- Журнал событий
- Профили пользователей
- Приоритеты пользователей
- Лицензирование
- Управление событиями и тревогами

	Отображение в режиме реального времени, воспроизведение записей, события, тревоги
	Management Server
	Operator Client / Configuration Client
	Камеры
	VRM
iSCSI	iSCSI
	Другие устройства.

5.1.2 Enterprise System

- Назначением системы уровня BVMS Enterprise System предоставляет возможнсть пользователю программы Operator Client для одновременного доступа к нескольким Management Servers (подсистемам).
- Клиенты при подключении к серверу Enterprise имеют доступ ко всем камерам и записям из подсистем.
- При подключении к серверу Enterprise клиенты в реальном времени получают все события и тревоги от всех подсистем.
- Характерные области применения:
  - Метрополитены
  - Аэропорты



	Отображение в режиме реального времени, воспроизведение записей, события, тревоги
	BVMS Enterprise Management Server
	BVMS Operator Client / Configuration Client
	Подсистема BVMS

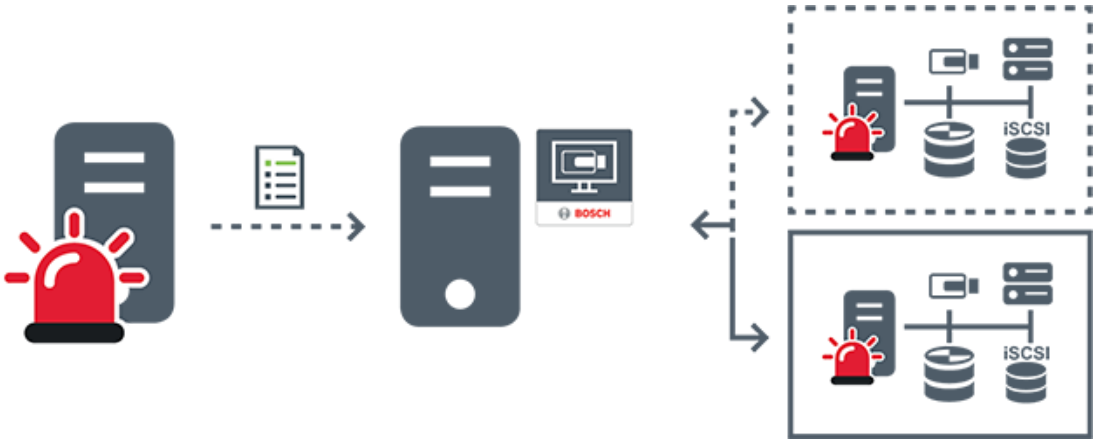
См.

- *Создание системы Enterprise, Страница 88*
- *Настройка списка серверов для корпоративной системы, Страница 88*
- *Настройка пользователей, разрешений и корпоративного доступа, Страница 364*
- *Доступ к системе, Страница 76*

5.1.3 Server Lookup

- Функция BVMS Server Lookup позволяет операторам подключаться к BVMSManagement Server из доступного списка серверов.
- Один пользователь Configuration Client или Operator Client может последовательно подключаться к нескольким системным точкам доступа.
- Системные точки доступа могут быть Management Server или Enterprise Management Server.
- Server Lookup использует специальный Management Server для размещения списка серверов.
- Функции Server Lookup и Management Server или Enterprise Management Server могут быть запущены на одном компьютере.
- Server Lookup поддерживает поиск системных точек доступа по имени или описанию.

– Operator Client, подключенный к Management Server, принимает события и тревоги с BVMS Management Server и отображает данные в режиме реального времени и воспроизведения записей.



	Отображение по требованию в режиме реального времени, воспроизведение записей, события, тревоги — подключено
	Отображение по требованию в режиме реального времени, воспроизведение записей, события, тревоги — не подключено
	Management Server
	Список серверов
	Operator Client
	Подключенная система BVMS из списка серверов
	Неподключенная система BVMS из списка серверов

См.

- *Настройка Server Lookup, Страница 133*
- *Страница «Список серверов/Адресная книга», Страница 132*
- *Использование просмотра сервера, Страница 76*
- *Экспорт списка серверов, Страница 134*
- *Импорт списка серверов, Страница 134*

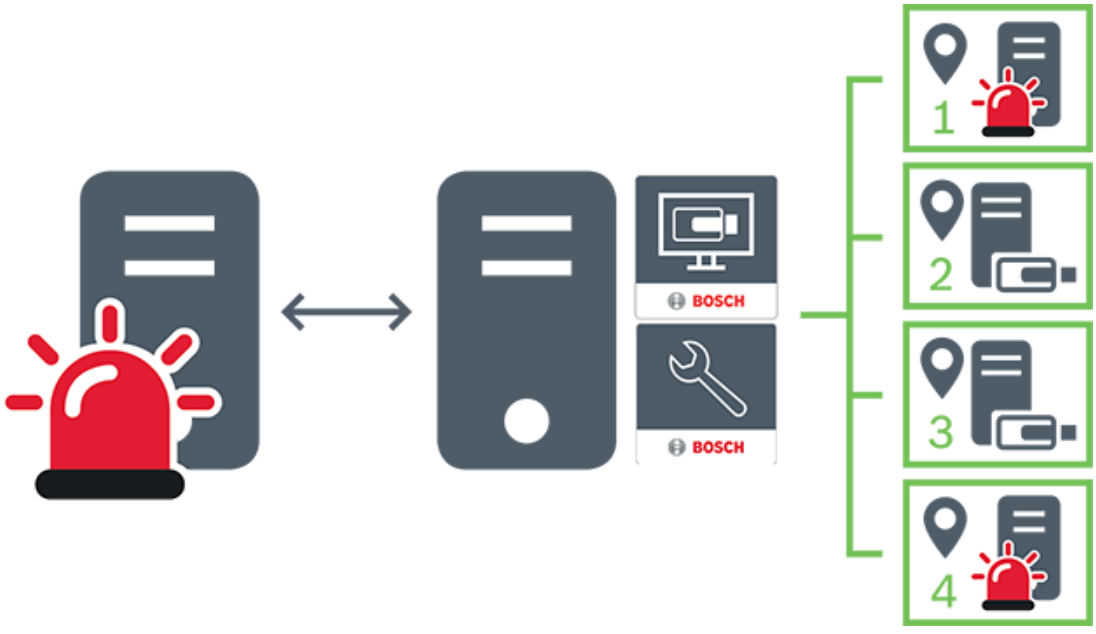
5.1.4 Unmanaged site

- Вариант построения системы BVMS со множеством небольших подсистем.
- Он позволяет настроить до 9999 местоположений в одном BVMS Management Server
- Операторы имеют доступ к видеоданным в реальном времени и записям с 20 sites одновременно.
- Для упрощения навигации объекты sites можно сгруппировать по папкам или расположить на картах. Предустановленные имя пользователя и пароль позволяют операторам быстро подключаться к site.

Функция unmanaged site поддерживает систему BVMS на основе IP, а также аналоговые решения DVR:

- Аналоговые регистраторы Bosch DIVAR AN 3000/5000
- Регистраторы DIVAR hybrid
- Регистраторы DIVAR network
- DIP 3000/7000 устройств записи на основе IP
- Отдельная система BVMS Management Server

Для добавления объекта site для централизованного мониторинга требуется только лицензия на каждый объект site; это не зависит от количества каналов на объекте site.



	Отображение в режиме реального времени, воспроизведение записей, события, тревоги
	Отображение в режиме реального времени по требованию и воспроизведение видеотрафика
	Management Server

	Operator Client / Configuration Client
	site
	DVR

См.

– *Добавление объекта unmanaged site вручную, Страница 221*

5.2 Запись

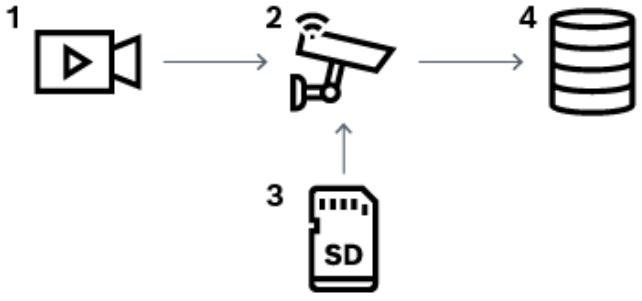
В данной главе описываются различные функции системы, связанные с записью и воспроизведением.

5.2.1 Автоматическая компенсация сети (ANR)

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

Использование по назначению

При сбое сети или центрального хранилища данных функция ANR обеспечивает передачу кодером записи, помещенной в локальный буфер, за недостающий период времени в центральное хранилище после устранения неполадки.
На следующем рисунке показана передача видеоданных после устранения неполадки сети или хранилища.



1	Видео
2	Кодер, IP-сеть
3	SD-карта (кольцевой буфер)

4	Получатель iSCSI (центральное хранилище)

Пример. Работа при сбое сети
Если возникает неожиданный сбой сети, функция ANR отправляет в центральное хранилище сохраненную в локальный буфер запись, когда доступ к сети восстанавливается.

Пример. Сохранение видеоданных при отсутствии доступа к сети
Поезд метро не имеет сетевого соединения с центральным хранилищем, когда он находится между станциями. Помещенную в буфер запись можно передавать в центральное хранилище только во время обычных остановок.
Проследите за тем, чтобы время, необходимое для передачи помещенной в буфер записи, не превышало продолжительность остановки.

Пример. ANR для записи по тревоге
Данные, предшествующие записи по тревоге, хранятся локально. Эти данные, предшествующие записи по тревоге, передаются в центральное хранилище только в случае срабатывания сигнала тревоги. Если сигнал тревоги не срабатывает, эти избыточные данные, предшествующие записи по тревоге, не передаются в центральное хранилище и, соответственно, не нагружают сеть.

Ограничения

Замечание!
Если в кодере заданы пароли для режимов user и live, воспроизведение с локальных носителей данных использовать невозможно. При необходимости снимите эти пароли.

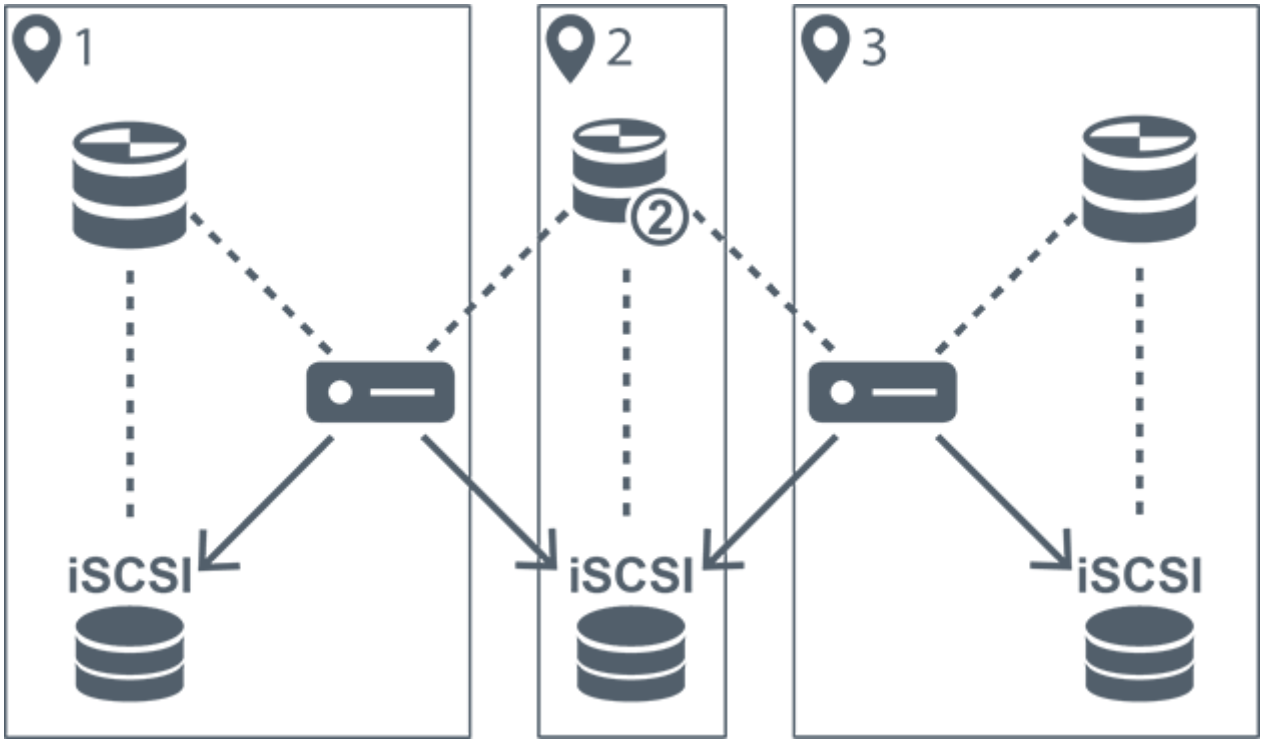
Функция ANR работает только с записью VRM.
Функция ANR не работает с кодером, для которого настроено безопасное подключение для отображения в реальном времени.
Для использования функции ANR необходимо предварительно настроить носитель данных кодера.
Кодер, для которого выполняется настройка функции ANR, должен иметь версию микропрограммного обеспечения 5.90 или выше. Не все типы кодеров поддерживают функцию ANR.
Функцию ANR невозможно использовать с двойной записью.
Система хранения iSCSI должна быть настроена соответствующим образом.
В следующем перечне приводятся возможные причины, не позволяющие настроить функцию ANR.
- Кодер недоступен (неверный IP-адрес, сбой сети и т. п.).
- Носитель данных кодера недоступен или находится в режиме "только чтение".
- Неверная версия микропрограммного обеспечения.
- Тип кодера не поддерживает функцию ANR.
- Включена двойная запись.

См.
- *Настройка устройства iSCSI, Страница 201*
- *Настройка носителей данных кодера, Страница 86*
- *Настройка функции ANR, Страница 314*

5.2.2 Двойная / резервная запись

Использование по назначению

Основной VRM обеспечивает нормальную запись с камер, входящих в систему. Для выполнения двойной записи с камер используется дополнительный VRM.
Двойная запись позволяет записывать видеоданные с одной камеры в разных местах. Двойная запись обычно выполняется с различными настройками потока и режимами записи. В качестве особого случая двойной записи можно настроить зеркальную запись, когда один и тот же видеосигнал записывается дважды в разных местах.
Двойная запись выполняется путем использования 2 серверов VRM, управляющих несколькими устройствами iSCSI, которые могут быть расположены в разных местах. Дополнительный VRM может обеспечивать управление дополнительной записью для нескольких основных VRM.
Пользователь может выбрать из записей, выполненных с помощью основного диспетчера VRM, и записей, выполненных с помощью дополнительного диспетчера VRM. При работе с одной камерой пользователь может переключиться к записям дополнительного или основного VRM. Пользователь также может отобразить записи одной и той же камеры, выполненные с помощью основного VRM и дополнительного VRM, одновременно.
Для двойной записи во время установки необходимо установить дополнительный диспетчер VRM.
Резервный диспетчер VRM используется для продолжения записи отказавшего компьютера основного VRM или дополнительного VRM.
На следующем рисунке приведен пример использования двойной записи.



1	Объект 1		Кодер
2	Центральный объект	iSCSI	Устройство хранения iSCSI

3	Объект 2	-------	Управляющее соединение
	Основной VRM	⟶	Видеопоток
	Вторичный VRM		

Ограничения

Двойную запись невозможно использовать с функцией ANR.

Cameo SDK поддерживает только воспроизведение основной записи.

См.

- *Настройка двойного режима записи в Таблице камер, Страница 314*
- *Добавление зеркального диспетчера VRM вручную, Страница 184*
- *Добавление резервного диспетчера VRM вручную, Страница 183*
- *Страница Камеры, Страница 297*

5.2.3 Режимы записи VRM

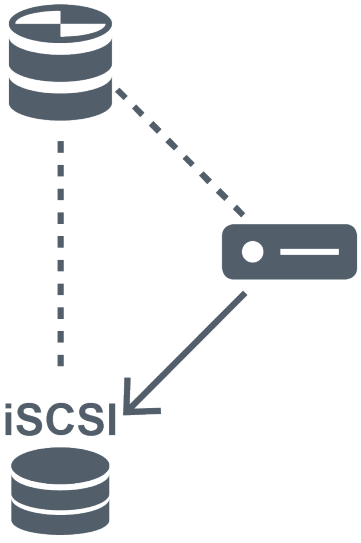
В этом разделе приведены рисунки, отображающие возможные режимы записи VRM.

Список возможных режимов записи VRM:

- Основная запись VRM
- Запись с зеркальным VRM
- Дополнительная запись VRM
- Резервная запись VRM

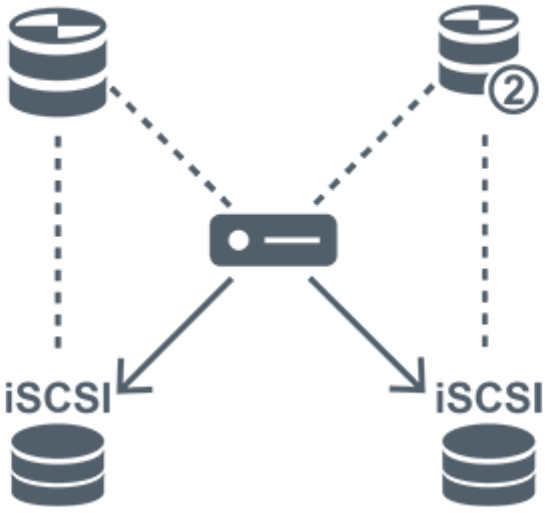
Сведения о записи ANR см. в разделе *Автоматическая компенсация сети (ANR), Страница 28*.

Основная запись VRM



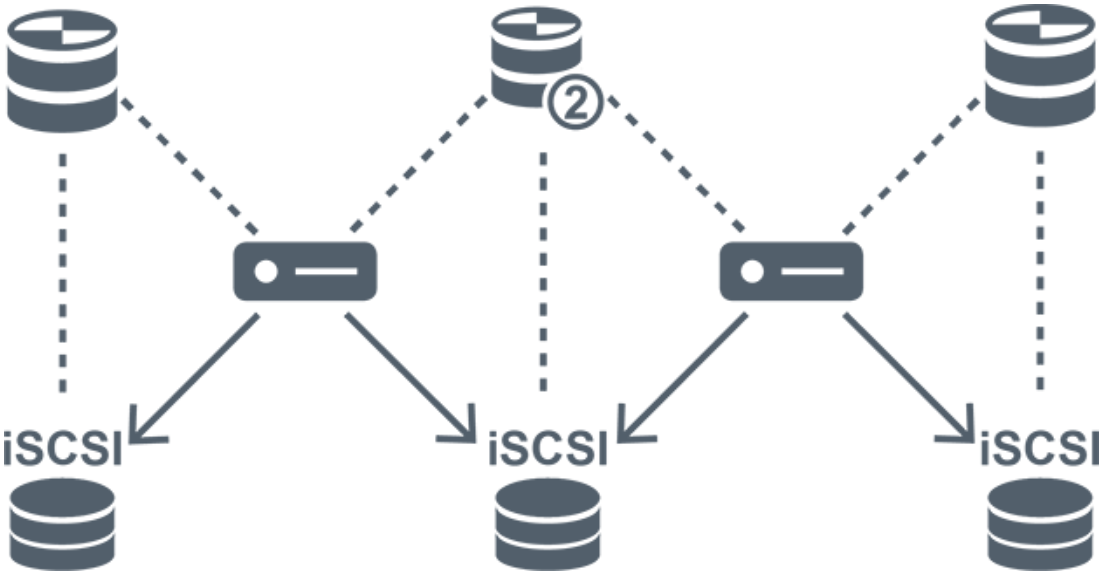
	Основной VRM		Управляющее соединение
	Устройство хранения iSCSI		Видеопоток
	Кодер		

Запись с зеркальным VRM



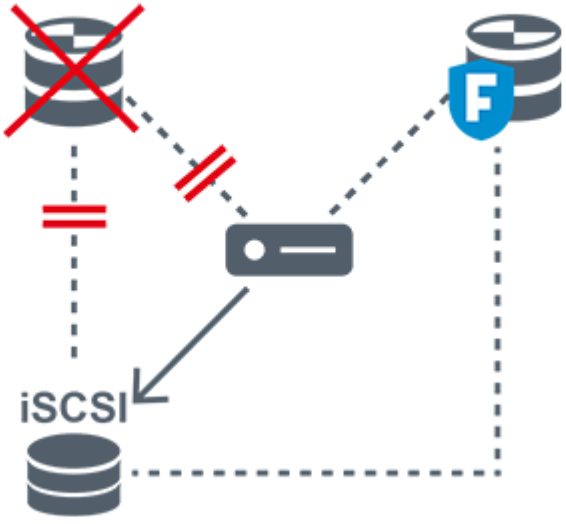
	Основной VRM		Дополнительный VRM
	Устройство хранения iSCSI		Управляющее соединение
	Кодер		Видеопоток

Вторичная запись VRM



	Основной VRM		Вторичный VRM
	Устройство хранения iSCSI		Управляющее соединение
	Кодер		Видеопоток

Резервная запись VRM



	Основной VRM		Первичный резервный VRM
	Устройство хранения iSCSI		Кодер

-------	Управляющее соединение	⟶	Видеопоток

5.2.4 Воспроизведение источников записи VRM

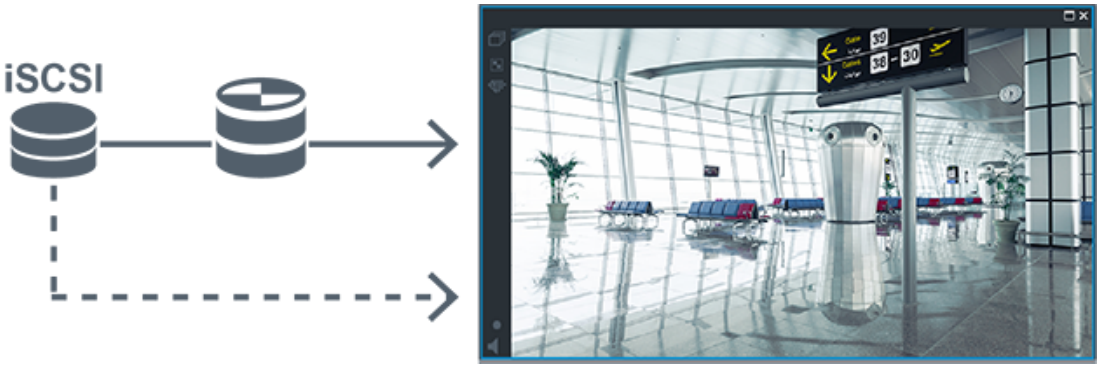
На следующих рисунках показаны Области изображений с воспроизведением со всех возможных источников записи VRM. На каждом рисунке показано устройство хранения, экземпляр VRM (при наличии) и часть области изображений в качестве примера воспроизведения. Если это необходимо, источник записи указан соответствующим значком на Панели области изображений.

- *Воспроизведение одной записи, Страница 34*
- *Воспроизведение двойной записи VRM, Страница 34*
- *Воспроизведение записи основного диспетчера VRM с помощью дополнительного резервного диспетчера VRM., Страница 35*
- *Воспроизведение записи вторичного VRM с помощью дополнительного резервного VRM., Страница 36*
- *Автоматическая компенсация сети, Страница 38*

Воспроизведение одной записи

Эта область изображений отображается, когда настроен только основной VRM. Выбрать другой источник записи невозможно.

------>: Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.

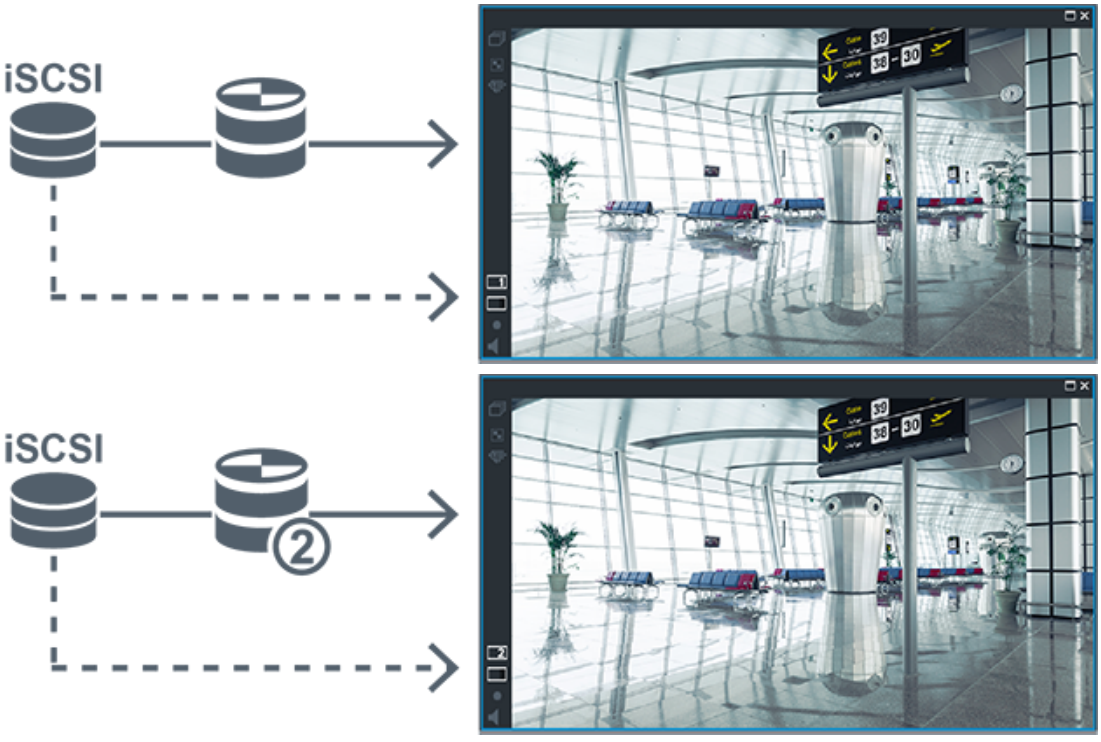


iSCSI	Устройство хранения iSCSI
	Основной VRM

Воспроизведение двойной записи VRM

Основной VRM и вторичный VRM настроены. Нажмите значок источника записи, чтобы отобразить первичное или вторичное воспроизведение.

Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.



iSCSI	Устройство хранения iSCSI
	Основной VRM
	Вторичный VRM

Воспроизведение записи основного диспетчера VRM с помощью дополнительного резервного диспетчера VRM.

Когда основной VRM работает, он обеспечивает воспроизведение. Резервный VRM находится в неактивном состоянии.

Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.

Если настроена запись вторичного VRM или ANR, можно переключить источник записи.

Если основной VRM не подключен, настроенный резервный VRM обеспечивает воспроизведение. Закройте область изображений и снова отобразите эту камеру в области изображений:

Если не подключен ни основной VRM, ни дополнительный основной резервный VRM, воспроизведение обеспечивается кодером. Закройте область изображений и снова отобразите эту камеру в области изображений.

	Устройство хранения iSCSI
	Основной VRM
	Основной резервный диспетчер VRM
	Кодер

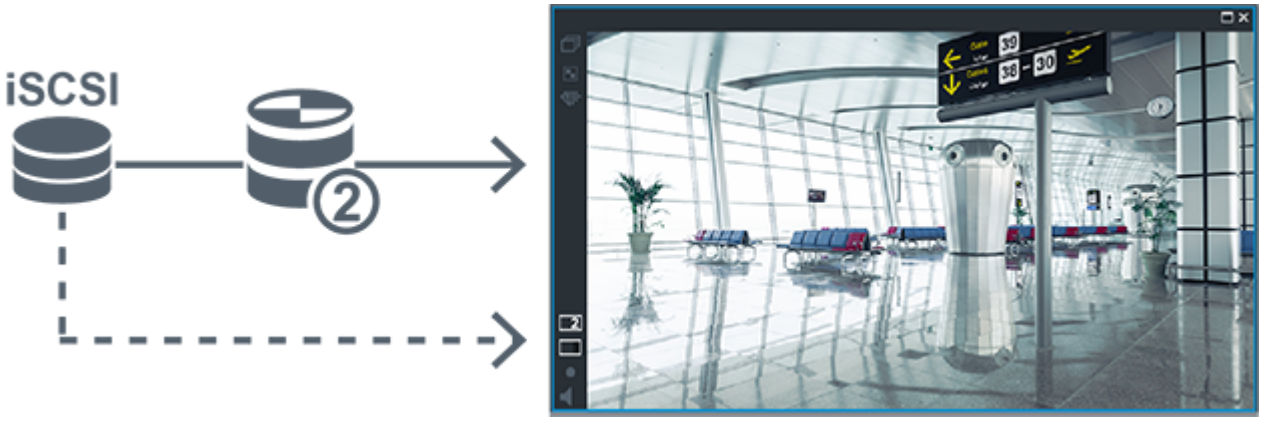
При воспроизведении с помощью кодера доступ возможен только к ограниченной части записи.

Воспроизведение записи вторичного VRM с помощью дополнительного резервного VRM.

Когда вторичный диспетчер VRM работает, он обеспечивает воспроизведение.

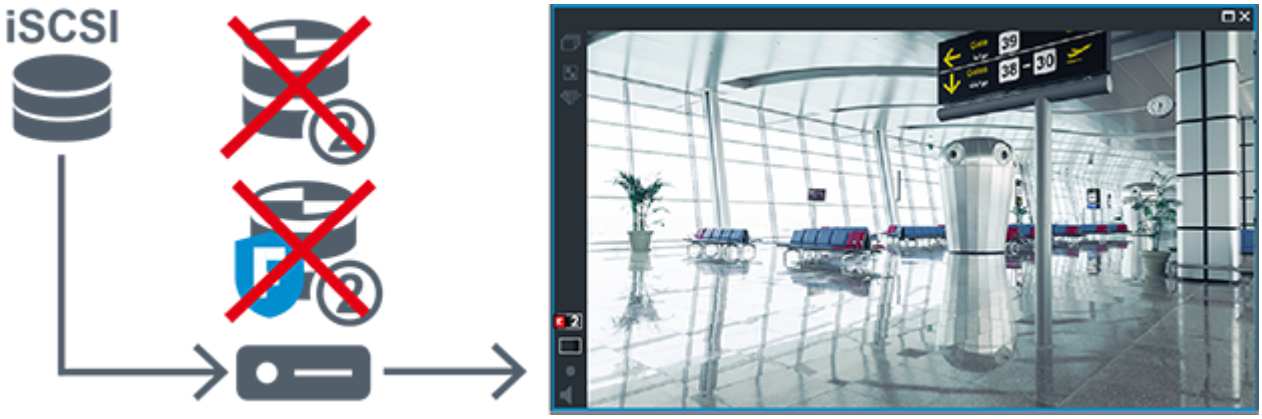
Резервный VRM находится в неактивном состоянии.

Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.



Если вторичный VRM не подключен, настроенный резервный VRM обеспечивает воспроизведение. Закройте область изображений и снова отобразите эту камеру в области изображений:

Если не подключен ни вторичный VRM, ни дополнительный вторичный резервный VRM, воспроизведение обеспечивается кодером. Закройте область изображений и снова перетащите эту камеру в область изображений.

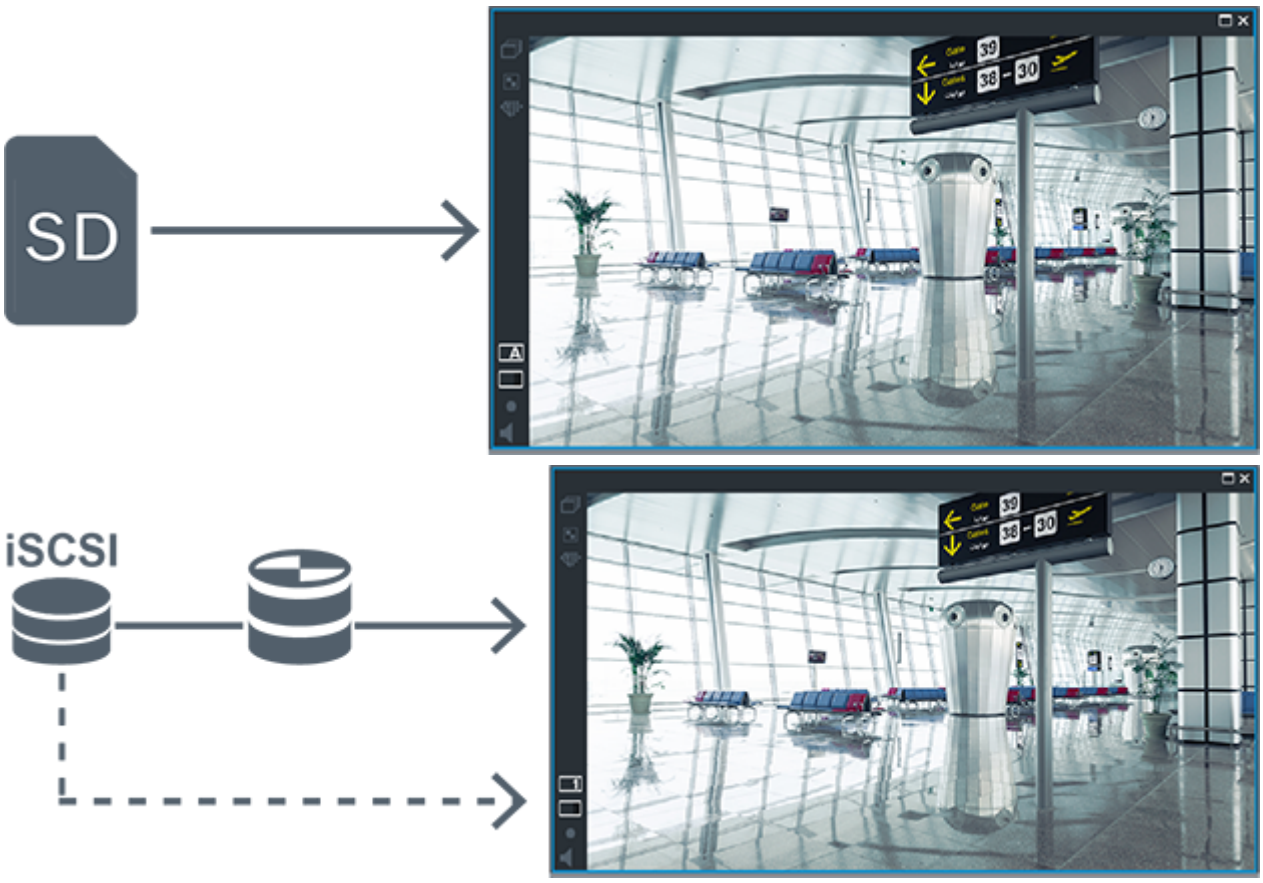


	Устройство хранения iSCSI
	Основной VRM
	Вторичный резервный диспетчер VRM

	Кодер

При воспроизведении с помощью кодера доступ возможен только к ограниченной части записи.

Автоматическая компенсация сети
Функция ANR не настроена. Нажмите значок источника записи для отображения основного воспроизведения (основное резервное воспроизведение, основное воспроизведение кодера) или воспроизведения ANR.
Если выполнена настройка для этой рабочей станции, воспроизведение обеспечивается непосредственно устройством хранения iSCSI.



iSCSI	Устройство хранения iSCSI
	Основной VRM
SD	Карта SD

5.2.5 Обзор событий, связанных с запоминающим устройством

В данном разделе описываются различные события, связанные с запоминающим устройством.

Состояние буферного хранилища
При сбое сети или центрального хранилища данных функция ANR обеспечивает передачу кодером записи, помещенной в локальный буфер, за недостающий период времени в центральное хранилище после устранения неполадки.
Состояния буфера:
– **Неизвестное состояние хранилища**
– **Состояние хранилища - в порядке**
– **Состояние хранилища - критический уровень наполнения буфера**
– **Состояние отказа хранилища**

Переполнение буферного хранилища
Это событие указывает на то, что буфер хранения уже заполнен и записи больше не передаются в центральное хранилище.

Состояние хранилища / Состояние вторичного хранилища
Состояние хранилища отображает состояние подключения между камерой и центральным хранилищем. Событие **Состояние отказа хранилища** запускается, если камера теряет связь с центральным хранилищем. Если отключение кратковременное, такое событие не обязательно означает, что видеоданные потеряны.
Состояния запоминающего устройства:
– **Неизвестное состояние хранилища**
– **Состояние хранилища - в порядке**
– **Состояние отказа хранилища**

Состояние монитора записи / Состояние дополнительного монитора записи
Это событие указывает, что ведется мониторинг записи. Пока камера может сохранять запись в буфер ОЗУ, авария не срабатывает. Событие **Состояние монитора записи: потеря записи** запускается, только если в течение последних двух минут видеоматериалы больше не могут быть сохранены в буфер ОЗУ и будут потеряны. Событие также отображает период времени, за который видеоматериалы потеряны.
Состояния монитора записи:
– **Состояние монитора записи: неизвестно**
– **Состояние монитора записи: ok**
– **Состояние монитора записи: потеря записи**

См.
– *Автоматическая компенсация сети (ANR), Страница 28*
– *Настройка событий и тревог, Страница 330*

5.3 Обработка сигналов тревоги

Тревоги могут быть настроены индивидуально для обработки одной или несколькими группами пользователей. При срабатывании тревоги она появляется в списке тревожных сигналов всех пользователей, принадлежащих к тем пользовательским группам, настройки которых позволяют принимать этот тревожное событие. После того как один из этих пользователей начинает обработку данной тревоги, она исчезает из списка тревожных сигналов других пользователей.
Тревоги отображаются на тревожном мониторе рабочей станции. Это поведение описывается в следующих разделах.

Движение тревожного события
1. В системе возникает тревожное событие.

2. Уведомления о тревоге появляются в списках тревожных сигналов всех пользователей, которые настроены на эту тревогу. Тревожное видеоизображение немедленно отображается на настроенных мониторах. Если этот тревожное событие является автоматически отображаемым (всплывающим), тревожное видеоизображение автоматически отображается также на тревожных мониторах рабочей станции Operator Client.
   Если тревожное событие сконфигурирован как автоматически отключающийся, он удаляется из списка тревожных сигналов по истечении времени автоотключения (настраиваемого в Configuration Client).
   В аналоговых мониторах режим квадрированного просмотра VIP XD временно заменяется полноэкранным режимом.
3. Один из пользователей принимает тревожное событие. На рабочей станции этого пользователя отображается тревожное видеоизображение (если оно еще не отображено автоматически). Тревожный сигнал удаляется из всех других списков тревожных сигналов и не отображается на экранах других операторов.
4. Пользователь, принявший тревожное событие, запускает поток заданий, который может включать в себя чтение плана действий и ввод комментариев. Этот шаг является факультативным: требования к потоку заданий могут быть настроены администратором.
5. В конечном итоге пользователь отключает тревожное событие. Это действие удаляет тревожное событие из списка тревожных сигналов, и он перестает отображаться на экране.
   В группе мониторов отображаются те камеры, которые отображались до возникновения тревожного события.

Окно тревожных изображений

1. Для отображения тревожного видеоизображения окно тревожных изображений занимает место окна изображения в режиме реального времени или окна воспроизведения записей на мониторе, который был настроен как монитор тревожных сигналов.
2. Каждому тревожному сигналу выделяется ряд областей изображения. С каждым тревожным сигналом может быть ассоциировано до 5 областей изображений. Эти области изображений могут отображать видео в режиме реального времени, воспроизводить запись или отображать карту.
   В группе мониторов каждый тревожный сигнал может выводить камеры в ряду мониторов. Количество камер в каждом ряду ограничено количеством столбцов в группе мониторов. Мониторы в столбце, который не используется для отображения тревожных видеоизображений, могут быть настроены на отображение текущего изображения или пустого экрана.
3. Тревожные сигналы с более высоким приоритетом отображаются над тревожными сигналами с более низким приоритетом как в рядах мониторов, так и в рядах отображения тревожных сигналов рабочей станции Operator Client.
4. Если окно тревожных изображений полностью занято рядами тревожных изображений и при этом должен быть отображен дополнительный тревожный сигнал, в нижнем ряду окна тревожных изображений будет отображаться последовательность тревожных сигналов с наиболее низким приоритетом. Вы можете переключаться между тревожными сигналами в стеке при помощи элементов управления слева от строки тревожного сигнала.

Можно переключаться между стеками тревожных сигналов в группе мониторов с помощью кнопок управления в окне **Мониторы** рабочей станции Operator Client. Мониторы с тревожными сигналами обозначены красными значками с мигающими «светодиодными» индикаторами.
Название, время и дата тревожного сигнала могут быть отображены на всех мониторах или только на первом мониторе в тревожном ряду.

5. В отношении тревожных сигналов с одинаковым приоритетом система может быть настроена администратором одним из двух способов:
   – Режим "Last-in-First-out" (LIFO): при этой конфигурации новые тревожные сигналы помещаются *над* старыми тревожными сигналами с тем же приоритетом.
   – Режим "First-in-First-out" (FIFO); при этой конфигурации новые тревожные сигналы помещаются *под* старыми тревожными сигналами с тем же приоритетом.
6. Ряд тревожных изображений может отображаться в окне тревожных изображений одним из двух способов:
   – При его создании (автоматическое всплывание). Это происходит, когда приоритет тревожного сигнала выше приоритета дисплея.
   – После принятия тревожного сигнала Это происходит, когда приоритет тревожного сигнала ниже приоритета дисплея.

Автоматически всплывающие тревожные сигналы

Тревожный сигнал может быть настроен как автоматически отображающийся (всплывающий) в окне тревожных сигналов, в соответствии с приоритетом. Дисплеям реального времени и воспроизведения каждой пользовательской группы также назначаются приоритеты. При получении тревожного сигнала с приоритетом, превышающим приоритет дисплея пользователя, этот тревожный сигнал автоматически отображает свой тревожный ряд в окне тревожных сигналов. Если окно тревожных сигналов не отображается в данный момент на экране, оно автоматически занимает место окна изображений в реальном времени или окна воспроизведения на мониторе, настроенном на отображение тревог.
Несмотря на то что всплывающие тревожные сигналы отображаются в окне тревожных сигналов, они не принимаются автоматически. Они могут одновременно отображаться на дисплеях нескольких пользователей. Когда пользователь принимает всплывающий тревожный сигнал, он удаляется из списка тревожных сигналов всех остальных пользователей и перестает отображаться на их дисплеях.

Обработка тревог в случае выключения системы

Все активные тревоги сохраняются по завершении работы сервера. Тревоги будут восстановлены и снова появится в окне **Список тревожных сигналов**, когда система перезапустится.
Тревоги в состоянии **Принято** или **Поток заданий** автоматически переводятся обратно в состояние **Активно** после перезагрузки системы. Комментарии, введенные для тревог в состоянии **Поток заданий**, сохраняются.

Замечание!
Данные тревог сохраняются автоматически каждую минуту, поэтому максимально возможная потеря данных — это данные, накопленные за одну минуту.

См.

– *Настройка длительности до и после срабатывания тревожного сигнала, Страница 336*

5.4 Сопоставление событий ONVIF

Замечание!
Следует помнить, что эта функция срабатывает в конце срока использования.
Воспользуйтесь ONVIF Camera Event Driver Tool для простого ONVIF сопоставления событий.
См. *Запуск ONVIF Camera Event Driver Tool из Configuration Client, Страница 217*.

Использование по назначению
Назначение — сопоставление событий ONVIF с событиями BVMS. События ONVIF могут запускать тревоги и запись BVMS.
Можно определить сопоставления событий по умолчанию только для определенного устройства ONVIF, для всех устройств ONVIF одного производителя и модели или для всех устройств ONVIF одного производителя. Сопоставления событий по умолчанию автоматически назначаются всем соответствующим кодерам ONVIF, добавляемым с помощью мастера сканирования BVMS или вручную.
При добавлении кодера ONVIF к конфигурации BVMS без подключения к этому кодеру ONVIF сопоставления событий не назначаются. Можно обновить такой кодер ONVIF, используя сопоставления событий с кодера ONVIF того же производителя или уже добавленной модели.
Задаются сопоставления событий для каждого из следующих источников:
- кодер ONVIF;
- камеры этого кодера ONVIF;
- реле этого кодера ONVIF;
- входы этого кодера ONVIF.

Пример
На камере ONVIF происходит событие обнаружения движения. Это событие должно запускать событие **Обнаружено движение** в BVMS.
Чтобы это произошло, для этой камеры ONVIF выполняется следующая настройка:
- раздел ONVIF (`MotionDetection`);
- элемент данных ONVIF (`motion`);
- тип данных ONVIF (`boolean`);
- значение данных ONVIF (`true`).

Примечание. Недостаточно настроить только событие **Обнаружено движение**.
Настройте также событие **Движение остановлено**. Необходимо всегда настраивать пару событий.

Импорт и экспорт таблицы сопоставлений
Таблицу сопоставлений можно экспортировать на компьютер, на котором она создана, и импортировать ее на другой компьютер, на котором недоступна необходимая таблица сопоставлений.

Устранение неисправностей
Для поиска и устранения неисправностей можно записывать файлы журнала.

См.
- *Настройка таблицы сопоставления ONVIF, Страница 250*
- *Включение журнала для событий ONVIF, Страница 392*
- *Страница "События кодера ONVIF", Страница 246*

5.5 Отключение при бездействии

Использование по назначению

Отключение при бездействии предназначено для защиты клиента Operator Client или Configuration Client в отсутствие оператора или администратора.

Для каждой группы пользователей можно задать такие настройки, чтобы Operator Client автоматически отключался по истечении заданного времени бездействия.

Для Configuration Client пользовательские группы недоступны. Настройка отключения при бездействии действует только для **администратора**.

Все операции с использованием клавиатуры, мыши и клавиатуры CCTV влияют на заданное время отключения при бездействии. Автоматические действия Operator Client не влияют на это время. Такие автоматические действия Configuration Client, как загрузка микропрограммного обеспечения или настройка iSCSI предотвращают отключение при бездействии.

Также можно настроить отключение при бездействии для веб-клиента BVMS.

Незадолго до отключения при бездействии диалоговое окно напоминает пользователю, что отключение при бездействии можно предотвратить каким-либо действием.

В журнал вносится запись о произошедшем отключении при бездействии.

Пример

Если рабочая станция находится в общественном месте, отключение при бездействии сводит к минимуму опасность получения несанкционированного доступа к Operator Client оставленной без присмотра рабочей станции.

Член группы администраторов должен автоматически отключаться по истечении времени бездействия, но дежурный (группа операторов) может просто смотреть видео без использования системы и не использовать отключение при бездействии.

Ограничения

Активность Client SDK не поддерживает отключение при бездействии, что означает, что активность Client SDK не влияет на заданный период времени.

См.

- *Диалоговое окно «Параметры» (меню «Настройки»), Страница 124*
- *Страница Свойства оператора, Страница 349*

5.6 Клиент Operator Client, независимый от версии

Для использования режима совместимости и на клиенте Operator Client, и на сервере Management Server должна быть версия выше 5.5.

Пользователь Operator Client может успешно подключиться к серверу Management Server, на котором используется программное обеспечение предыдущей версии.

Если сервер предоставляет конфигурацию новее, чем доступна на рабочей станции Operator Client, эта конфигурация автоматически копируется на рабочую станцию Operator Client. Пользователь может решить загрузить новую конфигурацию.

Клиент Operator Client предоставляет ограниченный набор функций и подключен к данному серверу Management Server.

Следующие функции, связанные с сервером Management Server, доступны после входа на сервер Management Server предыдущей версии:

- пользовательские настройки;
- запуск записи вручную;
- отображение состояний устройства;
- переключение состояний реле;

– поиск в журнале;
  Поиск событий невозможен.
– поиск сервера;
– удаленный экспорт.

5.6.1 Работа в режиме совместимости

 : это состояние Operator Client отображается в режиме совместимости.
В версиях выше 5.5 Operator Client будет работать в режиме совместимости, если версия Management Server ниже версии Operator Client.
В версиях выше 10.0 Operator Client будет работать в режиме совместимости в следующих случаях:
– Не все службы связи могут подключаться с помощью Operator Client.
– Пример. Management Server запущен и работает, но WebServiceHost отключен.
– В коммуникационном интерфейсе между клиентом Operator Client и сервером Management Server есть изменения.

Только семантические изменения интерфейса или частичная неработоспособность услуг могут привести к тому, что некоторые функции могут быть недоступными в Operator Client.

5.7 Режимы просмотра панорамной камеры

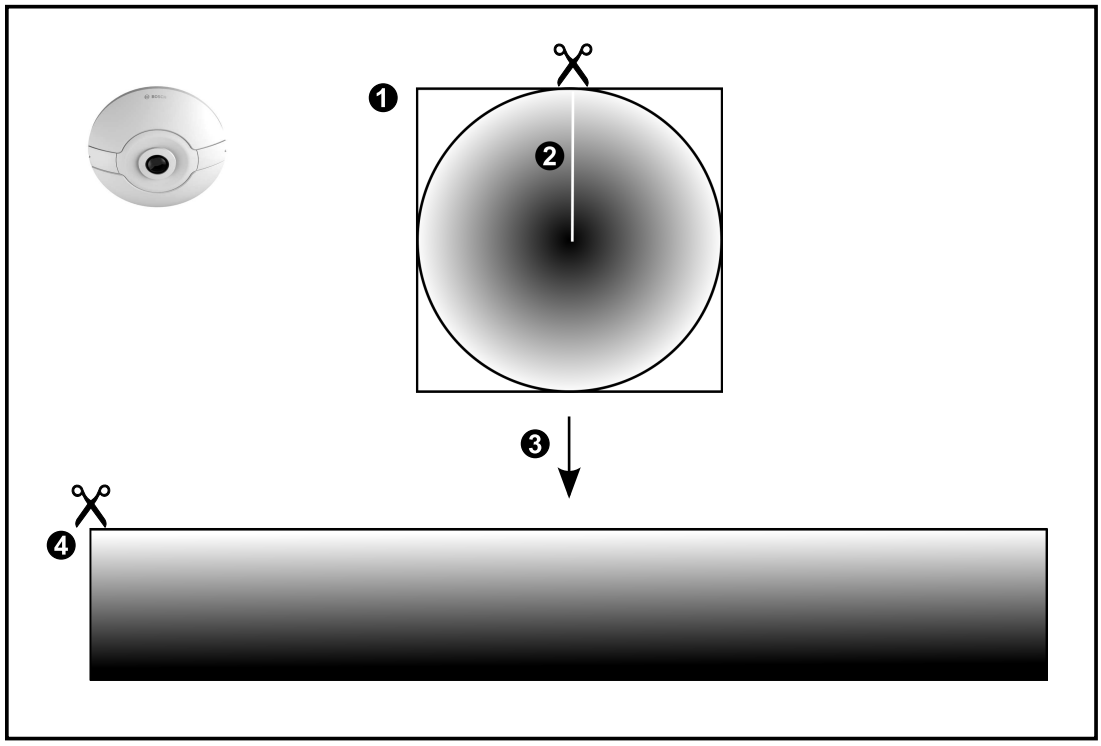
В этом разделе показаны режимы просмотра изображения с панорамной камеры, которые доступны в системе BVMS.
Доступны следующие режимы просмотра:
– Круговое представление
– Панорамное представление
– Кадрированное представление

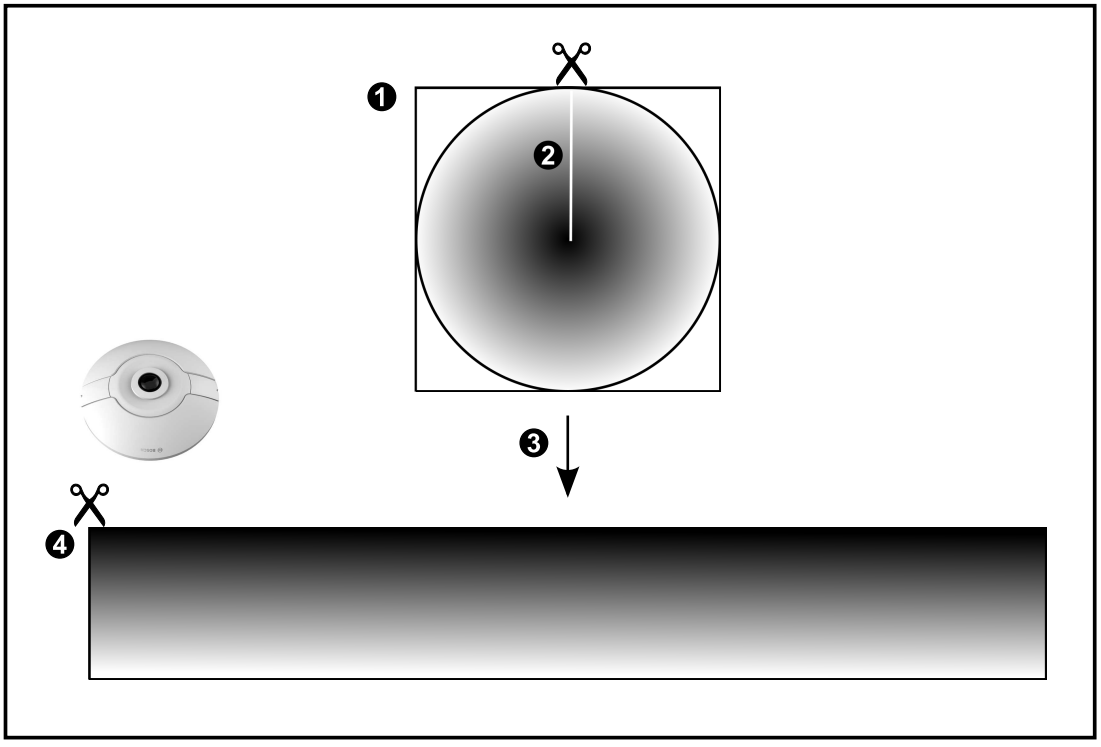
Панорамное и кадрированное представления создаются в результате операции устранения искажений в BVMS. Устранение искажений в камере не применяется. Администратор должен настроить положение установки панорамной камеры в Configuration Client.
Размер области изображений можно изменить требуемым образом. Соотношение сторон области изображений не ограничено соотношениями 4:3 и 16:9.

См.
– *Настройка предустановленных положений и дополнительных команд, Страница 311*

5.7.1 Панорамная камера 360°, монтируемая на полу или потолке

На рисунке ниже показана процедура устранения искажений для панорамной камеры 360°, монтируемой на полу или потолке.

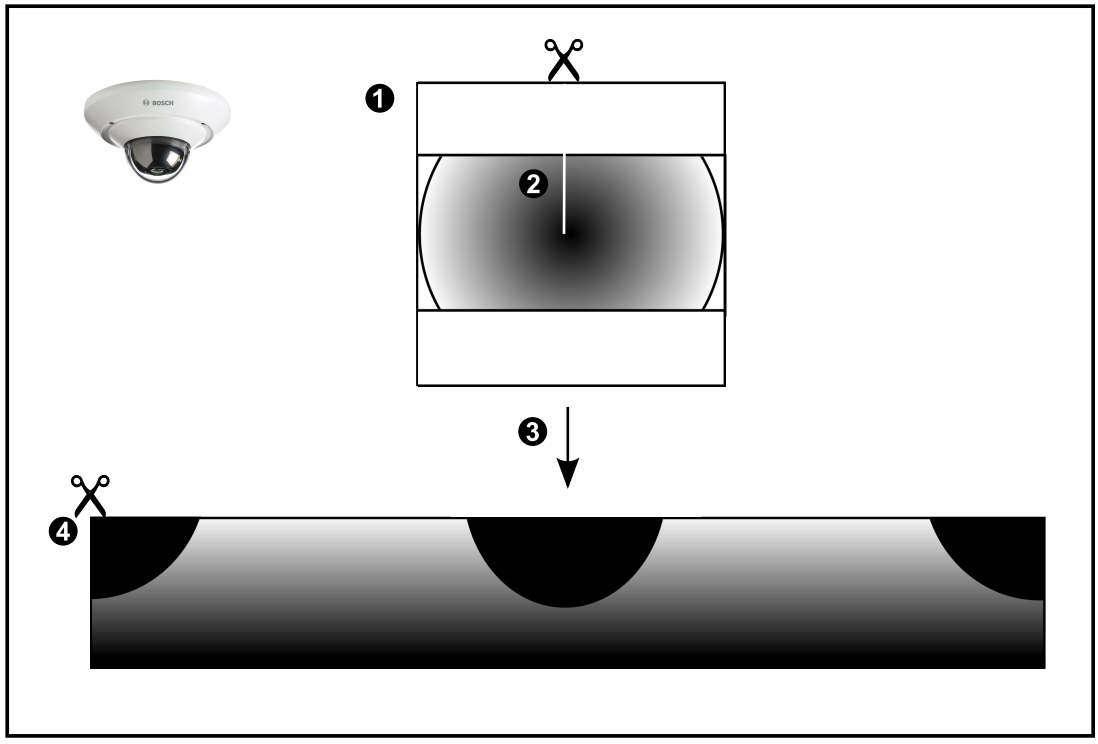


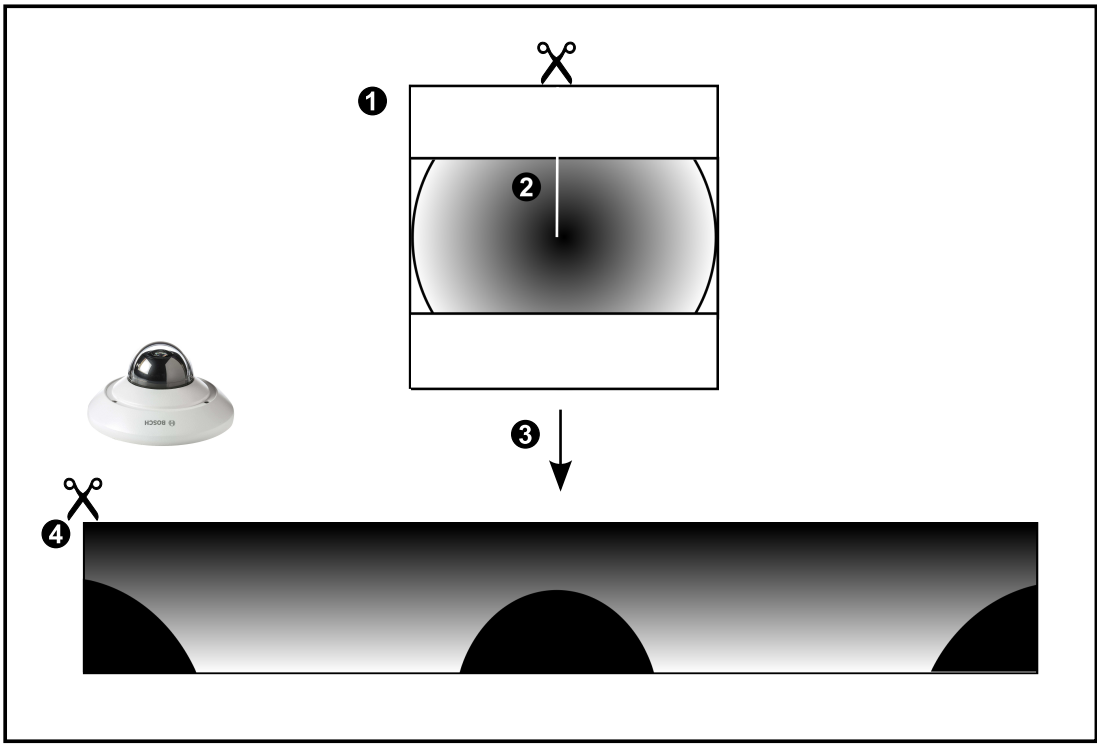


1	Изображение в виде целого круга	3	Устранение искажений
2	Линия разреза (оператор может изменять ее положение, если изображение не является увеличенным)	4	Панорамное представление

5.7.2 Панорамная камера 180°, монтируемая на полу или потолке

На рисунке ниже показана процедура устранения искажений для панорамной камеры 180°, монтируемой на полу или потолке.



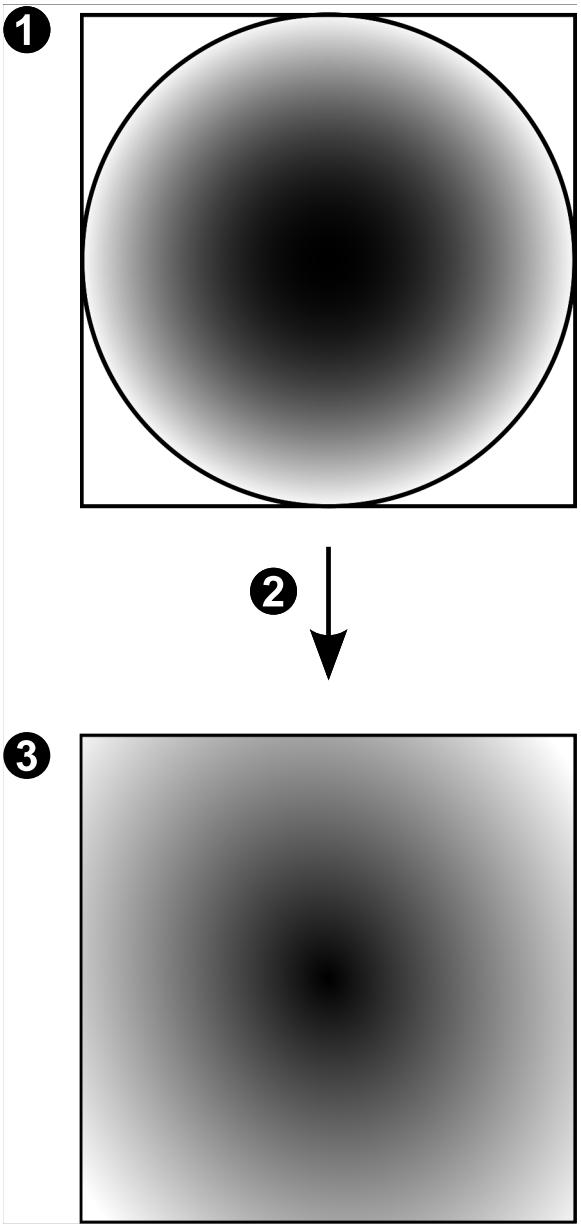


1	Изображение в виде целого круга	3	Устранение искажений

2	Линия разреза (оператор может изменять ее положение, если изображение не является увеличенным)	4	Панорамное представление

5.7.3 Панорамная камера 360°, монтируемая на стене

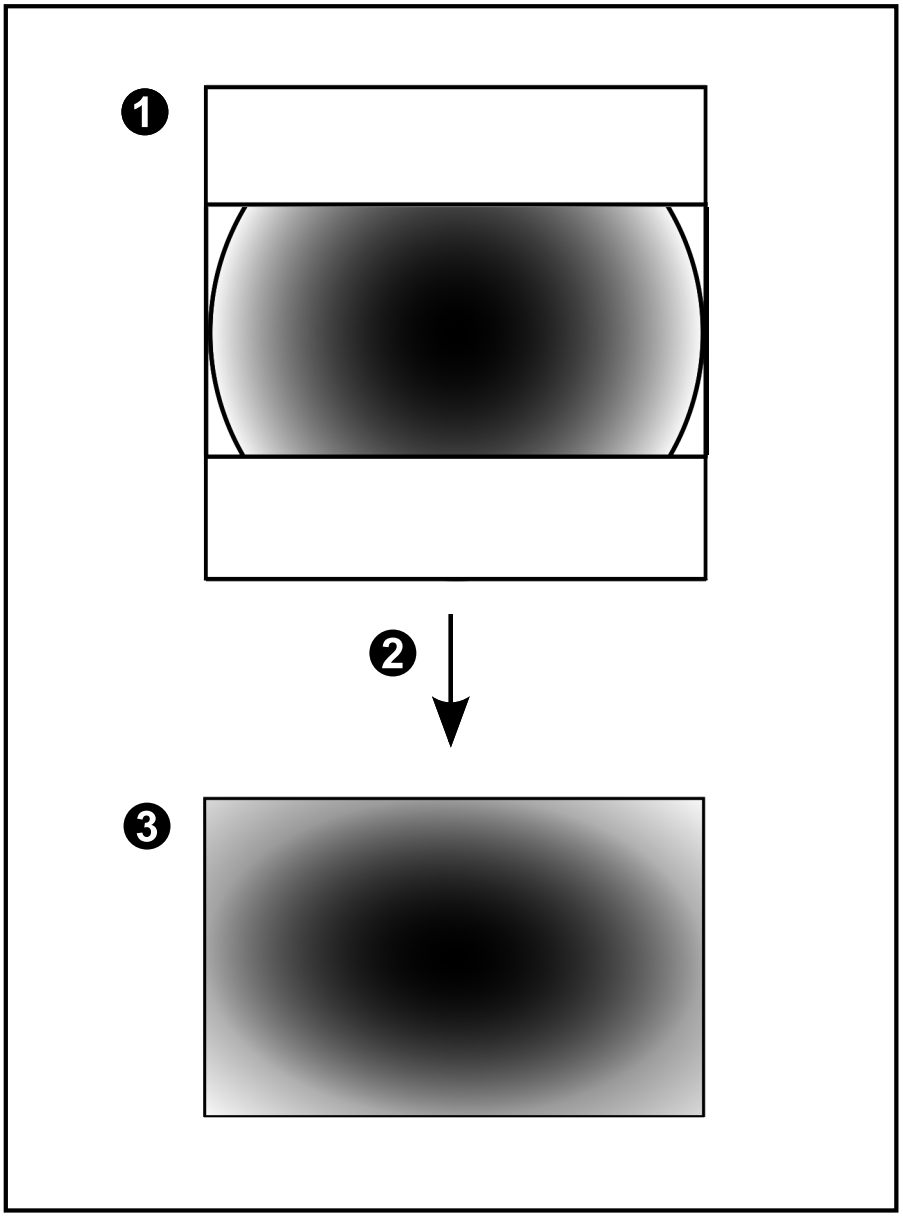
На рисунке ниже показана процедура устранения искажений для панорамной камеры 360°, монтируемой на стене.



1	Изображение в виде целого круга	3	Панорамное представление
2	Устранение искажений		

5.7.4 Панорамная камера 180°, монтируемая на стене

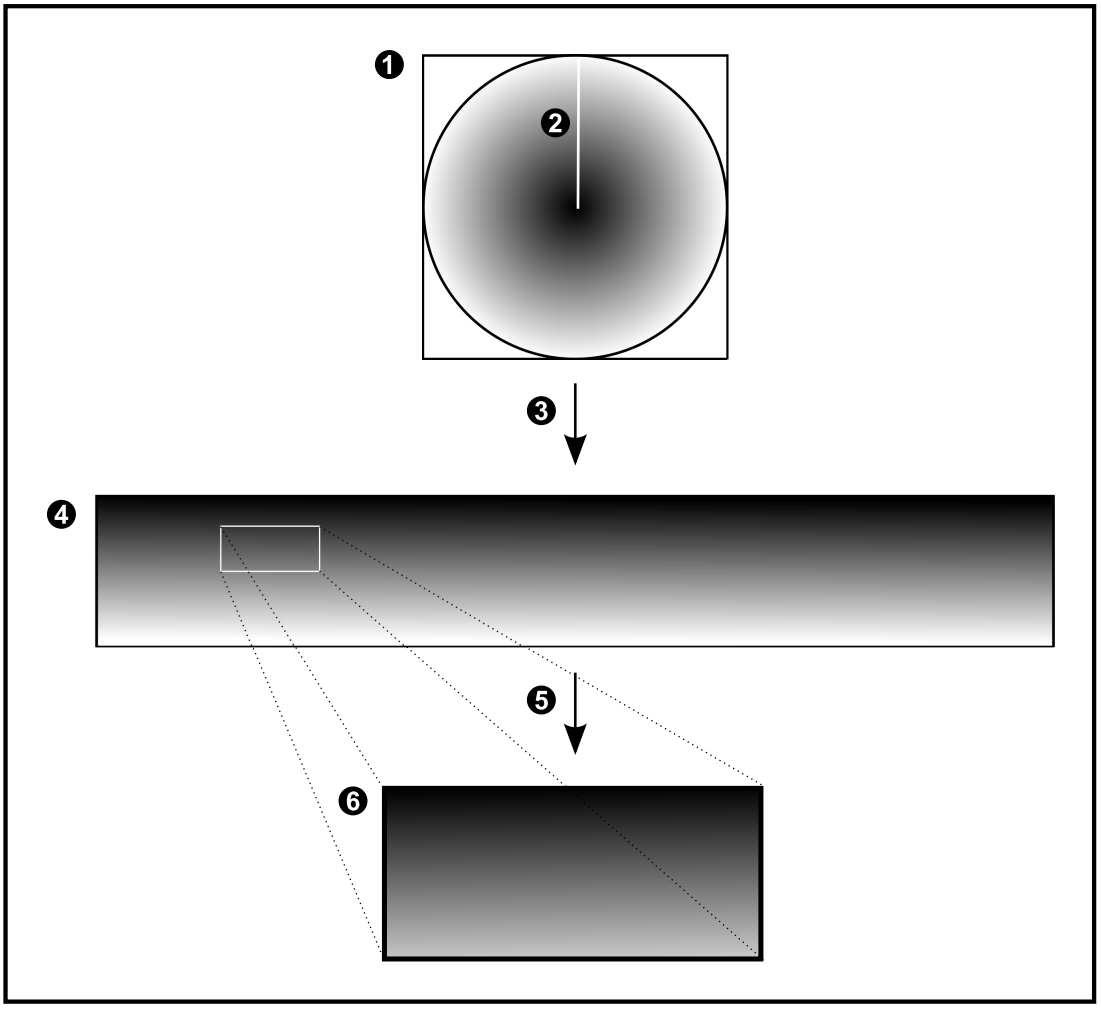
На рисунке ниже показана процедура устранения искажений для панорамной камеры 180°, монтируемой на стене.



1	Изображение в виде целого круга	3	Панорамное представление
2	Устранение искажений		

5.7.5 Кадрированное представление изображения с панорамной камеры

На рисунке ниже показана процедура кадрирования изображения для панорамной камеры 360°, монтируемой на полу или потолке.
Применяемый для кадрирования прямоугольный фрагмент является фиксированным. Фрагмент можно изменить в области кадрированного изображения с помощью имеющихся средств управления PTZ.



1	Изображение в виде целого круга	4	Панорамное представление
2	Линия разреза (оператор может изменять ее положение, если изображение не является увеличенным)	5	Кадрирование
3	Устранение искажений	6	Кадрированная область изображений

5.8 Туннелирование SSH

BVMS обеспечивает удаленное подключение благодаря использованию технологии туннелирования Secure Shell (SSH).
Туннелирование SSH позволяет создать зашифрованный туннель с помощью подключения протокол/сокет SSH. Этот зашифрованный туннель может передавать как шифрованные, так и нешифрованные данные. Реализация Bosch SSH также использует протокол Omni-Path — высокопроизводительный протокол связи с низкой задержкой от Intel.

Ограничения и технические характеристики

- Туннелирование SSH использует порт 5322. Этот порт не может быть изменен.
- Служба SSH должна быть установлена на тот же сервер, что и Management Server BVMS.
- Для учетных записей пользователей (Enterprise) должен быть настроен пароль. Учетные записи пользователей (Enterprise) без пароля не могут выполнять вход при использовании соединения по протоколу SSH.
- Камеры с локальным устройством хранения не поддерживают соединение по протоколу SSH.
- Configuration Client не может подключаться удаленно по протоколу SSH. Соединение с Configuration Client должно осуществляться посредством сопоставления портов.
- Operator Client проверяет соединение со службой SSH каждые 15 секунд. В случае разрыва соединения Operator Client раз в минуту перепроверяет наличие соединения.

Сопоставление портов

- Настройте один перенаправляющий порт для Management Server BVMS для использования порта 5322 для внутренних и внешних подключений.
  Это единственное сопоставление портов, которое необходимо выполнить для всей системы. Сопоставление портов
  BVMS не требуется.

Шифрованная связь

После установления подключения через туннель SSH все соединения между Management ServerBVMS и удаленным клиентом являются шифрованными.

5.9 Многопутевой ввод-вывод

BVMS обеспечивает многопутевой ввод-вывод для систем с двойными контроллерами. Многопутевой ввод-вывод является устойчивой к ошибкам технологией, подходящей для более чем одного физического подключения между камерой и ее iSCSI хранилищами через резервные сетевые подключения. При использовании многопутевого ввода-вывода запись и воспроизведение видеоданных возможны даже в случае сбоя iSCSI контроллера.

Необходимые условия и ограничения

- Установлен iSCSI модуль NetApp E2800 с двойным контроллером.
- Микропрограмма 6.43 позволяет устройствам, ведущими запись на E2800, использовать альтернативные пути.

– VRM 3.71 для мониторинга и ведения журнала устройств с включенным многопутевым входом-выходом.
– Два настроенных физических порта iSCSI на каждом контроллере: 2 x 2 RJ-45 или 2 x 2 оптических.
– Скорость соединения должна составлять 10 Гбит/с для обеспечения полноценной работы.
– Режим Dual–Simplex, используемый в E2700, больше не поддерживается.

Более подробные сведения об установке полного дуплекса DSA E2800 см. в Руководстве пользователя DSA E-Series E2800.

6 Поддерживаемое оборудование

Замечание!
Не следует подключать устройство к нескольким BVMS! Это может привести к пропускам в записи и другим нежелательным последствиям.

К BVMS можно подключить следующее аппаратное оборудование.

- Мобильные видеоклиенты, такие как iPhone или iPad через DynDNS
- Различные IP-камеры. кодеры иONVIFкамеры (только в режиме реального времени или через Video Streaming Gateway)
  Подключаются через сеть
- Кодеры, работающие только в режиме реального времени, с локальным хранилищем
  Подключаются через сеть
- Устройства хранения iSCSI
  Подключаются через сеть
- Аналоговые камеры
  Подключен к кодерам,
- Декодеры
  Подключаются через сеть
- Мониторы
  Подключаются к декодеру, к матричному коммутатору Bosch Allegiant, к клиентской рабочей станции BVMS
- матричный коммутатор Bosch Allegiant (версия микропрограммы: 8.75 или выше, версия MCS: 2.80 или выше)
  Подключается к COM-порту Management Server или к удаленному компьютеру и к IP-кодеру в сети.
- Клавиатура KBD-Universal XF
  Подключается к порту USB рабочей станции BVMS.
- Клавиатура Bosch IntuiKey
  Подключается к COM-порту рабочей станции BVMS (версия микропрограммного обеспечения 1.82 или выше) или к аппаратному декодеру (VIP XD).
  При подключении клавиатуры к рабочей станции пользователь может с клавиатуры управлять всей системой. При подключении клавиатуры к декодеру VIP XD пользователь может управлять с клавиатуры только мониторами.
- Почтовый сервер SMTP
  Подключаются через сеть
- POS
  Подключаются через сеть
- ATM
  Подключаются через сеть
- Устройство мониторинга сети
  Подключаются через сеть
- Модули ввода/вывода
  Подключаются через сеть
  Поддерживаются только устройства ADAM.

Все устройства, подключаемые через сеть, подключаются к коммутатору. Компьютеры BVMS также подключаются к этому устройству.

6.1 Установка аппаратного оборудования

BVMS поддерживает следующие компоненты оборудования:

- Клавиатура KBD-Universal XF
- Клавиатура Bosch IntuiKey
- Матричный коммутатор Bosch Allegiant с камерами и монитором: подключен к COM-порту одного из компьютеров сети и к IP-кодерам, подключенным к сети.
- Кодерыс аналоговыми камерами
- Кодерыс локальными хранилищами
- IP-камеры и камеры IP AutoDome
- Мониторы, подключенные к декодеру (возможны группы мониторов для обработки тревог)
- Системы DVR с камерами
- Устройства ATM / POS
- Модули ввода/вывода
  Поддерживаются только устройства ADAM.

6.2 Установка клавиатуры KBD Universal XF

Замечание!
Ознакомьтесь с руководством, входящим в комплект вашей клавиатуры KBD-Universal XF и доступным в интернет-каталоге продуктов.

Дополнительная информация
Для получения дополнительной информации, загрузки программного обеспечения и документации посетите страницу соответствующего продукта на веб-сайте www.boschsecurity.com.
К BVMS можно подключить следующее аппаратное оборудование.

- Мобильные видеоклиенты, такие как iPhone или iPad через DynDNS
- Различные IP-камеры. кодеры иONVIFкамеры (только в режиме реального времени или через Video Streaming Gateway)
  Подключаются через сеть
- Кодеры, работающие только в режиме реального времени, с локальным хранилищем
  Подключаются через сеть
- Устройства хранения iSCSI
  Подключаются через сеть
- Аналоговые камеры
  Подключен к кодерам,
- Декодеры
  Подключаются через сеть
- Мониторы
  Подключаются к декодеру, к матричному коммутатору Bosch Allegiant, к клиентской рабочей станции BVMS
- матричный коммутатор Bosch Allegiant (версия микропрограммы: 8.75 или выше, версия MCS: 2.80 или выше)
  Подключается к COM-порту Management Server или к удаленному компьютеру и к IP-кодеру в сети.

6.3 Подключение клавиатуры Bosch IntuiKey к BVMS

В данном разделе содержатся общие сведения о настройке клавиатуры Bosch IntuiKey.

6.3.1 Сценарии подключения клавиатур Bosch IntuiKey

Вы можете подключить клавиатуру Bosch IntuiKey к COM-порту рабочей станции BVMS (сценарий 1) или к аппаратному декодеру (напр,. VIP XD, сценарий 2).
При подключении клавиатуры к рабочей станции BVMS пользователь может управлять всей системой. При подключении клавиатуры к декодеру пользователь может управлять только аналоговыми мониторами системы.
При подключении клавиатуры к Enterprise Operator Client вы можете управлять камерами определенного Management Server, сначала нажав клавишу сервера для ввода номера сервера, а затем номера камеры.

Замечание!
Для подключения клавиатуры Bosch IntuiKey к рабочей станции BVMS используйте специальный кабель Bosch.
Для подключения клавиатуры Bosch IntuiKey к декодеру VIP XD вам потребуется кабель, соединяющий последовательный COM-порт клавиатуры с последовательным интерфейсом декодера. Сведения о подключении см. в Подключение клавиатуры CCTV к декодеру.

Поддерживается клавиатура Bosch IntuiKey, подключенная к рабочей станции BVMS

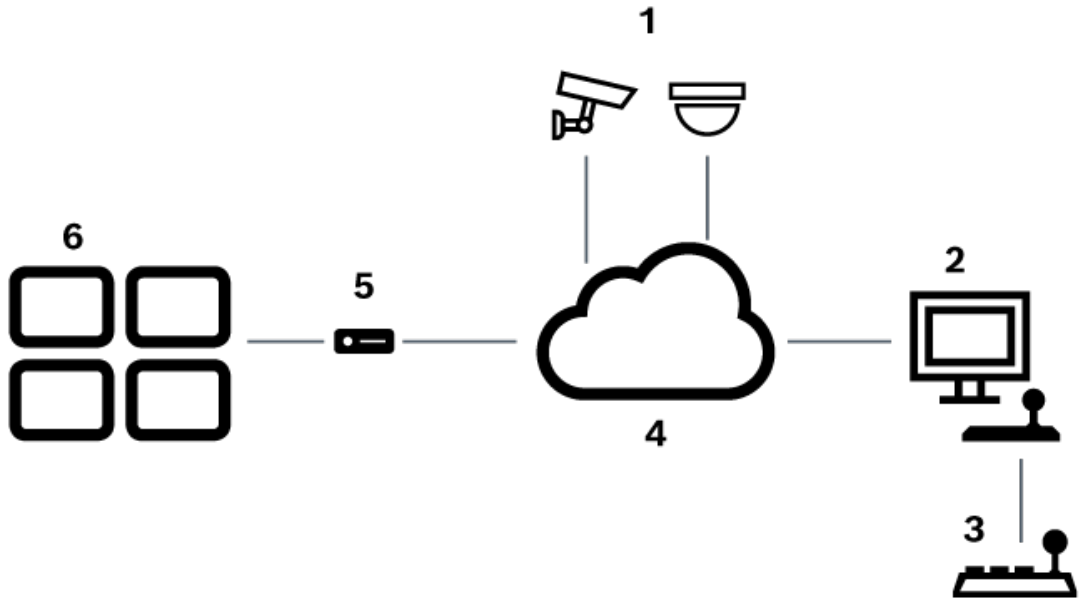


Рис. 6.1: Сценарий 1: клавиатура Bosch IntuiKey, подключенная к рабочей станции Bosch Video Management System

1	Различные камеры, подключенные к сети через кодеры
2	Рабочая станция BVMS
3	Клавиатура Bosch IntuiKey

4	Сеть BVMS
5	Декодер
6	Мониторы

Клавиатура Bosch IntuiKey, подключенная к декодеру

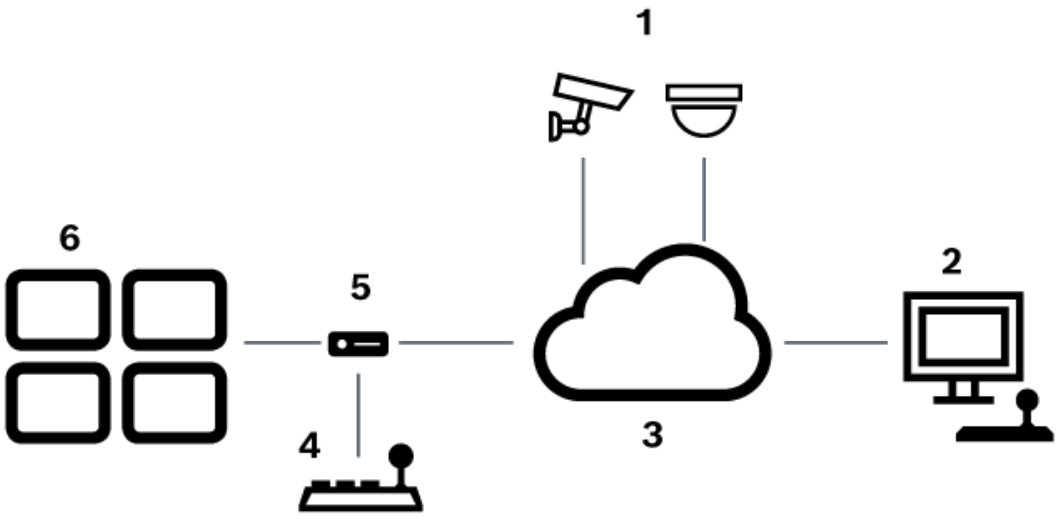


Рис. 6.2: Сценарий 2: клавиатура Bosch IntuiKey, подключенная к декодеру

1	Различные камеры, подключенные к сети через кодеры
2	Рабочая станция BVMS
3	Сеть BVMS
4	Клавиатура Bosch IntuiKey
5	Декодер
6	Мониторы

Подробные сведения обо всех окнах содержатся в следующих разделах:

– *Страница "Назначить клавиатуру", Страница 161*

Пошаговые инструкции содержатся в следующих разделах:

– *Настройка клавиатуры Bosch IntuiKey (страница «Настройки») (рабочая станция), Страница 142*
– *Настройка клавиатуры Bosch IntuiKey (декодер), Страница 150*
– *Настройка декодера для использования с клавиатурой Bosch IntuiKey, Страница 150*

См.

– *Страница "Назначить клавиатуру", Страница 161*

6.3.2 Подключение клавиатуры Bosch IntuiKey к декодеру

Настройка декодера

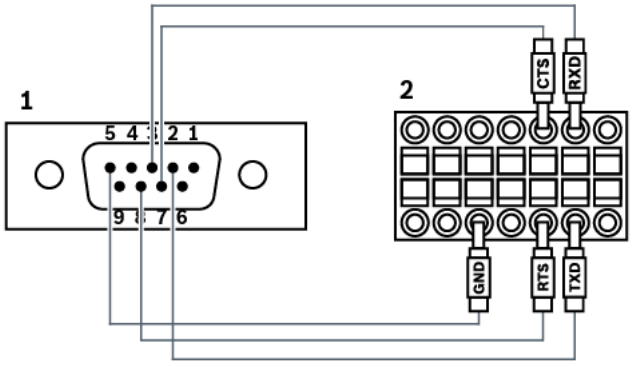
См. *Настройка декодера для использования с клавиатурой Bosch IntuiKey, Страница 150* для получения подробных сведений.

Соединение между COM-портом и декодером VIP XD

В следующей таблице перечислены соединения между адаптером RS232 и последовательным интерфейсом декодера VIP XD:

Адаптер RS232	Последовательный интерфейс декодера VIP XD
1	
2	TX
3	RX
4	
5	GND
6	
7	CTS
8	RTS
9	

На следующей иллюстрации показана схема расположения выводов стандартного адаптера RS232 (1) и схема расположения выводов последовательного адаптера декодера (2):



6.3.3 Обновление программного обеспечения клавиатуры Bosch IntuiKey

1. - Установите на каком-либо ПК загрузчик IntuiKey.
2. Запустите служебную программу IntuiKey Firmware Upgrade.
3. При помощи последовательного кабеля (обратитесь в службу поддержки Bosch, если у вас нет такого кабеля) подключите клавиатуру к этому ПК.
4. На клавиатуре нажмите программную клавишу Keyboard Control, затем Firmware Upgrade.
5. Введите пароль: 0 и 1 одновременно.
   Клавиатура находится в режиме начального загрузчика.
6. На компьютере нажмите Browse для выбора файла ПО: например, kbd.s20

7. Настройте COM-порт.
8. Нажмите кнопку Download, чтобы загрузить микропрограмму.
   На дисплее клавиатуры отображается Programming.
   Пока не нажимайте Clr. В противном случае клавиатура будет не пригодна к использованию после перезагрузки (см. примечание ниже).
9. Нажмите Browse, чтобы выбрать язык: например, 8900_EN_..82.s20.
   На дисплее клавиатуры отображается Programming.
10. Закройте служебную программу IntuiKey Firmware Upgrade.
11. На клавиатуре нажмите клавишу Clr для выхода.
    Клавиатура будет перезапущена. Подождите несколько секунд, пока не появится меню выбора языка клавиатуры.
12. Выберите требуемый язык с помощью программной клавиши.
    Отображается стандартная стартовая страница.

Замечание!
Для непосредственного запуска режима начального загрузчика можно отключить питание от клавиатуры, одновременно нажать 0 и 1, снова включить питание и отпустить 0 и 1.

6.4 Подключение матричного коммутатора Bosch Allegiant к BVMS

Матричный коммутатор BVMSAllegiant обеспечивает непрерывный доступ к аналоговым матричным камерам через интерфейс Operator Client Камеры Allegiant выглядят почти так же, как и IP-камеры. Единственное различие заключается в небольшом значке с сеткой, указывающем на то, что это камера Allegiant. Вы можете отображать эти камеры, используя те же задания, что и для IP-камер. Они включены как в логическое дерево, так и на карты участков, и пользователи могут добавлять их в дерево избранного. При поддержке оконного управления видеоизображением с камеры PTZ, подключенной к Allegiant, эти камеры могут быть отображены на мониторах, подключенных к IP-декодерам.
BVMS соединяется с матричным коммутатором посредством ПО Allegiant MCS (Master Control Software). Программа MCS запускается и работает в фоновом режиме. Это программное обеспечение представляет собой эффективный, событийно управляемый интерфейс для соединения с Allegiant. Оно обеспечивает быструю передачу в реальном времени от коммутатора Allegiant к BVMS. Например, если в результате повреждения кабеля возникла потеря сигнала в Allegiant, системе BVMS немедленно отправляется уведомление. Вы также можете запрограммировать BVMS таким образом, чтобы она реагировала на тревоги Allegiant.

6.4.1 Общие сведения о подключении Bosch Allegiant

Чтобы установить подключение между BVMS и системой матричных коммутаторов Allegiant, необходимо настроить канал управления между BVMS и матричным коммутатором Allegiant.
Возможны два сценария:

– Локальное подключение
  Management Server управляет коммутатором Allegiant.
– Удаленное соединение
  Специальный ПК Bosch Allegiant, подключенный к сети, контролирует матричный коммутатор Allegiant.

Локальное подключение

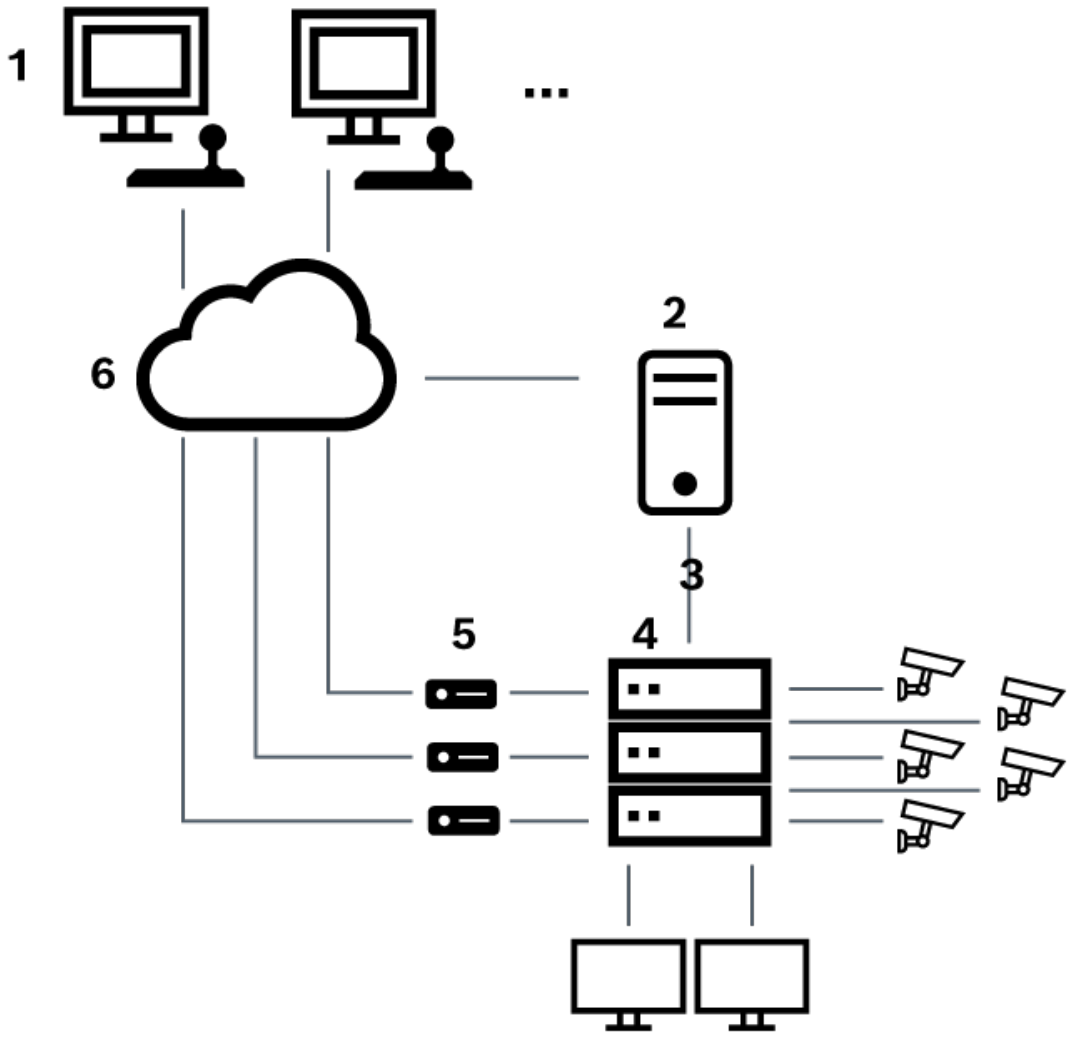


Рис. 6.3: Локальное подключение Bosch Video Management System к матричному коммутатору Bosch Allegiant

1	Клиентские рабочие станции BVMS
2	Management Server с ПО Master Control
3	Разъем RS-232
4	Матричный коммутатор Allegiant
5	Кодеры
6	Сеть

Удаленное соединение

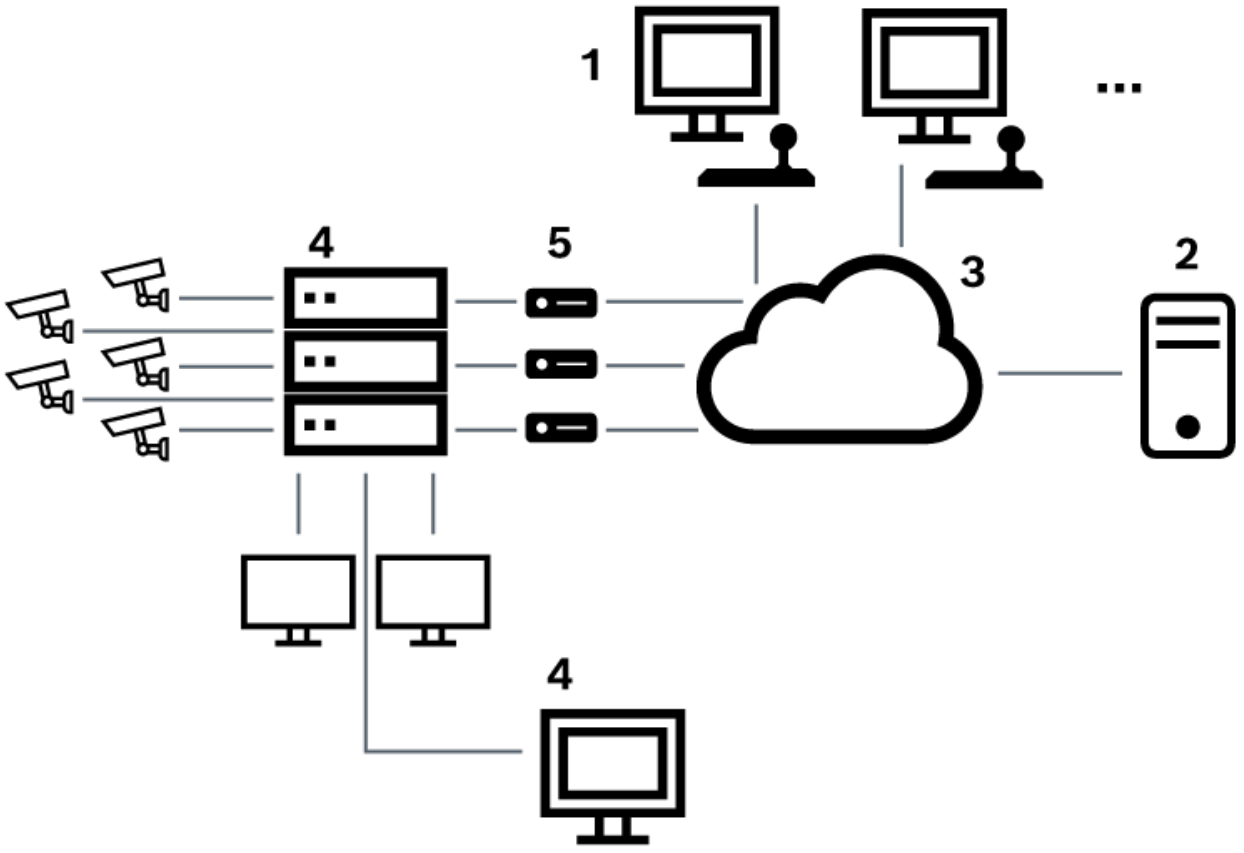


Рис. 6.4: Удаленное подключение Bosch Video Management System к матричному коммутатору Bosch Allegiant

1	Клиентские рабочие станции BVMS
2	Management Server с ПО Master Control
3	Сеть
4	ПК Allegiant с программным обеспечением MCS
5	Разъем RS-232
6	Кодеры
7	Матричный коммутатор Allegiant

6.4.2 Настройка контрольного канала

Для настройки контрольного канала следует выполнить следующие действия:

- Подключения
- Установка программного обеспечения
- Создание файла конфигурации Allegiant
- Добавление матричного коммутатора Allegiant к BVMS
- Настройка имен пользователей

Подключения

Для настройки контрольного канала между BVMS и матричным коммутатором Allegiant подключите один ПК через последовательный порт RS-232 к порту консоли Allegiant (используйте для подключения указанный кабель Bosch). Это может быть BVMS Management Server или любой другой компьютер в сети.

Установка программного обеспечения Allegiant Master Control Software

1. Остановите службу Management Server, если она запущена (**Пуск** > **Контрольная панель** > **Службы** > Щелчок правой кнопкой BVMS Management Server > **Stop**)
2. Установите Allegiant Master Control Software на Management Server и на ПК Allegiant (при наличии).
3. На удаленном ПК Allegiant настройте запуск программы Allegiant Network Host (ld_alghw.exe) при загрузке. В результате запускаются необходимые службы Allegiant, позволяющие другим компьютерам в сети получить доступ к Allegiant. Это ПО работает в фоновом режиме. Нет необходимости подключать к компьютеру защитный ключ.
   Чтобы служба запускалась на компьютере автоматически, следует скопировать ссылку на ld_alghw.exe в папку "Автозагрузка".

Создание файла конфигурации Bosch Allegiant

1. При помощи ПО Allegiant Master Control Software, создайте файл конфигурации Allegiant, в котором указан компьютер, подключенный к матричному коммутатору Allegiant. Для этого требуется защитный ключ Master Control.
2. В меню Transfer выберите Communication Setup. В списке Current Host введите DNS-имя компьютера, подключенного к матричному коммутатору Allegiant, и введите параметры последовательного порта (номер COM-порта, скорость передачи и т.д.), подключенного к Allegiant. Это позволит ПО Master Control Software на Management Server или ПК соединиться с системой Allegiant. В случае неудачи следует удостовериться, что ПО Master Control Software или программа Allegiant Network Host запущена на компьютере, подключенном к матричному коммутатору Allegiant, а параметры безопасности сети позволяют получить удаленный доступ к этому компьютеру.
3. В меню Transfer выберите пункт Upload. Выделите все таблицы и нажмите Upload. Чтобы сохранить файл конфигурации, выберите каталог.
4. Выйдите из Master Control Software.

Добавление матричного коммутатора Bosch Allegiant к BVMS

1. Запустите службу BVMSManagement Server, запустите Configuration Client и добавьте устройство Allegiant, добавив файл конфигурации (для получения пошаговых инструкций см. Добавление устройства).
2. Удостоверьтесь, что файл конфигурации Allegiant Master Control Software, используемый в BVMS, соответствует текущей конфигурации Allegiant.
   BVMS запускает необходимые компоненты ПО Master Control Software в фоновом режиме.

Настройка имени пользователя для подключения к службам Allegiant

Если матричный коммутатор Allegiant подключен к компьютеру в сети, а не к Management Server, следует удостовериться, что подключение к службам Allegiant на этом компьютере и на Management Server осуществляется с одной и той же учетной записи пользователя. Этот пользователь должен быть членом группы администраторов.

Более подробные сведения содержатся в документации

Подробные сведения обо всех окнах содержатся в следующих разделах:

– *Страница Матричные коммутаторы, Страница 138*

Пошаговые инструкции содержатся в следующих разделах:

– *Настройка устройства Bosch Allegiant, Страница 139*

См.

– *Страница Матричные коммутаторы, Страница 138*

6.4.3 Понятие о сателлитной конфигурации Allegiant компании Bosch

Матричные коммутаторы Allegiant позволяют объединить несколько систем Allegiant при помощи сателлитной конфигурации. В этом случае система BVMS рассматривает несколько систем Allegiant как одну большую систему, что обеспечивает доступ ко всем камерам во всех системах.

В сателлитной системе Allegiant выходы мониторов подчиненной системы Allegiant связаны с видеовходами главной системы Allegiant. Такое соединение называют магистральной линией. Кроме того, между главной и подчиненной системами устанавливается контрольный канал. При запросе камеры из подчиненной системы Allegiant главной системой Allegiant, в подчиненную систему отправляется команда, требующая перевести запрашиваемую камеру на магистральную линию. В это же время главная система Allegiant переключает вход магистральной линии на запрашиваемый выход монитора главной системы Allegiant. На этом видеоподключение подчиненной камеры к главному монитору завершается.

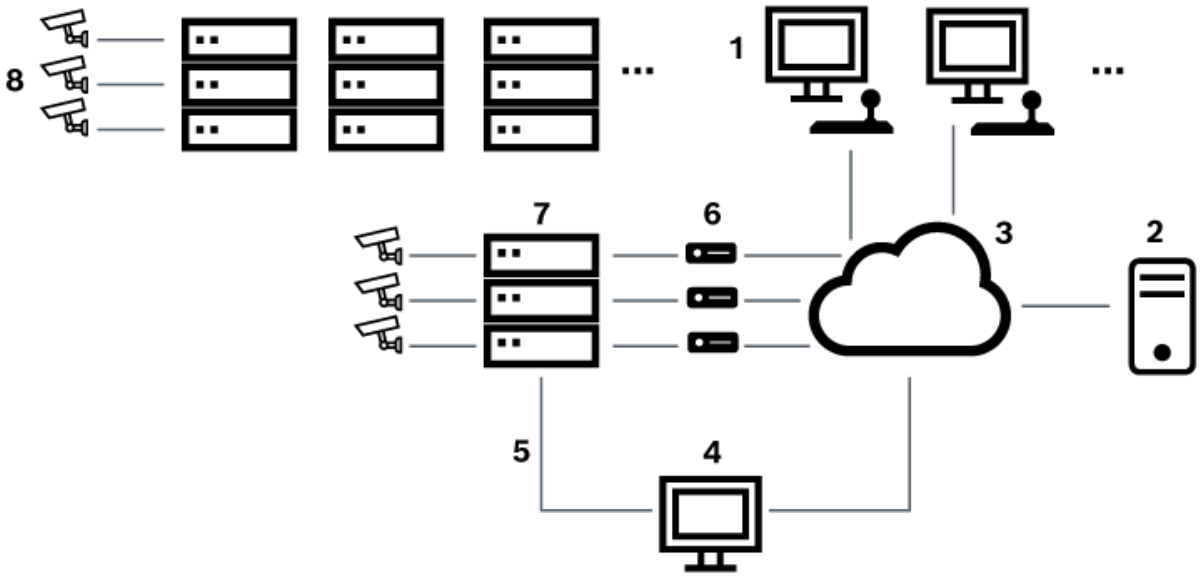


Рис. 6.5: Система Bosch Allegiant, расширенная за счет сателлитных коммутаторов

1	Клиентские рабочие станции BVMS
2	Management Server с ПО Master Control
3	Сеть
4	ПК Allegiant с программным обеспечением MCS
5	Разъем RS-232
6	Кодеры
7	Матричный коммутатор Allegiant

8	Сателлитный матричный коммутатор Allegiant

Сателлитная концепция может быть применена таким образом, что система Allegiant может быть одновременно главной и подчиненной. Таким образом, каждая система Allegiant может просматривать камеры с других систем. Необходимо только подключить магистральные и контрольные линии в обоих направлениях и правильно сконфигурировать таблицы Allegiant.
Эта концепция может расширяться практически безгранично. Система Allegiant может иметь множество подчиненных систем и сама может быть подчиненной по отношению ко многим главным. Вы можете запрограммировать таблицы Allegiant таким образом, чтобы разрешить или запретить пользователям доступ к камерам в соответствии с требованиями конкретного участка.

6.5 Команды Allegiant CCL, поддерживаемые в системе BVMS

Чтобы использовать команды CCL, вам потребуется руководство пользователя CCL. Данное руководство доступно в онлайн-каталоге продукции в разделе документации для каждого матричного коммутатора Allegiant LTC.

Поддерживаемые команды	**Описание**	**Примечания**
Переключение/ последовательность		
LCM	Переключение логической камеры на монитор	LCM, LCM+ и LCM-эквивалентны.
LCMP	Переключение логической камеры на монитор с вызовом препозиций	
MON+CAM	Переключение физической камеры на монитор	
MON-RUN	Запуск последовательности по номеру монитора	
MON-HOLD	Удержание последовательности по номеру монитора	
SEQ-REQ	Запрос последовательности	
SEQ-ULD	Выгрузка последовательности	
Приемное/ исполнительное устройство		

Поддерживаемые команды	Описание	Примечания
Переключение/ последовательность		
R/D	Основные команды управления	
REMOTE-ACTION	Одновременная команды управления панорамированием/ наклоном/ масштабированием	
REMOTE-TGL	Переключить команды управления панорамированием/ наклоном/ масштабированием	
PREPOS-SET	Установить препозицию	
PREPOS	Вызов препозиции	
AUX-ON AUX-OFF	Вспомогательные команды управления – Вспомогательные команды активированы – Вспомогательные команды деактивированы	
VARSPEED_PTZ	Команды управления переменной скоростью	
Тревога		Используется для управления виртуальными входами. Например, «+тревога 1» закрывает виртуальный вход 1, «-тревога 1» открывает виртуальный вход 1
+ALARM	Активировать тревогу	Открывает виртуальный вход в BVMS.
-ALARM	Деактивировать тревогу	Закрывает виртуальный вход в BVMS.
Система		
TC8x00>HEX	Установить шестнадцатеричный режим	

Поддерживаемые команды	Описание	Примечания
Переключение/ последовательность		
TC8x00>DECIMAL	Установить десятичный режим	

7 Используйте самую актуальную версию ПО

Перед первым использованием устройства установите самую актуальную версию ПО. Для обеспечения оптимальных функциональных возможностей, совместимости, производительности и безопасности регулярно обновляйте ПО в течение всего срока эксплуатации устройства. Следуйте инструкциям в документации к продукту в отношении обновлений ПО.

Мы выпускаем обновления только для общедоступных и ограничено доступных версий программного обеспечения. Подробнее:

Поддержка и обслуживание программного обеспечения Bosch Building Technologies.

Более подробную информацию можно получить по следующим ссылкам:

- общие сведения: https://www.boschsecurity.com/xc/en/support/product-security/
- рекомендации по безопасности, а именно список обнаруженных уязвимых мест и предлагаемых решений: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Компания Bosch не берет на себя никакой ответственности за какой-либо ущерб, вызванный эксплуатацией ее продуктов при использовании устаревшего ПО.

8 Начало работы

В данном разделе содержится информация о том, как приступить к работе с BVMS.

8.1 Установка программных модулей

Замечание!
Установите на компьютер все необходимые модули программного обеспечения.

Установка

Закройте Configuration Client, прежде чем запустить установку BVMS.

1. запустите Setup.exe или запустите программу установки BVMS на экране приветствия.
2. В следующем диалоговом окне выберите модули, которые должны быть установлены на данном компьютере.
3. Следуйте инструкциям на экране.

8.2 Использование мастера настройки конфигурации

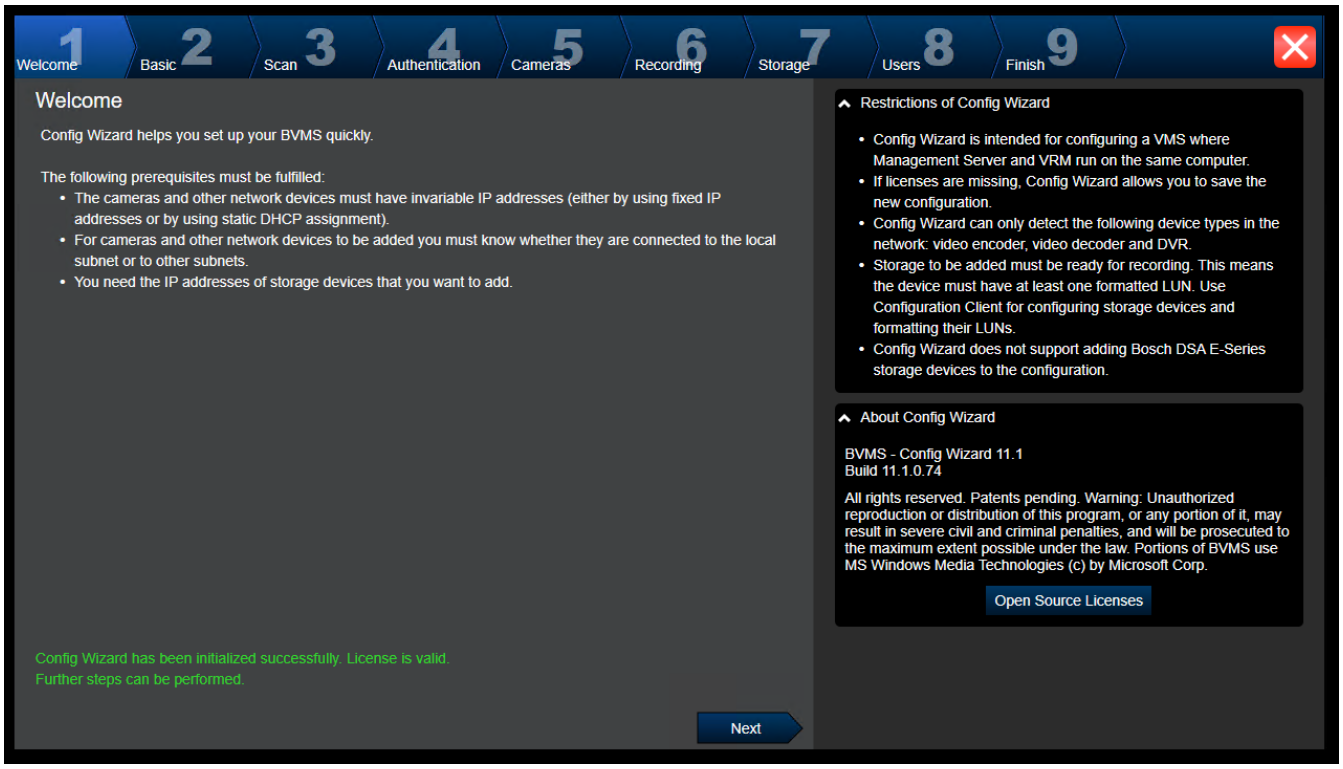
Config Wizard предназначен для простой и быстрой настройки небольших систем. Config Wizard помогает настроить конфигурацию системы, включая VRM, систему iSCSI, Mobile Video Service, камеры, профили записи и группы пользователей.
При стандартной установке программного обеспечения системы iSCSI необходимо добавлять вручную.
Группы пользователей и их разрешения настраиваются автоматически. Можно добавлять или удалять пользователей и задавать пароли.
Config Wizard может получить доступ к Management Server только на локальном компьютере.
Активированную конфигурацию можно сохранить в качестве резервной копии и импортировать эту конфигурацию позднее. После импорта импортированную конфигурацию можно изменить.
Config Wizard добавляет локальный VRM автоматически как при стандартной установке ПО, так и в случае DIVAR IP 3000 и DIVAR IP 7000.
В случае DIVAR IP 3000 и DIVAR IP 7000 локальное устройство iSCSI также добавляется автоматически, если оно еще не доступно.
В случае DIVAR IP 3000 и DIVAR IP 7000 локальная служба Mobile Video Service добавляется автоматически, если она еще не доступна.

Замечание!
Если в системе необходимо использовать декодеры, убедитесь, что все кодеры используют один и тот же пароль для уровня авторизации user.

Для запуска Config Wizard**:**

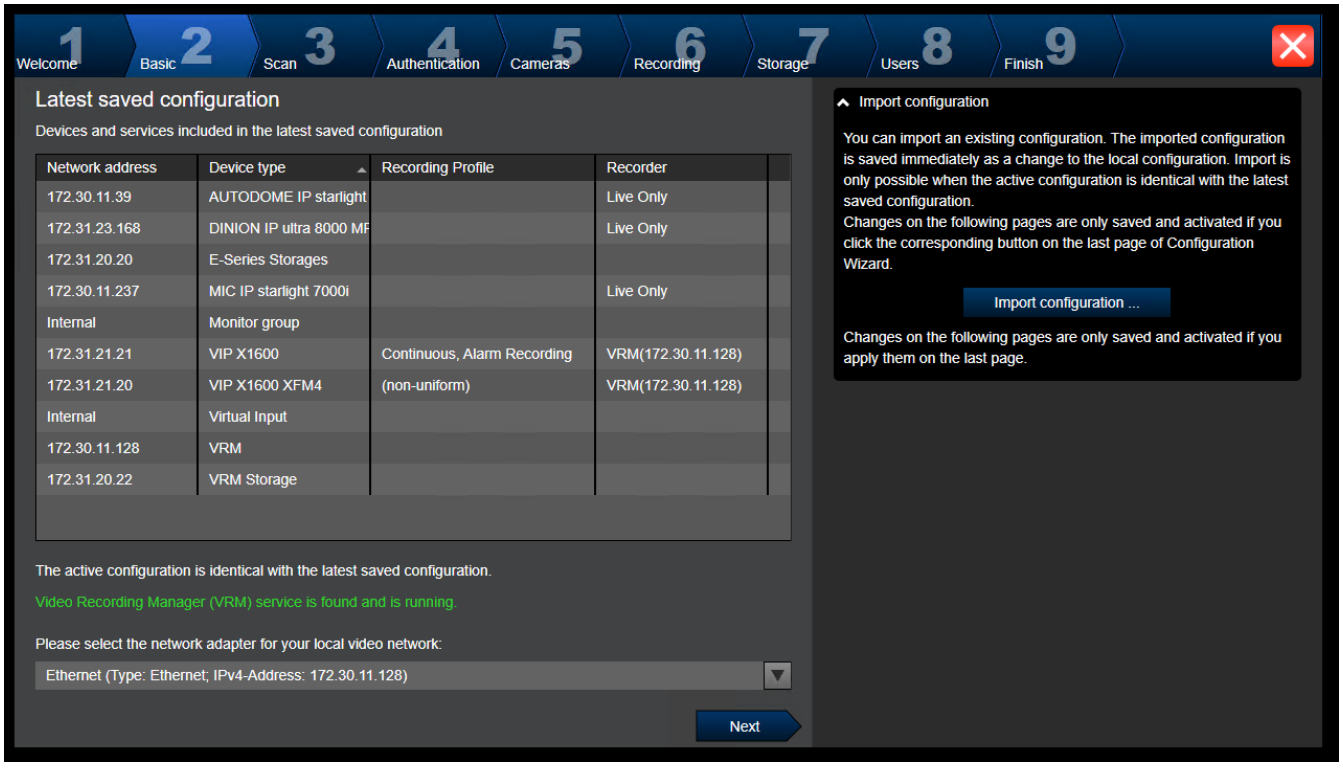
- нажмите **Пуск** > **Все программы** > BVMS > Config Wizard
  Откроется страница Welcome.

Страница Welcome



- Нажмите **Next**, чтобы продолжить.

Страница Basic

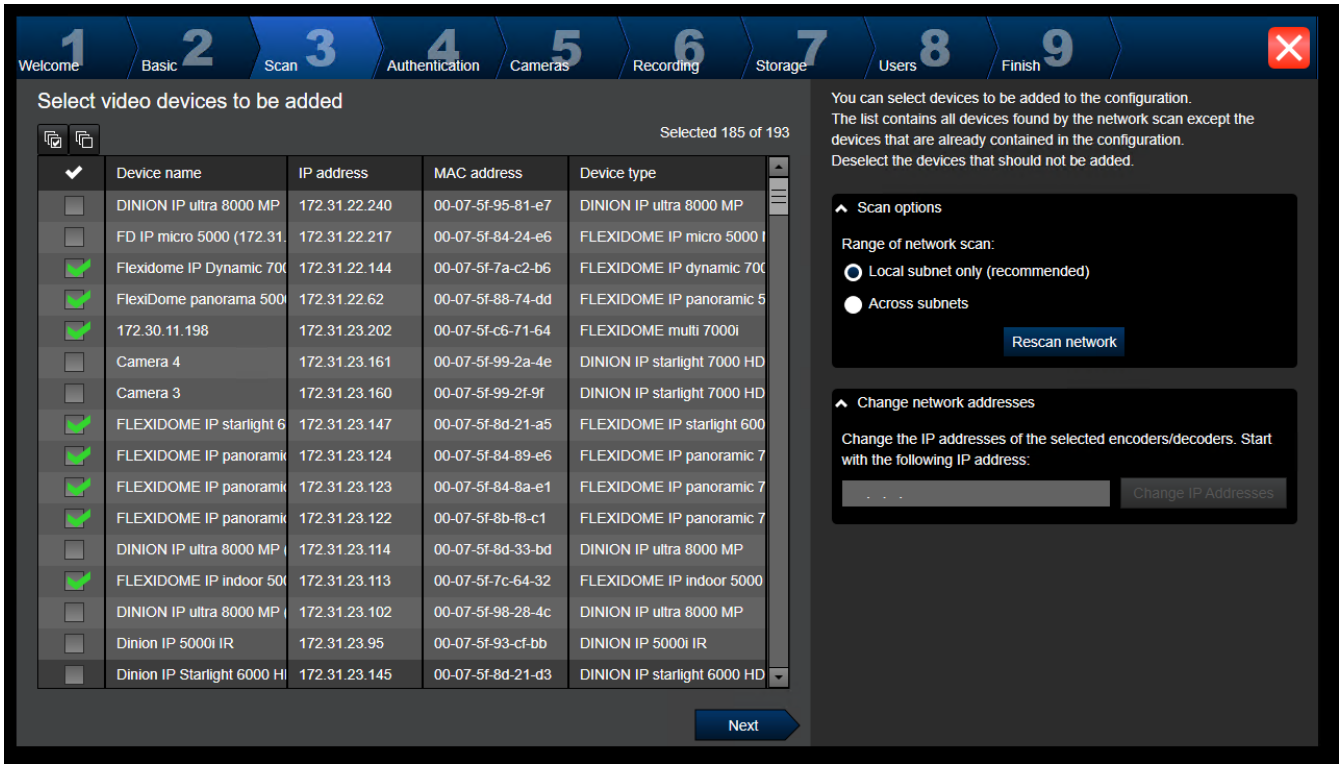


На этой странице отображается последняя сохраненная конфигурация. Можно импортировать файл BVMS в качестве изменения для имеющейся конфигурации. Это изменение сохраняется, но не активируется при нажатии **Next**.

Можно выбрать сетевой адаптер своего компьютера, подключенного к видеоустройствам (IP-камеры, кодеры, декодеры, системы хранения iSCSI) системы. IP-адрес этого сетевого адаптера используется как IP-адрес системы VRM, VSG и локальной системы хранения iSCSI.

Нажмите **Port Mapping**, чтобы задать внешний IP-адрес или DNS-имя, если будет производиться доступ к системе через Интернет.

Страница Scan



Примечание.

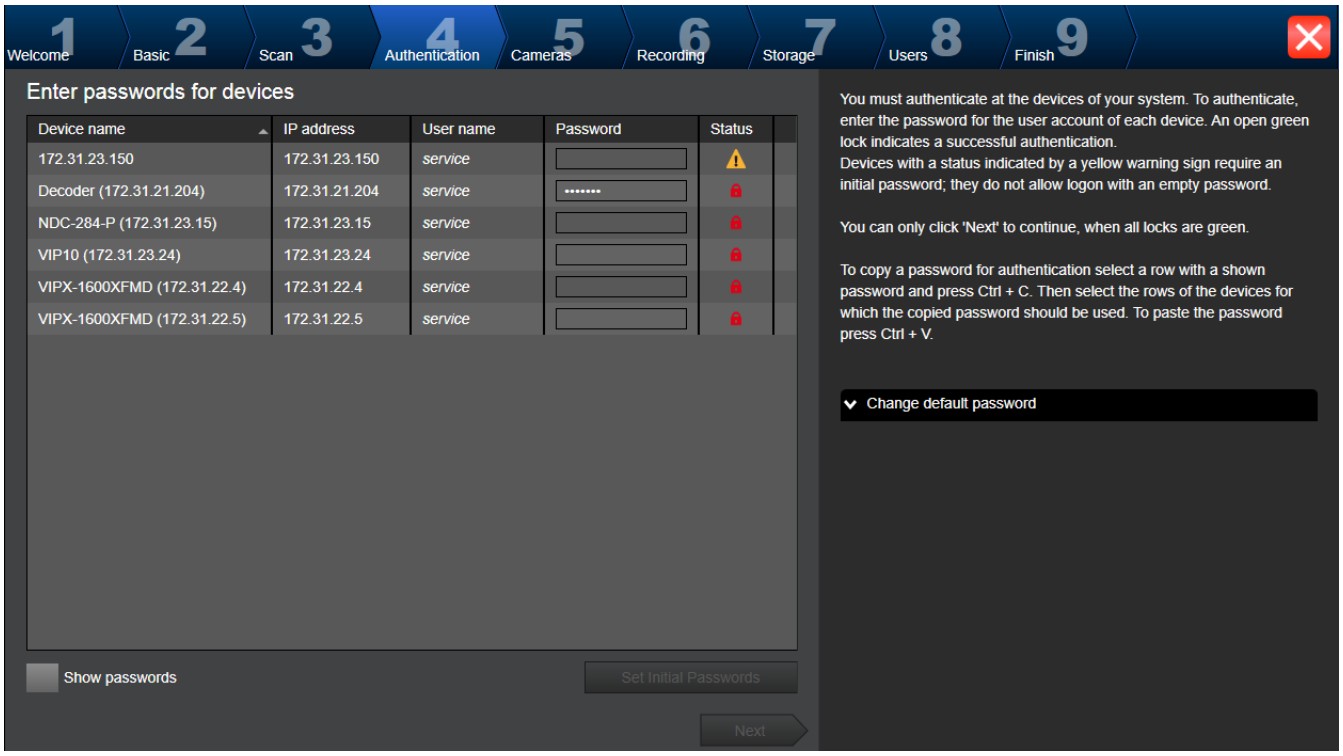
Поиск устройств может занять некоторое время. Поиск можно отменить. Все уже найденные устройства будут отображены в таблице.

На этой странице отображаются все видеоустройства, не включенные в последнюю сохраненную конфигурацию.

Снимите флажки для тех устройств, которые не должны быть добавлены в конфигурацию, а затем нажмите **Next**.

Если выбранное устройство находится в диапазоне IP-адресов, отличном от диапазона системы DIVAR IP, IP-адрес устройства можно изменить, задав начальный адрес диапазона IP-адресов устройства.

Страница Authentication



Эта страница используется для проверки подлинности всех видеоустройств, защищенных паролем. Для облегчения проверки подлинности с помощью одного пароля для нескольких устройств можно использовать буфер обмена (CTRL+C, CTRL+V).

1. Нажмите **Show passwords**.
2. Выберите строку с успешно прошедшим проверку подлинности устройством (отображается зеленый замок), нажмите CTRL+C, выберите несколько строк с красным замком и нажмите CTRL+V).

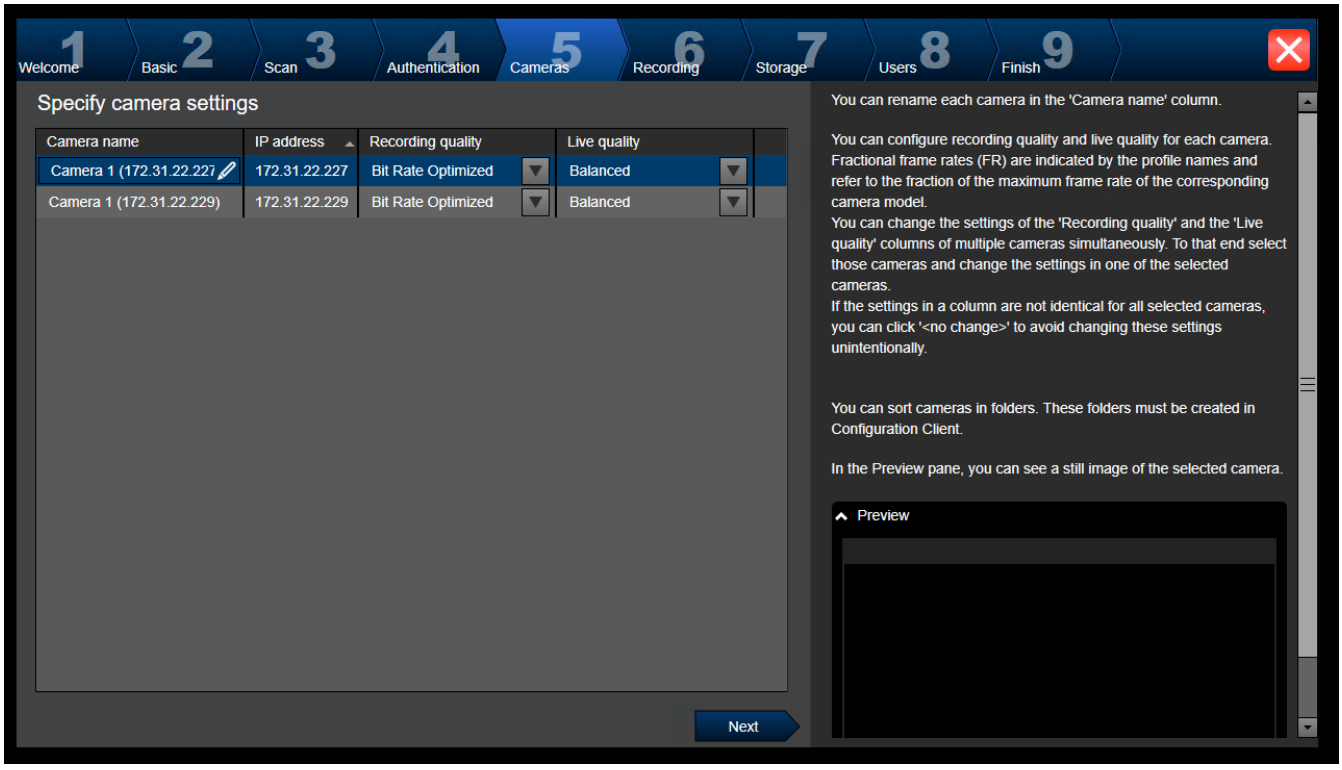
Проверка пароля выполняется автоматически, если следующий символ в поле пароля не вводится в течение нескольких секунд или кнопка мыши нажимается вне поля пароля. Можно установить глобальный пароль по умолчанию для всех устройств, которые в данный момент не защищены паролем.

Если для устройства требуется начальный пароль, отображается  .

Для установки начального пароля:

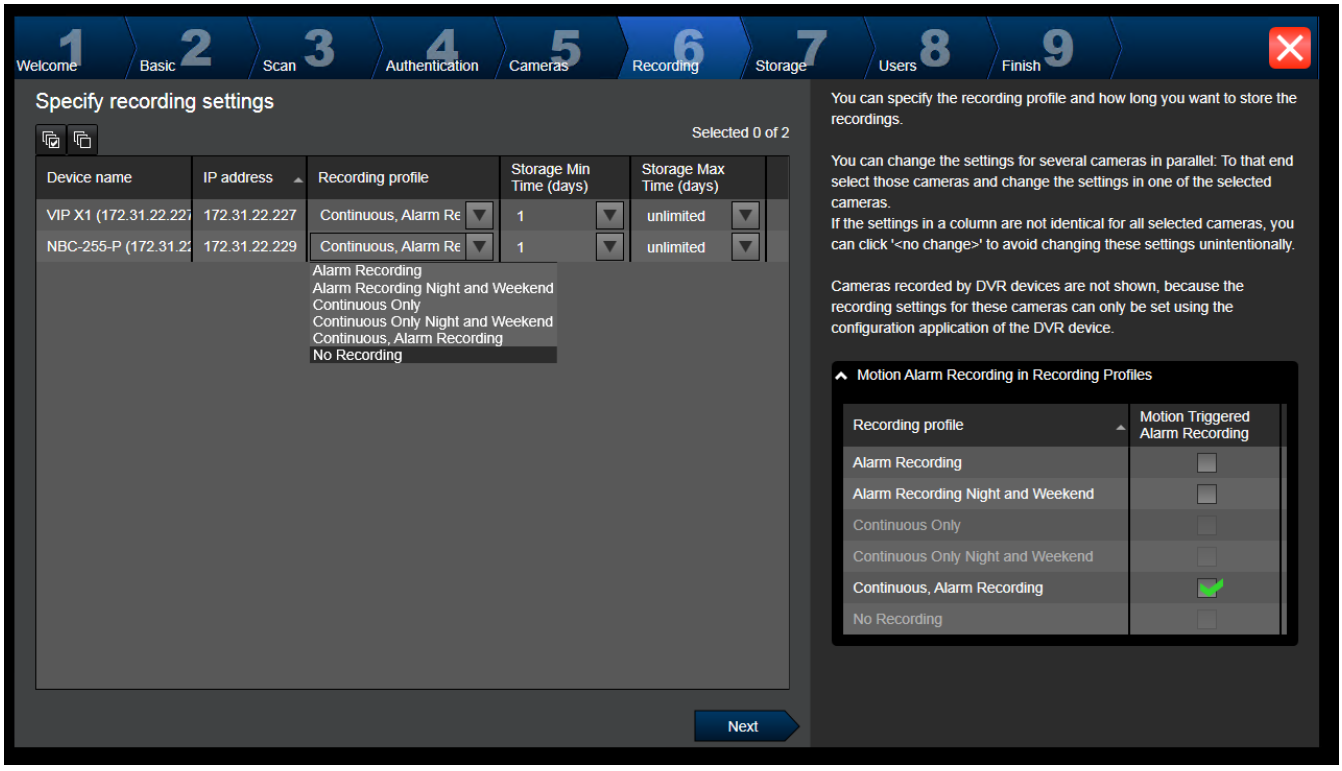
1. Введите пароль в поле **Password**.
2. Нажмите **Set Initial Passwords**.
   Установлен первоначальный пароль.
   Примечание: пока вы не установили первоначальный пароль для всех устройств в списке, которые требуют начального пароля, вы не сможете продолжить работу.
3. Нажмите **Next**, чтобы продолжить.

Страница Cameras



Эта страница используется для управления камерами системы.

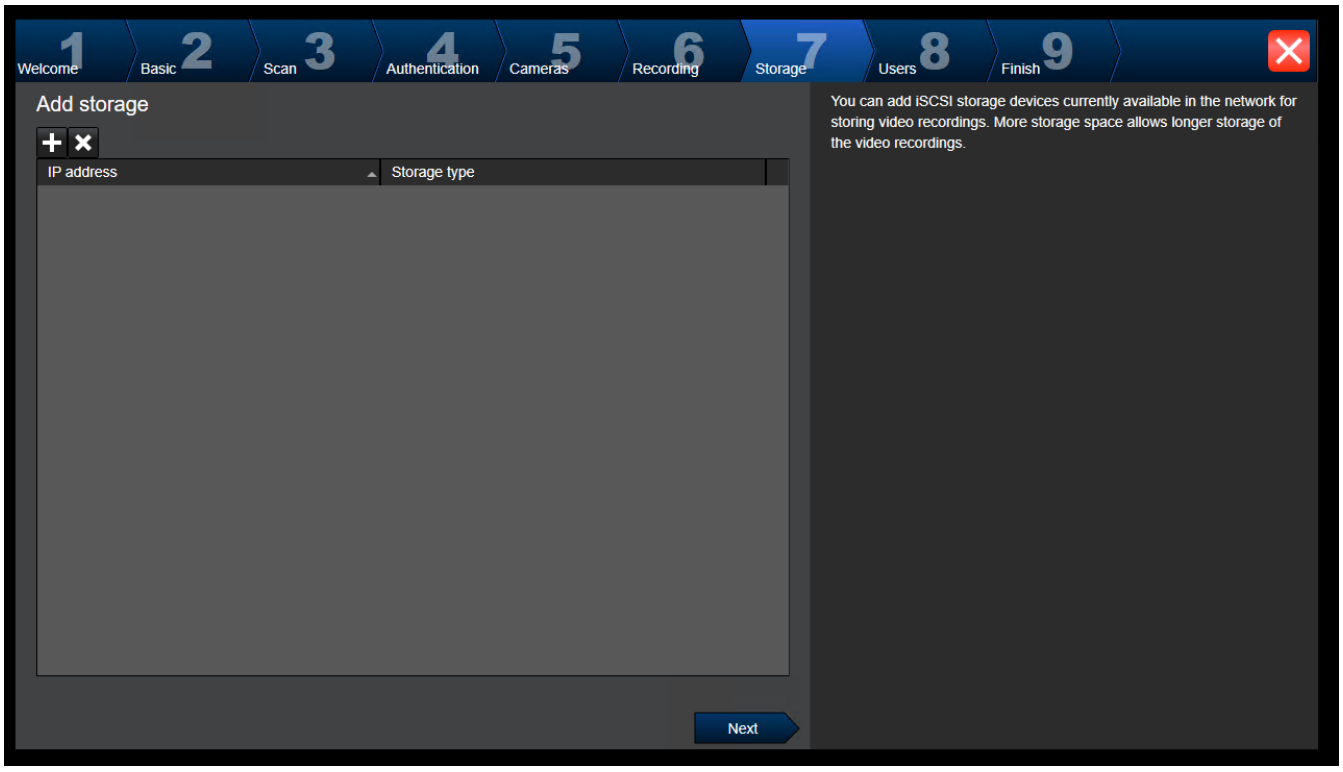
Страница Recording



На этой странице отображаются только новые добавленные камеры. После включения этой конфигурации невозможно изменить назначение профилей этих камер.

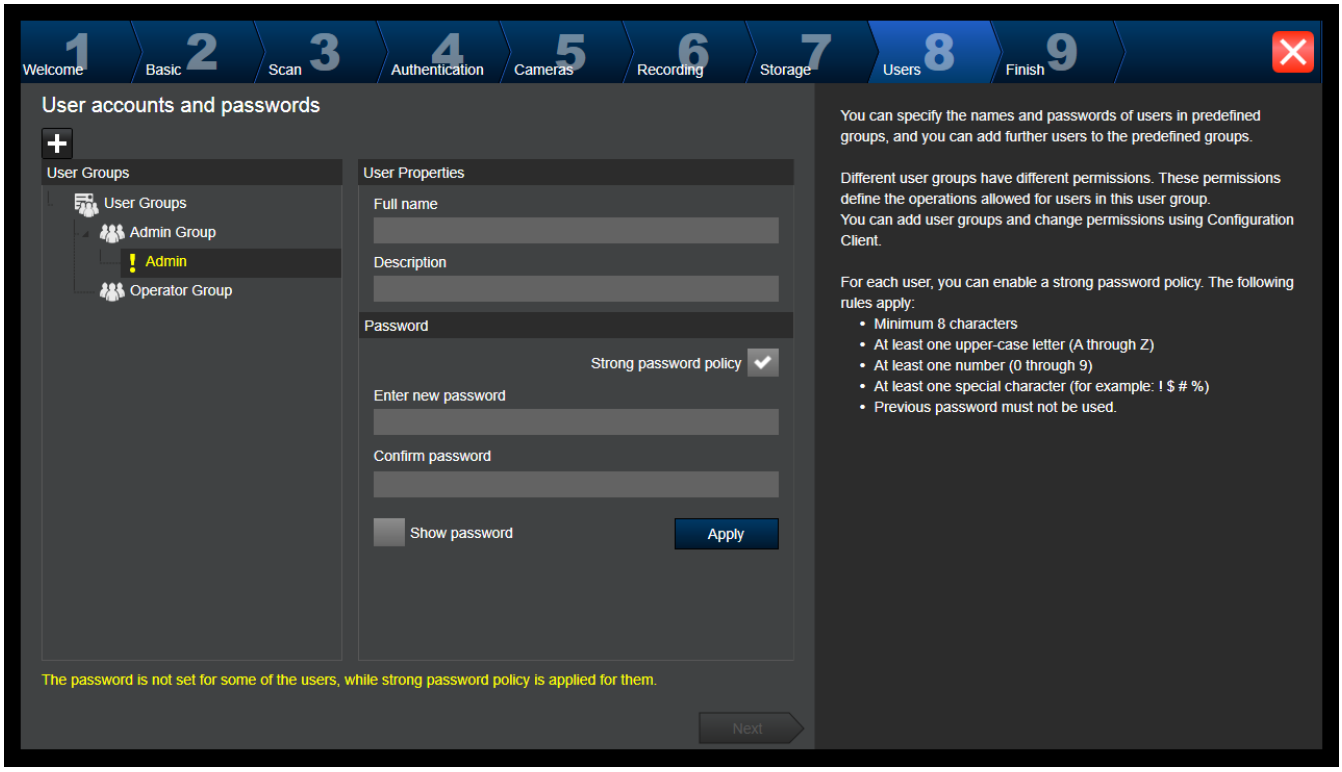
Можно включить запись по движению для профилей записи, для которых включена как запись, так и запись по тревоге. При необходимости настройте запись и запись по тревоге в Configuration Client (диалоговое окно **Настройки записи по расписанию**). VCA активируется автоматически для всех новых добавляемых камер.

Страница Storage



На этой странице можно добавлять дополнительные устройства хранения iSCSI

Страница Users



На этой странице можно добавить новых пользователей в существующие пользовательские группы.

- Введите имя пользователя и описание для каждого нового пользователя и задайте пароль.

Strong password policy

Флажок **Strong password policy** предварительно установлен для всех вновь созданных пользовательских групп.

Мы настоятельно рекомендуем сохранить этот параметр в целях обеспечения защиты вашего компьютера от несанкционированного доступа.

Применяются следующие правила:

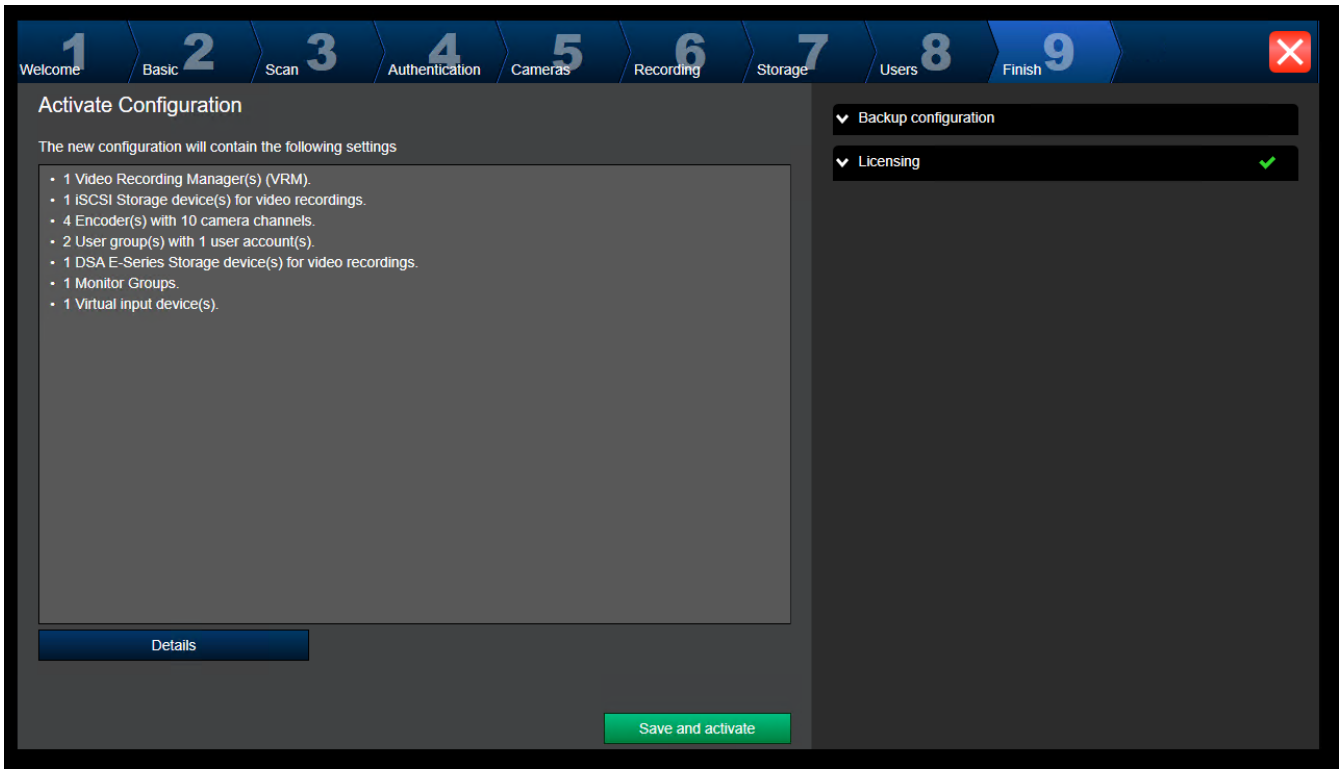
- Минимальная длина пароля соответствует указанной на странице **Политики учетных записей** для соответствующих групп пользователей.
- Не используйте один из предыдущих паролей.
- Используйте по крайней мере одну букву в верхнем регистре (A–Z).
- Используйте по крайней мере одну цифру (0–9).
- Используйте по крайней мере один специальный символ (например, ! $ # %).

- Нажмите кнопку **Apply**, чтобы применить параметры, затем нажмите **Next**для продолжения.

  Примечание: вы не сможете продолжить работу до тех пор, пока для всех пользователей, для которых установлен флажок **Strong password policy**, не будут заданы пароли. Чтобы продолжить, задайте недостающие пароли.

Используйте Configuration Client для добавления групп пользователей и изменения разрешений групп пользователей.

Страница Finish



Прежде чем активировать конфигурацию, необходимо выполнить следующие действия:

– Установить глобальный пароль по умолчанию для всех устройств, которые в данный момент не защищены паролем.
– При необходимости активировать лицензию.

Глобальный пароль по умолчанию

Если в клиенте Configuration Client отключен параметр **Enforce password protection on activation** (**Параметры** -> **Опции**), для активации не обязательно предоставлять глобальный пароль по умолчанию.

Лицензирование

Разверните пункт **Licensing** и нажмите кнопку **License Wizard**, чтобы проверить или активировать пакет лицензий.

После нажатия кнопки **Save and activate** конфигурация активируется.

После успешной активации снова открывается страница **Finish**. Теперь при желании можно сохранить резервную копию данной конфигурации; для этого нажмите **Save backup copy**.

После нажатия кнопки **Save and activate** конфигурация активируется.

После успешной активации снова открывается страница **Готово**. Теперь при желании можно сохранить резервную копию данной конфигурации; для этого нажмите **Save backup copy**.

8.3 Запуск Configuration Client

Замечание!

Только пользователи группы администраторов могут подключиться к Configuration Client.

Предварительно настроенный пользователь группы администраторов по умолчанию — Admin. Только этот пользователь может подключиться к Configuration Client при первом запуске Configuration Client.
После запуска Configuration Client можно переименовать пользователя Admin и изменить пароль.

Примечание.
Невозможно запустить Configuration Client, если другой пользователь на другом компьютере в системе уже запустил модуль Configuration Client.

Запуск Configuration Client

1. В меню **Пуск** выберите **Программы** > BVMS > Configuration Client.
   Отобразится диалоговое окно для входа в систему.
2. Введите свое имя пользователя в поле **Имя пользователя:**.
   При первом запуске приложения введите в качестве имени пользователя Admin, пароль при этом не требуется.
3. Введите пароль в поле **Пароль:**.
4. Нажмите **ОК**.
   Приложение запустится.

Когда пользователь-администратор впервые запускает Configuration Client, отображается диалоговое окно **Нарушение политики паролей** с предложением установить пароль для учетной записи администратора. Мы настоятельно рекомендуем сохранить этот параметр и задать надежный пароль для учетной записи администратора в соответствии с требованиями политики паролей.

См.
- *Строгая политика паролей , Страница 364*
- *Настройка группы администраторов, Страница 369*

8.4 Настройка языка Configuration Client

Настройка языка Configuration Client не зависит от языковых настроек Windows.

Чтобы настроить язык:

1. В меню **Настройки** выберите пункт **Параметры...**.
   Откроется диалоговое окно **Параметры**.
2. В списке **Язык** выберите нужный язык.
   При выборе **Системный язык** используется язык, настроенный в Windows.
3. Нажмите **ОК**.
   Языковые настройки вступают в силу после перезапуска приложения.

8.5 Настройка языка Operator Client

Настройка языка Operator Client не зависит от языковых настроек Windows и настроек модуля Configuration Client. Это действие выполняется в модуле Configuration Client.

Чтобы настроить язык:

1. Нажмите **Группы пользователей** >  . Перейдите на вкладку **Свойства группы пользователей**. Перейдите на вкладку **Рабочие разрешения**.
2. В списке **Язык** выберите нужный язык.
3. Нажмите  , чтобы сохранить настройки.

4. Нажмите  для активации конфигурации.
   Перезапуск Operator Client.

8.6 Поиск устройств

Главное окно > **Устройства**

Можно выполнять поиск следующих устройств для добавления с помощью диалогового окна **BVMS Scan Wizard**:

- Устройства VRM
- Кодеры
- Кодеры с локальным хранилищем и работающие только в режиме реального времени
- Кодеры ONVIF, работающие только в режиме реального времени
- Кодеры с локальными хранилищами
- Декодеры
- Устройства шлюза Video Streaming Gateway (VSG)
- Устройства DVR

Сведения о добавлении устройств путем поиска см. в разделе о соответствующем устройстве в главе *Страница Устройства, Страница 128*.

См.

- *Добавление устройств VRM путем поиска, Страница 177*
- *Добавление устройства ONVIF, работающего только в режиме реального времени, путем сканирования, Страница 245*
- *Добавление устройств, работающих только в режиме реального времени, путем поиска, Страница 218*
- *Добавление устройства, Страница 129*

8.7 Доступ к системе

Для доступа к системе выполните следующие действия:

1. Выполните одно из следующих действий для выбора сетевого адреса нужной системы:
   - Нажмите заранее выбранный элемент списка.
   - Введите сетевой адрес вручную.
   - Выберите сетевой адрес с помощью Server Lookup.
2. Вход в нужную систему:
   - Система с одним сервером
   - Система Enterprise

8.8 Использование просмотра сервера

- Функция BVMS Server Lookup позволяет операторам подключаться к BVMSManagement Server из доступного списка серверов.
- Один пользователь Configuration Client или Operator Client может последовательно подключаться к нескольким системным точкам доступа.
- Системные точки доступа могут быть Management Server или Enterprise Management Server.
- Server Lookup использует специальный Management Server для размещения списка серверов.

– Функции Server Lookup и Management Server или Enterprise Management Server могут быть запущены на одном компьютере.
– Server Lookup поддерживает поиск системных точек доступа по имени или описанию.
– Operator Client, подключенный к Management Server, принимает события и тревоги с BVMS Management Server и отображает данные в режиме реального времени и воспроизведения записей.

Доступ:

1. Запустите клиент Operator Client или Configuration Client.
   Откроется диалоговое окно входа в систему.
2. В списке **Соединение:** выберите пункт **<Адресная книга...>** для Configuration Client или **<Адресная книга...>** для Operator Client.
   Если для сервера задан внутренний и внешний IP-адреса, они будут указаны.
   При первом выборе **<Адресная книга...>** или **<Адресная книга...>** откроется диалоговое окно **Server lookup**.
3. Введите допустимый сетевой адрес необходимого сервера в поле **Адрес сервера (Enterprise) Management Server**.
4. Введите допустимые имя пользователя и пароль.
5. При необходимости нажмите пункт **Запомнить параметры**.
6. Нажмите **OK**.
   Откроется диалоговое окно **Server lookup**.
7. Выберите необходимый сервер.
8. Нажмите **OK**.
9. Если у выбранного сервера есть и внутренний, и внешний сетевые адреса, появится сообщение, спрашивающее, используете ли вы компьютер, расположенный во внутренней сети выбранного сервера.
   Имя сервера добавляется в список **Соединение:** в диалоговом окне входа.
10. Выберите этот сервер в списке **Соединение:** и нажмите кнопку **OK**.
    Если вы установили флажок **Запомнить параметры**, при следующем доступе этот сервер можно выбрать напрямую.

8.9 Активация лицензии на программное обеспечение

При установке BVMS в первый раз, необходимо активировать лицензии на программные пакеты, которые вы заказали, включая базовый пакет и все расширения и/или дополнительные возможности.

Для активации системы:

1. запустите BVMS Configuration Client.
2. В меню **Сервис** нажмите **Диспетчер лицензий...**.
   Откроется диалоговое окно **Диспетчер лицензий**.
3. Нажмите **Добавить** , чтобы добавить свои лицензии.
   Отобразится **Добавить лицензию** диалоговое окно.
4. Следуйте инструкциям в диалоговом окне.
5. После успешной активации закройте диалоговое окно **Добавить лицензию**.
6. Закройте диалоговое окно **Диспетчер лицензий**.

Дополнительную информацию можно найти в соответствующем официальном документе по лицензированию BVMS.

См.

- *Диалоговое окно «Проверка лицензий» (меню «Инструменты»), Страница 79*
- *Диалоговое окно «Диспетчер лицензий» (меню «Инструменты»), Страница 78*
- *Добавить диалоговое окно лицензии, Страница 79*
- *Обзор активации лицензии BVMS, Страница 19*

8.9.1 Диалоговое окно «Диспетчер лицензий» (меню «Инструменты»)

Главное окно > меню **Сервис** > команда **Диспетчер лицензий...**

Позволяет лицензировать заказанный пакет BVMS и обновлять его дополнительными возможностями.

Состояние лицензии

Индикация состояния лицензии.

"Отпечаток пальца" системы

Для получения поддержки мы рекомендуем предоставить **"Отпечаток пальца" системы**.

Объект установки

При активации базовой лицензии в Bosch Remote Portal вы предоставляете информацию о месте установки своей системы. Здесь отображается эта информация.

Примечание: Вы также можете предоставлять эту информацию в других лицензиях, но здесь отображается только информация, представленная с базовой лицензией.

Лицензии

1. Нажмите **Добавить** , чтобы добавить свои лицензии.
   Отобразится **Добавить лицензию** диалоговое окно.
2. Следуйте инструкциям в диалоговом окне.

Действующая лицензия

Отображает действующую базовую лицензию, которую вы активировали.

Функциональные возможности

- Нажмите **Инспектор лицензий...**.
  Откроется диалоговое окно **Инспектор лицензий**.

Показывает количество установленных лицензионных функций.

Можно проверить, не превышает ли количество установленных лицензий BVMS количество приобретенных лицензий.

Установленная версия BVMS

Показывает установленную версию BVMS, например 11.0.

Лицензированные версии BVMS

Показывает все версии BVMS, которые включены в текущий файл лицензии и поддерживаются текущим предоставленным файлом лицензии.

Например, BVMS 11.0 и все последующие вспомогательные номера версии BVMS 11.x.

Дата активации

Отображает дату активации установленной версии BVMS.

Дата окончания срока действия

Отображает дату окончания действия установленной версии BVMS. Дата окончания действия применяется только при установке резервной лицензии или демонстрационных лицензий для продажи.

Software Maintenance Agreement

Дата окончания срока действия

Если вы приобрели и активировали любой вариант Software Maintenance Agreement, то дата окончания срока действия отображается здесь.

См.

- *Активация лицензии на программное обеспечение, Страница 77*
- *Добавить диалоговое окно лицензии, Страница 79*
- *Диалоговое окно «Проверка лицензий» (меню «Инструменты»), Страница 79*

8.9.1.1 Добавить диалоговое окно лицензии

Главное окно> **Сервис** меню > **Диспетчер лицензий...** команда > **Лицензии** > **Добавить**
Позволяет добавлять в систему приобретенные лицензии или демонстрационные лицензии с веб-сайта Bosch Remote Portal remote.boschsecurity.com BVMS.
Чтобы добавить лицензии, следуйте инструкциям в диалоговом окне.
Дополнительную информацию можно найти в соответствующем официальном документе по лицензированию BVMS.

8.9.2 Добавить диалоговое окно лицензии

Главное окно> **Сервис** меню > **Диспетчер лицензий...** команда > **Лицензии** > **Добавить**
Позволяет добавлять в систему приобретенные лицензии или демонстрационные лицензии с веб-сайта Bosch Remote Portal remote.boschsecurity.com BVMS.
Чтобы добавить лицензии, следуйте инструкциям в диалоговом окне.
Дополнительную информацию можно найти в соответствующем официальном документе по лицензированию BVMS.

8.9.3 Диалоговое окно «Проверка лицензий» (меню «Инструменты»)

Главное окно > меню **Сервис**, нажмите команду **Инспектор лицензий...** > диалоговое окно **Инспектор лицензий**
Показывает количество установленных лицензионных функций.
Можно проверить, не превышает ли количество установленных лицензий BVMS количество приобретенных лицензий.
Примечание: Если текущая конфигурация системы не соответствует ограничениям установленных в данный момент лицензий, то активировать конфигурацию невозможно.

8.10 Обслуживание BVMS

В данном разделе содержится информация об обслуживании недавно установленной или обновленной системы BVMS.
Для проведения обслуживания системы выполните следующие действия.

- Экспортируйте конфигурацию BVMS и настройки пользователя. История версий (все версии конфигурации, активированные ранее) не экспортируется. Рекомендуется активировать конфигурацию перед экспортом.
  - Информацию об этой процедуре см. в разделе *Чтобы экспортировать параметры конфигурации:, Страница 80*.

или

- Выполните резервное копирование elements.bvms. Это необходимо, если требуется восстановить (Enterprise) Management Server, включая историю версий. Настройки пользователя не включаются.
  - Информацию об этой процедуре см. в разделе *Выполнение резервного копирования., Страница 80*.
- Сохраните файл конфигурации VRM (config.xml)
  - Информацию об этой процедуре см. в разделе *Сохранение конфигурации VRM., Страница 80*.

Экспортированная конфигурация не содержит историю системы. Откат конфигурации невозможен.

Вся конфигурация системы, включая полную историю изменений системы, сохраняется в одном файле.
C:\ProgramData\Bosch\VMS\Elements.bvms.

Чтобы экспортировать параметры конфигурации:

1. В меню **Система** нажмите кнопку **Конфигурация экспорта...**
   Откроется диалоговое окно **Экспортировать файл конфигурации**.
   Примечание. Если текущая рабочая копия конфигурации не активирована (активен ), экспортируется данная рабочая копия, а не активированная конфигурация.
2. Нажмите **Сохранить**.
3. Введите имя файла.
   Экспортируется текущая конфигурация. Создается ZIP-файл с базой данных и данными пользователя.

Выполнение резервного копирования.

1. Остановите службу **Central Server** BVMS в (Enterprise) Management Server.
2. Скопируйте файл elements.bvms в требуемый каталог для резервного копирования.
3. Запустите службу **Central Server** BVMS в (Enterprise) Management Server.

Конфигурация VRM сохраняется в одном зашифрованном файле config.xml.
Этот файл можно скопировать и сохранить для создания резервной копии, когда служба VRM запущена и работает.
Этот файл зашифрован и содержит все необходимые данные VRM, такие как:

- Данные пользователя
- Все системные устройства и их соответствующие параметры VRM

Части конфигурации VRM также сохраняются в конфигурации BVMS. Если в эти данные вносятся какие-либо изменения, данные записываются в config.xml после активации конфигурации BVMS.
Следующие настройки не сохраняются в конфигурации BVMS:

- **Настройки VRM** > **Основные параметры**
- **Сеть** > **SNMP**
- **Обслуживание** > **Дополнительно**
- **Параметры записи**
- **Балансировка загрузки**

Если на одной из этих страниц вносятся какие-либо изменения, они незамедлительно записываются на сервер VRM и не сохраняются в конфигурации BVMS.

Сохранение конфигурации VRM.

- Скопируйте Config.xml в безопасное место.
  Этот файл можно найти в следующем каталоге для основного диспетчера VRM:
  C:\ProgramData\Bosch\VRM\primary
  Этот файл можно найти в следующем каталоге для вторичного диспетчера VRM:
  C:\ProgramData\Bosch\VRM\\secondary

8.11 Замена устройства

В данном разделе содержится информация о способах восстановления системы, например, когда происходит сбой устройства и его необходимо заменить.

Предварительное условие
Операции обслуживания выполнены.

См.

– *Обслуживание BVMS, Страница 79*

8.11.1 Замена MS / EMS

Разницы между заменой Management Server и Enterprise Management Server нет.
Можно либо восстановить конфигурацию старого Management Server или Enterprise Management Server, а также можно импортировать экспортированную конфигурацию.
При восстановлении конфигурации идентификатор сервера остается неизменным.
При импорте конфигурации используется идентификатор сервера новой системы. Новый идентификатор сервера требуется, если необходимо создать Enterprise System с помощью экспортированной конфигурации, которая импортируется на каждом Management Server в качестве шаблона. Каждый Management Server в этой Enterprise System должен иметь уникальный идентификатор сервера.
Можно импортировать экспортированную конфигурацию и настройки пользователя этой конфигурации. Настройки пользователя содержат пользователей, которые были добавлены в эту конфигурацию и соответствующие им настройки в Operator Client, такие как размеры окон и закладки.
Примечание. Импорт конфигурации не восстанавливает историю версий старой конфигурации. При импорте конфигурации настройки пользователя не импортируются. Необходимо вручную восстанавливать экспортированные настройки пользователя.

Чтобы импортировать конфигурацию:

1. В меню **Система** нажмите **Import configuration ...**.
   Откроется диалоговое окно **Импортировать файл конфигурации**.
2. Выберите требуемый файл для импорта и нажмите кнопку **Открыть**.
   Откроется диалоговое окно **Импортировать конфигурацию**.
3. Введите соответствующий пароль и нажмите кнопку **OK**.
   Клиент Configuration Client перезапускается. Необходимо снова войти в систему.
   Импортированная конфигурация не активируется, но ее можно изменить в клиенте Configuration Client.

Восстановление экспортированной конфигурации.

Доступ к этому файлу (копирование, удаление) возможен, только если служба **Central Server** BVMS остановлена.

1. Остановите службу **Central Server** BVMS в (Enterprise) Management Server.
2. При необходимости переименуйте резервный файл в Elements.bvms.
3. Замените существующий Elements.bvms.
4. Запустите службу **Central Server** BVMS в (Enterprise) Management Server.

Примечание. Для сброса настроек системы до пустой конфигурации остановите службу и удалите Elements.bvms.
Другие файлы конфигурации:

– Elements.bvms.bak (начиная с версии 2.2) — автоматически сохраненный резервный файл последней активации, включая историю версий. Последующие изменения конфигурации, которые не активировались, не включаются.
– Elements_Backup******.bvms: Конфигурация более ранней версии. Этот файл создается после обновления программного обеспечения.

Восстановление экспортированных настроек пользователя.

1. Разархивируйте zip-файл, созданный во время экспорта при обслуживании.
   Кнопка `Файл export.bvms` и `каталог UserData` извлекаются из архива.
2. На требуемом (Enterprise) Management Server скопируйте `каталог UserData` каталог в `C:\ProgramData\Bosch\VMS\`.

8.11.2 Замена VRM

Необходимые условия

– Установленная ОС с соответствующими сетевыми параметрами и надлежащей версией VRM.

Для замены устройства VRM из BVMS:

1. запустите BVMS Configuration Client.
2. В Дереве устройств выберите устройство VRM.
3. Задайте настройки на следующих страницах, затем сохраните и активируйте конфигурацию.

– Главное окно > **Устройства** > разверните > разверните >

– Главное окно > **Устройства** > разверните > разверните > **Настройки VRM** > **Основные параметры**

– Главное окно > **Устройства** > разверните > разверните > **Сеть** > **SNMP**

– Главное окно > **Устройства** > разверните > разверните > **Обслуживание** > **Дополнительно**

– Главное окно > **Устройства** > разверните > разверните > > > **Дополнительные параметры** > **Очередность записи**

– Главное окно > **Устройства** > разверните > разверните > > iSCSI > **Балансировка загрузки**

Для замены устройства VRM без BVMS:

Используется исходный резервный файл config.xml с устройства VRM, содержащий все параметры конфигурации (дальнейшая настройка не требуется).

1. Остановите службу **Video Recording Manager**.
2. Скопируйте config.xml на новый сервер.
3. Запустите службу **Video Recording Manager**.

Замена устройства iSCSI (запланированный резерв).

1. Добавьте новое устройство iSCSI.
2. С помощью Configuration Manager на устройстве iSCSI, подлежащем замене, настройте все логические устройства как работающие только в режиме чтения.

Примечание. Можно удалить старое устройство iSCSI, когда старые записи более не требуются.

Замечание!

Во время настройки нового устройства iSCSI рекомендуется использовать тот же пароль CHAP, что и для старого устройства.

При использовании нового пароля CHAP обязательно сделайте новый пароль общесистемным паролем CHAP и назначьте его для всех устройств iSCSI.

В противном случае вы не сможете проводить проверку подлинности на устройстве iSCSI и отображать непосредственное воспроизведение с устройства iSCSI.

8.11.3 Замена кодера или декодера

Замечание!
Не удаляйте устройство из Дерева устройств, если необходимо сохранить его записи. Для замены устройства замените оборудование.

Замена кодера/декодера такого же типа
Необходимым условием является устройство с заводскими настройками по умолчанию (IP-адрес = 192.168.0.1).

1. Отключите старое устройство от сети.
2. Не удаляйте устройство из Дерева устройств в BVMS Configuration Client! При удалении устройства из VRM запись теряется.
3. Подключите новое устройство такого же типа к сети.

Замечание!
Для следующих шагов требуется указанный ранее IP-адрес по умолчанию. При использовании назначенных DHCP IP-адресов выполнение начального поиска устройства невозможно.

4. Configuration Client: в меню **Аппаратное обеспечение** нажмите **Первоначальный поиск устройств...**.
   Откроется диалоговое окно **Первоначальный поиск устройств**.
5. Щелкните ячейку, чтобы изменить нужный адрес. Для изменения нескольких адресов выберите нужные строки. Можно выбрать несколько устройств, нажав клавишу CTRL или SHIFT. Затем щелкните правой кнопкой мыши выбранные строки и нажмите **Установить IP-адреса...** или нажмите **Установить маску подсети...** для изменения соответствующих значений.
   Необходимо ввести маску подсети и IP-адрес.
   Маска подсети и IP-адрес должны соответствовать заменяемому устройству.
6. Нажмите **OK**.
7. Через несколько секунд можно получить доступ к устройству в Дереве устройств.
8. Измените все необходимые настройки устройства, которыми не управляет система BVMS (см. информацию ниже).
9. Сохранить и активировать.

Примечания.
– Начальный поиск устройств находит только устройства, имеющие дублированные IP-адреса или IP-адрес по умолчанию (192.168.0.1).
– Не используйте поиск VRM для обнаружения устройств с параметрами по умолчанию, поскольку после этого вы не сможете изменить IP-адрес.

Замена кодера с назначенным DHCP IP-адресом.
Необходимым условием является кодер с заводскими настройками по умолчанию (IP-адрес заданный DHCP).

1. Подсоедините кодер напрямую к порту Ethernet своего компьютера.
2. Запишите параметры конфигурации сетевого адаптера TCP/IPv4, чтобы восстановить их в дальнейшем.
3. Для сетевого адаптера своего компьютера задайте следующий фиксированный IP-адрес и маску подсети:
   192.168.0.2
   255.255.255.0
4. Запустите Internet Explorer.

5. В строке **Адрес** введите 192.168.0.1.
   Отобразится веб-страница устройства.
6. Нажмите **Параметры**, затем нажмите **Сеть**.
7. На странице **Сеть** в списке **DHCP** выберите **Off (Выкл.)**.
8. В поле **IP-адрес**, поле **Маска подсети** и поле **Адрес шлюза** введите необходимые значения, действующие в вашей сети.
9. Нажмите **Уст. и перезагр.**.
10. Восстановите конфигурацию сетевого адаптера.

Замена кодера/декодера другого типа устройства

– Отключите старое устройство от сети.
– Не удаляйте устройство из Дерева устройств в BVMS Configuration Client!
– Подключите новое устройство нового типа к сети.

Главное окно **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или

Главное окно > **Устройства** > Развернуть  > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Изменить декодер** > Диалоговое окно **Изменить декодер**

После замены устройства можно обновить его функциональные возможности. Текст сообщения информирует о том, соответствуют ли полученные возможности устройства возможностям, сохраненным в BVMS.

Для обновления:

1. Нажмите кнопку **ОК**.
   Отображается окно сообщения со следующим текстом:
   Если применить данные возможности устройства, могут измениться настройки записи и событий для данного устройства. Проверьте эти настройки.

2. Нажмите кнопку **ОК**.
   Выполняется обновление возможностей устройства.

Замена камеры VSG

При замене камеры VSG убедитесь, что используемая для замены камера имеет тот же тип, тот же IP-адрес и тот же профиль ONVIF, что и у старой камеры.
Кроме того необходимо задать следующие настройки на новой камере AXIS через веб-интерфейс камеры VSG перед заменой старой камеры AXIS:

– Задать пароль для основного пользователя
– Настроить синхронизацию времени

– Отключить адрес локального канала
– Создать пользователя ONVIF
– Отключить защиту атак повторного воспроизведения

Настройки, задаваемые системой BVMS

Кодеры и декодеры, настроенные в системе BVMS, управляются сервером BVMS и поэтому не могут использоваться совместно с другими приложениями.
Можно использовать BVMS Device Monitor для проверки того, какое устройство отображает несоответствующую конфигурацию, которая отличается от конфигурации BVMS.
BVMS Configuration Client содержит страницы конфигурации для всех устройств BVIP. Охват настроек зависит от конкретной модели BVIP (напр. VIPX 1600 XFM4).
BVMS обеспечивает управление всеми параметрами BVIP, необходимыми для полной интеграции в систему BVMS.
Настройки, задаваемые системой BVMS.

– Название камеры
– Настройки сервера времени
– Управление записями (профили, время хранения, графики)
– Определения настроек качества
– Пароли

Хранятся в конфигурации BVMS, но не меняются на устройствах:

– IP-адрес (IP-адреса можно менять с помощью BVMS IP Device Configuration)
– Имена реле / вводов (отображаются различия имен устройств и имен, заданных в BVMS)

Системные события для различающихся конфигураций устройств

– События SystemInfo создаются после исправления конфигурации устройства во время периодической проверки.
– События SystemWarning создаются после обнаружения несоответствующей конфигурации на устройстве в первый раз. Последующие проверки не приводят к созданию такого события, пока конфигурация не будет исправлена путем активации или периодического исправления.
– События SytemError создаются после обнаружения ошибки конфигурации во время активации или периодических проверок. Последующие проверки не приводят к созданию такого события, пока конфигурация не будет исправлена путем активации или периодического исправления.

8.11.4 Замена клиента оператора

Замена рабочей станции Operator Client.

1. Замените компьютер.
2. Запустите установку BVMS на новом компьютере.
3. В списке компонентов для установки выберите Operator Client.
   При необходимости выберите другие компоненты, которые были установлены на замененном компьютере.
4. Установите программное обеспечение.

8.11.5 Заключительные проверки

Проверка замены MS / EMS и замены Operator Client.

1. Активируйте конфигурацию.
2. Запустите Operator Client.

3. Проверьте Логическое дерево в Operator Client.
   Оно должно быть идентичным Логическому дереву в Configuration Client.

Проверка замены VRM.

- Запустите VRM Monitor и проверьте активные записи.

8.11.6 Восстановление Divar IP 3000/7000

См. руководства по установке для DIVAR IP 3000 или DIVAR IP 7000. В разделе по восстановлению устройства можно найти информацию по необходимым действиям.

8.12 Настройка синхронизации времени

Замечание!
Убедитесь, что время на всех компьютерах системы BVMS синхронизировано с Management Server. В противном случае можно потерять записи.
Настройте программное обеспечение сервера времени на Management Server. На других компьютерах настройте IP-адрес Management Server как сервера времени с использованием стандартных процедур Windows.

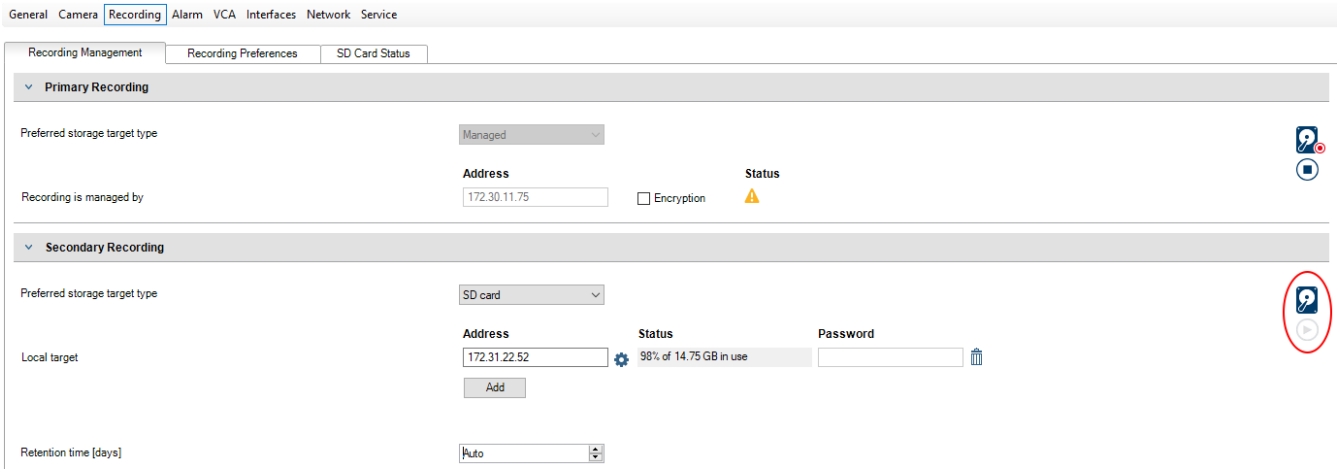
8.13 Настройка носителей данных кодера

Главное окно > **Устройства** > разверните > разверните > > > **Дополнительные параметры** > **Управление записями**

Примечание. Убедитесь, что требуемые камеры этого кодера добавлены в Логическое дерево.

Для использования функции ANR необходимо настроить носитель данных кодера.

Примечание. Если необходимо настроить носитель данных кодера, который уже добавлен в систему и записан с помощью VRM, убедитесь, что остановлена вторичная запись:



Функция ANR работает только на кодерах с версией микропрограммного обеспечения 5.90 и выше. Не все типы кодеров поддерживают ANR, даже если установлена верная версия микропрограммного обеспечения.

Настройка носителя данных кодера

1. В разделе **Вторичная запись** в списке **Предпочитаемый тип целевого хранилища** выберите носитель данных. В зависимости от типа устройства будут доступны разные носители.

2. При необходимости нажмите кнопку ..., чтобы отформатировать носитель данных. После успешного форматирования носитель данных будет готов к использованию с функцией ANR.
3. Настройте функцию ANR для этого кодера на странице **Камеры и запись**.

См.

– *Страница "Управление записью", Страница 242*
– *Настройка функции ANR, Страница 314*

9 Создание системы Enterprise

Выполните следующие действия, чтобы создать Enterprise System на Enterprise Management Server и на нескольких компьютерах Management Server:

1. *Настройка списка серверов для корпоративной системы, Страница 88*
2. *Создание Enterprise User Group, Страница 89*
3. *Создание Enterprise Account, Страница 89*

Для использования корпоративной системы Enterprise System необходимо наличие действующих лицензий.

См.

– *Enterprise System, Страница 24*

9.1 Настройка списка серверов для корпоративной системы

Главное окно > **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**

В списке серверов соответствующего Management Server можно настроить несколько компьютеров Management Server.

Для одновременного доступа необходимо настроить одну или несколько групп Enterprise User Group. В результате Management Server меняется на Enterprise Management Server. Пользователь Operator Client может войти в систему с именем пользователя Enterprise User Group, чтобы получить одновременный доступ к компьютерам Management Server, настроенным в списке серверов.

Рабочие привилегии настраиваются на Enterprise Management Server в **Группы пользователей**, на вкладке Enterprise User Group.

Привилегии для устройств настраиваются на каждом Management Server в **Группы пользователей**, на вкладке Enterprise Access.

– Нажмите  для сохранения настроек.

– Нажмите  для отмены последней настройки.

– Нажмите  для активации конфигурации.

Добавление серверов.

1. Нажмите **Добавить сервер**.
   Отображается диалоговое окно **Добавить сервер**.
2. Введите отображаемое имя сервера и адрес частной сети (DNS-имя или IP-адрес).
   Примечание. При использовании соединения по протоколу SSH введите адрес в следующем формате:
   ssh://IP-адрес или имя_сервера:5322
3. Нажмите **OK**.
4. Повторите эти действия для добавления всех необходимых компьютеров Management Server.

Чтобы добавить столбцы:

- Щелкните правой кнопкой мыши на заголовке таблицы, затем нажмите **Добавить столбец**.
  Можно добавить до 10 столбцов.
  Чтобы удалить столбец, щелкните на нем правой кнопкой мыши и нажмите **Удалить столбец**.

⇨ При экспорте списка серверов также будут экспортированы добавленные столбцы.
Компьютеры Management Server для вашей Enterprise System настроены.

См.
- *Enterprise System, Страница 24*
- *Страница «Список серверов/Адресная книга», Страница 132*
- *Страница Пользовательские группы, Страница 340*
- *Использование просмотра сервера, Страница 76*

9.2 Создание Enterprise User Group

Главное окно > **Группы пользователей**
Вы выполняете задачу создания Enterprise User Group для Enterprise System на Enterprise Management Server.
Вы создаете Enterprise User Group с пользователями для настройки их рабочих разрешений. Эти рабочие разрешения отображаются в Operator Client, подключенном к Enterprise Management Server . Примером рабочего разрешения является пользовательский интерфейс тревожного монитора.

Чтобы создать Enterprise User Group:
1. Нажмите вкладку **Enterprise User Groups**.
   Примечание. Вкладка **Enterprise User Groups** доступна только при наличии соответствующей лицензии и при условии, что один или несколько компьютеров Management Server настроены в **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**.
2. Нажмите  .
   Откроется диалоговое окно **Создать группу пользователей Enterprise User Group**.
3. Введите имя и описание.
4. Нажмите кнопку **OK**.
   Enterprise User Group добавлена в соответствующее дерево.
5. Щелкните правой кнопкой по новой группе Enterprise и выберите **Переименовать**.
6. Введите нужное имя и нажмите клавишу ВВОД.
7. На странице **Рабочие разрешения** требуемым образом настройте рабочие разрешения и доступ к серверу для настроенных компьютеров Management Server.

См.
- *Страница Свойства пользовательской группы, Страница 342*
- *Страница Свойства оператора, Страница 349*
- *Страница Приоритеты, Страница 353*
- *Страница Интерфейс пользователя, Страница 353*
- *Страница Доступ к серверу, Страница 354*

9.3 Создание Enterprise Account

Главное окно > **Группы пользователей**

Замечание!
Прежде чем вы сможете добавить Enterprise Account, необходимо задать конфигурацию по меньшей мере одного устройства в дереве устройств.

Вы выполняете задачу создания Enterprise Account на Management Server. Повторите те же действия на каждом Management Server, являющемся элементом вашей Enterprise System.
Вы создаете Enterprise Account для настройки разрешений для устройств Operator Client с помощью Enterprise System.

Чтобы создать Enterprise Account:

1. Перейдите на вкладку **Доступ Enterprise**.
2. Нажмите  .
   Откроется диалоговое окно **Создать учетную запись Enterprise Account**.
3. Введите имя и описание.
4. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей.
   Введите ключ в соответствии с требованиями к ключам и подтвердите его.
5. Нажмите кнопку **OK**.
   Новая учетная запись Enterprise Account добавлена в соответствующее дерево.
6. Щелкните правой кнопкой по новой Enterprise Account и выберите **Переименовать**.
7. Введите нужное имя и нажмите клавишу ВВОД.
8. На странице **Разрешения устройств** настройте, если требуется, учетные данные, а также разрешения устройств.

См.

- *Строгая политика паролей , Страница 364*
- *Страница Учетные данные, Страница 348*
- *Страница Логическое дерево, Страница 349*
- *Страница События и тревоги, Страница 347*
- *Страница Приоритеты управления, Страница 346*
- *Страница Разрешения камеры, Страница 344*
- *Страница Разрешения декодера, Страница 347*

9.4 Проверка подлинности на основе токена

Enterprise Account позволяет Enterprise руководству заказчика получить доступ к Management Server, настроенному в списке доступа к серверу Enterprise Management Server.
Безопасность Enterprise Account гарантируется ключом. В случае изменения такого ключа его также необходимо изменить на Management Server и на Enterprise Management Server. Кроме того, необходимо активировать измененную конфигурацию. Если у вас большое число Management Server, подключенных к Enterprise Management Server, на это может потребоваться значительное время.

Вместо защиты Enterprise Account с применением имени пользователя и ключа можно настроить проверку подлинности на основе токена.

1. Токен создается Enterprise Management Server.
2. Токен подписывают с помощью сертификата под названием Token Issuer.
3. Management Server предоставляет доступ при наличии действительного токена. Management Server предоставляет доступ только тогда, когда на Management Server настроено доверие сертификату Token Issuer.

Необходимые условия

Для подписи и проверки токена необходимо получить сертификат или цепочку сертификатов.

Примечание: сертификаты не генерируются и не устанавливаются BVMS. Вы должны получить и установить их самостоятельно. BVMS может использовать сертификаты, установленные в Windows Certificate Store.

На Enterprise Management Server и Management Server существуют разные требования. Ниже поясняем, в каких случаях требуются сертификаты.

Сертификат

- Для Enterprise Management Server требуется сертификат и соответствующий закрытый ключ.
- Для Management Server требуется сертификат.

Цепочка сертификатов

Цепочка сертификатов начинается с сертификата Root, который используется для подписи другого сертификата. Этот сертификат затем можно использовать еще раз для подписи следующего сертификата. Длину цепочек сертификатов можно определить самостоятельно.

- Для Enterprise Management Server необходима полная цепочка сертификатов. Для последнего сертификата в цепи (Token Issuer) требуется закрытый ключ.
- В зависимости от установленных настроек токена доступа для Management Server требуются только отдельные элементы цепочки сертификатов.

Для того, чтобы настроить проверку подлинности на основе токена, необходимо выполнить следующие действия:

1. Настроить конфигурацию Enterprise Management Server
- Определить проверку подлинности токена доступа для Enterprise Accounts
- Настроить параметры токена доступа
2. Настроить конфигурацию Management Server
- Указать доверенные сертификаты
- Запретить доступ к Enterprise Account с помощью ключа

См. технический документ о проверке подлинности на основе токена для получения более подробной информации.

См.

- *Диалоговое окно «Параметры токена доступа» (меню «Настройки»), Страница 122*
- *Страница Доступ к серверу, Страница 354*

10 Настройка командных сценариев

В этом разделе приводится описание способов настройки Командных сценариев. Командные сценарии располагаются в разных местах BVMS.

1. Нажмите  для сохранения настроек.
2. Нажмите  для отмены последней настройки.
3. Нажмите  для активации конфигурации.

Замечание!
Серверные сценарии активируются во время перезапуска службы Management Server, даже если не выполняется активация из Configuration Client.

10.1 Управление командными сценариями

Главное окно

Командный сценарий можно создать при помощи следующих языков программирования сценариев:

– C#
– VB.Net

Вы не можете изменить язык существующего командного сценария.

Вы можете создать клиентский или серверный сценарий.

К каждому сценарию вы можете добавлять скриптлеты.

Чтобы получить справку по вводу кода, нажмите  в диалоговом окне **Редактор командных сценариев**. Отображается справка Bosch Script API.

Добавление скриптлета сервера:

1. В меню **Сервис** выберите команду **Редактор командных сценариев...**.
   Если командный сценарий еще не создан, откроется диалоговое окно **Выберите язык сценария**.
2. В списке **Язык сценария:** выберите необходимую запись.
   Откроется диалоговое окно **Редактор командных сценариев**.
3. На левой панели диалогового окна **Редактор командных сценариев** щелкните правой кнопкой мыши пункт ServerScript и нажмите **Создать команду**.
   Будет добавлен новый скриптлет.
4. Введите свой код.

Добавление скриптлета клиента:

1. В меню **Сервис** выберите команду **Редактор командных сценариев...**.
   Если командный сценарий еще не создан, откроется диалоговое окно **Выберите язык сценария**.
2. В списке **Язык сценария:** выберите необходимую запись.
   Откроется диалоговое окно **Редактор командных сценариев**.
3. На левой панели диалогового окна **Редактор командных сценариев** щелкните правой кнопкой мыши пункт ClientScript и нажмите **Создать команду**.
   Будет добавлен новый скриптлет.
4. Введите свой код.

Удаление скриптлета:

1. Откройте диалоговое окно **Редактор командных сценариев**.

2. Откройте вкладку **Серверный сценарий** или **Клиентский сценарий**.
3. Щелкните правой кнопкой мыши нужное событие в дереве событий и нажмите  .
   Скриптлет будет удален.

Чтобы выйти из диалогового окна Редактор командных сценариев:

- Нажмите  .

См.

– *Диалоговое окно Редактор командных сценариев, Страница 318*

10.2 Настройка автоматического запуска командного сценария

Главное окно > **Тревожные сигналы** >  или  > Столбец **Параметры тревог** > ...
В результате данных настроек клиентский командный сценарий будет запущен в следующих случаях:

– Запуск рабочей станции.
– Прием тревожного события пользователем.

Чтобы настроить командный сценарий, выполняющийся при запуске рабочей станции:

См Настройка командного сценария запуска.

Чтобы настроить командный сценарий, выполняющийся после того, как пользователь принял тревожный сигнал:

1. Щелкните вкладку **Поток заданий**.
2. Выберите соответствующий клиентский сценарий из списка **Выполнить следующий клиентский сценарий после принятия тревоги:**.
   Этот сценарий будет запущен сразу после приема пользователем тревожного сигнала.

См.

– *Диалоговое окно Параметры тревог, Страница 325*
– *Настройка командного сценария, выполняющегося при запуске (страница «Настройки»), Страница 94*

10.3 Импорт командного сценария

Главное окно

Можно импортировать командные сценарии, созданные на другом компьютере. Файл должен быть составлен на том же языке сценариев, который используется в вашей системе.

Чтобы импортировать командный сценарий:

1. В меню **Сервис** выберите команду **Редактор командных сценариев...**.
   Откроется диалоговое окно **Редактор командных сценариев**.
2. Нажмите  .
   Откроется диалоговое окно открытия файла.
3. Выберите нужный файл сценария и нажмите кнопку **OK**.

См.

– *Диалоговое окно Редактор командных сценариев, Страница 318*

10.4 Экспорт командного сценария

Главное окно

Можно экспортировать командные сценарии, созданные на другом компьютере.

Чтобы экспортировать командный сценарий:

1. В меню **Сервис** выберите команду **Редактор командных сценариев...**.
   Откроется диалоговое окно **Редактор командных сценариев**.
2. Нажмите  .
   Откроется диалоговое окно сохранения файла.
3. Введите имя нужного файла сценария и нажмите кнопку **OK**.

См.

– *Диалоговое окно Редактор командных сценариев, Страница 318*

10.5 Настройка командного сценария, выполняющегося при запуске (страница «Настройки»)

Главное окно > **Устройства** > Разверните  >  > **Настройки**

Можно настроить командный сценарий, который будет запущен при запуске Operator Client на выбранной рабочей станции.

Вы должны создать соответствующий командный сценарий.

Сведения о создании командного сценария см. *Управление командными сценариями, Страница 92*.

Чтобы настроить командный сценарий:

- Выберите нужный командный сценарий из списка **Сценарий запуска:**.

См.

– *Страница Рабочая станция, Страница 141*

11 Управление параметрами конфигурации

Главное окно

Вы должны активировать текущую конфигурацию, чтобы она вступила в силу для Management Server and Operator Client. Система напоминает вам о необходимости активации при выходе из Configuration Client.

Каждая активированная конфигурация сохраняется с датой и описанием (при необходимости).

Вы всегда можете восстановить последнюю активированную конфигурацию. Все конфигурации, сохраненные за это время, будут утрачены.

Текущую конфигурацию можно экспортировать в файл конфигурации и впоследствии импортировать этот файл. В результате этой операции восстанавливается экспортированная конфигурация. Все конфигурации, сохраненные за это время, будут утрачены.

– Нажмите  для сохранения настроек.

– Нажмите  для отмены последней настройки.

– Нажмите  для активации конфигурации.

11.1 Активация текущей конфигурации

Главное окно

Вы можете активировать текущую конфигурацию. Если пользователь принял ее, то Operator Client использует активированную конфигурацию после следующего запуска. Если активация была произведена принудительно, то все открытые экземпляры Operator Client закрываются и запускаются заново. Пользователю каждой копии Operator Client обычно не нужно выполнять вход заново.

Можно настроить время отложенной активации. Если настроено время отложенной активации, рабочая конфигурация активируется не сразу же, а в установленное время. При более поздней настройке времени активации (отложенной или нет), это время становится активным в данный момент. Первое настроенное время активации удаляется.

При выходе из Configuration Client система напоминает вам о необходимости активации текущей рабочей копии конфигурации.

Невозможно активировать конфигурацию, содержащую устройство без защиты паролем.

Замечание!

Если активация была произведена принудительно, то каждый экземпляр Operator Client перезапускается при активации конфигурации. Избегайте ненужных активаций. Рекомендуется выполнять активацию ночью или в периоды низкой активности.

Замечание!

Если в системе содержатся устройства без защиты паролем, необходимо обеспечить безопасность этих устройств, чтобы можно было выполнить активацию. Это принудительное использование пароля можно отключить.

Чтобы активировать текущую конфигурацию:

1. Нажмите  .
   Откроется диалоговое окно **Активировать конфигурацию**.
   Если конфигурация содержит устройства без защиты паролем, выполнение активации невозможно. В этом случае отображается диалоговое окно **Защита устройств паролем по умолчанию...**.
   Выполните инструкции в этом диалоговом окне и нажмите кнопку **Применить**.
   Диалоговое окно **Активировать конфигурацию** снова откроется.
2. При необходимости введите время отложенной активации. По умолчанию текущее время устанавливается как время активации. Если не изменить время отложенной активации, активация выполняется немедленно.
   В случае необходимости установите флажок **Принудительная активация для всех модулей Operator Client**.
3. Введите описание и нажмите кнопку **OK**.
   Текущая конфигурация активируется.
   Каждая рабочая станция Operator Client немедленно перезапускается, если имеется подключение к сети и выполняется принудительная активация. Если рабочая станция не подключена к сети, она перезапускается сразу после подключения.
   Если настроено время отложенной активации, конфигурация активируется позже.

Примечание. Отложенная активация не выполняется до тех пор, пока пользователь не выйдет из Configuration Client.

См.

- *Диалоговое окно «Защита устройств с помощью всеобщего пароля по умолчанию» (меню «Оборудование»), Страница 108*
- *Диалоговое окно «Активировать конфигурацию» (меню «Система»), Страница 107*

11.2 Активация конфигурации

Главное окно

Можно активировать предыдущую версию конфигурации, сохраненную ранее.

Чтобы активировать конфигурацию:

1. В меню **Система** выберите пункт **Диспетчер активации...**.
   Откроется диалоговое окно **Диспетчер активации**.
2. Выберите из списка конфигурацию, которую вы хотите активировать.
3. Нажмите кнопку **Активировать**.
   Откроется окно сообщения.
4. Нажмите **OK**.
   Откроется диалоговое окно **Активировать конфигурацию**.
5. При необходимости установите флажок **Принудительная активация для всех модулей Operator Client**. Каждая рабочая станция Operator Client автоматически перезапускается для активации новой конфигурации. Пользователь не может отклонить новую конфигурацию.
   Если не установлен флажок **Принудительная активация для всех модулей Operator Client**, на каждой рабочей станции Operator Client на несколько секунд появится диалоговое окно. Пользователи могут отказаться или принять новую конфигурацию. Диалоговое окно закрывается автоматически через несколько секунд, если пользователь не совершил никаких действий. В этом случае новая конфигурация не принимается.

См.

- *Диалоговое окно «Активировать конфигурацию» (меню «Система»), Страница 107*
- *Диалоговое окно «Диспетчер активации» (меню «Система»), Страница 107*

11.3 Экспорт параметров конфигурации

Главное окно

Данные конфигурации устройства BVMS могут быть экспортированы в ZIP-файл. В этом ZIP-файле содержится файл базы данных (`Export.bvms`) и данных пользователя (`DAT`-файл).

Эти файлы можно использовать для восстановления конфигурации системы, ранее экспортированной на том же (Enterprise) Management Server, или импорта на другой (Enterprise) Management Server. Файл данных пользователя нельзя импортировать, но с его помощью можно вручную восстановить конфигурацию пользователя.

Чтобы экспортировать параметры конфигурации:

1. В меню **Система** нажмите кнопку **Конфигурация экспорта...**.
   Откроется диалоговое окно **Экспортировать файл конфигурации**.
   Примечание. Если текущая рабочая копия конфигурации не активирована (активен ), экспортируется данная рабочая копия, а не активированная конфигурация.
2. Нажмите **Сохранить**.
3. Введите имя файла.
   Экспортируется текущая конфигурация. Создается ZIP-файл с базой данных и данными пользователя.

См.

- *Импорт параметров конфигурации, Страница 97*

11.4 Импорт параметров конфигурации

Главное окно

Рассматриваются следующие сценарии:

- импорт конфигурации, ранее экспортированной (выполнено резервное копирование) на том же сервере;
- импорт шаблона конфигурации, подготовленного и экспортированного на другом сервере;
- импорт конфигурации более ранней версии BVMS.

Конфигурацию можно импортировать, только если сохранены и активированы последние изменения текущей рабочей копии.

Для импорта данных конфигурации нужен соответствующий пароль.

Невозможно импортировать данные пользователя.

Чтобы импортировать конфигурацию:

1. В меню **Система** нажмите **Import configuration ...**.
   Откроется диалоговое окно **Импортировать файл конфигурации**.
2. Выберите требуемый файл для импорта и нажмите кнопку **Открыть**.
   Откроется диалоговое окно **Импортировать конфигурацию**.
3. Введите соответствующий пароль и нажмите кнопку **ОК**.
   Клиент Configuration Client перезапускается. Необходимо снова войти в систему.
   Импортированная конфигурация не активируется, но ее можно изменить в клиенте Configuration Client.

Замечание!
Чтобы продолжить редактировать конфигурацию, активированную для Management Server, выполните откат в диалоговом окне **Активировать конфигурацию**.

См.
– *Экспорт параметров конфигурации, Страница 97*

11.5 Экспорт конфигурационных данных в OPC

Главное окно
Вы можете экспортировать конфигурационные данные устройства BVMS в файл XML для последующего импорта в приложение сервера OPC. Файл должен быть сохранен в директории bin установленного экземпляра BVMS.
Для настройки соединения между BVMS и BIS доступны руководство по подключению BVMS к BIS и технические примечания к BVMS OPC Server.

Замечание!
Установите сервер BIS и BVMS Management Server на разные компьютеры.
При установке обоих серверов на один компьютер производительность системы будет снижена. Кроме того, могут возникнуть серьезные проблемы с работой программного обеспечения.

Чтобы экспортировать параметры конфигурации:
1. В меню **Система** нажмите **Экспорт сведений об устройстве для OPC...**.
   Откроется диалоговое окно **Экспорт файла со сведениями об устройстве**.
2. Введите имя файла и нажмите кнопку **Сохранить**.
   Файл будет сохранен.
   Этот файл можно импортировать в приложение сервера OPC.

11.6 Проверка состояния кодеров/декодеров

Главное окно > меню **Аппаратное обеспечение** > команда **Монитор устройств...** > диалоговое окно **Монитор устройств**
Состояние всех активированных кодеров/декодеров можно проверить в Дереве устройств.

См.
– *Диалоговое окно «Монитор устройств» (меню «Оборудование»), Страница 113*

11.7 Настройка мониторинга SNMP

Главное окно

Настройка:
1. В меню **Настройки** нажмите **Настройки SNMP...**.
   Отображается диалоговое окно **Настройки SNMP**.
2. Установите требуемые параметры и нажмите **OK**.

Отключение SNMP GetRequest.
- Удалите содержимое поля **Порт SNMP GET**.
  BVMS более не принимает данные SNMP GetRequest.

См.
– *Диалоговое окно «Настройки SNMP» (меню «Настройки»), Страница 118*

11.8 Создание отчета

Главное окно

Можно создавать отчеты, собирающие сведения о текущей конфигурации.

Создание отчета:

1. В меню **Отчеты** выберите необходимую команду.
   Откроется соответствующее диалоговое окно.
2. Нажмите **Экспорт CSV**.
3. Введите путь и имя файла для нового отчета.
4. Откройте файл CSV в Microsoft Excel или другом приложении для работы с электронными таблицами, чтобы проверить его содержимое.

См.

- *Диалоговое окно "Расписания записей", Страница 116*
- *Диалоговое окно "Расписания задач", Страница 116*
- *Диалоговое окно "Камеры и параметры записи", Страница 117*
- *Диалоговое окно "Параметры качества потока", Страница 117*
- *Диалоговое окно "Настройки событий", Страница 117*
- *Диалоговое окно "Настройки составных событий", Страница 117*
- *Диалоговое окно "Настройки тревог", Страница 117*
- *Диалоговое окно "Настроенные пользователи", Страница 117*
- *Диалоговое окно "Группы пользователей и учетные записи", Страница 117*
- *Диалоговое окно "Рабочие разрешения", Страница 118*

12 примеры конфигурации

В данном разделе содержатся примеры конфигурации выбранных устройств в BVMS.

12.1 Добавление моста Bosch ATM/POS

В данном примере описано, как настроить мост ATM/POS Bridge Bosch.

Конфигурирование ATM/POS Bridge

1. Убедитесь, что устройство подключено к сети.
2. Чтобы настроить IP-адрес и маску подсети устройства, подключите его к COM-порту компьютера при помощи кабеля RS232 (используйте для подключения кабель, указанный в спецификациях Bosch). Подробнее см. в руководстве по установке Bosch ATM/POS Bridge.
3. Запустите на компьютере сеанс работы программы Hyperterminal (обычно: **Пуск** > **Программы** > **Стандартные** > **Связь** > **Hyper Terminal**).
4. Введите имя сеанса и нажмите кнопку **OK**.
5. Выберите номер COM-порта и нажмите **OK**.
6. Введите следующие параметры COM-порта:
   - 9600 бит/с
   - 8 бит данных
   - без проверки четности
   - 1 стоповый бит
   - аппаратное управление потоком

   Нажмите **OK**.
7. нажмите F1 для отображения меню системных параметров устройства.
8. Введите 1 для установки IP-адреса и маски подсети.
9. Оставьте стандартные значения для портов:
   - port1: **4201**
   - port2: **4200**

Добавление моста ATM/POS Bridgек BVMS

1. Подключите устройство к сети BVMS.
2. Запустите Configuration Client.
3. Щелкнуть **Устройства**, Развернуть логическое дерево, Развернуть  , Щелкнуть правой кнопкой мыши  , Щелкнуть **Добавить мост ATM/POS Bosch**.
   Откроется диалоговое окно **Добавить мост ATM/POS Bosch**.
4. Введите имя и ранее установленные настройки.
5. Нажмите вкладку **Входы** и выберите нужные входы.
6. Нажмите  , чтобы сохранить настройки.
7. Нажмите **События**.
8. Развернуть  , Развернуть **Вход моста POS**, Щелкнуть **Ввод данных**.
9. В списке **Активировать тревогу** выберите **Всегда**, чтобы данное событие всегда активировало тревогу. При необходимости активации тревоги событием только в течение определенного периода времени, выберите расписание.
10. Нажмите  , чтобы сохранить настройки.
11. Нажмите **Тревожные сигналы**.

12. Установите нужные настройки тревоги для данного события.
13. Нажмите  , чтобы сохранить настройки и нажмите  , чтобы включить конфигурацию.
14. Выполните тест, чтобы убедиться, что тревожный сигнал работает должным образом.

12.2 Добавление входа сигнализации Bosch Allegiant

После добавления устройства Bosch Allegiant в BVMS следует добавить тревожные входы Allegiant.

1. В дереве устройств нажмите запись устройства Allegiant.
2. Выберите вкладку **Входы** и нажмите **Добавить вход**.
3. Добавьте нужные тревожные входы.
4. Нажмите **События**.
5. В дереве событий разверните **Устройства Allegiant**, разверните **Вход Allegiant** и нажмите **Вход закрыт** или **Вход открыт** (в зависимости от приложения).
6. В списке **Активировать тревогу** выберите **Всегда**, чтобы данное событие всегда активировало тревогу. При необходимости активации тревоги событием только в течение определенного периода времени, выберите расписание.
7. Нажмите  , чтобы сохранить настройки и нажмите  , чтобы включить конфигурацию.
8. Выполните тест, чтобы убедиться, что тревожный сигнал работает должным образом.

12.3 Добавление и настройка 2 камер Dinion IP для записи VRM

В данном разделе описываются способы добавления 2 камер Dinion IP для записи VRM, способы настройки различных параметров записи и способы настройки поиска для этих камер.

Предварительные условия.

Диспетчер видеозаписи и устройства iSCSI настроены правильно.

Это означает следующее.

– Диспетчер видеозаписи добавлен в логическое дерево.
– Устройство iSCSI с настроенным получателем и LUN назначено данному диспетчеру видеозаписи.

Чтобы добавить IP-камеры к существующему диспетчеру видеозаписи (VRM):

Главное окно > **Устройства** > Развернуть 

1. Щелкните правой кнопкой мыши  и выберите команду **Добавить кодер**.
   Откроется диалоговое окно **Добавить кодер**.
2. Введите IP-адрес IP-камеры и выберите тип кодера (Dinion IP).
   Нажмите **OK**.
   Повторите это же действие для другой IP-камеры.

Чтобы добавить IP-камеры в логическое дерево, выполните следующие действия.

Главное окно > **Карты и структура**

- Перетащите камеры в логическое дерево.

Чтобы изменить свойства камеры:

Главное окно > **Камеры и запись** >  > Вкладка 

1. В столбце **Видеоизображение в реальном времени** настройте параметры качества отображения изображений в реальном времени. Для этих устройств можно настроить параметры качества только для каждой камеры, но не в соответствии с расписанием.
2. Установите соответствующие параметры в других столбцах.

Чтобы настроить параметры записи для камер, выполните следующие действия.

1. Нажмите  .
2. Выберите соответствующую серию устройств.
3. Выберите соответствующие параметры записи.
4. Выберите соответствующее расписание записи, например, **День**.
5. В **Непрерывная запись или запись перед тревожным сигналом** выберите нужный режим записи, поток и качество.
   Если выбран режим записи, **До тревоги**, в параметре **Продолжительность** можно выбрать время записи по тревоге в секундах до тревожного сигнала.
6. В столбце **Запись по тревоге** нажмите **Продолжительность** на ячейку и введите требуемое время записи в секундах после срабатывания сигнала тревоги.
7. Повторите эти действия, чтобы настроить параметры записи для другой камеры из данной серии устройств.

13 Главные окна Configuration Client

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

В данном разделе содержится информация о некоторых основных окнах приложения, имеющихся в BVMSConfiguration Client.

13.1 Окно Конфигурация

Главное окно
Используется для настройки системы. Кнопки на панели инструментов представляют собой ссылки на различные страницы, которые вы должны настроить для работы системы. Они расположены в той последовательности, в которой рекомендуется осуществлять настройки.

- нажмите на элемент дерева для отображения всех доступных страниц свойств.

Устройства	Нажмите для отображения страницы **Устройства** со всеми устройствами, подключенными к системе.
Карты и структура	Нажмите для отображения страницы **Карты и структура** с логическим деревом, деревом устройств и картами.
Расписания	Нажмите для отображения страницы **Расписания записей** и **Расписания задач**.
Камеры и запись	Нажмите для отображения страницы **Камеры и запись** с таблицей камер и параметрами записи для всех камер.
События	Нажмите для отображения страницы **События**.
Тревожные сигналы	Нажмите для отображения страницы **Тревожные сигналы**.
Группы пользователей	Нажмите для отображения страницы **Группы пользователей** со всеми пользователями.
	нажмите для сохранения параметров активного окна.
	нажмите для восстановления сохраненных параметров активного окна. **Примечание:** Восстановлению подлежат только те параметры, которые были сделаны в BVMS, а не те, что были установлены непосредственно на устройстве. Это может привести к дальнейшей недоступности устройств.
	Нажмите для отображения диалогового окна **Активировать конфигурацию**.

	нажмите для удаления выделенного элемента. (Доступно не на всех страницах).
	нажмите для переименования выделенного элемента. (Доступно не на всех страницах).
	Нажмите для отображения справочной информации, относящейся к активному окну.
	Нажмите, если нужно обновить информацию о состояниях для всех устройств и сведения о возможностях устройств (доступно не на каждой странице). Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите **Обновить состояние**. **Примечание.** Если у вас крупная система с несколькими тысячами настроенных устройств, процесс обновления состояний и возможностей устройств может занять длительное время.

13.2 Команды меню

команды меню Система

Сохранить изменения	Сохраняет изменения, внесенные на данной странице.
Отменить все изменения на странице	Восстанавливает последние сохраненные параметры на странице.
Диспетчер активации...	Отображает диалоговое окно **Диспетчер активации**.
Конфигурация экспорта...	Отображает диалоговое окно **Экспортировать файл конфигурации**.
Импортировать конфигурацию...	Отображает диалоговое окно **Импортировать файл конфигурации**.
Экспорт сведений об устройстве для OPC...	Отображает диалоговое окно создания файла конфигурации, который можно импортировать в систему управления сторонних производителей.
Выход	Выход из программы.

Команды меню Аппаратное обеспечение

Первоначальный поиск устройств...	Отображает диалоговое окно **Первоначальный поиск устройств**.
Защита устройств паролем по умолчанию...	Отображает диалоговое окно **Защита устройств глобальным паролем по умолчанию**.
Защитить хранилища iSCSI паролем CHAP...	Отображает диалоговое окно **Защита хранилищ iSCSI паролем CHAP**.

Изменить пароли устройств...	Отображает диалоговое окно **Изменить пароли устройств**.
Обновить микропрограмму устройства...	Отображает диалоговое окно **Обновить микропрограмму устройства**.
Изменить IP-адрес устройства и сетевые параметры...	Отображает диалоговое окно **Изменить IP-адрес и сетевые параметры устройства**.
Монитор устройств...	Отображает диалоговое окно **Монитор устройств**.

Команды меню Сервис

Редактор командных сценариев...	Отображает диалоговое окно **Редактор командных сценариев**
Диспетчер ресурсов...	Отображает диалоговое окно **Диспетчер ресурсов**.
Конструктор последовательностей...	Отображает диалоговое окно **Конструктор последовательностей**.
Диспетчер лицензий...	Отображает диалоговое окно **Диспетчер лицензий**.
Инспектор лицензий...	Отображает диалоговое окно **Инспектор лицензий**.

Команды меню Отчеты

Расписания записи...	Отображает диалоговое окно отчета **Расписания записей**.
Параметры записи по расписанию...	Отображает диалоговое окно отчета **Параметры записи по расписанию**.
Расписания задач...	Отображает диалоговое окно отчета **Расписания задач**.
Камеры и параметры записи...	Отображает диалоговое окно отчета **Параметры камер и записи**.
Параметры качества потока...	Отображает диалоговое окно отчета **Параметры качества потока**.
Параметры событий...	Отображает диалоговое окно отчета **Настройки событий**.
Параметры составного события...	Отображает диалоговое окно отчета **Настройки сложных событий**.
Параметры тревог...	Отображает диалоговое окно отчета **Настройки тревог**.
Настроенные пользователи...	Отображает диалоговое окно отчета **Настроенные пользователи**.
Группы пользователей и учетные записи...	Отображает диалоговое окно отчета **Группы пользователей и учетные записи**.

Разрешения устройства...	Отображает диалоговое окно отчета **Разрешения для устройств**.
Разрешения для операторов	Отображает диалоговое окно отчета **Рабочие разрешения**.
Разрешения конфигурировании...	Отображает диалоговое окно отчета **Разрешения конфигурирования**.
Разрешения группы пользователей	Отображает диалоговое окно отчета **Разрешения группы пользователей**.
Параметры безопасности...	Отображает диалоговое окно отчета **Параметры безопасности**.
Обойденные устройства...	Отображает диалоговое окно отчета **Обойденные устройства**.

Команды меню Настройки

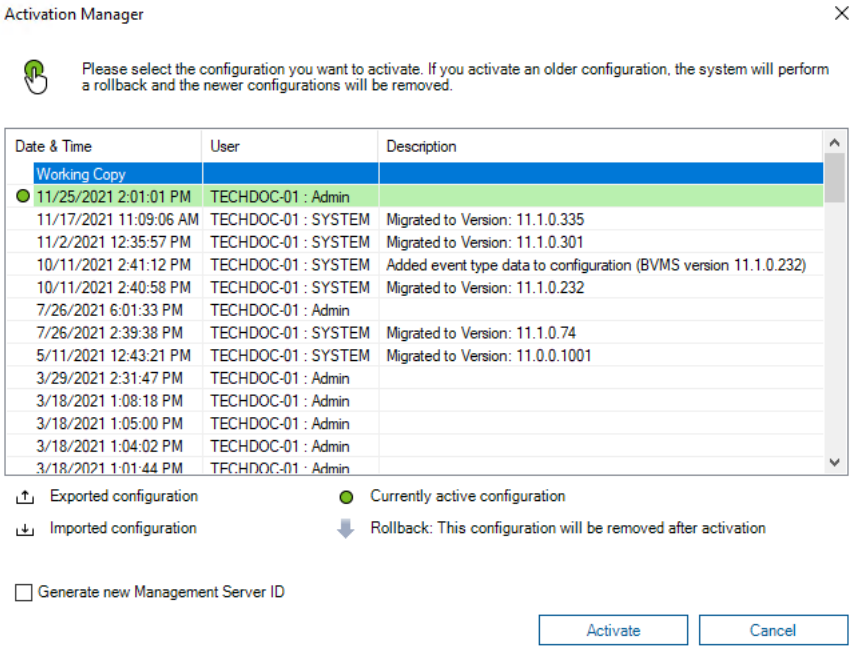
Параметры тревог...	Отображает диалоговое окно **Настройки тревог**.
Настройки SNMP...	Отображает диалоговое окно **Настройки SNMP**.
Параметры сервера LDAP...	Отображает диалоговое окно **Параметры сервера LDAP**.
Определить порядок групп пользователей LDAP...	Отображает диалоговое окно **Определить порядок групп пользователей LDAP...**.
Параметры доверенного сертификата...	Отображает диалоговое окно **Параметры маркера доступа** .
Установить качество записи...	Отображается диалоговое окно **Параметры доверенного сертификата**. **Примечание:** Меню **Параметры доверенного сертификата...** доступно только при запуске Configuration Client с правами администратора, и если у пользователя, который входит в систему, есть разрешение **Настройка групп пользователей/ Enterprise Accounts** .
Параметры...	Отображает диалоговое окно **Параметры качества потока** .
Параметры...	Отображает диалоговое окно **Параметры**.

Команды меню Справка

Показать справку	Отображает справку приложения BVMS.
О программе...	Отображает диалоговое окно, содержащее информацию об установленной системе, например, номер версии.

13.3 Диалоговое окно «Диспетчер активации» (меню «Система»)

Главное окно > меню **Система** > команда **Диспетчер активации...**
Позволяет активировать текущую конфигурацию или вернуться к предыдущей конфигурации.



Активировать
Нажмите для отображения диалогового окна **Активировать конфигурацию**.

См.
- *Активация текущей конфигурации, Страница 95*
- *Активация конфигурации, Страница 96*

13.4 Диалоговое окно «Активировать конфигурацию» (меню «Система»)

Главное окно > 
Позволяет ввести описание текущей копии конфигурации, которая должна быть активирована.

Установить время отложенной активации
Нажмите для выбора времени отложенной активации.
Примечание. Отложенная активация не выполняется до тех пор, пока пользователь не выйдет из Configuration Client.

Принудительная активация для всех модулей Operator Client
Если флажок установлен, каждая рабочая станция Operator Client автоматически перезапускается для активации новой конфигурации. Пользователь не может отказаться от новой конфигурации.

Если не установлен флажок, то на каждой рабочей станции Operator Client на несколько секунд появится диалоговое окно. Пользователи могут отказаться или принять новую конфигурацию. Диалоговое окно закрывается автоматически через несколько секунд, если пользователь не совершил никаких действий. В этом случае новая конфигурация не принимается.

См.

– *Активация текущей конфигурации, Страница 95*

13.5 Диалоговое окно «Первоначальный поиск устройств» (меню «Оборудование»)

Главное окно > меню **Аппаратное обеспечение**, нажмите команду **Первоначальный поиск устройств...**

Отображает устройства с двойными IP-адресами или IP-адресами по умолчанию (192.168.0.1).

Позволяет изменять эти IP-адреса и маски подсети.

Прежде чем изменять IP-адрес, необходимо ввести правильную маску подсети.

13.6 Диалоговое окно «Защита устройств с помощью всеобщего пароля по умолчанию» (меню «Оборудование»)

Главное окно > меню **Аппаратное обеспечение** > команда **Защита устройств паролем по умолчанию...**

или

Главное окно > 

Это диалоговое окно появляется, если ожидается выполнение активации и если конфигурация содержит устройства без защиты паролем. Оно позволяет ввести всеобщий пароль по умолчанию, применяемый ко всем затрагиваемым устройствам.

Обновить состояния и функции

Нажмите для повторного сканирования сети для поиска устройств, не защищенных паролем.

Global default password

Введите пароль, используемый для всех не защищенных в данный момент устройств.

Показать пароли

Нажмите, чтобы все пароли в этом диалоговом окне стали видимы.

Enforce password protection on activation

Установите этот флажок. Если функция включена, необходимо применить всеобщий пароль по умолчанию для устройств, которые не защищены паролем.

Применить

Нажмите, чтобы применить всеобщий пароль по умолчанию.

Откроется диалоговое окно **Изменение паролей**. Перечисляются изменения паролей.

Нажмите **ОК**, чтобы закрыть окно.

Если началась активация конфигурации, отображается диалоговое окно **Диспетчер активации**.

См.

– *Активация текущей конфигурации, Страница 95*

13.7 Защитите хранилища iSCSI с помощью CHAP в диалоговом окне пароля (меню аппаратного обеспечения)

Используйте это диалоговое окно для настройки паролей CHAP на устройствах iSCSI и VRM . Система автоматически передает эти пароли на учетные записи **Пользователь** и **Получатель** кодеров, декодеров и VSG устройств.
На новых добавленных устройствах пароли устанавливаются автоматически при активации конфигурации.
Примечание. Установка пустого пароля CHAP приводит к удалению пароля CHAP с устройств iSCSI и VRM .

Замечание!
- Для всех устройств DSA E-Series пароль CHAP устанавливается автоматически.
- Устройства VRM передают пароль CHAP на кодеры. Однако для обеспечения записи необходимо установить пароль CHAP на соответствующем устройстве iSCSI.
- На всех устройствах DIVAR IP необходимо вручную установить пароль CHAP. См. соответствующее руководство DIVAR IP для получения подробных инструкций. В противном случае запись прекратится или не будет работать воспроизведение.

Глобальный пароль CHAP
Введите iSCSI пароль CHAP, необходимый для проверки подлинности устройства хранения iSCSI и активации прямого воспроизведения с iSCSI.

Подтвердите глобальный пароль CHAP
Подтвердить пароль CHAP для iSCSI.

Отобразить пароль
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Применить
Нажмите, чтобы применить пароль CHAP.
Примечание: Проверьте результат работы. Возможно, пароль CHAP нужно будет устанавливать вручную на некоторых устройствах iSCSI.

13.8 Диалоговое окно «Изменить пароли устройств» (меню «Оборудование»)

Главное окно > **Устройства** > **Изменить пароли устройств** > диалоговое окно **Изменить пароли устройств**
или
Главное окно > меню **Аппаратное обеспечение** > команда **Изменить пароли устройств...** > диалоговое окно **Изменить пароли устройств**

Нажмите, чтобы обновить информацию о состоянии всех устройств. Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите **Обновить состояние**.
Примечание. Если у вас большая система с несколькими тысячами настроенных устройств, процесс обновления состояния может занять длительное время.

Нажмите, чтобы выбрать все доступные устройства сразу.

Показать пароли
Установите флажок, если вы хотите, чтобы настроенные пароли отображались в читаемой форме.

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.
Примечание. Только если флажок **Показать пароли** установлен, можно также выполнить поиск паролей.

В этой таблице можно установить следующие свойства доступных IP-устройств:
– Пароль сервиса
– Пароль пользователя
– Пароль Live
– Пароль пункта назначения

Чтобы изменить пароль для IP-устройств:
1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и щелкните **Изменить пароль...**.
   Отобразится диалоговое окно **Изменить пароли устройств**.
3. Выберите требуемый тип пароля.
4. Введите новый пароль.
5. Нажмите **OK**.
   Новый пароль будет применен для выбранного устройства.

Чтобы изменить параметры для нескольких устройств:
См *Настройка нескольких кодеров / декодеров, Страница 240*.

13.9 Диалоговое окно «Обновить микропрограммное обеспечение устройства» (меню «Оборудование»)

Главное окно > меню **Аппаратное обеспечение** > команда **Обновить микропрограмму устройства...** > диалоговое окно **Обновить микропрограмму устройства**

Нажмите, чтобы обновить информацию о состоянии всех устройств. Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите **Обновить состояние**.
Примечание. Если у вас большая система с несколькими тысячами настроенных устройств, процесс обновления состояния может занять длительное время.

Нажмите, чтобы выбрать все доступные устройства сразу.

Нажмите для обновления версии микропрограммы.

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Порядок обновления микропрограммы:

1. Выберите требуемое устройство.
2. Нажмите **Обновить микропрограмму**.
   Откроется информационное окно Configuration Client.
3. Нажмите **OK**.
   Откроется проводник.
4. Выберите файл с обновлением.
5. Нажмите **Открыть**.
   Откроется окно **Состояние отправки программного обеспечения**.
6. Чтобы начать загрузку, нажмите **Начало**.
7. Нажмите **Закрыть**.
   Микропрограмма обновлена.

Чтобы изменить параметры для нескольких устройств:
См *Настройка нескольких кодеров / декодеров, Страница 240*.

13.10 Диалоговое окно «Изменить IP-адрес и сетевые параметры устройства» (меню «Оборудование»)

Главное окно > меню **Аппаратное обеспечение** > команда **Изменить IP-адрес устройства и сетевые параметры...** > диалоговое окно **Изменить IP-адрес и сетевые параметры устройства**

Нажмите, чтобы обновить информацию о состоянии всех устройств. Можно обновить состояние отдельного устройства: щелкните устройство правой кнопкой мыши и выберите **Обновить состояние**.
Примечание. Если у вас большая система с несколькими тысячами настроенных устройств, процесс обновления состояния может занять длительное время.

Нажмите, чтобы выбрать все доступные устройства сразу.

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

В этой таблице можно установить следующие свойства доступных IP-устройств:
– Краткое имя
– IP-адрес
– Маска подсети
– IP-адрес шлюза

Замечание!
Вместо использования команд вы можете ввести соответствующие параметры в нужном поле.

Чтобы задать отображаемые имена для IP-устройств:
1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и щелкните **Задать краткие имена...**. Отображается диалоговое окно **Задать краткие имена**.
3. В поле **Начинать с:** введите первую строку.
4. Нажмите **Рассчитать**. В поле **Заканчивать:** отображается последняя из ряда строк для выбранного устройства.
5. Нажмите **OK**.
6. В диалоговом окне **Изменить IP-адрес и сетевые параметры устройства** нажмите **Применить**.
   Вычисляемое имя будет обновлено в выбранном устройстве.

Диалоговое окно Задать отображаемые имена

Начинать с:
Введите первое имя.

Заканчивать:
Отображает последнее имя для выбранных устройств после нажатия кнопки **Рассчитать**.

Рассчитать
Нажмите для расчета диапазона кратких имен выбранных устройств.

Чтобы задать IP-адреса для IP-устройств:
1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и выберите **Установить IP-адреса...**. Отображается диалоговое окно **Установить IP-адреса**.
3. В поле **Начинать с:** введите первый IP-адрес.
4. Нажмите **Рассчитать**. В поле **Заканчивать:** отображается последний из ряда IP-адресов для выбранного устройства.
5. Нажмите **OK**.
6. В диалоговом окне **Изменить IP-адрес и сетевые параметры устройства** нажмите **Применить**.
   Новый IP-адрес вступит в силу в выбранном устройстве.

Диалоговое окно Установить IP-адреса

Начинать с:
Введите первый IP-адрес.

Заканчивать:
Отображает последний IP-адрес для выбранных устройств после нажатия кнопки **Рассчитать**.

Рассчитать
Нажмите для расчета диапазона IP-адресов выбранных устройств.

Чтобы задать маску подсети/идентификатор шлюза для IP-устройств:
1. Щелкните нужное поле.
2. Введите соответствующее значение.
3. Нажмите **Применить**.
   Новое значение будет применено для выбранного устройства.

Применить
Нажмите для применения введенных значений без закрытия диалогового окна.

Чтобы изменить параметры для нескольких устройств:
См *Настройка нескольких кодеров / декодеров, Страница 240*.

13.11 Диалоговое окно «Монитор устройств» (меню «Оборудование»)

Главное окно > меню **Аппаратное обеспечение** > команда **Монитор устройств...** > диалоговое окно **Монитор устройств**
Позволяет проверять состояние кодеров и декодеров в Дереве устройств, которые активны в системе BVMS.

Отображаемое имя
Имя устройства, заданное в BVMS.

Сетевой адрес
IP-адрес устройства.

Состояние

Возможно отображение следующих состояний.

- **Настроенные** — конфигурация этого устройства активирована.
- **Несоответствие конфигурации** — конфигурация этого устройства не активирована.
- **Неизвестно** — определение состояния невозможно.
- **Не подключено** — не подключено.

Последняя проверка

Дата и время начала работы диалогового окна и выполнения проверки. Пока диалоговое окно отображается, устройства не повторяются повторно.

См.

- *Проверка состояния кодеров/декодеров, Страница 98*

13.12 Диалоговое окно «Редактор командных сценариев» (меню «Инструменты»)

Подробную информацию см. в разделе *Диалоговое окно Редактор командных сценариев, Страница 318*.

См.

- *Диалоговое окно Редактор командных сценариев, Страница 318*

13.13 Диалоговое окно «Диспетчер ресурсов» (меню «Инструменты»)

Подробную информацию см. в разделе *Диалоговое окно Диспетчер ресурсов, Страница 273*.

См.

- *Диалоговое окно Диспетчер ресурсов, Страница 273*

13.14 Диалоговое окно «Конструктор последовательностей» (меню «Инструменты»)

Подробную информацию см. в разделе *Диалоговое окно Конструктор последовательностей, Страница 276*.

См.

- *Диалоговое окно Конструктор последовательностей, Страница 276*

13.15 Диалоговое окно «Диспетчер лицензий» (меню «Инструменты»)

Главное окно > меню **Сервис** > команда **Диспетчер лицензий...**

Позволяет лицензировать заказанный пакет BVMS и обновлять его дополнительными возможностями.

Состояние лицензии

Индикация состояния лицензии.

"Отпечаток пальца" системы

Для получения поддержки мы рекомендуем предоставить **"Отпечаток пальца" системы**.

Объект установки

При активации базовой лицензии в Bosch Remote Portal вы предоставляете информацию о месте установки своей системы. Здесь отображается эта информация.

Примечание: Вы также можете предоставлять эту информацию в других лицензиях, но здесь отображается только информация, представленная с базовой лицензией.

Лицензии

1. Нажмите **Добавить** , чтобы добавить свои лицензии.
   Отобразится **Добавить лицензию** диалоговое окно.
2. Следуйте инструкциям в диалоговом окне.

Действующая лицензия

Отображает действующую базовую лицензию, которую вы активировали.

Функциональные возможности

- Нажмите **Инспектор лицензий...**.
  Откроется диалоговое окно **Инспектор лицензий**.

Показывает количество установленных лицензионных функций.
Можно проверить, не превышает ли количество установленных лицензий BVMS количество приобретенных лицензий.

Установленная версия BVMS

Показывает установленную версию BVMS, например 11.0.

Лицензированные версии BVMS

Показывает все версии BVMS, которые включены в текущий файл лицензии и поддерживаются текущим предоставленным файлом лицензии.
Например, BVMS 11.0 и все последующие вспомогательные номера версии BVMS 11.x.

Дата активации

Отображает дату активации установленной версии BVMS.

Дата окончания срока действия

Отображает дату окончания действия установленной версии BVMS. Дата окончания действия применяется только при установке резервной лицензии или демонстрационных лицензий для продажи.

Software Maintenance Agreement

Дата окончания срока действия

Если вы приобрели и активировали любой вариант Software Maintenance Agreement, то дата окончания срока действия отображается здесь.

См.

- *Активация лицензии на программное обеспечение, Страница 77*
- *Добавить диалоговое окно лицензии, Страница 115*
- *Диалоговое окно «Проверка лицензий» (меню «Инструменты»), Страница 115*

13.15.1 Добавить диалоговое окно лицензии

Главное окно> **Сервис** меню > **Диспетчер лицензий...** команда > **Лицензии** > **Добавить**
Позволяет добавлять в систему приобретенные лицензии или демонстрационные лицензии с веб-сайта Bosch Remote Portal remote.boschsecurity.com BVMS.
Чтобы добавить лицензии, следуйте инструкциям в диалоговом окне.
Дополнительную информацию можно найти в соответствующем официальном документе по лицензированию BVMS.

13.16 Диалоговое окно «Проверка лицензий» (меню «Инструменты»)

Главное окно > меню **Сервис**, нажмите команду **Инспектор лицензий...** > диалоговое окно **Инспектор лицензий**

Показывает количество установленных лицензионных функций.
Можно проверить, не превышает ли количество установленных лицензий BVMS количество приобретенных лицензий.
Примечание: Если текущая конфигурация системы не соответствует ограничениям установленных в данный момент лицензий, то активировать конфигурацию невозможно.

13.17 Диалоговое окно «Мониторинг рабочих станций» (меню «Инструменты»)

Главное окно > меню **Сервис** > команда **Мониторинг рабочих станций...** > диалоговое окно **Мониторинг рабочих станций**

Отображает список всех рабочих станций, подключенных к BVMS Management Server.
Примечание. В списке отображаются все подключенные клиенты Operator Clients и Cameo SDK.

Чтобы отключить рабочую станцию:
1. Выберите соответствующий элемент списка.
2. Нажмите **Отключить**.
   Примечание. Эта функция активна только для пользователей с соответствующим разрешением.
3. Нажмите **Да**.
   Если соответствующий клиент Operator Client отключится, выбранный элемент списка исчезнет.

Примечание. Отключать можно только рабочие станции Operator Client.

13.18 Диалоговые окна «Отчеты» (меню «Отчеты»)

В этой главе описаны все диалоговые окна, доступные для отчетов о конфигурации.

См.
– *Создание отчета, Страница 99*

13.18.1 Диалоговое окно "Расписания записей"

Главное окно > меню **Отчеты** > команда **Расписания записи...**
Открывает список настроенных расписаний записей.
- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.2 Диалоговое окно Настройки записи по расписанию

Главное окно > меню **Отчеты** > команда **Параметры записи по расписанию...**
Открывает список параметров настроенных расписаний записей.
- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.3 Диалоговое окно "Расписания задач"

Главное окно > меню **Отчеты** > команда **Расписания задач...**
Открывает список настроенных расписаний задач.
- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.4 Диалоговое окно "Камеры и параметры записи"

Главное окно > меню **Отчеты** > команда **Камеры и параметры записи...**

Открывает список параметров записи, настроенных в таблице камер и таблице записи.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.5 Диалоговое окно "Параметры качества потока"

Главное окно > меню **Отчеты** > команда **Параметры качества потока...**

Открывает список настроенных параметров качества потока для всех камер.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.6 Диалоговое окно "Настройки событий"

Главное окно > меню **Отчеты** > команда **Параметры составного события...**

Открывает список событий, для которых настроено расписание вызова тревожного сигнала.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.7 Диалоговое окно "Настройки составных событий"

Главное окно > меню **Отчеты** > команда **Параметры составного события...**

Открывает список всех составных событий.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.8 Диалоговое окно "Настройки тревог"

Главное окно > меню **Отчеты** > команда **Параметры тревог...**

Открывает список всех настроек тревог для настроенных тревог, включая параметры в диалоговом окне **Параметры тревог**.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.9 Диалоговое окно "Настроенные пользователи"

Главное окно > меню **Отчеты** > команда **Настроенные пользователи...**

Открывает список пользователей, которым разрешен вход в Operator Client.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.10 Диалоговое окно "Группы пользователей и учетные записи"

Главное окно > меню **Отчеты** > команда **Группы пользователей и учетные записи...**

Открывает список настроенных групп пользователей, Enterprise Accounts, Enterprise User Groups и групп двойной авторизации.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.11 Диалоговое окно "Разрешения для устройств"

Главное окно > меню **Отчеты** > команда **Разрешения устройства...**

Открывает список разрешений на использование настроенных устройств для каждой группы пользователей.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.12 Диалоговое окно "Рабочие разрешения"

Главное окно > меню **Отчеты** > команда **Разрешения для операторов**

Открывает список разрешений на использование Operator Client для каждой группы пользователей.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.13 Диалоговое окно «Разрешения конфигурации»

Главное окно > меню **Отчеты** > команда **Разрешения конфигурировании...**

Открывает список разрешений на использование Configuration Client для каждой группы пользователей.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.14 Диалоговое окно «Разрешения групп пользователей»

Главное окно > меню **Отчеты** > команда **Разрешения группы пользователей**

Открывает список разрешений для настройки групп пользователей для каждой группы пользователей.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.15 Диалоговое окно «Параметры безопасности»

Главное окно > меню **Отчеты** > команда **Параметры безопасности...**

Открывает список настроенных параметров безопасности для каждой группы пользователей и Enterprise User Groups.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.16 Диалоговое окно «Разрешения приложения»

Главное окно > меню **Отчеты** > команда **Разрешения приложений...**

Показывает список всех групп пользователей и их разрешения для приложений.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.18.17 Диалоговое окно «Обход устройств»

Главное окно > меню **Отчеты** > команда **Обойденные устройства...**

Открывает список всех настроенных устройств, а также тех, которые обходятся.

- Нажмите кнопку **Экспорт CSV**, чтобы сохранить все данные из этого диалогового окна в CSV-файл.

13.19 Диалоговое окно «Настройки тревог» (меню «Настройки»)

См. *Диалоговое окно Настройки тревог, Страница 322* для получения подробных сведений.

13.20 Диалоговое окно «Настройки SNMP» (меню «Настройки»)

Главное окно > меню **Настройки** > команда **Настройки SNMP...**

Позволяет настроить мониторинг SNMP на компьютере Management Server.

Пользователь задает, для какого события отправляется ловушка SNMP, какую-либо дополнительную информацию о системе и IP-адреса компьютеров, которые будут получать ловушки SNMP от BVMS.

Сервер отправляет ловушки SNMP, когда события происходят. Эти ловушки можно получать используя приемник SNMP в Configuration Client с помощью инструмента **Журнал регистрации запросов SNMP**. Также можно использовать другое программное обеспечение, которое может получать ловушки SNMP.
Агент SNMP в BVMS поддерживает SNMP GetRequest. Когда управляющее ПО SNMP (например, iReasoning MIB Browser) отправляет SNMP GetRequest в адрес BVMS Management Server, Management Server отправляет соответствующее ответное сообщение.
Файл MIB расположен в следующем файле:

```
<installation_directory>\Bosch\VMS\bin\BVMS.mib
```

Поддерживаются только SNMPv1 и v2.
Примечания. SNMPv1 и SNMPv2 не являются полностью совместимыми. Поэтому не рекомендуется использовать SNMPv1 и SNMPv2 совместно.

Порт SNMP GET
Введите номер порта для SNMP GetRequest. Это порт, где агент SNMP системы BVMS Management Server ожидает SNMP GetRequest.
Примечание. BVMS не использует стандартный номер порта 161 для SNMP GetRequest, поскольку этот порт может использоваться агентом SNMP компьютера, где установлено ПО BVMS Management Server.
Значение по умолчанию: `12544`.

Контакт системы
Введите контактные данные для системы BVMS. Эту информацию можно получить с помощью SNMP GetRequest, используя OID .1.3.6.1.2.1.1.4.

Описание системы
Введите описание своей системы BVMS. Эту информацию можно получить с помощью SNMP GetRequest, используя OID .1.3.6.1.2.1.1.4.

Расположение системы
Введите расположение своей системы BVMS. Эта строка должна указывать физическое расположение сервера, например здание, номер помещения, номер стойки и т. п.
Эту информацию можно получить с помощью SNMP GetRequest, используя OID .1.3.6.1.2.1.1.6.

Приемники запросов
Введите IP-адрес компьютера, куда система BVMS должна отправлять ловушки SNMP.

Фильтр запросов
Щелкните, чтобы выбрать события в дереве событий и отфильтровать отправляемые ловушки SNMP.

См.
– *Настройка мониторинга SNMP, Страница 98*

13.21 Диалоговое окно «Настройки LDAP сервера» (меню «Настройки»)

Главное окно > меню **Настройки** > команда **Параметры сервера LDAP...**
Здесь вы вводите параметры сервера LDAP, которые настраиваются вне BVMS. Вам понадобится помощь администратора, настраивавшего сервер LDAP.
Все поля являются обязательными, за исключением полей в области **Тест пользователя/Группа пользователей**.

Параметры сервера LDAP

Сервер LDAP
Введите имя или IP-адрес сервера LDAP.

Порт
Введите номер порта LDAP-сервера (по умолчанию HTTP: 389, HTTPS: 636)

Безопасное соединение
Установите флажок, чтобы включить защиту передачи данных.

Механизм аутентификации
Параметр «Согласовать» позволяет выбрать соответствующий протокол проверки подлинности.
Параметр «Простой» позволяет передавать учетные данные для входа в систему в незашифрованном открытом тексте.

Аутентификация с помощью прокси-сервера

Анонимный
Используется для входа в систему в качестве гостя. Выберите этот параметр, если LDAP-сервер поддерживает его и вы не можете настроить конкретного пользователя прокси-сервера.

Используйте следующие учетные данные

Имя пользователя
Введите уникальное имя пользователя прокси-сервера. Этот пользователь необходим для того, чтобы пользователи группы BVMS имели доступ к серверу LDAP.

Пароль
Введите пароль пользователя прокси-сервера.

Тест
нажмите, чтобы проверить, имеет ли пользователь прокси-сервера доступ к серверу LDAP.

Основание LDAP для пользователя
Введите уникальное имя (DN = распознаваемое имя) пути LDAP, где вы хотите осуществить поиск пользователя.
Пример для DN основания LDAP: CN=Users,DC=Security,DC=MyCompany,DC=com

Фильтр для пользователя
Выберите фильтр, используемый для поиска уникального имени пользователя. Примеры определены заранее. Замените %username% действительным именем пользователя.

Основание LDAP для группы
Введите уникальное имя пути LDAP, где вы хотите осуществить поиск групп.
Пример для DN основания LDAP: CN=Users,DC=Security,DC=MyCompany,DC=com

Фильтр для поиска членов групп
Выберите фильтр, используемый для поиска члена группы.
Примеры определены заранее. Замените %usernameDN% фактическим именем пользователя и его DN.

Фильтр поиска группы
Не оставляйте это поле пустым. Если запись отсутствует, вы не можете назначить группу LDAP пользовательской группе BVMS.
Выберите фильтр для поиска пользовательской группы.
Примеры определены заранее.

Тест пользователя/Группа пользователей
Записи в этой области не сохраняются после нажатия на **OK**. Они служат только для тестирования.

Имя пользователя
Введите имя тестового пользователя. Пропустите DN.

Пароль
Введите пароль тестового пользователя.

Тест пользователя
Нажмите, чтобы проверить, правильна ли комбинация имени пользователя и пароля.

Группа (DN)
Введите уникальное имя группы, с которой связан пользователь.

Тест группы
Нажмите для проверки связи пользователя с группой.

См.
– *Выбор связанной группы LDAP, Страница 370*

13.21.1 Связывание группы LDAP

Группу LDAP можно связать с группой пользователей BVMS, чтобы пользователи этой группы LDAP имели доступ к Operator Client. Пользователи группы LDAP имеют права доступа группы пользователей в соответствии с настройками группы LDAP.
Возможно, потребуется помощь ИТ-администратора, ответственного за сервер LDAP.
Группы LDAP настраиваются в стандартных группах пользователей или в Enterprise User Groups.

Замечание!
Если группа LDAP связана с группой пользователей BVMS, пользователи этой группы LDAP могут запускать Operator Client с использованием единого входа.

Замечание!
Пользователь LDAP может быть связан с несколькими группами пользователей LDAP, которые, в свою очередь, связаны с определенной группой пользователей BVMS. Пользователь LDAP получает права группы пользователей BVMS, которая расположена выше других групп пользователей LDAP, связанных с этим пользователем LDAP.

Чтобы связать группу LDAP:
1. Нажмите **Параметры сервера LDAP...**.
   Откроется диалоговое окно **Параметры сервера LDAP**.
2. Введите параметры вашего сервера LDAP и нажмите **OK**.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

См.
– *Диалоговое окно «Настройки LDAP сервера» (меню «Настройки»), Страница 119*
– *Страница Свойства пользовательской группы, Страница 342*

13.22 Диалоговое окно «Определить порядок группы пользователей LDAP» (меню «Настройки»)

Отображает список **Изменить порядок групп пользователей LDAP**. В списке отображаются группы пользователей LDAP, а также связанные с ними группы пользователей BVMS и Enterprise User Groups. Порядок расположения групп можно изменять перетаскиванием или с помощью кнопок со стрелками вверх и вниз.

Замечание!
Пользователь LDAP может быть связан с несколькими группами пользователей LDAP, которые, в свою очередь, связаны с определенной группой пользователей BVMS. Пользователь LDAP получает права группы пользователей BVMS, которая расположена выше других групп пользователей LDAP, связанных с этим пользователем LDAP.

13.23 Диалоговое окно «Параметры токена доступа» (меню «Настройки»)

Главное окно > меню **Настройки** > команда **Параметры маркера доступа...**
Если вы настроили вход на Management Server с помощью токена доступа, сначала необходимо определить его параметры.
Токен создается на Enterprise Management Server и подписывается сертификатом из хранилища сертификатов на локальном компьютере. Необходимо идентифицировать сертификат, чтобы знать, какой сертификат использовать.
Примечание: BVMS не поддерживает сертификаты, которые используют алгоритм безопасного хеширования SHA-1 и имеют длину ключа меньше 2048 бит.

Свойства сертификата подписи
Введите строку свойств, чтобы идентифицировать соответствующий сертификат.
Примечание: если критерию соответствует несколько сертификатов, используется самый новый из действующих сертификатов.

Следуйте правилам, чтобы ввести действительную строку свойств в поле **Свойства сертификата подписи**:
- Строка состоит из одного или нескольких условий.
- Условия разделены точкой с запятой (;).
- Условия представляют собой пары из имени свойств сертификата и ожидаемого значения, разделенные знаком равно (=).
- Имена свойств сертификатов могут состоять из одной или нескольких частей, разделенных точкой (.).
- Имена свойств сертификатов и ожидаемые значения не чувствительны к регистру.

Примеры:
`SubjectName.CN=BVMS Token Issuer;Parent.SubjectName.CN=BVMS Intermediate`
- Часть Общего имени (`CN`) в имени Субъекта сертификата должна быть равна `BVMS Token Issuer`.
- Кроме того, часть Общего имени в имени Субъекта родительского сертификата должна быть равна `BVMS Intermediate`. Родительским является тот сертификат, который использовался для подписи текущего сертификата.

`Parent.Thumbprint=A95FF7C6EC374127174D3AFA8EA67C94E8E66C3F`

– Отпечаток родительского сертификата должен соответствовать указанному.

Список поддерживаемых имен свойств сертификатов:

Название	Тип возврата
Отпечаток	Строка
Серийный номер	Строка
Имя Субъекта	Распознаваемое имя субъекта
Имя эмитента	Распознаваемое имя эмитента
Родитель	Сертификат, использованный для подписи текущего сертификата (эмитент CA)

Список поддерживаемых имен свойств на распознаваемом имени:

Название	Тип возврата
CN	Строка: общее имя
OU	Строка: название организационной единицы
O	Строка: название организации
L	Строка: название местоположения
Ю	Строка: название штата или региона
C	Строка: название страны

Примеры использования распознаваемого имени:

– `SubjectName.CN=verisign authority`
– `IssueName.C=DE`
– `Parent.Parent.SubjectName.O=Bosch Security Systems`

Цепочка сертификатов

Установите флажок, чтобы включить цепочку сертификатов.

Примечание: если на Management Server уже установлен точно такой же сертификат, не обязательно включать цепочку сертификатов.

Количество включенных сертификатов

Введите точное количество сертификатов, которые включены в токен доступа.

Примечание: вы не должны включать сертификат Root.

Срок действия маркера доступа

Введите время в часах, чтобы установить, сколько времени токены будут действительны после их создания в Enterprise Management Server.

См.

– *Проверка подлинности на основе токена, Страница 90*

13.24 Диалоговое окно «Параметры доверенного сертификата» (меню «Настройки»)

Главное окно > меню **Настройки** > команда **Параметры доверенного сертификата...**

Это диалоговое окно позволяет ввести отпечаток сертификата, используемый Management Server для проверки подлинности токена доступа.

Примечание. Меню **Параметры доверенного сертификата...** доступно только после запуска Configuration Client с правами администратора и в том случае, если у пользователя, который входит в учетную запись, есть разрешение **Настройка групп пользователей/Enterprise Accounts**.

Отпечаток доверенного сертификата
Здесь отображается уже сконфигурированный отпечаток или пустой отпечаток, если конфигурация не может быть найдена в регистре. Введите или измените отпечаток корневого сертификата.
Предоставленный отпечаток записывается в путь `HKEY_LOCAL_MACHINE\SOFTWARE\Bosch Sicherheitssysteme GmbH\Bosch Video Management System\TrustedCertificates` к ключу «BvmsTrustedCertificate».
Примечание: при экспорте конфигурации отпечаток не включается в экспорт.
Примечание: BVMS не поддерживает сертификаты, которые используют алгоритм безопасного хеширования SHA-1 и имеют длину ключа меньше 2048 бит.

13.25 Диалоговое окно «Параметры» (меню «Настройки»)

Примечание: Для некоторых функций необходимо приобретать соответствующую лицензию.

Главное окно > меню **Настройки** > команда **Параметры...**

Configuration Client

Язык
Позволяет вам настроить язык Configuration Client. При выборе **Системный язык** используется язык, настроенный в Windows.
Этот параметр включается при перезапуске клиента Configuration Client.

Автоматический выход
Позволяет настраивать автоматический выход из клиента Configuration Client. По истечении заданного времени будет выполнен выход из клиента Configuration Client. Изменения на страницах конфигурации следующих устройств на странице **Устройства** не сохраняются автоматически и теряются после выхода из системы после периода бездействия:
- Кодеры
- Декодеры
- Устройства VRM
- Устройства iSCSI
- Устройства VSG

Все остальные новые изменения конфигурации сохраняются автоматически.
Примечание. Изменения в диалоговых окнах, не подтвержденные нажатием кнопки **ОК**, не сохраняются.

Scan options
Позволяет вам настроить, если это возможно, поиск устройств в соответствующей подсети или по подсетям.

Operator Client

Множественный вход

Разрешить несколько раз входить в систему с использованием одного имени пользователя
Позволяет указать, что пользователи BVMS SDK, веб-клиента BVMS, мобильного приложения BVMS или Operator Client могут выполнять одновременно несколько входов с использованием одного имени пользователя.

Параметры сервера

Строка подключения к базе данных
Позволяет настроить строку подключения для базы данныхжурнала.

Замечание!
Эту строку следует изменять только в тех случаях, когда вы хотите настроить удаленный сервер SQL для журнала, и только если вы знакомы с технологией сервера SQL.

Срок хранения
Позволяет вам задать максимальный срок хранения записей в журнале. По истечении заданного срока хранения записи будут автоматически удаляться.
Этот параметр включается после активации конфигурации.

Для редактирования следующих параметров необходимо разрешение:

Параметры Audit Trail
Audit Trail
Включить или отключить функцию Audit Trail.
Примечание. Страница Audit Trail отображается в Configuration Client, только когда функция включена.

Максимальный период хранения
Позволяет вам задать максимальный срок хранения записей Audit Trail. По истечении заданного срока хранения записи будут автоматически удаляться.

Язык
Выберите язык записей Audit Trail.
Исключение. Все записи Audit Trail из категории фильтров **Устройства (конфигурация камеры)** будут отображаться на языке, настроенном в Configuration Client.

Примечание. Установите базу данных Audit Trail, выбрав ее при настройках BVMS (дополнительная функция настроек).
Параметры Audit Trail активируются только после активации конфигурации.

Устройства

Группа мониторов
Позволяет указать, что пользователи могут управлять всеми группами мониторов с каждого клиентского компьютера BVMS. Впоследствии не понадобится настраивать этот компьютер как рабочую станцию в дереве устройств.

Выбор потока декодера
Позволяет настроить таким образом, чтобы все декодеры в системе использовали совместимый поток, который не обязательно должен быть потоком реального времени. Этот параметр включается после активации конфигурации.

Сервер времени для кодера
Позволяет сконфигурировать настройки сервера времени для кодеров. По умолчанию используется IP-адрес центрального сервера.

Функции системы

Карты

Тип фоновой карты
Позволяет выбрать тип фоновой карты для глобальной карты. При наличии доступа к Интернету (онлайн-режим) доступны следующие типы карт:
- **Карта улиц HERE**
- **Темная карта улиц HERE**
- **Спутниковая карта HERE**

Если у вас нет доступа к Интернету (автономный режим), выберите **Нет**.

Пользовательский ключ API
Введите свой API-ключ для использования онлайн-карт (Here).

Показать ключ API
Установите флажок, чтобы показывать ключ API.

Замечание!
При переключении типа фоновой карты с онлайн (Here карты) на автономный (**Нет**) или наоборот теряются все активные точки положения камер и окна просмотра карт.
Для глобальной карты можно задать только один фон. Этот фон применим ко всем окнам просмотра карт.

Map-based tracking assistant

Включить функцию системы
Позволяет настроить для пользователя Operator Client возможность использования Map-based tracking assistant.

Расширенное отображение состояния

Отключить выделение активных точек цветом на картах
Позволяет вам настроить отключение мигающих активных точек на картах.

Включено расширенное отображение состояния (выделение активных точек цветом на картах в зависимости от состояния)
Позволяет указать для всех событий состояния, что активные точки устройств, принадлежащих этому событию, при возникновении настроенного события выделяются цветом фона и миганием.

Включить расширенное отображение тревоги (выделение активных точек цветом на картах в зависимости от тревоги)
Позволяет указать для всех тревог, что активные точки устройств, принадлежащих этой тревоге, при возникновении настроенной тревоги выделяются цветом фона и миганием.
Настроить отображение дополнительного состояния можно после сохранения конфигурации. Активные точки отображаются на карте в Operator Client после активации конфигурации.

Экспорт с помощью Privacy overlay

Включить функцию системы

Позволяет настроить для пользователя Operator Client возможность экспортировать видео с помощью Privacy overlay.

14 Страница Устройства

Главное окно > **Устройства**

Замечание!
BVMS Viewer не поддерживает устройства декодирования.

Отображает дерево устройств и страницы настроек.
Количество элементов под записью отображается в квадратных скобках.
Позволяет настраивать доступные устройства, такие как устройства Mobile Video Service, кодеры ONVIF, устройства Bosch Video Streaming Gateway, кодеры, декодеры, устройства VRM, кодеры с локальным хранилищем, аналоговые матрицы или периферийные устройства, например ATM/POS Bridge.

Примечание:
Устройства отображаются в дереве и группируются в соответствии с физической сетевой структурой и категориями устройств.
Источники видеосигнала, например кодеры, группируются по VRMs.

Чтобы искать элементы:

- Введите запрос в поле поиска и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

- Щелкните элемент дерева для отображения соответствующей страницы.

14.1 Обновление состояний и возможностей устройств

Главное окно > **Устройства**
Например, после обновления микропрограммы может потребоваться синхронизировать возможности всех настроенных декодеров, кодеров и устройств VSG. С помощью этой функции возможности каждого устройства сравниваются с возможностями, уже хранящимися в BVMS. В дереве устройств можно обновить возможности сразу всех устройств одновременно.
Можно также скопировать в буфер обмена список устройств, чьи возможности изменились. Затем этот список можно вставить, например, в текстовый редактор для детального анализа изменений.
Список устройств вставляется из буфера обмена в формате CSV (значения, разделенные запятыми) и содержит следующую информацию:

- устройство;
- тип устройства;
- IP-адрес.

Примечание. Если у вас крупная система с несколькими тысячами настроенных устройств, процесс обновления состояний и возможностей устройств может занять длительное время.

Замечание!
Сведения о возможностях извлекаются только для доступных устройств. Узнать, доступно устройство или нет, можно, проверив состояние устройства.

Чтобы обновить состояния и возможности устройств:

1. Нажмите  .
   Откроется диалоговое окно **Обновить возможности устройства**. Для всех устройств будет обновлена информация о состоянии, будут получены сведения о возможностях устройств.
   При наличии устройств, сведения о возможностях которых не актуальны, соответствующие устройства отобразятся в списке и станет доступна кнопка **Обновить**.
2. При необходимости нажмите **Скопируйте список устройств в буфер обмена.**
3. Нажмите **Обновить**.
4. Нажмите **OK**.

⇨ Сведения о возможностях устройств будут обновлены.

Замечание!
Информация о состояниях всех устройств будет обновлена в любом случае, даже если вы отмените диалоговое окно **Обновление возможностей устройств**.

14.2 Изменение пароля для IP-устройств

Главное окно > **Устройства** >  **Изменить пароли устройств** > диалоговое окно **Изменить пароли устройств**
или
Главное окно > меню **Аппаратное обеспечение** > команда **Изменить пароли устройств...** > диалоговое окно **Изменить пароли устройств**

Чтобы изменить пароль для IP-устройств:

1. Выберите требуемое устройство.
2. Щелкните правой кнопкой мыши выбранное устройство и щелкните **Изменить пароль...**.
   Отобразится диалоговое окно **Изменить пароли устройств**.
3. Выберите требуемый тип пароля.
4. Введите новый пароль.
5. Нажмите **OK**.
   Новый пароль будет применен для выбранного устройства.

Подробную информацию см. в разделе *Диалоговое окно «Изменить пароли устройств» (меню «Оборудование»), Страница 109*.

Чтобы изменить параметры для нескольких устройств:
См *Настройка нескольких кодеров / декодеров, Страница 240*.

См.
– *Диалоговое окно «Изменить пароли устройств» (меню «Оборудование»), Страница 109*

14.3 Добавление устройства

Главное окно > **Устройства**

Следующие устройства добавляются в дерево устройств вручную. Это означает, что для добавления необходимо знать сетевой адрес устройства.

- IP-видеоустройства производства Bosch
- Аналоговый матричный коммутатор
  Чтобы добавить устройство Bosch Allegiant, необходим правильный файл конфигурации Allegiant.
- Рабочая станция BVMS
  На рабочей станции должно быть установлено программное обеспечение Operator Client.
- Устройство связи
- Bosch ATM/POS Bridge, устройство DTP
- Виртуальный вход
- Устройство мониторинга сети
- Клавиатура Bosch IntuiKey
- Клавиатура KBD-Universal XF
- Группа мониторов
- Модуль ввода/вывода
- Эмуляция CCL Allegiant
- Охранная панель производства Bosch
- Устройство для анализа на стороне сервера
- Системы контроля и управления доступом компании Bosch

Можно выполнять поиск следующих устройств для добавления с помощью диалогового окна **BVMS Scan Wizard**:

- Устройства VRM
- Кодеры
- Кодеры с локальным хранилищем и работающие только в режиме реального времени
- Кодеры ONVIF, работающие только в режиме реального времени
- Кодеры с локальными хранилищами
- Декодеры
- Устройства шлюза Video Streaming Gateway (VSG)
- Устройства DVR

Замечание!

После добавления устройства нажмите для сохранения настроек

Замечание!

Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.

Диалоговое окно BVMS Scan Wizard

Главное окно > **Устройства** > Развернуть > Щелкнуть правой кнопкой мыши > Щелкнуть **Поиск кодеров** > Диалоговое окно **BVMS Scan Wizard**

Главное окно > **Устройства** > Развернуть > Щелкнуть правой кнопкой мыши > Щелкнуть **Поиск шлюзов Video Streaming Gateway** > Диалоговое окно **BVMS Scan Wizard**

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши > Щелкнуть **Поиск кодеров, работающих только в реальном времени**> Диалоговое окно **BVMS Scan Wizard**

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши > Щелкнуть **Поиск кодеров локального хранилища** > Диалоговое окно **BVMS Scan Wizard**

Главное окно > **Устройства** > Развернуть > Развернуть > Щелкнуть правой кнопкой мыши > Щелкнуть **Поиск декодеров** > Диалоговое окно **BVMS Scan Wizard**

Это диалоговое окно позволяет выполнить поиск доступных устройств в сети, настроить их и добавить их в систему в рамках одной процедуры.

Использовать

Нажмите для выбора устройства, которое необходимо добавить в систему.

Тип (недоступно для устройств VSG)

Отображает тип устройства.

Отображаемое имя

Отображает имя устройства, которое был введено в Дереве устройств.

Сетевой адрес

Отображает IP-адрес устройства.

Имя пользователя

Отображает имя пользователя, настроенное на устройстве.

Пароль

Введите действующий пароль для проверки подлинности на этом устройстве.

Состояние

Отображает состояние проверки подлинности.

— успешно

— неудачно

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши > Щелкнуть **Выполнить поиск устройств VRM**> Диалоговое окно BVMS Scan Wizard

Замечание!

Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

Роль

Выберите нужное значение в списке.

В следующей таблице перечислены функции, которые может выполнять каждый тип VRM:

Функция / тип	Основной VRM	Дополнительный VRM
Основная (стандарт)	X	
Дополнительная (стандарт)		X
Основная резервная	X	
Дополнительная резервная		X
Зеркальный		X

Основному диспетчеру VRM можно добавить устройство VRM со следующими функциями:

– Резервный VRM
– Зеркальный VRM

Дополнительному диспетчеру VRM можно добавить устройства VRM со следующими функциями:

– Резервный VRM

Ведущий VRM

Выберите нужное значение в списке.

Имя пользователя

Отображает имя пользователя, настроенное на устройстве VRM.

При необходимости можно ввести другое имя пользователя.

См.

– *Добавление устройств VRM путем поиска, Страница 177*
– *Добавление кодера в пул VRM, Страница 227*
– *Добавление кодера, работающего только в режиме реального времени, Страница 227*
– *Добавление кодера локального хранилища, Страница 227*
– *Поиск устройств, Страница 76*

14.4 Страница «Список серверов/Адресная книга»

Главное окно > **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**

Можно добавить несколько компьютеров Management Server для одновременного доступа в BVMS Enterprise System. Также можно добавить несколько компьютеров Management Server для последовательного доступа к Server Lookup.

Можно добавить дополнительные столбцы в список серверов. Это позволяет добавлять дополнительные сведения, которые пользователь может использовать для поиска с помощью Server Lookup. Добавленные столбцы также будут отображаться на странице **Доступ к серверу** (главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Доступ к серверу**).

Добавить сервер

Нажмите для отображения диалогового окна **Добавить сервер**.

Удалить сервер:

Нажмите, чтобы удалить записи Management Server.

Management Server
Отображаются имена всех добавленных компьютеров Management Server. Каждую запись можно изменить.

Примечание: при использовании подключения SSH введите адрес в следующем формате:
ssh://IP или servername:5322

Частный сетевой адрес
Отображаются частные сетевые адреса всех добавленных компьютеров Management Server. Каждую запись можно изменить.

Номер сервера
Отображаются логические номера всех добавленных компьютеров Management Server. Каждую запись можно изменить.

Описание сервера
Введите описание для Management Server. Это описание необходимо, чтобы найти его в списке всех доступных серверов, если требуется монопольный доступ к Management Server, например, чтобы очистить тревожный сигнал, поступающий из другой системы управления.

Нажмите для получения пошаговых инструкций:
- *Настройка списка серверов для корпоративной системы, Страница 88*
- *Настройка Server Lookup, Страница 133*
- *Экспорт списка серверов, Страница 134*
- *Импорт списка серверов, Страница 134*

См.
- *Туннелирование SSH, Страница 51*

14.4.1 Диалоговое окно Добавить сервер

Главное окно > **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**

Имя сервера
Введите отображаемое имя сервера Management Server.

Примечание: при использовании подключения SSH введите адрес в следующем формате:
ssh://IP или servername:5322

Частный сетевой адрес
Введите частный IP-адрес или DNS-имя Management Server.

Общедоступный сетевой адрес
Введите общедоступный сетевой адрес.

Описание сервера
Введите описание Management Server.

14.4.2 Настройка Server Lookup

Для просмотра сервера пользователь Operator Client или Configuration Client входит в систему с именем пользователя из обычной группы пользователей, а не как пользователь Enterprise User Group.

См.

- *Server Lookup, Страница 25*
- *Страница «Список серверов/Адресная книга», Страница 132*
- *Использование просмотра сервера, Страница 76*

14.4.3 Настройка списка серверов

Главное окно > **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**

Добавление серверов.

1. Нажмите **Добавить сервер**.
   Отображается диалоговое окно **Добавить сервер**.
2. Введите отображаемое имя сервера и адрес частной сети (DNS-имя или IP-адрес).
   Примечание. При использовании соединения по протоколу SSH введите адрес в следующем формате:
   ssh://IP-адрес или имя_сервера:5322
3. Нажмите **OK**.
4. Повторите эти действия для добавления всех необходимых компьютеров Management Server.

Чтобы добавить столбцы:

- ▸ Щелкните правой кнопкой мыши на заголовке таблицы, затем нажмите **Добавить столбец**.
  Можно добавить до 10 столбцов.
  Чтобы удалить столбец, щелкните на нем правой кнопкой мыши и нажмите **Удалить столбец**.
- ⇨ При экспорте списка серверов также будут экспортированы добавленные столбцы.

См.

- *Настройка списка серверов для корпоративной системы, Страница 88*

14.4.4 Экспорт списка серверов

Главное окно > **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**

Можно экспортировать список серверов со всеми настроенными свойствами для редактирования и дальнейшего импорта.

При внесении изменений в экспортированный файл CSV во внешнем редакторе обратите внимание на ограничения, описанные в разделе Список серверов.

Порядок выполнения экспорта:

1. Щелкните заголовок таблицы правой кнопкой мыши и нажмите **Экспорт списка серверов...**.
2. Введите имя для экспортного файла и нажмите **Сохранить**.
- ⇨ Все столбцы списка серверов экспортируются в виде файла CSV.

Дополнительная информация

- *Server Lookup, Страница 25*
- Список серверов
- *Страница «Список серверов/Адресная книга», Страница 132*

14.4.5 Импорт списка серверов

Главное окно > **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**

Если вы внесли изменения в экспортированный файл CSV во внешнем редакторе, обратите внимание на ограничения, описанные в разделе Список серверов.

Импорт.

1. Щелкните заголовок таблицы правой кнопкой мыши и нажмите **Импорт списка серверов...**.
2. Нажмите нужный файл, затем нажмите **Открыть**.

Дополнительная информация

– *Server Lookup, Страница 25*
– Список серверов
– *Страница «Список серверов/Адресная книга», Страница 132*

14.5 Страница DVR (цифровой видеорегистратор)

Главное окно > **Устройства** >  > 

Отображает страницы свойств выбранного цифрового видеорегистратора.
Позволяет интегрировать цифровой видеорегистратор в вашу систему.

- Щелкните вкладку для перехода к соответствующей странице свойств.

Замечание!
В данном случае вы настраиваете не систему DVR, а только интеграцию устройства DVR в BVMS.

Замечание!
Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.

См.

– *Цифровые видеорегистраторы, Страница 135*
– *Настройка интеграции цифрового видеорегистратора, Страница 138*

14.5.1 Цифровые видеорегистраторы

В этой главе предоставляются общие сведения о цифровых видеорегистраторах, которые можно интегрировать в BVMS.
Некоторые модели цифровых видеорегистраторов (например, DHR-700) поддерживают запись с кодеров / IP-камер. Другие модели цифровых видеорегистраторов поддерживают только аналоговые камеры.
Кодеры / IP-камеры не следует интегрировать в конфигурацию двух видеосистем (цифровые видеорегистраторы или системы управления видео).
Если кодеры / IP-камеры подключены к цифровому видеорегистратору, который уже интегрирован в BVMS, такие кодеры / IP-камеры не обнаруживаются при поиске сетевых устройств BVMS в сети. Это также верно для поиска в сети, запущенного из Configuration Client или Config Wizard.
Если цифровой видеорегистратор с подключенными кодерами / IP-камерами интегрирован в BVMS и эти кодеры / IP-камеры уже добавлены в BVMS, отображается предупреждение. Удалите такие кодеры / IP-камеры из данного цифрового видеорегистратора или BVMS.
Config Wizard не добавляет в конфигурацию цифровые видеорегистраторы с конфликтующими IP-камерами.

Цифровые видеорегистраторы поддерживают ограниченное число одновременных подключений. Это число определяет максимальное количество пользователей Operator Client, которые могут одновременно отображать видео с цифрового видеорегистратора без отображения черных областей изображений.

Замечание!
Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.

Замечание!
DIVAR AN 3000/5000: обратите внимание, что при удалении видеоданных с цифрового видеорегистратора всегда удаляется не менее полного часа видеоданных. Например, если выбрать период времени с 6:50 до 7:05, фактически будут удалены все видеоданные с 6:00 до 8:00.

Гибридные и сетевые HD-видеорегистраторы Bosch серии 700: удаление всегда начинается с точки начала записи на всех камерах, которые отображаются в Operator Client, и заканчивается в указанной вами точке во времени.

См.
- *Страница DVR (цифровой видеорегистратор), Страница 135*
- *Настройка интеграции цифрового видеорегистратора, Страница 138*

14.5.2 Добавление устройств DVR путем поиска

Для добавления цифровых видеорегистраторов с помощью поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Выполнить поиск устройств DVR**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.
   В столбце **Состояние** успешные входы в систему обозначены значком .
   Неудачные попытки входа обозначены значком .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

14.5.3 Диалоговое окно "Добавить цифровой видеорегистратор"

Главное окно > **Устройства** > Разверните  >  > **Добавить цифровой видеорегистратор**

Позволяет вручную добавить цифровой видеорегистратор.

Сетевой адрес / порт

Введите IP-адрес вашего цифрового видеорегистратора. При необходимости измените номер порта.

Имя пользователя:

Введите имя пользователя для подключения к цифровому видеорегистратору.

Пароль:

Введите пароль для подключения к цифровому видеорегистратору.

Безопасность

Флажок **Безопасное соединение** установлен по умолчанию.

Если безопасное подключение невозможно, отображается соответствующее сообщение. Нажмите, чтобы снять флажок.

Замечание!

Если флажок **Безопасное соединение** установлен, подключения команд и управления защищены. Потоковая передача видеоданных не защищена.

См.

– *Добавление устройства, Страница 129*

14.5.4 Вкладка "Настройки"

Главное окно > **Устройства** >  >  > вкладка **Настройки**

Отображает сетевые параметры цифрового видеорегистратора, подключенного к вашей системе. Позволяет при необходимости изменять настройки.

14.5.5 Вкладка "Камера"

Главное окно > **Устройства** >  >  > вкладка **Камеры**

Все видеоканалы цифрового видеорегистратора отображаются как камеры. Позволяет вам удалять камеры.

Видеовход, отключенный в цифровом видеорегистраторе, отображается в BVMS как активная камера, так как для этого входа существуют более ранние записи.

14.5.6 Вкладка "Входы"

Главное окно > **Устройства** >  >  > вкладка **Входы**

Отображаются все выходы цифрового видеорегистратора.

Позволяет вам удалять элементы.

14.5.7 Вкладка "Реле"

Главное окно > **Устройства** >  >  > вкладка **Реле**

Отображаются все реле цифрового видеорегистратора. Позволяет вам удалять элементы.

14.5.8 Настройка интеграции цифрового видеорегистратора

Главное окно > **Устройства** > Разверните  > 

Замечание!
Добавьте DVR с помощью учетной записи администратора устройства. Использование учетной записи пользователя DVR с ограниченными разрешениями может привести к тому, что некоторые возможности не будут доступны в BVMS, например использование управления камерой PTZ.

Замечание!
В данном случае вы настраиваете не систему DVR, а только интеграцию устройства DVR в BVMS.

Удаление элемента:
1. Нажмите вкладку **Настройки**, вкладку **Камеры**, вкладку **Входы** или вкладку **Реле**.
2. Щелкните элемент правой кнопкой мыши и выберите **Удалить**. Элемент будет удален из системы.

Замечание!
Для восстановления удаленного элемента щелкните правой кнопкой мыши по устройству DVR и нажмите **Повторить сканирование устройства DVR**.

Переименование устройства DVR.
1. Щелкните устройство DVR правой кнопкой мыши и нажмите **Переименовать**.
2. Введите новое имя.

См.
- *Добавление устройства, Страница 129*
- *Страница DVR (цифровой видеорегистратор), Страница 135*

14.6 Страница Матричные коммутаторы

Главное окно > **Устройства** >  > 
Отображает страницы свойств устройства Bosch Allegiant.
В данном случае вы настраиваете не устройство Bosch Allegiant, а соответствующие параметры BVMS. Сведения о подключении устройств Allegiant к BVMS содержатся в разделе **Понятия** настоящей справки. В данном разделе содержится основная информация по данным вопросам.
Дополнительно можно настроить приоритеты управления для магистральных линий Allegiant.

- нажмите вкладку для перехода к соответствующей странице свойств.

См.
- *Настройка устройства Bosch Allegiant, Страница 139*
- *Подключение матричного коммутатора Bosch Allegiant к BVMS, Страница 58*

14.6.1 Добавление устройства Bosch Allegiant

Чтобы добавить устройство Bosch Allegiant:

1. Щелкните правой кнопкой мыши  и выберите команду **Добавить Allegiant**. Откроется диалоговое окно **Открыть**.
2. Выберите соответствующий файл конфигурации Allegiant и нажмите кнопку **ОК**. Устройство Bosch Allegiant будет подключено к системе.

Примечание. Можно добавить только один матричный коммутатор Bosch Allegiant.

14.6.2 Настройка устройства Bosch Allegiant

Главное окно > **Устройства** > Разверните  > 

В данном случае вы настраиваете не устройство Bosch Allegiant, а соответствующие параметры BVMS.

Чтобы назначить выход кодеру:

1. Перейдите на вкладку **Выходы**.
2. В столбце **Использование** щелкните **Цифровая магистраль** в нужных ячейках.
3. В столбце **Кодер** выберите требуемый кодер.

Добавление входа к устройству Bosch Allegiant:

1. Перейдите на вкладку **Входы**.
2. Нажмите **Добавить входы**. В таблицу будет добавлена новая строка.
3. Введите в ячейки требуемые параметры.

Удаление входа:

1. Перейдите на вкладку **Входы**.
2. Выберите нужную строку таблицы.
3. Нажмите **Удалить вход**. Строка будет удалена из таблицы.

См.

- *Подключение клавиатуры Bosch IntuiKey к BVMS, Страница 55*
- *Страница Соединение, Страница 140*
- *Страница Камеры, Страница 141*
- *Страница Выходы, Страница 139*
- *Страница Входы, Страница 140*

14.6.3 Страница Выходы

Главное окно > **Устройства** > Разверните  >  > вкладка **Выходы**

Позволяет настроить использование выхода устройства Bosch Allegiant и назначить выходу кодер.

Для сохранения видеоданных с выхода устройства Bosch Allegiant в системе BVMS вы должны назначить выходу кодер. Этот кодер должен быть подключен к выходу.

№

Отображает номер выхода.

Логический № Allegiant

Отображает логический номер выхода в пределах Allegiant.

Логический номер BVMS

Позволяет изменить логический номер выхода в пределах BVMS. Если вы введете номер, который уже используется, появляется соответствующее сообщение.

Имя
Отображает имя выхода.

Использование
Позволяет изменить использование выхода.
При выборе **Цифровая магистраль** можно назначить кодер этому выходу в поле **Кодер**. Выход Allegiant становится совместимым с сетью.
При выборе **Монитор Allegiant** в Operator Client пользователь может назначить сигнал камеры аппаратному монитору. Управление PTZ возможно, если камера настроена как камера PTZ. В Operator Client пользователь не может перетащить эту камеру в область изображений.
При выборе **Не используется** пользователь не может назначить монитор камере Allegiant.

Кодер
Позволяет назначить выход кодеру. Можно выбрать кодер только в том случае, если вы установили флажок **Цифровая магистраль**. Кодер блокируется для логического дерева. Если вы назначили кодер, уже присутствующий в логическом дереве, он удаляется оттуда. В Operator Client пользователь не может перетащить камеру на область изображений.

См.
– *Настройка устройства Bosch Allegiant, Страница 139*

14.6.4 Страница Входы

Главное окно > **Устройства** > Разверните  >  > вкладка **Входы**
Позволяет добавлять входы к устройству Bosch Allegiant.

Добавить вход
Нажмите, чтобы добавить в таблицу строку для указания нового входа.

Удалить вход
Нажмите для удаления строки из таблицы.

№ входа
Введите номер входа. Если вы введете номер, который уже используется, появляется соответствующее сообщение.

Имя входа
Введите имя входа.

См.
– *Настройка устройства Bosch Allegiant, Страница 139*

14.6.5 Страница Соединение

Главное окно > **Устройства** > Разверните  >  > вкладка **Соединение**
Отображает имя файла конфигурации Bosch Allegiant.
BVMS может считывать информацию из файла конфигурации, имеющего формат структурированного хранилища, содержащего имена и информацию о конфигурации всех камер, подключенных к устройству Bosch Allegiant.

Обновить конфигурацию
Нажмите для выбора файла конфигурации BoschAllegiant.

См.

– *Настройка устройства Bosch Allegiant, Страница 139*

14.6.6 Страница Камеры

Главное окно > **Устройства** > Разверните  >  > вкладка **Камеры**
Отображает таблицу камер, подключенных к устройству Bosch Allegiant.

№

Отображает последовательный номер камеры.

Логический № Allegiant

Отображает логический номер камеры.

Название камеры

Отображает название камеры.

См.

– *Настройка устройства Bosch Allegiant, Страница 139*

14.7 Страница Рабочая станция

Главное окно > **Устройства** > разверните  > 
На рабочей станции должно быть установлено программное обеспечение Operator Client.
Позволяет настроить следующие параметры рабочей станции:

– Добавьте CCTV клавиатуру, подключенную к рабочей станции Bosch Video Management System.
– Выберите командный сценарий, исполняемый при запуске рабочей станции.
– Выберите поток по умолчанию для отображения в реальном времени. Вы можете выбрать потоки для камер с двумя или несколькими потоками.

Примечание. Невозможно настроить клавиатуру CCTV для рабочей станции по умолчанию. Это возможно только для определенно настроенных рабочих станций.

Чтобы добавить клавиатуру Bosch IntuiKey, которая подключена к декодеру, разверните  и нажмите  .

См.

– *Добавление рабочей станции вручную, Страница 141*
– *Настройка командного сценария, выполняющегося при запуске (страница «Настройки»), Страница 142*

14.7.1 Добавление рабочей станции вручную

Чтобы добавить рабочую станцию BVMS:

1. Щелкните правой кнопкой мыши  .
2. Нажмите **Добавить рабочую станцию**.
   Откроется диалоговое окно **Добавить рабочую станцию**.
3. Введите соответствующее значение.

4. Нажмите **ОК**.

Рабочая станция будет добавлена в систему.

Чтобы добавить рабочую станцию BVMS по умолчанию:

- Щелкните правой кнопкой мыши .

Нажмите **Добавить рабочую станцию по умолчанию**.

Рабочая станция будет добавлена в систему.

Замечание!
Вы можете добавить только одну рабочую станцию по умолчанию.

Если рабочая станция по умолчанию настроена, параметры применяются для каждой рабочей станции, которая подключена к данному серверу и не настраивается отдельно. Если рабочая станция настроена, применяются параметры данной рабочей станции, а не рабочей станции по умолчанию.

14.7.2 Настройка клавиатуры Bosch IntuiKey (страница «Настройки») (рабочая станция)

Главное окно > **Устройства**> Разверните >

Чтобы настроить клавиатуру Bosch IntuiKey, подключенную к рабочей станции:

1. Перейдите на вкладку **Настройки**.
2. В поле **Keyboard Settings** введите необходимые параметры.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.

– *Страница Рабочая станция, Страница 141*

14.7.3 Настройка командного сценария, выполняющегося при запуске (страница «Настройки»)

Главное окно > **Устройства** > Разверните > > **Настройки**

Можно настроить командный сценарий, который будет запущен при запуске Operator Client на выбранной рабочей станции.

Вы должны создать соответствующий командный сценарий.

Сведения о создании командного сценария см. *Управление командными сценариями, Страница 92*.

Чтобы настроить командный сценарий:

- Выберите нужный командный сценарий из списка **Сценарий запуска:**.

См.

– *Страница Рабочая станция, Страница 141*

14.7.4 Страница Настройки

Главное окно > **Устройства** > разверните > > вкладку **Настройки**

Позволяет настроить сценарий, который будет выполняться при запуске Operator Client на рабочей станции.
Позволяет настроить TCP или UDP в качестве протокола передачи для всех камер, которые отображаются в режиме реального времени на рабочей станции.
Позволяет указать, какой поток IP-устройства используется для отображения в реальном времени.
Позволяет включить поиск для данной рабочей станции.
Можно также настроить клавиатуру, подключенную к данной рабочей станции.

Сетевой адрес:
Введите DNS-имя или IP-адрес вашей рабочей станции.

Сценарий запуска:
Выберите сценарий, который должен запускаться при запуске Operator Client рабочей станции. Этот сценарий можно создать или импортировать на странице **События**.

Протокол камеры по умолчанию:
Выберите протокол передачи данных по умолчанию, используемый для всех камер, назначенных логическому дереву на данной рабочей станции.

Переопределить настройки со страницы "Камеры и запись"
Установите флажок, чтобы активировать выбор нужного потока для отображения в реальном времени.
Примечание. Для цифровых видеорегистраторов, которые предоставляют более 1 потока (например, DIVAR AN 3000/5000), здесь также изменяется параметр "Поток просмотра в реальном времени" этого цифрового видеорегистратора. Параметры потоков просмотра в реальном времени для цифровых видеорегистраторов недоступны на странице **Камеры и запись**.

Поток в реальном времени
Выберите необходимый поток для просмотра в реальном времени. Вы можете выбрать потоки для камер с двумя или несколькими потоками.
При выборе **Оптимизирован размер области изображения** разрешение каждой отображаемой камеры настраивается автоматически в соответствии с размером области изображений в зависимости от разрешения используемого монитора. Это полезно для отображения нескольких камер с большим разрешением, например, камер 4K ultra HD. Только камеры с потоками, разрешение которых можно настроить независимо друг от друга, могут регулировать разрешение в соответствии с областью изображения. Пользователь Operator Client может изменить выбор потока для каждой камеры отдельно.

Двухпотоковые камеры
Выберите поток по умолчанию для отображения в режиме реального времени для камер с двойным потоком.

Многопотоковые камеры
Выберите поток по умолчанию для отображения в режиме реального времени для камер с несколькими потоками.

Использовать вместо этого транскодированный поток (если доступен)
Установите флажок, чтобы включить использование транскодированного потока, если он доступен. Этот транскодированный поток используется для просмотра в реальном времени вместо выбранного потока.
Чтобы в BVMS был доступен транскодированный поток, необходимо установить MVS, либо на компьютере VRM должен быть встроенный аппаратный транскодер.

При отображении камеры в режиме реального времени используется набор потоков по умолчанию для рабочей станции. Если у камеры нет потока 2 или сервис транскодирования (программный и аппаратный) недоступен, будет использоваться поток 1, даже если в параметрах рабочей станции настроен другой параметр.

Использовать прямое воспроизведение из системы хранения данных
Установите флажок для отправки видеопотока непосредственно с устройства хранения на эту рабочую станцию. Теперь поток не передается через VRM. Рабочей станции все равно требуется подключение к VRM, чтобы обеспечить правильное воспроизведение.
Примечание. Прямое воспроизведение с устройства хранения iSCSI можно использовать только в случае, если вы установили глобальный пароль CHAP iSCSI.

Извлечение видео в режиме реального времени не с камеры, а через шлюз Video Streaming Gateway
Отображение списка устройств Video Streaming Gateway. Выберите необходимые записи для передачи видеоданных через сегменты с низкой пропускной способностью между источником видео и данной рабочей станцией.
Примечание: если вы выберете устройство Video Streaming Gateway для получения видеоизображения в реальном времени, **Видеоизображение в реальном времени** - **Профиль** на странице **Камеры и запись** станет устаревшим. Вместо этого для видеоизображения в реальном времени также будет использоваться параметр **Запись** - **Профиль**.

Тип клавиатуры:
Выберите тип клавиатуры, подключенной к рабочей станции.

Порт:
Выберите COM-порт, который используется для подключения клавиатуры.

Скорость (бит/с):
Выберите максимальную скорость передачи (в битах в секунду), с которой данные должны передаваться через этот порт. Обычно это значение соответствует максимальной скорости, поддерживаемой компьютером или устройством, с которым осуществляется связь.

Информационные биты:
Отображает количество битов, используемых для каждого передаваемого и принимаемого символа.

Стоповые биты:
Отображает время между каждым передаваемым символом (если время измеряется в битах).

Четность:
Отображает тип контроля четности, используемый для данного порта.

Тип порта:
Отображает тип соединения, которое используется для подключения клавиатуры Bosch IntuiKey к рабочей станции.

См.
– *Настройка командного сценария, выполняющегося при запуске (страница «Настройки»), Страница 142*

14.7.5 Изменение сетевого адреса рабочей станции

Главное окно > **Устройства** > Развернуть 

Для изменения IP-адреса:

1. Щелкните правой кнопкой мыши  и выберите команду **Изменить сетевой адрес**.
   Откроется диалоговое окно **Изменить сетевой адрес**.
2. Измените список в поле в соответствии с вашими требованиями.

14.8 Страница Декодеры

Главное окно > **Устройства** > Развернуть  > 
Позволяет добавлять и настраивать декодеры.

Замечание!
BVMS Viewer не поддерживает устройства декодирования.

Замечание!
Если в системе необходимо использовать декодеры, убедитесь, что все кодеры используют один и тот же пароль для уровня авторизации user.

См.
- *Поиск устройств, Страница 76*
- *Страница «Кодер/декодер/камера Bosch», Страница 224*

14.8.1 Добавление кодера вручную

Главное окно > **Устройства** > Развернуть  > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить декодер** > Диалоговое окно **Добавить кодер**
Позволяет добавить кодер вручную. Это особенно полезно, если необходимо добавить какое-либо IP-видеоустройство производства Bosch (только для VRM).

Внимание.
Если добавляется IP-видео кодер Bosch с выбранным параметром **<Автоопределение>**, это устройство должно быть доступно в сети.

Добавление IP-видеоустройства производства Bosch:

1. Разверните , разверните , щелкните правой кнопкой мыши .
   Или
   щелкните правой кнопкой мыши .
   Или
   щелкните правой кнопкой мыши .
2. Нажмите **Добавить кодер**.
   Откроется диалоговое окно **Добавить кодер**.
3. Введите соответствующий IP-адрес.
4. В списке выберите **<Автоопределение>**, введите пароль устройства и нажмите **Проверить подлинность.**
   Или
   В списке выберите конкретный тип кодера или **<Камера с одним заполнителем>**.
5. Нажмите **ОК**.
   Устройство добавляется в систему.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

Диалоговое окно Добавить кодер

Сетевой адрес

Введите действительный IP-адрес.

Тип кодера

Для устройства с известным типом выберите соответствующий элемент. Устройство не обязательно должно быть доступно в сети.

Если требуется добавить какое-либо IP-видеоустройство производства Bosch, выберите **<Автоопределение>**. Это устройство должно быть доступно в сети.

Если вы хотите добавить камеру для конфигурирования в автономном режиме, выберите **<Камера с одним заполнителем>**.

Имя пользователя

Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль

Введите действующий пароль для аутентификации на устройстве.

Отобразить пароль

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Проверить подлинность

Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

14.8.2 Диалоговое окно «Изменить кодер / Изменить декодер»

Главное окно **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**

или

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**

или

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**

или

Главное окно > **Устройства** > Развернуть  > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Изменить декодер** > Диалоговое окно **Изменить декодер**

Позволяет проверить и обновить возможности устройства. Устройство подключается при открытии этого диалогового окна. Запрашивается пароль, и возможности устройства сравниваются с возможностями устройства, сохраненными вBVMS.

Имя

Отображает имя устройства. При добавлении IP-видеоустройства производства Bosch имя устройства генерируется системой. При необходимости измените значение.

Сетевой адрес

Введите сетевой адрес устройства. При необходимости измените номер порта.

Имя пользователя

Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль

Введите действующий пароль для аутентификации на устройстве.

Отобразить пароль

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Проверить подлинность

Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

Безопасность

Флажок **Безопасное соединение** установлен по умолчанию.

Если безопасное подключение невозможно, отображается соответствующее сообщение. Нажмите, чтобы снять флажок.

Следующие декодеры поддерживают безопасное соединение:

- VJD 7000
- VJD 8000
- VIP XD HD

Замечание!
Соединение между декодером и кодером безопасно, только если они настроены с использованием безопасного соединения.

Поток видео
UDP: обеспечивает зашифрованную многоадресную потоковую передачу для поддерживаемых устройств декодирования.
TCP: обеспечивает зашифрованную одноадресную потоковую передачу для поддерживаемых устройств декодирования.
Примечание: если для кодера не настроен адрес многоадресной передачи, декодер извлекает поток через одноадресную передачу.

Замечание!
BVMS не поддерживает камеры Bosch, подключенные к VSG.
BVMS поддерживает только шифрование UDP для платформ старше CPP13.

Возможности устройства
Отображаемые возможности устройства можно упорядочивать по категориям или по алфавиту.
Текст сообщения информирует о том, соответствуют ли автоматически определенные возможности устройства возможностям данного устройства.
Нажмите **OK** для применения изменений возможностей устройства после обновления устройства.

См.
- *Шифрование видео в режиме реального времени («Изменение кодера»), Страница 230*
- *Обновление возможностей устройства («Изменение кодера»), Страница 231*

14.8.3 Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»)

Главное окно > **Устройства** > Развернуть > Развернуть > >
или
Главное окно > **Устройства** > >
или
Главное окно > **Устройства** > >
или
Главное окно > **Устройства** > разверните > разверните >
Определите или измените отдельный пароль для каждого уровня. Введите пароль (не более 19 символов; без специальных символов) для выбранного уровня.

Для изменения пароля выполните следующие действия.

1. щелкните правой кнопкой мыши и нажмите **Изменить пароль...**.
   Откроется диалоговое окно **Введите пароль**.
2. Из списка **Введите имя пользователя** выберите пользователя, для которого необходимо изменить пароль.

3. В поле **Введите пароль для пользователя** введите новый пароль.
4. Нажмите **OK**.
⇨ Пароль на устройстве изменится незамедлительно.

Пароль препятствует несанкционированному доступу к устройству. Для ограничения доступа могут быть использованы различные уровни авторизации.
Надлежащая защита паролем обеспечивается только в тех случаях, когда все более высокие уровни авторизации также защищены паролем. Таким образом, всегда следует начинать с самого высокого уровня авторизации при назначении паролей.
Можно задать и изменить пароль для каждого уровня авторизации, если вы вошли в учетную запись пользователя «service».
Устройство имеет три уровня авторизации: service, user и live.
– service представляет собой высший уровень авторизации. Ввод правильного пароля дает доступ ко всем функциям и позволяет изменять все параметры конфигурации.
– user представляет собой средний уровень авторизации. На этом уровне можно эксплуатировать устройство, воспроизводить записи и управлять камерой, однако невозможно изменять конфигурацию.
– live представляет собой низший уровень авторизации. На этом уровне можно только просматривать видеоизображения в реальном времени и переключаться между различными экранами изображений в реальном времени.
Для декодера уровень авторизации live заменяется следующим уровнем авторизации:
– destination password (доступно только для декодеров)
Используется для доступа к кодеру.

См.
– *Предоставление пароля пункта назначения декодеру («Проверка подлинности...»), Страница 220*

14.8.4 Профиль декодера

Позволяет настроить различные параметры отображения видео на мониторе VGA.

Название монитора
Введите название монитора. Название монитора позволяет дистанционно идентифицировать местонахождение монитора. Используйте название, которое позволит максимально просто и однозначно идентифицировать местонахождение.

Нажмите  , чтобы обновить имя в дереве устройств.

Стандартный
Выберите выходной сигнал используемого монитора. Имеется восемь предварительно настроенных профилей параметров для мониторов VGA, кроме параметров PAL и NTSC для аналоговых видеомониторов.

Замечание!
Выбор параметра VGA со значениями, выходящими за пределы спецификаций монитора, может привести к серьезному повреждению монитора. Обратитесь к технической документации используемого вами монитора.

Компоновка окна
Выберите компоновку изображений по умолчанию для монитора.

Размер VGA-экрана
В данном поле введите соотношение сторон экрана (например, 4 x 3) или физические размеры экрана в миллиметрах. Устройство будет использовать эту информацию для точного масштабирования, не вносящего искажений в видеоизображение.

14.8.5 Данные на мониторе

Устройство распознает помехи передачи и отображает предупреждающее сообщение на мониторе.

Показывать помехи передачи
Выберите **Включено**, если на мониторе должно отображаться предупреждающее сообщение в случае возникновения помех передачи.

Чувствительность к помехам
Переместите ползунок, чтобы отрегулировать уровень помех, при котором отображается предупреждающее сообщение.

Текст уведомления о помехах
Введите текст предупреждения, которое отображается на мониторе при потере связи. Максимальная длина сообщения составляет 31 символ.

14.8.6 Настройка клавиатуры Bosch IntuiKey (декодер)

Главное окно > **Устройства**> разверните  >

Замечание!
Клавиатуру KBD-Universal XF невозможно подключить к декодеру.

Чтобы настроить клавиатуру Bosch IntuiKey, подключенную к декодеру:

1. Щелкните ячейку в столбце **Соединение** и выберите соответствующий декодер. Вы также можете выбрать рабочую станцию, если к ней подключена клавиатура Bosch IntuiKey.

   Рабочую станцию необходимо настроить на странице  .
2. В поле **Параметры подключения** введите необходимые параметры.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.
- *Страница "Назначить клавиатуру", Страница 161*
- *Сценарии подключения клавиатур Bosch IntuiKey, Страница 55*
- *Подключение клавиатуры Bosch IntuiKey к декодеру, Страница 57*

14.8.7 Настройка декодера для использования с клавиатурой Bosch IntuiKey

Главное окно > **Устройства** > Разверните  > Разверните 
Выполните следующие действия для настройки декодера VIP XD, подключенного к клавиатуре Bosch IntuiKey.

Чтобы настроить декодер:

1. Выберите соответствующий декодер, используемый для подключения к клавиатуре Bosch IntuiKey.

2. Перейдите на вкладку **Периферия**.
3. Убедитесь, что установлены следующие параметры:
   - Функция последов. порта:: **Прозрачный**
   - Скорость обмена данными:: **19200**
   - Стоповые биты: **1**
   - Контроль четности: **Нет**
   - Режим интерфейса: **RS232**
   - Полудуплексный режим:: **Выкл.**

См.
- *Сценарии подключения клавиатур Bosch IntuiKey, Страница 55*
- *Подключение клавиатуры Bosch IntuiKey к декодеру, Страница 57*
- *Обновление программного обеспечения клавиатуры Bosch IntuiKey, Страница 57*

14.8.8 Удалить логотип декодера

Нажмите для удаления логотипа, который был установлен на веб-странице декодера.

14.9 Страница «Группы мониторов»

Главное окно > **Устройства** > разверните  > 

Позволяет добавить и настроить группы мониторов. Группа мониторов назначается рабочей станции BVMS в  .

Замечание!
Невозможно управлять группой мониторов в Operator Client, если соединение с Management Server потеряно.

См.
- *Добавление группы мониторов вручную, Страница 151*
- *Настройка группы мониторов, Страница 152*
- *Настройка предустановленных положений и дополнительных команд, Страница 311*
- *Настройка тревоги, Страница 335*
- *Диалоговое окно Параметры тревог, Страница 325*
- *Диалоговое окно «Выбрать содержимое области изображений» (MG), Страница 324*

14.9.1 Добавление группы мониторов вручную

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить группу мониторов**

1. Нажмите **Добавить группу мониторов**.
   Отобразится диалоговое окно **Добавить группу мониторов**. Введите имя новой группы мониторов.
2. Нажмите «ОК».
   Группа мониторов добавлена в систему.
3. Нажмите **Карты и структура**.

4. Перетащите группу мониторов в Логическое дерево.

14.9.2 Настройка группы мониторов

Главное окно > **Устройства** > разверните  >  > 

Замечание!
Невозможно управлять группой мониторов в Operator Client, если соединение с Management Server потеряно.

Вы можете настроить мониторы в группе мониторов логически по столбцам и строкам. Это расположение не обязательно должно соответствовать реальному расположению мониторов.

Для настройки группы мониторов выполните следующие действия.

1. Перетащите соответствующий мониторы из вкладки **Неназначенные мониторы** в поле группы мониторов.
2. На вкладке **Схема** выберите соответствующую схему.
3. Перетащите любую доступную камеру из вкладки **Камеры** в область мониторов слева.
   Логический номер камеры отображается черным цветом в области мониторов, а цвет этой области меняется.
4. Измените логические номера областей изображений соответствующим образом. Если ввести номер, который уже используется, появляется соответствующее сообщение.
5. На вкладке **Параметры** можно выбрать, будут ли отображаться имя и номер камеры в области мониторов. Вы также можете выбрать расположение этой информации.

Изображение монитора
Номер, выделенный полужирным шрифтом черного цвета, если он присутствует, обозначает логический номер первоначальной камеры. Номер светло-черного цвета является логическим номером монитора.
Чтобы отменить назначение камеры, щелкните правой кнопкой мыши в области мониторов и выберите **Очистить область** или перетащите камеру за пределы области изображений.

См.
– *Добавление группы мониторов вручную, Страница 151*

14.10 Страница Устройства связи

Главное окно > **Устройства** > разверните  > 
Позволяет добавлять и настраивать устройства связи.
Можно настроить следующее устройство связи:
– Электронная почта

См.
– *Настройка устройства связи, Страница 154*

14.10.1 Добавление сервера электронной почты/SMTP

Чтобы добавить устройство связи:

1. Разверните  , щелкните правой кнопкой мыши  и нажмите **Добавить устройство E-mail/SMTP**.
   Откроется диалоговое окно **Добавить устройство E-mail/SMTP**.
2. Введите соответствующие параметры.
3. Нажмите **ОК**.
   Устройство связи будет добавлено в систему.

Диалоговое окно Добавить устройство E-mail/SMTP

Имя:
Введите отображаемое имя сервера электронной почты.

14.10.2 Страница Сервер SMTP

Главное окно > **Устройства** > разверните  > разверните  > 
Позволяет настроить параметры электронной почты вашей системы. На странице **События** можно назначить событие электронному сообщению. Когда это событие происходит, система отправляет электронное сообщение. Вы можете получать электронную почту в BVMS.

Имя сервера SMTP
Введите имя сервера электронной почты. Информацию об этом вы можете получить у своего провайдера. Обычно это IP-адрес или DNS-имя вашего почтового сервера.

Адрес отправителя
Введите адрес электронной почты, который используется системой в качестве адреса отправителя сообщений электронной почты, например в случае тревоги.

SSL/TLS
Установите флажок, чтобы включить использование защищенного соединения SSL/TLS. В этом случае автоматически выбирается сетевой порт 587.

Порт
Введите номер сетевого порта для исходящей почты. Информацию об этом вы можете получить у своего провайдера.
Если параметр **SSL/TLS** отключен, автоматически выбирается порт 25.
При необходимости можно выбрать другой порт.

Время ожидания при соединении (сек)
Введите количество секунд бездействия, после которых подключение будет прервано.

Проверка подлинности
Установите флажок напротив нужного способа аутентификации. Информацию об этом вы можете получить у своего провайдера.

Имя пользователя
Введите имя пользователя для аутентификации на сервере электронной почты. Информацию об этом вы можете получить у своего провайдера.

Пароль:
Введите пароль для аутентификации на сервере электронной почты. Информацию об этом вы можете получить у своего провайдера.

Отправить тестовое электронное сообщение
Нажмите для отображения диалогового окна **Отправить тестовое электронное сообщение**.

См.
– *Настройка устройства связи, Страница 154*

14.10.3 Настройка устройства связи

Главное окно > **Устройства** > разверните  > разверните 
Чтобы настроить устройство связи:

1. Нажмите  .
2. Установите необходимые параметры.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.
– *Добавление сервера электронной почты/SMTP, Страница 153*
– *Страница Сервер SMTP, Страница 153*

14.10.4 Диалоговое окно Отправить тестовое электронное сообщение

Главное окно > **Устройства** > разверните  > разверните  >  > кнопка
Отправить тестовое электронное сообщение
Позволяет отправить тестовое электронное сообщение.

От:
Введите адрес электронной почты отправителя.

Кому
Введите адрес электронной почты получателя.

Тема
Введите тему электронного сообщения.

Сообщение
Введите текст сообщения.

Отправить тестовое электронное сообщение
Нажмите для отправки сообщения.

См.
– *Настройка устройства связи, Страница 154*

14.11 Страница ATM/POS

Главное окно > **Устройства** > Развернуть  > 
Позволяет добавлять и настраивать периферийные устройства, например ATM/POS Bridge Bosch.
Чтобы добавить несколько мостов к одному серверу необходимо использовать разные порты.

См.

– *Добавление моста Bosch ATM/POS, Страница 100*
– *Настройка периферийных устройств, Страница 156*

14.11.1 Добавление моста Bosch ATM/POS вручную

Главное окно > **Устройства** > Развернуть > Щелкнуть правой кнопкой мыши > **Добавить мост ATM/POS Bosch**.

Позволяет добавить устройство ATM Bosch.

Чтобы добавить периферийное устройство:

1. Разверните , щелкните правой кнопкой мыши и нажмите **Добавить мост ATM/POS Bosch**.
   Отобразится диалоговое окно **Добавить мост ATM/POS Bosch**.
2. Введите соответствующие параметры.
3. Нажмите кнопку **ОК**.
   Периферийное устройство будет добавлено в систему.

Диалоговое окно Добавить мост ATM/POS Bosch

Имя:
Введите соответствующее имя устройства.

IP-адрес:
Введите IP-адрес устройства.

Порт 1:
Введите номер порта, используемый как слушающий порт ATM/POS Bridge.

Порт 2:
Введите номер порта, используемый как слушающий порт BVMS Management Server.

Замечание!
При добавлении нескольких мостов ATM/POS Bridges в систему убедитесь, что номера порта 2 на каждом из устройств отличаются. Использование одного номера для порта 2 несколько раз может привести к потере данных ATM/POS.

См.

– *Добавление моста Bosch ATM/POS, Страница 100*

14.11.2 Страница Мост ATM/POS Bosch

Главное окно > **Устройства** > Развернуть > Развернуть > > вкладка **Мост ATM/POS Bosch**

Позволяет настроить устройство ATM/POS Bridge Bosch.

IP-адрес:
Введите IP-адрес устройства.

Порт 1:
Введите номер порта, используемый как слушающий порт ATM/POS Bridge.

Порт 2:
Введите номер порта, используемый как слушающий порт BVMS Management Server.

Замечание!
При добавлении нескольких мостов ATM/POS Bridges в систему убедитесь, что номера порта 2 на каждом из устройств отличаются. Использование одного номера для порта 2 несколько раз может привести к потере данных ATM/POS.

См.
- *Настройка периферийных устройств, Страница 156*
- *Добавление моста Bosch ATM/POS, Страница 100*

14.11.3 Настройка периферийных устройств

Главное окно > **Устройства** > разверните > разверните > **Мост ATM/POS Bosch**
или
Главное окно > **Устройства** > разверните > разверните > **Устройство DTP** >

Чтобы настроить периферийное устройство:
- Измените требуемые параметры.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

См.
- *Страница Настройки ATM, Страница 156*
- *Страница Мост ATM/POS Bosch, Страница 155*
- *Страница "Настройки DTP", Страница 156*

14.11.4 Страница "Настройки DTP"

Главное окно > **Устройства** > разверните > разверните >
Позволяет настраивать устройство DTP с не более чем 4 устройствами ATM, подключенными к этому устройству DTP.

Последовательный порт
Выберите соответствующий порт из списка.

См.
- *Страница Настройки ATM, Страница 156*
- *Настройка периферийных устройств, Страница 156*

14.11.5 Страница Настройки ATM

Главное окно > **Устройства** > разверните > разверните > >

Позволяет настраивать устройство ATM, подключенное к DTP.

Номер входа устройства DTP
Выберите требуемый номер ввода. Если этот номер уже используется другим устройством ATM, можно поменять номера вводов.

Время ожидания подключения [часы]
Введите необходимое количество часов. Если в течение этого периода устройство ATM не отправило никаких транзакционных данных, система BVMS считает, что соединение разорвано. Запускается соответствующее событие. Событие **Не авторизовано** доступно для устройства ATM, но не имеет к нему отношения.
Ввод значения **0** означает, что проверка соединения не выполняется.

Входы данных
Нажмите, чтобы включить необходимые вводы и введите требуемое имя для вводов.

См.
– *Настройка периферийных устройств, Страница 156*

14.11.6 Страница Входы

Главное окно > **Устройства** > Развернуть > Развернуть > > вкладка **Входы**
Позволяет настраивать вводы моста ATM/POS Bridge Bosch.

См.
– *Настройка периферийных устройств, Страница 156*
– *Добавление моста Bosch ATM/POS, Страница 100*

14.12 Устройства чтения кредитных карточек

Главное окно > **Устройства** > Разверните > > Вкладка **Глобальные настройки для устройств чтения кредитных карточек**
Можно настроить параметры, которые будут действительны для всех устройств чтения кредитных карточек в системе.

Последовательный порт
Выберите последовательный порт, к которому подключено устройство чтения кредитных карточек.

Заблокировано
Позволяет добавлять коды банковской маршрутизации для блокировки. Это означает, что карточки с введенными здесь характеристиками не обладают авторизацией для доступа. Доступ блокируется устройством чтения кредитных карточек. Необходимо установить следующий режим по умолчанию отпирания электрического замка двери для устройства чтения кредитных карточек: **Автоматически**
Этот список может содержать элементы с подстановочными символами.
?: означает любой символ или отсутствие символа в этой позиции.
*: означает последовательность (один или несколько символов) любых символов или их отсутствие (исключение: отдельный символ * означает, что все коды банковской сортировки блокируются).

Игнорировать код страны на картах ЕС
Нажмите, чтобы включить режим, в котором система BVMS не анализирует используемые данные карточки для определения страны, в которой карта была выпущена. Доступ возможен для карточек с другим кодом страны.

14.12.1 Диалоговое окно "Добавление устройства чтения кредитных карточек"

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > команда **Добавить устройство чтения кредитных карточек**
Можно добавить устройство чтения кредитных карточек.

Имя
Введите имя для устройства.

Идентификатор устройства
Выберите уникальный номер для устройства. Если доступных номеров нет, в систему уже добавлено максимальное количество устройств чтения кредитных карточек.

14.12.2 Страница "Параметры устройства чтения кредитных карточек"

Главное окно > **Устройства** > разверните  >  >  > вкладка **Настройки для устройства чтения кредитных карт**
Можно настроить устройство чтения кредитных карточек.

Идентификатор устройства
Отображает уникальный номер устройства.

Включить защиту от скимминга
Нажмите, чтобы включить режим, в котором система BVMS запускает событие, когда подключенный скиммер обнаруживает скимминг. Этот режим поддерживается не всеми типами устройств чтения кредитных карточек.

Режим открывания электрического замка двери по умолчанию
Открыть: дверь открыта и любой человек может получить доступ без карты.
Закрыто: дверь закрыта независимо от того, какая карта вставляется.
Автоматически: дверь открывается, только когда в считыватель вставляется карта с авторизацией для доступа.

Включить управление на основе расписания
Нажмите, чтобы включить режим, в котором можно назначать расписание для выбранного режима отпирания замка двери.
Когда расписание становится активным, BVMS переключает устройство чтения кредитных карточек в соответствующий режим отпирания.
Если выбранные расписания накладываются друг на друга, действительный режим отпирания двери определяется по следующему приоритету режимов: 1. **Открыть** 2. **Закрыто** 3. **Автоматически**

14.13 Страница Виртуальные входы

Главное окно > **Устройства** > Развернуть  > 
Отображает виртуальные входы, сконфигурированные в вашей системе.
Позволяет добавить новые виртуальные входы и удалить существующие.

Добавить входы
Нажмите для отображения диалогового окна добавления новых виртуальных входов.

Удалить входы
Нажмите для удаления выбранного виртуального входа.

Номер
Отображает номер виртуального входа.

Имя
нажмите ячейку, чтобы изменить имя виртуального входа.

14.13.1 Добавление виртуальных входов вручную

Главное окно > **Устройства** > разверните  > кнопка **Добавить входы**
Позволяет добавить новые виртуальные входы.

Для добавления виртуального входа выполните следующие действия.

1. Разверните  и щелкните  .
   Откроется соответствующая страница.
2. Нажмите **Добавить входы**.
   В таблицу будет добавлена новая строка.
3. Настройте необходимые параметры.
4. Нажмите **Добавить**.
   Виртуальный вход будет подключен к системе.

Диалоговое окно Добавить входы

Начало:
Выберите первый номер новых виртуальных входов.

Конец:
Выберите последний номер новых виртуальных входов.

Имя:
Введите имя каждого нового виртуального входа. Добавляется последовательный номер.

Добавить
Нажмите для добавления новых виртуальных вводов.

14.14 Страница SNMP

Главное окно > **Устройства** > разверните  > 
Позволяет добавить и настроить измерения SNMP для поддержания качества сети.

См.
– *Настройка приемника запросов SNMP (страница приемника запросов SNMP), Страница 160*

14.14.1 Добавление SNMP вручную

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > команда **Добавить SNMP**
Позволяет добавить систему сетевого мониторинга к системе BVMS.

Для добавления устройства мониторинга сети выполните следующие действия.

1. Разверните  , щелкните правой кнопкой мыши  и нажмите **Добавить SNMP**.
   Откроется диалоговое окно **Добавить SNMP**.
2. Введите имя устройства SNMP.
   Устройство мониторинга сети будет подключено к системе.

Диалоговое окно Добавить SNMP

Имя:
Введите имя устройства мониторинга сети.

См.
– *Настройка приемника запросов SNMP (страница приемника запросов SNMP), Страница 160*

14.14.2 Настройка приемника запросов SNMP (страница приемника запросов SNMP)

Главное окно > **Устройства**> разверните 

Чтобы настроить SNMP trap receiver, выполните следующие действия.

1. Нажмите  для отображения страницы **Приемник запросов SNMP**.
2. Установите требуемые параметры.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

Страница Приемник запросов SNMP.

Главное окно > **Устройства** > разверните  > разверните 
Позволяет выбрать устройства для мониторинга и выбрать OID trap SNMP, которые запускают событие для выбранного устройства при получении.

Замечание!
Следует ввести IP-адрес Bosch Video Management System Management Server в качестве trap-приемника мониторимых устройств.

Устройства отправки запросов SNMP:
Позволяет ввести диапазон IP-адресов отслеживаемых сетевых устройств. Для мониторинга отдельного устройства введите соответствующий IP-адрес в ячейке **Диапазон от**.
Будьте внимательны при изменении этих адресов. При вводе неверного адреса мониторинг устройства прекращается.

Правила фильтров запросов SNMP:
Позволяют ввести идентификаторы объектов и соответствующие значения. Для расширения диапазона фильтра можно использовать такие подстановочные знаки, как «*» и «?». При вводе идентификаторов объектов и значений в нескольких строках эти правила фильтра должны соблюдаться одновременно, чтобы событие было

активировано. В каждом из столбцов можно ввести регулярное выражение в фигурных скобках {}. Если эти символы находятся вне скобок, выражение не считается регулярным.

Показать средство регистрации запросов
Нажмите, чтобы отобразить диалоговое окно **Журнал регистрации запросов SNMP** для отслеживания идентификаторов запросов SNMP.

14.14.3 Диалоговое окно Журнал регистрации запросов SNMP

Главное окно > **Устройства** > разверните  > разверните  > выберите универсальный приемник ловушек SNMP > нажмите **Показать средство регистрации запросов**
Позволяет отслеживать OIDловушкиSNMP. Можно получать ловушки от всех устройств в сети или только от выбранных. Можно фильтровать получаемые запросы и добавлять идентификаторы объектов и значения выбранных запросов в таблицу **Правила фильтров запросов SNMP:**.

Старт/Пауза
Нажмите для запуска или остановки процесса отслеживания.

Только запросы отправителя
Введите IP-адрес или DNS-имя устройства. Отслеживаются только запросы данного устройства.

Только запросы, содержащие
Введите строку, которую должен содержать запрос. Пользуйтесь подстановочными символами * и ?. Строки в фигурных скобках {} рассматриваются как регулярные выражения. Отслеживаются только запросы, содержащие данную строку.

Полученные запросы
Отображаются запросы, полученные в процессе отслеживания.

Нажмите, чтобы удалить все записи в поле **Полученные запросы**.

Подробные сведения о запросе
Отображаются подробные сведения о запросе. Можно скопировать идентификатор объекта и значение в таблицу **Правила фильтров запросов SNMP:**.

См.
– *Настройка приемника запросов SNMP (страница приемника запросов SNMP), Страница 160*

14.15 Страница "Назначить клавиатуру"

Главное окно > **Устройства** > Разверните  > 
Позволяет добавить клавиатуруKBD-Universal XF (подключенную к рабочей станции BVMS) или клавиатуру Bosch IntuiKey (подключенную к рабочей станции BVMS или декодеру).

Для добавления клавиатуры CCTV выполните следующие действия.
Примечание. Для добавления клавиатуры необходимо сначала добавить рабочую станцию.

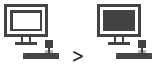
1. Разверните  и щелкните  .
   Откроется соответствующая страница.
2. Нажмите **Добавить клавиатуру**.
   В таблицу будет добавлена новая строка.
3. В соответствующем поле столбца **Тип клавиатуры** выберите нужный тип клавиатуры:
   Клавиатура IntuiKey
   KBD-Universal XF Keyboard
4. В соответствующем поле столбца **Соединение** выберите рабочую станцию, к которой подключена клавиатура.
5. Настройте необходимые параметры.
   Клавиатура будет добавлена в систему.

Добавить клавиатуру
Нажмите, чтобы добавить в таблицу строку для настройки клавиатуры.

Удалить клавиатуру
Нажмите, чтобы удалить выделенную строку.

Тип клавиатуры
Отображает тип клавиатуры, подключенной к рабочей станции или декодеру.
Нажмите ячейку, чтобы выбрать необходимый тип клавиатуры.

– **IntuiKey**
  Выберите этот тип, если вы подключили клавиатуру IntuiKey производства Bosch.
– **KBD-Universal XF Keyboard**
  Выберите этот тип, если вы подключили клавиатуру KBD-Universal XF.

Соединение
Выберите в ячейке тип устройства, к которому подключена клавиатура. При выборе рабочей станции клавиатура также добавляется на страницу  .

Порт
Выберите в ячейке соответствующий COM-порт.

Скорость (бит/с)
Выберите в ячейке максимальную скорость передачи (в битах в секунду), с которой данные должны передаваться через этот порт. Обычно это значение соответствует максимальной скорости, поддерживаемой компьютером или устройством, с которым осуществляется связь.

Информационные биты
Отображает количество информационных битов, используемых для каждого передаваемого и принимаемого символа.

Стоповые биты
Отображает время между каждым передаваемым символом (если время измеряется в битах).

Четность
Отображает тип контроля четности, используемый для данного порта.

Тип порта
Отображает тип соединения, которое используется для подключения клавиатуры Bosch IntuiKey к рабочей станции.

См.

- *Настройка декодера для использования с клавиатурой Bosch IntuiKey, Страница 150*
- *Настройка клавиатуры Bosch IntuiKey (страница «Настройки») (рабочая станция), Страница 142*
- *Настройка клавиатуры Bosch IntuiKey (декодер), Страница 150*

14.16 Страница Модули ввода/вывода

Главное окно > **Устройства** > разверните >

Позволяет добавить и настроить модули ввода/вывода.

В настоящее время поддерживаются только устройства ADAM.

См.

- *Настройка модуля ввода/вывода, Страница 163*

14.16.1 Добавление модуля ввода/вывода вручную

Чтобы добавить модуль ввода/вывода:

1. Разверните , щелкните правой кнопкой мыши и нажмите **Добавить новое устройство ADAM**.
   Отображается диалоговое окно **Добавить ADAM**.
2. Введите IP-адрес устройства.
3. Выберите тип устройства.
   Отобразится соответствующая страница.
4. Если нужно, перейдите на вкладку **ADAM**, чтобы изменить краткие имена входов.
5. Если нужно, перейдите на вкладку **Имя**, чтобы изменить краткие имена реле.

Замечание!

Вы также можете выполнить поиск устройств ADAM (**Выполнить поиск устройств ADAM**). Будут определены IP-адреса устройств. При доступности тип устройства выбран заранее. Вы должны подтвердить этот выбор.

14.16.2 Настройка модуля ввода/вывода

Главное окно > **Устройства**> Разверните > Разверните >

Чтобы настроить модуль ввода/вывода:

Замечание!

Избегайте изменения типа устройства.

При уменьшении количества входов или реле удаляются все данные конфигурации удаленных входов или реле.

1. Перейдите на вкладку **ADAM**.
2. Выберите соответствующий тип устройства из списка **Тип ADAM:**.
3. Перейдите на вкладку **Входы**.
4. В столбце **Имя** при необходимости измените краткое имя входа.
5. Перейдите на вкладку **Реле**.
6. При необходимости измените имя реле в столбце **Реле**.

Изменение IP-адреса:

1. В дереве устройств щелкните правой кнопкой мыши устройство ADAM.

2. Выберите **Изменить сетевой адрес**.
3. Введите новый IP-адрес и нажмите **OK**.
4. Активируйте конфигурацию.

⇨ Новый IP-адрес используется для доступа к устройству.

См.

– *Страница Модули ввода/вывода, Страница 163*

14.16.3 Страница ADAM

Главное окно > **Устройства** > Разверните > > > Вкладка **ADAM**

Отображается информация о выбранном устройстве ADAM.

Позволяет изменить краткое имя устройства ADAM.

Тип ADAM:

Выберите соответствующий тип устройства.

Входов всего:

Отображает общее количество входов, доступных для этого типа устройства.

Реле/выходов всего:

Отображает общее количество реле, доступных для этого типа устройства.

14.16.4 Страница Входы

Главное окно > **Устройства** > Разверните > > > Вкладка **Входы**

Позволяет изменять краткие имена входов выбранного устройства ADAM.

Номер

Отображает логический номер входа.

Имя

Щелкните ячейку, чтобы изменить краткое имя входа.

14.16.5 Страница Реле

Главное окно > **Устройства** > Разверните > > > Вкладка **Реле**

Позволяет изменять краткие имена реле выбранного устройства ADAM.

Номер

Щелкните ячейку, чтобы изменить логический номер реле.

Имя

Введите краткое имя реле.

14.17 Страница Эмуляция Allegiant CCL

Главное окно > **Устройства** > Разверните > CCL

Позволяет активировать эмуляцию Allegiant CCL.

Команды Allegiant CCL, поддерживаемые в системе BVMS, Страница 63 содержит команды CCL, поддерживаемые в Bosch Video Management System.

Примечание.
Не настраивайте эмуляцию Allegiant CCL и устройство Allegiant на один и тот же COM-порт. Если для обоих устройств настроить один и тот же COM-порт, будет работать устройство Allegiant. В доступе устройству эмуляции Allegiant CCL отказывается с выводом соответствующего сообщения.
Для решения данной проблемы Management Server необходимо оснастить двумя разными COM-портами или подключить устройство Allegiant к другому компьютеру.

Включить эмуляцию Allegiant CCL
Установите флажок, чтобы включить эмуляцию

Скорость в бодах
Введите значение скорости передачи в бит/сек.

Стоповые биты
Выберите количество стоповых битов на символ.

Контроль четности
Выберите тип контроля четности.

Подтверждение связи
Выберите необходимый метод для управления потоком.

Модель
Выберите модель Allegiant, которую необходимо эмулировать.

См.
– *Настройка эмуляции Allegiant CCL, Страница 165*

14.17.1 Добавление эмуляции Allegiant CCL вручную

Для добавления эмуляции Allegiant CCL выполните следующие действия.

1. Разверните  , нажмите  .
   Откроется вкладка **Эмуляция Allegiant CCL**.
2. Установите флажок **Включить эмуляцию Allegiant CCL**.
3. Настройте необходимые параметры.
   Сервис эмуляции Allegiant CCL будет запущен на устройстве Management Server.

14.17.2 Команды Allegiant CCL

Можно использовать команды CCL для переключения IP-камер или кодеров на IP-декодеры, если оба типа устройств настроены в BVMS. Команды CCL невозможно использовать для прямого управления аналоговыми камерами или самой матрицей Allegiant.
Эмуляция Allegiant CCL запускается как внутренняя служба BVMS, которая транслирует команды CCL матричного коммутатора в BVMS. Следует настроить COM-порт Management Server для прослушивания этих команд CCL. Эмуляция CCL способствует обмену между существующими устройствами Allegiant и Bosch Video Management System или использованию Bosch Video Management System с приложениями, поддерживающими команды Allegiant CCL. Управление старым оборудованием Allegiant, настроенным в BVMS, с помощью этих команд невозможно.

14.17.3 Настройка эмуляции Allegiant CCL

эмуляции CCL > **Устройства**> Развернуть  > 

Чтобы использовать команды CCL, вам потребуется руководство пользователя CCL. Данное руководство доступно в онлайн-каталоге продукции в разделе документации для каждого матричного коммутатора Allegiant LTC.
В разделе *Команды Allegiant CCL, поддерживаемые в системе BVMS, Страница 63* перечислены команды CCL, которые поддерживаются в системе Bosch Video Management System.

Чтобы настроить эмуляцию CCL Allegiant:

1. Нажмите **Включить эмуляцию Allegiant CCL**.
2. Установите параметры связи в соответствии с потребностями.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.

– *Страница Эмуляция Allegiant CCL, Страница 164*

14.18 Страница Мобильный видеосервис

Главное окно > **Устройства** > 

Позволяет добавить в BVMS одну или несколько записей служб транскодирования. Эта служба транскодирования приспосабливает видеопоток с камеры, настроенной в BVMS, к доступной пропускной способности сети. Благодаря этому мобильные видеоклиенты, такие как iPhone, iPad или веб-клиент, могут получать видеоданные в режиме реального времени или воспроизведения через ненадежные сетевые соединения с ограниченной пропускной способностью.

См.

– *Добавление Mobile Video Service вручную, Страница 167*

14.18.1 Mobile Video Service

Mobile Video Service транскодирует видеопотоки от источника в соответствии с полосой пропускания, доступной подключенным клиентам. Интерфейсы Mobile Video Service предназначены поддерживать клиенты на нескольких платформах, например мобильные устройства (IOS: iPad, iPhone) и HTML-клиент Windows Internet Explorer.
Mobile Video Service основан на Microsoft Internet Information Service.
Одна мобильная служба может синхронно обслуживать несколько клиентов.
В отношении ограничений см. лист данных и Технические заметки Mobile Video Service, доступные в интернет-каталоге изделий для BVMS.

Служба Internet Information Service

Настройте параметры службы Internet Information Service на компьютере, на котором планируете установить MVS для BVMS.

Замечания по установке

Нельзя добавлять Mobile Video Service (MVS) в Configuration Client, если время между компьютером Configuration Client и компьютером Mobile Video Service не синхронизировано. Убедитесь в том, что время между задействованными компьютерами синхронизировано.
Перед установкой службы Mobile Video Service установите и задайте конфигурацию службы Internet Information Service (IIS). Если служба IIS не установлена, установка Mobile Video Service на BVMS будет прервана.

Во время установки BVMS выберите компонент Mobile Video Service для выполнения его установки.
Нельзя установить VRM и Mobile Video Service на одном компьютере.
Не рекомендуется устанавливать Mobile Video Service на компьютер, на который установлен Management Server.
С помощью мобильного приложения можно выполнять следующие действия:
- Отображение видео
  - Живой просмотр
  - Воспроизведение
- Контроль состояния сети и сервера

См.
- *Добавление Mobile Video Service вручную, Страница 167*

14.18.2 Добавление Mobile Video Service вручную

Главное окно > **Устройства** > > щелкните правой кнопкой мыши  > нажмите **Добавить Mobile Video Service**
Вы можете добавить одну или несколько записей Mobile Video Service в систему BVMS.
Для добавления выполните следующие действия.
1. Введите URI системы Mobile Video Service.
2. Нажмите **OK**.

⇨ Теперь Mobile Video Service и Management Server знают друг о друге, а Mobile Video Service может принимать данные конфигурации от Management Server.

Диалоговое окно Добавить Mobile Video Service

URI
Введите URI своего Mobile Video Service. Следуйте синтаксическим правилам, приведенным в примере:

https://www.MyDomain.org/mvs
Такая запись всегда должна начинаться с https://, даже если не настроен шифрованный доступ к вашему веб-серверу.

14.19 Страница "Охранные панели"

Главное окно > **Устройства** > Разверните  > 
Позволяет добавлять и настраивать охранные панели производства Bosch. Устройство должно быть подключено и доступно.
После добавления охранной панели в дереве устройств в иерархическом порядке отображаются области, точки, двери и реле.
Можно удалить или переименовать панель, любые область, точку, дверь и реле.
После изменения конфигурации охранной панели необходимо повторить сканирование устройства, чтобы отобразить изменения в BVMS.

Замечание!
Все тревожные события, которые могут возникать в точке, автоматически конфигурируются как тревога BVMS.
Пример: пожарная тревога

Замечание!
Если дверь не назначена точке в конфигурации охранной панели, добавленной к BVMS, тревога с этой двери не вызывает событие BVMS, а следовательно, событие BVMS не возникает.

14.19.1 Добавление тревожной панели вручную

Главное окно > **Устройства** > разверните > щелкните правой кнопкой мыши > команда **Добавить панель**
Позволяет добавить тревожную панель производства Bosch.

Для добавления тревожной панели выполните следующие действия.

1. Разверните , щелкните правой кнопкой мыши и нажмите **Добавить панель**.
   Откроется диалоговое окно **Добавление тревожной панели**.
2. Введите соответствующее значения.
3. Нажмите **ОК**.
   В систему будет добавлена тревожная панель.

Диалоговое окно Добавление тревожной панели

Сетевой адрес
Введите IP-адрес устройства.

Сетевой порт
Выберите номер порта, настроенный на устройстве.

Код доступа автоматизации
Введите пароль для проверки подлинности на устройстве.

14.19.2 Страница "Настройки"

Главное окно > **Устройства** > разверните > разверните > > вкладка **Настройки**
Позволяет изменять настройки подключения тревожной панели.

14.20 Страница «Системы контроля и управления доступом»

Главное окно > **Устройства** > разверните >
Позволяет добавлять и настраивать системы контроля и управления доступом от Bosch. Устройство должно быть подключено и доступно. После добавления системы контроля и управления доступом контроллер, входы, считывающие устройства и двери отображаются в дереве устройств иерархически.
Контроллер, входы, считывающие устройства и двери можно удалить или переименовать на странице **Карты и структура**.
После изменения конфигурации или иерархии контроллеров, считывателй или дверей в системе контроля и управления доступом необходимо повторно сканировать устройство, чтобы применить изменения в BVMS.

Сертификат HTTPS для Client
Для обеспечения безопасности соединения между системой контроля и управления доступом и BVMS необходимо экспортировать сертификат клиента из системы контроля и управления доступом и импортировать его в BVMS. Этот процесс описан в разделе **Сертификат HTTPS для Client** документации по системе контроля и управления доступом.

Замечание!
Если сертификат не добавлен, системы не смогут обмениваться данными.

14.20.1 Добавление системы контроля и управления доступом

Главное окно > **Устройства** > разверните  > 

Для добавления системы контроля и управления доступом выполните следующие действия.

1. Щелкните правой кнопкой мыши  .
2. Нажмите **Добавить систему контроля доступа**.
   Откроется диалоговое окно **Добавить систему контроля доступа**.

Примечание. При добавлении системы контроля и управления доступом настроенные двери, считыватели, входы и реле отображаются в дереве устройств на странице **Карты и структура**.

Диалоговое окно Добавить систему контроля доступа

Имя хоста / порт HTTPS
Введите имя хоста устройства. При необходимости измените номер порта.

Имя пользователя
Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль
Введите действующий пароль для аутентификации на устройстве.

Для проверки подключения выполните следующие действия.

1. Нажмите кнопку «Подключиться».
   Система BVMS Configuration Client попытается подключиться к системе контроля и управления доступом и получить необходимую информацию.
2. Нажмите «ОК».
   Система контроля и управления доступом будет добавлена в систему на основе показанной информации.

14.20.2 Изменение системы контроля и управления доступом

Главное окно > **Устройства** > разверните  >  > 

Для изменение системы контроля и управления доступом выполните следующие действия.

1. Щелкните правой кнопкой мыши  .

2. Нажмите **Изменить систему контроля доступа**.
   Откроется диалоговое окно **Изменить систему контроля доступа**.

14.20.3 Страница «Настройки»

Главное окно > **Устройства** > разверните > > > вкладка **Параметры**
Позволяет изменить настройки подключения системы контроля и управления доступом.

14.21 Страница Video Analytics

Главное окно > > **Устройства** > Разверните >
Позволяет добавлять устройства Video Analytics, Person Identification (PID) и LPR.

14.21.1 Страница параметров видеоаналитики

Главное окно > > **Устройства** > разверните > разверните > **Video Analytics** > страница **Параметры Video Analytics**
Можно добавить устройство видеоаналитики на стороне сервера.
Должны быть доступны учетные данные и путь установки приложения для просмотра аналитики, используемого для устройства видеоаналитики.

Сетевой адрес
Введите IP-адрес устройства видеоаналитики. Имена DNS запрещены.

Имя пользователя
Введите имя пользователя в соответствии с настройками в устройстве видеоаналитики.

Пароль
Введите пароль, настроенный на устройстве для анализа на стороне сервера.

Путь к приложению для просмотра аналитики
Введите относительный путь установки приложения для просмотра аналитики.
Указывается путь относительно `C:\Program Files (x86)\` на компьютере, на котором используется приложение для просмотра.
Пример. Приложение для просмотра аналитики (`AnalyticsViewer.exe`) установлено в следующем каталоге:

```
C:\Program Files (x86)\VideoAnalytics\
```

Укажите следующий путь в поле **Путь к приложению для просмотра аналитики**:

```
VideoAnalytics\AnalyticsViewer.exe
```

14.21.2 Добавление устройства Video Analytics

Главное окно > **Устройства** > щелкните правой кнопкой мыши > команда **Добавить устройство Video Analytics** > диалоговое окно **Добавить устройство Video Analytics**
При добавлении устройства для анализа на стороне сервера необходимо указать учетные данные для нового устройства.

Добавление устройства серверной аналитики

1. Разверните  , щелкните правой кнопкой мыши  и выберите пункт **Добавить устройство Video Analytics**.
   Отображается диалоговое окно **Добавить устройство Video Analytics**.
2. Введите соответствующее значения.
3. Нажмите кнопку **OK**.
   Устройство добавлено в систему.

Диалоговое окно Добавить устройство Video Analytics

Сетевой адрес
Введите IP-адрес устройства видеоаналитики. Имена DNS запрещены.

Имя пользователя
Введите имя пользователя в соответствии с настройками в устройстве видеоаналитики.

Пароль
Введите пароль, настроенный на устройстве для анализа на стороне сервера.

14.21.3 Страница устройств Person Identification

Главное окно > > **Устройства** > развернуть  > развернуть  >  страница устройств Person Identification
Позволяет добавить устройство Person Identification. Устройство должно быть подключено и доступно. Вы можете добавить камеры к устройству Person Identification и настроить события и тревоги Person Identification.

Группы лиц
На вкладке **Группы лиц** можно добавлять и настраивать группы людей.

Камеры
На вкладке **Камеры** можно добавить камеры к устройству Person Identification. Добавленные камеры отображаются в списке.
Примечание. Сначала добавьте соответствующие камеры в логическое дерево.

14.21.4 Добавление Person Identification Device (PID)

Замечание!
В случае сбоя центрального сервера необходимо восстановить конфигурацию BVMS и сертификат Bosch VMS CA. В противном случае вы не сможете использовать существующее устройство PID без перезапуска, что приведет к удалению всех сохраненных лиц.
Рекомендуется создать резервную копию конфигурации BVMS и сертификата Bosch VMS CA.

При добавлении устройства Person Identification убедитесь, что сертификат, отображаемый в диалоговом окне **Добавить устройство Person Identification Device,** соответствует добавляемому PID.
Начиная с BVMS 10.1, можно добавлять несколько устройств PID.
Первое добавленное устройство PID становится ведущим устройством, которое подключается к системе BVMS. Это первое устройство PID устанавливает соединение с другими устройствами PID, и в этом устройстве хранится база данных людей.

Примечание. Прежде чем удалять первое добавленное устройство PID, необходимо удалить все остальные настроенные устройства PID.

Чтобы добавить устройство Person Identification:

1. Разверните .
2. Щелкните правой кнопкой мыши .
3. Нажмите **Добавить устройство Person Identification Device**.
   Отображается диалоговое окно **Добавить устройство Person Identification Device**.
4. Введите соответствующее значения.
5. Нажмите **Посмотреть сертификат...,** чтобы проверить, соответствует ли сертификат PID.
6. Чтобы подтвердить выбор, нажмите кнопку **OK**.
7. Нажмите **OK**.
   Устройство будет добавлено в систему.

Диалоговое окно Добавить устройство Person Identification Device

Сетевой адрес
Введите IP-адрес устройства.

Номер порта
Введите номер порта устройства.

См.
- *Восстановление доступа к PID после сбоя центрального сервера BVMS, Страница 172*
- *Чтобы экспортировать параметры конфигурации:, Страница 97*

14.21.5 Страница PID

Главное окно > **Устройства** > Развернуть > Развернуть > Person Identification страница устройств > PID

Подключение
На вкладке **Подключение** отображаются сетевой адрес и номер порта Person Identification Device. Параметры подключения Person Identification Device доступны только для чтения.

14.21.6 Восстановление доступа к PID после сбоя центрального сервера BVMS

Замечание!
В случае сбоя центрального сервера необходимо восстановить конфигурацию BVMS и сертификат Bosch VMS CA. В противном случае вы не сможете использовать существующее устройство PID без перезапуска, что приведет к удалению всех сохраненных лиц.
Рекомендуется создать резервную копию конфигурации BVMS и сертификата Bosch VMS CA.

Дополнительные сведения о сохранении конфигурации BVMS см. в разделе *Чтобы экспортировать параметры конфигурации:, Страница 80*. Управление сертификатами осуществляется вне BVMS в приложении для Windows **Управление сертификатами компьютеров**.

Замечание!
Сертификаты содержат конфиденциальную информацию. Для их защиты выполните следующие действия.
-Установите надежный пароль.
- Сохраните сертификат в ограниченной зоне, например на сервере, не являющемся общедоступным.
- Убедитесь, что только уполномоченный персонал может получить доступ к сертификату.

Чтобы создать резервную копию сертификата Bosch VMS CA:
1. Откройте приложение для Windows **Управление сертификатами компьютеров**.
2. В папке **Доверенные корневые центры сертификации** выберите сертификат Bosch VMS CA.
3. Экспортируйте сертификат с закрытым ключом, выбрав **Да, экспортировать закрытый ключ**.
4. Используйте формат Personal Information Exchange.
5. Введите надежный пароль.
6. Сохраните сертификат как PFX-файл.

Чтобы восстановить доступ к PID с нового установленного центрального сервера BVMS:
1. Откройте приложение для Windows **Управление сертификатами компьютеров**.
2. Импортируйте PFX-файл, содержащий сертификат Bosch VMS CA, в папку **доверенных корневых центров сертификации** нового центрального сервера. Включить все расширенные свойства.
3. Импортируйте резервную копию конфигурации BVMS.

См.
– *Экспорт параметров конфигурации, Страница 97*

14.21.7 Добавление камер к Person Identification Device (PID)

Вы можете добавить камеры к устройству Person Identification, если они уже добавлены в логическое дерево.

Чтобы добавить камеры к устройству Person Identification:
1. Разверните  .
2. Разверните  .
3. Нажмите  .
4. Перейдите на вкладку **Камеры**.

5. Перетащите нужные камеры из окна **Логическое дерево** в окно **Камеры**.
   Или
   дважды нажмите нужные камеры в окне **Логическое дерево**.
   Камеры добавляются в устройство Person Identification и отображаются в списке **Камеры**.

14.21.8 Настройка параметров камеры для тревог Person Identification

Для каждой доступной камеры можно настроить параметры тревог Person Identification, чтобы сократить количество ложных тревог.

Параметр камеры

Название	Информация о значении	Описание
Вероятность порога (%)	По умолчанию: 55 % Мин.: 0 % Макс.: 100 %	Минимальная вероятность положительной идентификации лица для создания события Person Identification.
Размер лица (%)	По умолчанию: 7,5 % Мин.: 5 % Макс.: 100 %	Минимальный размер обнаруживаемого лица по сравнению с размером всего видеокадра.
Мин. число кадров	По умолчанию: 4 Мин.: 1	Минимальное количество последовательных видеокадров, на которых должно появиться лицо для его обнаружения.
Анализируемые кадры (%)	По умолчанию: 100 % Мин.: 10 % Макс.: 100 %	Процент кадров, анализируемых для идентификации людей. Значение 50 % означает, что анализируется каждый второй кадр.

14.21.9 Настройка групп людей

Главное окно > > **Устройства** > Разверните > 

Чтобы настроить группы людей:

1. Выберите вкладку **Группы лиц**.
2. Нажмите для добавления новой группы лиц.
3. Введите соответствующее значения.
4. Нажмите для удаления группы лиц.

Замечание!
Вы не можете удалить или изменить значения группы по умолчанию.

Таблица групп лиц

Группа лиц	Введите имя группы лиц.
Цвет тревоги	Дважды щелкните для выбора цвета тревоги.
Название тревоги	Введите название тревоги, которое будет отображаться в модуле Operator Client.

Чтобы изменить значения в таблице групп лиц:
1. Дважды щелкните соответствующее поле таблицы.
2. Измените значение.

Приоритет тревожного сигнала
На **Тревожные сигналы** странице можно установить приоритет тревог Person Identification.

Замечание!
Для каждой камеры соответствующей группы лиц можно установить различные приоритеты тревоги.
Вы также можете изменить приоритет тревоги для группы лиц по умолчанию.

См.
– *Страница Тревожные сигналы, Страница 321*

14.21.10 Добавление устройства LPR

Главное окно > > **Устройства** > развернуть > > 

Устройства LPR идентифицируют и распознают номерные знаки. Можно настроить соответствующие события и сигналы тревоги LPR.
Если устройство LPR должно распознавать конкретные номерные знаки, сначала нужно настроить список соответствующих номерных знаков непосредственно в устройстве LPR. Более подробную информацию см. в пользовательской документации к устройству.

Замечание!
Устройство должно быть подключено и доступно.
Система BVMS подключается только в том случае, если на устройстве LPR активирована проверка подлинности, а также указаны имя пользователя и пароль. Имя пользователя и пароль не могут быть пустыми.

Чтобы добавить устройство LPR:

1. Щелкните правой кнопкой мыши  .
2. Нажмите **Добавить устройство LPR**.
   Откроется диалоговое окно **Добавить устройство LPR**.
3. Введите соответствующие значения.
4. Нажмите **Проверить подлинность**.

5. Нажмите **OK**.
   Устройство будет добавлено в систему.

Замечание!
В конфигурации устройства LPR необходимо указать IP-адрес сервера Management Server системы BVMS. В противном случае система BVMS не будет получать события от этого устройства LPR.

Диалоговое окно Добавить устройство LPR

Сетевой адрес
Введите IP-адрес устройства.

Номер порта
Введите номер порта устройства.

Имя пользователя
Введите действительное имя пользователя для проверки подлинности в устройстве.

Пароль
Введите действующий пароль для аутентификации на устройстве.

Проверить подлинность
Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

14.22 Страница Устройства VRM

Главное окно > **Устройства** > Разверните >
Позволяет добавлять и настраивать устройства VRM. Устройству VRM необходимы, по крайней мере, кодер, iSCSI-устройство, LUN, назначенное данному iSCSI-устройству, и пул хранения. Текущие версии микропрограммного обеспечения см. в замечаниях к версии и технических характеристиках.

Замечание!
После того как вы добавили устройство iSCSI с соответствующими кодерами в свою систему BVMS, вы должны добавить IQN каждого кодера к данному устройству iSCSI (действительно для некоторых типов устройств iSCSI).
Подробную информацию см. в разделе *Настройка устройства iSCSI, Страница 201*.

Замечание!
Убедитесь, что время на компьютере VRM синхронизировано с Management Server. В противном случае можно потерять видеозаписи.
Настройте программное обеспечение сервера времени на сервере Management Server. На компьютере VRM настройте IP-адрес сервера Management Server в качестве сервера времени, используя стандартные процедуры Windows.

См.
- *Настройка многоадресной передачи, Страница 243*
- *Синхронизация конфигурации BVMS, Страница 186*
- *Страница Настройки VRM, Страница 180*
- *Страница "Пул", Страница 187*

– *Страница устройства iSCSI, Страница 196*
– *Изменение пароля устройства VRM, Страница 182*

14.22.1 Добавление устройств VRM путем поиска

Главное окно > **Устройства** >

В сети необходима служба VRM, запущенная на компьютере, и устройство iSCSI.

Замечание!
При добавлении устройства iSCSI без настроенных целевых объектов и устройств LUN запустите конфигурацию по умолчанию и добавьте IQN каждого кодера к данному устройству iSCSI.
При добавлении устройства iSCSI с настроенными целевыми объектами и устройствами LUN добавьте IQN каждого кодера к данному устройству iSCSI.
Подробную информацию см. в разделе *Настройка устройства iSCSI, Страница 201*.

Для добавления устройств VRM путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши и выберите команду **Выполнить поиск устройств VRM**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. В списке **Роль** выберите нужную роль.
   Доступная для выбора новая роль зависит от текущего типа устройства VRM.
   Если выбрать **Зеркальный** или **Резервный**, потребуется выполнить дополнительное действие.
4. В списке **Роль** выберите нужную роль.
   Новая роль, которую вы можете выбрать, зависит от текущего типа устройства VRM.
5. Нажмите **Далее >>**
6. В списке **Ведущий VRM** выберите ведущий VRM для выбранного зеркального или резервного VRM.
7. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
8. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.
   В столбце **Состояние** успешные входы в систему обозначены значком .
   Неудачные попытки входа обозначены значком .
9. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Примечание. Все устройства VRM добавляются по умолчанию с безопасным соединением.

Чтобы изменить безопасное/небезопасное соединение:

1. Щелкните правой кнопкой мыши .

2. Нажмите **Изменить устройство VRM**.
   Откроется диалоговое окно **Изменить устройство VRM**.
3. Установите флажок **Безопасное соединение**.
   Используемый порт автоматически меняется на порт HTTPS.
   Или
   снимите флажок **Безопасное соединение**.
   Используемый порт автоматически меняется на порт RCPP.

См.

- *Добавление устройства, Страница 129*
- *Страница Устройства VRM, Страница 176*
- *Настройка устройства iSCSI, Страница 201*
- *Двойная / резервная запись, Страница 30*

14.22.2 Добавление основного или вторичного VRM вручную

Главное окно > **Устройства** > щелкните правой кнопкой мыши  > нажмите **Добавить VRM** > диалоговое окно **Добавить VRM**

Позволяет добавить устройство VRM. Можно выбрать тип устройства и ввести учетные данные.

Назначить резервный диспетчер VRM основному VRM можно, только когда оба диспетчера подключены к сети и успешно прошли проверку подлинности. Затем синхронизируются пароли.

Можно добавить основной VRM вручную, если вам известны IP-адрес и пароль.

Для добавления основного устройства VRM выполните следующие действия.

1. Настройте необходимые параметры для устройства VRM.
2. В списке **Тип** выберите элемент **Первичный**.
3. Нажмите **ОК**.

Будет добавлено устройство VRM.

Можно добавить вторичный VRM вручную, если вам известны IP-адрес и пароль.

Замечание!
Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

Для добавления вторичного VRM выполните следующие действия.

1. Настройте необходимые параметры для устройства VRM.
2. В списке **Тип** выберите элемент **Вторичный**.
3. Нажмите **ОК**.

Будет добавлено устройство VRM.

Теперь можно настроить вторичный VRM, как любой другой основной VRM.

Диалоговое окно Добавить VRM

Имя

Введите отображаемое имя устройства.

Сетевой адрес / порт

Введите IP-адрес своего устройства.

Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.
Вы можете изменить номер порта, если порты по умолчанию не используются.

Тип
Выберите необходимый тип устройства.

Имя пользователя
Введите имя пользователя для проверки подлинности.

Пароль
Введите пароль для проверки подлинности.

Показать пароль
Нажмите, чтобы пароль в этом диалоговом окне стал виден.

Безопасность
По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.

Замечание!
При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду **Изменить устройство VRM** и установите или снимите флажок **Безопасное соединение**.

Тест
Нажмите, чтобы проверить, подключено ли устройство и успешно ли выполнена проверка подлинности.

Свойства
При необходимости измените номера портов для порта HTTP и порта HTTPS. Это возможно только в тех случаях, когда добавляется или изменяется диспетчер VRM, который не подключен. Если диспетчер VRM подключен, эти значения поступают из сети, и их невозможно изменить.
В строке таблицы **Ведущий VRM** указывается выбранное устройство, если это возможно.

См.
- *Редактирование устройства VRM, Страница 179*
- *Добавление зеркального диспетчера VRM вручную, Страница 184*
- *Добавление резервного диспетчера VRM вручную, Страница 183*

14.22.3 Редактирование устройства VRM

Главное окно > **Устройства**
Позволяет изменить устройство VRM.

Чтобы изменить безопасное/небезопасное соединение:

1. Щелкните правой кнопкой мыши  .
2. Нажмите **Изменить устройство VRM**.
   Откроется диалоговое окно **Изменить устройство VRM**.

3. Установите флажок **Безопасное соединение**.
   Используемый порт автоматически меняется на порт HTTPS.
   Или
   снимите флажок **Безопасное соединение**.
   Используемый порт автоматически меняется на порт RCPP.

Замечание!
После обновления до новой версии рекомендуется изменить включить безопасное соединение.

Подробные сведения о параметрах диалогового окна **Изменить устройство VRM** см. в главе «Добавление основного или вторичного VRM вручную».

См.
– *Добавление основного или вторичного VRM вручную, Страница 178*

14.22.4 Страница Настройки VRM

Главное окно > **Устройства** > разверните  >  > **Основные параметры** > **Настройки VRM**

Имя инициатора на сервере
Отображает имя инициатора iSCSI-сервера VRM Server.

14.22.5 Страница SNMP

Главное окно > **Устройства** > разверните  > разверните  > **Сеть** > **SNMP**

1. Адрес узла SNMP 2. Адрес узла SNMP
VRM поддерживает SNMP (Simple Network Management Protocol) для управления сетевыми компонентами и может отправлять SNMP-сообщения (запросы) по IP-адресам. Устройство поддерживает SNMP MIB II в стандартизированном коде. Чтобы посылать запросы SNMP, введите в данном поле IP-адреса одного или двух устройств назначения. Некоторые события отправляются только как запросы SNMP. Описание содержится в файле MIB.

14.22.6 Страница "Учетные записи"

Чтобы настроить размещение изображений и экспортировать видеофрагменты в формате файла MP4, необходимо создать учетную запись для сохранения и доступа к ним. Можно создать не более четырех (4) учетных записей.

Тип
Выберите тип учетной записи: **FTP** или **Dropbox**.

IP-адрес
Введите IP-адрес сервера, на котором требуется сохранять изображения.

Имя пользователя
Введите имя пользователя для сервера.

Пароль
Введите пароль, который дает вам право доступа к серверу. Чтобы проверить пароль, нажмите **Проверить** справа.

Проверить
Нажмите, чтобы проверить пароль.

Путь
Введите точный путь для размещения изображений и видеофрагментов на сервере.

14.22.7 Страница Дополнительно

Главное окно > **Устройства** > разверните  > разверните  > **Обслуживание** > **Дополнительно**

Регистрация RCP+ / Регистрация данных отладки / Регистрация данных воспроизведения / Регистрация данных VDP / Регистрация данных производительности
Включите различные журналы для VRM Server и Configuration Manager.
Файлы журнала для VRM Server хранятся в компьютере, на котором запущен сервер VRM Server, и их можно просмотреть или загрузить при помощи VRM Monitor.
Файлы журнала для Configuration Manager хранятся локально в следующем каталоге: %USERPROFILE%\My Documents\Bosch\Video Recording Manager\Log

Срок хранения (в днях)
Укажите срок хранения для файлов журнала в днях.

Полный дамп-файл памяти
Устанавливайте этот флажок только в случае необходимости, например, если в службе технической поддержки потребуют полную сводку состояния основной памяти.

Поддержка Telnet
Устанавливайте этот флажок, если требуется поддержка доступа по протоколу Telnet. Устанавливать только в случае необходимости.

Замечание!
Для интенсивной регистрации в журналах необходимы значительные ресурсы центрального процессора и емкость жесткого диска.
Не пользуйтесь интенсивной регистрацией постоянно.

14.22.8 Шифрование записи для VRM

Зашифрованная запись для кодеров VRM не включена по умолчанию.
Вам необходимо включить зашифрованную запись для основного или вторичного VRM отдельно.

Замечание!
Перед тем как включить шифрование видеозаписи в первый раз, необходимо создать резервный ключ (резервную копию сертификата). Для каждого устройства VRM требуется лишь один раз создать резервный ключ.
Если обычный ключ шифрования будет потерян, видеозаписи можно будет расшифровать с помощью резервного ключа.

Мы рекомендуем хранить копию резервного ключа в надежном месте (например, в сейфе).

Для создания резервного ключа:
1. Выберите соответствующее устройство VRM.
2. Откройте вкладку **Обслуживание**.
3. Выберите вкладку **Шифрование записи**.
4. Нажмите **Резервный ключ**.
5. Выберите расположение хранилища сертификатов.

6. Введите пароль, отвечающий требованиям к сложности пароля, и подтвердите его.
7. Нажмите **Создать**.
   Будет создан резервный ключ (резервная копия сертификата).

Чтобы активировать/деактивировать шифрование видеозаписи:

1. Выберите соответствующее устройство VRM.
2. Откройте вкладку **Обслуживание**.
3. Выберите вкладку **Шифрование записи**.
4. Установите/снимите флажок **Включить шифрование видеозаписи**.
5. Нажмите  .

Примечание. Шифрование активируется только после изменения следующего блока.
Для этого может потребоваться некоторое время.
Убедитесь, что кодеры выполняют шифрование.

Чтобы убедиться, что кодеры VRM выполняют шифрование:

1. Выберите соответствующее устройство VRM.
2. Откройте вкладку **Обслуживание**.
3. Выберите вкладку **Шифрование записи**.

Примечание. Это также можно посмотреть на вкладке **Monitoring** в VRM Monitor.

Замечание!
Все кодеры VRM, поддерживающие шифрование, автоматически шифруют видеозапись после активации шифрования в VRM.
Для каждого кодера шифрование может быть отключено.
Кодеры VSG всегда выполняют шифрование, если шифрование активировано в VRM.

Чтобы активировать или деактивировать шифрование видеозаписи для одного кодера VRM:

1. Выберите соответствующий кодер VRM.
2. Откройте вкладку **Запись**.
3. Откройте вкладку **Управление видеозаписью**.
4. Установите/снимите флажок **Шифрование**.
5. Нажмите  .

14.22.9 Изменение пароля устройства VRM

Главное окно > **Устройства** > Разверните  > 

Изменение пароля:

1. Щелкните  правой кнопкой мыши, затем щелкните **Изменить пароль VRM**.
   Отображается диалоговое окно **Изменить пароль**.
2. В поле **Старый пароль** введите необходимый пароль.
3. В поле **Новый пароль** введите новый пароль, нажмите второе поле **Новый пароль** и снова введите новый пароль.

Нажмите **ОК**.

- ▸ Подтвердите введенные данные в следующем диалоговом окне.
- ⇨ Пароль на устройстве изменяется незамедлительно.

14.22.10 Добавления пула VRM

Главное окно > **Устройства** > Развернуть 

Добавление пула VRM:

- Щелкните правой кнопкой мыши  или  и выберите команду **Добавить пул**. В систему добавляется новый пул.

См.

– *Пул хранения iSCSI, Страница 196*

14.22.11 Добавление резервного диспетчера VRM вручную

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить резервный VRM** > диалоговое окно **Добавить резервный VRM**

Замечание!
Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

Как основной VRM, так и вторичный VRM могут взять на себя функции резервного VRM. Основной резервный VRM добавляется к основному VRM, а вторичный резервный VRM — ко вторичному VRM.
Можно добавить устройство резервного VRM вручную, если известны IP-адрес и пароль.
Изначально выбранный VRM является ведущим VRM для этого избыточного VRM.
ВЫ можете добавить устройство резервного VRM. Вы можете добавить его вручную или выбрать устройство из списка просканированных устройств VRM.
Назначить резервный диспетчер VRM основному VRM можно, только когда оба диспетчера подключены к сети и успешно прошли проверку подлинности. Затем синхронизируются пароли.

Добавление устройства резервного VRM

1. Задайте необходимые параметры для устройства VRM.
2. Убедитесь, что выбран верный основной диспетчер VRM. Если это не так, отмените процедуру.
3. Нажмите **ОК**.

⇨ Устройство резервного VRM добавляется к выбранному основному VRM.

Диалоговое окно Добавить резервный VRM

Сетевой адрес
Введите IP-адрес устройства или выберите сетевой адрес в списке **Просканированные VRM**.

Просканированные VRM
Отображает список просканированных компьютеров VRM. Для повтора сканирования закройте диалоговое окно и снова отобразите диалоговое окно.

Замечание!
Резервное устройство VRM наследует параметры, настроенные в ведущем устройстве VRM. При изменении параметров ведущего устройства VRM соответствующим образом меняются параметры резервного устройства VRM.

См.

– *Двойная / резервная запись, Страница 30*

14.22.12 Добавление зеркального диспетчера VRM вручную

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Добавить зеркальный VRM** > диалоговое окно **Добавить VRM**

Замечание!
Для настройки конфигурации вторичной системы VRM необходимо сначала установить соответствующее ПО на требуемый компьютер. Запустите Setup.exe и выберите **Вторичный VRM**.

Только дополнительный VRM может взять на себя функцию зеркального VRM. Можно добавить зеркальный VRM к основному VRM.
Устройство зеркального VRM можно добавить вручную, если известны IP-адрес и пароль.
Изначально выбранный VRM является основным VRM для этого зеркального VRM.

Добавление устройства зеркального VRM:

1. Задайте необходимые параметры для устройства VRM.
2. Убедитесь, что выбран верный основной диспетчер VRM. Если это не так, отмените процедуру.
3. Нажмите **OK**.

Устройство зеркального VRM добавляется к выбранному основному VRM.

Диалоговое окно Добавить VRM

Имя
Введите отображаемое имя устройства.

Сетевой адрес / порт
Введите IP-адрес своего устройства.
Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.
Вы можете изменить номер порта, если порты по умолчанию не используются.

Тип
Выберите необходимый тип устройства.

Имя пользователя
Введите имя пользователя для проверки подлинности.

Показать пароль
Нажмите, чтобы пароль в этом диалоговом окне стал виден.

Пароль
Введите пароль для проверки подлинности.

Безопасность
По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.

Замечание!
При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду **Изменить устройство VRM** и установите или снимите флажок **Безопасное соединение**.

Тест
Нажмите, чтобы проверить, подключено ли устройство и успешно ли выполнена проверка подлинности.

Свойства
При необходимости измените номера портов для порта HTTP и порта HTTPS. Это возможно только в тех случаях, когда добавляется или изменяется диспетчер VRM, который не подключен. Если диспетчер VRM подключен, эти значения поступают из сети, и их невозможно изменить.
В строке таблицы **Ведущий VRM** указывается выбранное устройство, если это возможно.

См.
- *Добавление основного или вторичного VRM вручную, Страница 178*
- *Двойная / резервная запись, Страница 30*

14.22.13 Добавление кодеров путем поиска

Для добавления кодеров путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.
   В столбце **Состояние** успешные входы в систему обозначены значком  .
   Неудачные попытки входа обозначены значком  .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

14.22.14 Добавление устройств VSG путем поиска

Для добавления устройств VSG путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск шлюзов Video Streaming Gateway**.
   Откроется диалоговое окно **BVMS Scan Wizard**.

2. Выберите необходимые устройства VSG, выберите пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

   В столбце **Состояние** успешные входы в систему обозначены значком .

   Неудачные попытки входа обозначены значком .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

14.22.15 Синхронизация конфигурации BVMS

Главное окно > **Устройства** > разверните > щелкните правой кнопкой мыши > команда **Синхронизация конфигурации BVMS**

В версии BVMS 6.0 поддерживается версия VRM 3.50. Если вы не обновите VRM до версии 3.50 во время обновления системы BVMS до версии 6.0, запись продолжится, однако вы не можете изменить конфигурацию старого VRM.

Если вы обновили программное обеспечение VRM до версии 3.50, необходимо вручную синхронизировать конфигурацию BVMS.

14.22.16 Импорт конфигурации из VRM

Главное окно > **Устройства** > Разверните >

При необходимости замены основного устройства VRM можно импортировать конфигурацию предыдущего основного устройства VRM .

Примечание: Это возможно только для основных устройств VRM .

Предварительные условия: Выполнена резервная копия предыдущего файла конфигурации устройства VRM (config.xml). Как создать резервную копию, см. в *Обслуживание BVMS, Страница 79*.

Для того, чтобы импортировать конфигурацию из VRM:

1. Скопируйте резервную копию файла VRM конфигурации (config.xml) в C:\ProgramData\Bosch\VRM\primary.
2. Щелкните правой кнопкой мыши .
3. Выберите **Импортировать конфигурацию из VRM**.
   Предыдущая конфигурация VRM импортирована.

Замечание!
Импортируется только кодер VSG и конфигурация iSCSI.
Необходимо изменить все остальные конфигурации, например, добавить необходимые устройства в **Логическое дерево**, настройки аварий или параметры записи.

14.23 Страница "Пул"

Главное окно > **Устройства** > Разверните  > Разверните  > 

Позволяет настраивать запись для всех устройств, собираемых данным пулом хранилищ.

Идентификация пула

Отображает номер пула.

Режим настроек записи

– **При отказе**

Записи сохраняются только на первичный целевой объект. Если сохранение на эту цель невозможно, запись будет сохранена на объект, указанный как вторичный. Ситуация отказа возникает, если основная система хранения (цель) по какой-либо причине не предоставляет блоки хранения, например: система хранения (цель) отключена, сетевая ошибка или не осталось места.

Список вторичных целевых объектов можно оставить пустым. В этом случае резервирование невозможно, однако количество необходимых сеансов iSCSI сокращается, на вторичном целевом объекте не выделяется дисковое пространство. Это снижает нагрузку на систему и увеличивает время хранения записей.

Примечание: Для каждой камеры и кодера в таком случае необходимо настроить основной и вторичный целевые объекты.

– **Автоматический**

Балансировка нагрузки настраивается автоматически. **Автоматический** режим выполняет автоматическую оптимизацию времени хранения для доступных целевых объектов iSCSI. Чтобы назначить блоки вторичного целевого объекта iSCSI, выберите **ВКЛ** (on) в списке **второстепенных целей**.

Период проверки работоспособности (дн.)

Укажите необходимый период времени. После окончания этого периода Video Recording Manager программа анализирует, является ли распределение памяти в **автоматическом** режиме оптимальным. Если нет, то программа Video Recording Manager вносит изменения.

Использование второстепенной цели

Позволяет выбрать, распределять ли блоки от второго целевого объекта.
Выберите **Вкл.** или **Выкл.** для включения или отключения использования второстепенного целевого объекта.

– **ВКЛ.**: Выбрать **ВКЛ.** позволяет использовать второстепенный целевой объект, чтобы сократить разрыв записи в случае отказа первичного целевого объекта. Если первичный целевой объект доступен, то блоки второстепенного целевого объекта не используются, но место для хранения резервируется. Такая избыточность сокращает доступное пространство для хранения записей.
– **ВЫКЛ.**: Выберите **ВЫКЛ.**, если вы не хотите использовать второстепенный целевой объект. В случае сбоя первичного целевого объекта программе Video Recording Manager требуется больше времени для перенастройки. Это означает, что разрыв в записи увеличивается.

Резервирование блоков на время простоя

Введите число дней, в течение которых будет производиться запись с назначенных кодеров, когда VRM Server недоступен.
Например, если задать 4, то запись будет производиться в течение приблизительно 4 дней простоя VRM Server.

Если в системе имеются устройства с низким значением потока, можно существенно снизить предварительно выделенное пространство на диске. Это обеспечивает правильное распределение емкости хранилища и увеличивает время хранения.

Разрешить LUN более 2 ТБ

Нажмите, чтобы включить использование устройств LUN больше 2 ТБ.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:

- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMSне позволяет выполнять следующие действия:

- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

См.

- *Добавление устройства LUN, Страница 205*
- *Добавления пула VRM, Страница 183*

14.23.1 Настройка автоматического режима записи в пуле

Главное окно > **Устройства** > Разверните  > Разверните  > 

Примечание.

Если ранее был настроен резервный режим записи, эта настройка будет перезаписана.

Настройка

- В списке **Режим настроек записи** выберите **Автоматически**.
  После активации конфигурации активируется **Автоматически** режим записи. На странице **Очередность записи** кодера отображаются списки первичных и вторичных целевых объектов.

Дополнительная информация

- *Настройка резервного режима записи на кодере, Страница 242*

14.23.2 Добавление кодера вручную

Главное окно > **Устройства** > Развернуть  > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**

или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**

или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Добавить декодер** > Диалоговое окно **Добавить кодер**
Позволяет добавить кодер вручную. Это особенно полезно, если необходимо добавить какое-либо IP-видеоустройство производства Bosch (только для VRM).

Внимание.
Если добавляется IP-видео кодер Bosch с выбранным параметром **<Автоопределение>**, это устройство должно быть доступно в сети.

Добавление IP-видеоустройства производства Bosch:

1. Разверните  , разверните  , щелкните правой кнопкой мыши  .
   Или
   щелкните правой кнопкой мыши  .
   Или
   щелкните правой кнопкой мыши  .
2. Нажмите **Добавить кодер**.
   Откроется диалоговое окно **Добавить кодер**.
3. Введите соответствующий IP-адрес.
4. В списке выберите **<Автоопределение>**, введите пароль устройства и нажмите **Проверить подлинность.**
   Или
   В списке выберите конкретный тип кодера или **<Камера с одним заполнителем>**.
5. Нажмите **ОК**.
   Устройство добавляется в систему.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

Диалоговое окно Добавить кодер
Сетевой адрес
Введите действительный IP-адрес.

Тип кодера
Для устройства с известным типом выберите соответствующий элемент. Устройство не обязательно должно быть доступно в сети.
Если требуется добавить какое-либо IP-видеоустройство производства Bosch, выберите **<Автоопределение>**. Это устройство должно быть доступно в сети.
Если вы хотите добавить камеру для конфигурирования в автономном режиме, выберите **<Камера с одним заполнителем>**.

Имя пользователя
Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль
Введите действующий пароль для аутентификации на устройстве.

Отобразить пароль
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Проверить подлинность
Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

14.23.3 Добавление устройства iSCSI вручную

Главное окно > **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство iSCSI** > диалоговое окно **Добавить устройство iSCSI**
Позволяет добавить устройство iSCSI в VRM.

Добавление устройства iSCSI:

1. Щелкните правой кнопкой мыши  и выберите команду **Добавить устройство iSCSI**.
   Откроется диалоговое окно **Добавить устройство iSCSI**.
2. Введите требуемое имя для отображения, сетевой адрес устройства iSCSI и тип устройства и нажмите **OK**.
   Устройство iSCSI добавляется к выбранному пулу VRM.
   При необходимости добавьте целевые объекты и устройства LUN.

Диалоговое окно Добавить устройство iSCSI

Имя
Введите отображаемое имя для устройства.

Сетевой адрес
Введите действительный сетевой адрес устройства.

Тип устройства iSCSI
Выберите соответствующий тип устройства.

Имя пользователя
Введите имя пользователя для проверки подлинности.

Пароль
Введите пароль для проверки подлинности.

Вкл. мониторинг
Если устройство DIVAR IP выбрано в качестве устройства типа iSCSI и поддерживается какой-либо мониторинг SNMP (Simple Network Management Protocol) для данного типа устройств DIVAR IP, то включен флажок **Вкл. мониторинг**.
Установите флажок, чтобы разрешить мониторинг состояния устройства DIVAR IP. Теперь BVMS автоматически принимает и подавляет ловушки SNMP устройства DIVAR IP и активирует события и аварийные предупреждения мониторинга состояния (например, ЦП, ЗУ, вентилятор...). По умолчанию срабатывает только критически важные аварийные предупреждения.
Примечание: Сначала обязательно настройте SNMP на устройстве DIVAR IP.
Примечание: Эта настройка доступна только для поддерживаемых устройств.

Дополнительную информацию о настройке SNMP на устройстве DIVAR IP можно найти в соответствующих документах DIVAR IP.

Дополнительная информация

– *Добавление устройств VRM путем поиска, Страница 177*

См.

– *Страница SNMP, Страница 159*
– *Настройка мониторинга SNMP, Страница 98*

14.23.4 Добавление Video Streaming Gateway вручную

Главное окно > **Устройства** > Разверните  > 
Можно добавлять устройства VSG в пул VRM.

Для добавления устройства VSG вручную выполните следующие действия.

1. Щелкните правой кнопкой мыши  и щелкните **Добавить шлюз Video Streaming Gateway**.
   Откроется диалоговое окно **Добавить шлюз Video Streaming Gateway**.
2. Задайте необходимые параметры для устройства VSG.
3. Нажмите **Добавить**.

⇨ Устройство VSG будет добавлено в систему. Изображения с камер, назначенных этому устройству VSG, будут записываться.

Диалоговое окно Добавить шлюз Video Streaming Gateway

Щелкните правой кнопкой мыши  > **Добавить шлюз Video Streaming Gateway** > диалоговое окно **Добавить шлюз Video Streaming Gateway**

Имя
Введите необходимое отображаемое имя для устройства.

Имя пользователя
Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

Сетевой адрес / порт
Введите IP-адрес устройства.
Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.
Можно изменить номер порта, если порты по умолчанию не используются или если экземпляры VSG настроены в другом порядке.

Порты по умолчанию

Экземпляр VSG	Порт RCPP	Порт HTTPS
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448

Экземпляр VSG	Порт RCPP	Порт HTTPS
7	8762	8449

Пароль
Введите действующий пароль для аутентификации на устройстве.

Show password
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Безопасность
По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.
Начиная с VSG версии 7.0, VSG поддерживает безопасное соединение.

Замечание!
При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду **Изменить шлюз Video Streaming Gateway** и установите или снимите флажок **Безопасное соединение**.

Тест
Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

См.
– *Изменение шлюза Video Streaming Gateway, Страница 209*

14.23.5 Добавление устройства iSCSI DSA E-Series вручную

Главное окно > **Устройства** >  > разверните  > 
Вы можете добавить устройство iSCSI серии E-Series, которое уже инициализировано, или устройство iSCSI серии E-Series, которое не инициализировано.
вы можете добавить устройства LUN больше 2 ТБ, если пул настроен для использования больших устройств LUN.
Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:
– Устройства VRM версии ниже 3.60
– Устройства VSG с версией микропрограммного обеспечения ниже 6.30
– Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMSне позволяет выполнять следующие действия:
– Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
– Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
– Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
– Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.

– Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

для добавления инициализированного устройства iSCSI:

1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.
   Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
2. Введите IP-адрес управления и пароль.
3. Нажмите **Подключиться**
   . Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполнятся.
4. Нажмите **OK**.
   Устройство будет добавлено в систему.
   Автоматически сканируются доступные целевые объекты, и отображаются устройства LUN.
   Вы можете использовать устройство iSCSI.
   Если пул настроен для использования больших устройств LUN и для устройства iSCSI настроены большие устройства LUN, в столбце **Большой LUN** отображается флажок для соответствующих устройств LUN.

Чтобы добавить не инициализированное устройство iSCSI:

1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.
   Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
2. Введите IP-адрес управления и пароль.
3. Нажмите **Подключиться**
   . Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполнятся.
4. Нажмите **OK**.
   Устройство будет добавлено в систему.
5. Нажмите  , затем нажмите  .
6. Перейдите на вкладку **Базовая конфигурация**.
7. Введите требуемый объем устройства LUN.
   Если вы введете значение больше 2 ТБ, потребуется настроить пул для использования устройств LUN больше 2 ТБ.
8. Нажмите кнопку **Инициализировать**.
   Создаются устройства LUN.
9. Нажмите **Закрыть**.
10. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.
    Устройства LUN отображаются с неизвестным состоянием.
11. Сохраните и активируйте конфигурацию.
12. Форматирование всех устройств LUN.

13. После добавления устройства iSCSI с двойным контроллером удалите требуемые устройства LUN из первого контроллера, правой кнопкой мыши щелкните второй контроллер и выберите **Сканировать целевой объект** для добавления этих устройств LUN.

Диалоговое окно Добавить устройство серии DSA E-Series

Главное окно > **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство серии DSA E-Series** > диалоговое окно **Добавить устройство серии DSA E-Series**

Позволяет добавить устройство iSCSI DSA E-Series. IP-адрес управления этого типа устройства отличается от IP-адреса хранилища iSCSI. Этот IP-адрес управления используется для автоматического обнаружения и настройки устройства.

Имя

Введите отображаемое имя устройства.

Адрес управления

Введите IP-адрес для автоматической настройки устройства.

Пароль:

Введите пароль для данного устройства.

Тип DSA E-Series

Отображает тип устройства.

Сетевой адрес канала iSCSI

Отображает IP-адрес или порт iSCSI устройства. При наличии можно выбрать другой IP-адрес.

Адрес управления

Отображает IP-адрес для автоматической конфигурации второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

Сетевой адрес канала iSCSI

Отображает IP-адрес порта iSCSI второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

Подключиться

Нажмите, чтобы определить параметры устройства.

Если подключение установлено, поля в группе **Контроллер** и в группе **Второй контроллер** заполнятся.

См.

- *Страница "Базовая конфигурация", Страница 202*
- *Форматирование LUN, Страница 206*

14.23.6 Добавление кодеров путем поиска

Для добавления кодеров путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**. Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.

3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

   В столбце **Состояние** успешные входы в систему обозначены значком .

   Неудачные попытки входа обозначены значком .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Значок указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

14.23.7 Добавление устройств VSG путем поиска

Для добавления устройств VSG путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши и выберите команду **Поиск шлюзов Video Streaming Gateway**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые устройства VSG, выберите пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

   В столбце **Состояние** успешные входы в систему обозначены значком .

   Неудачные попытки входа обозначены значком .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

14.23.8 Настройка двойного режима записи в Дереве устройств

Главное окно > **Устройства** > разверните > > >
Для настройки двойной записи функцию ANR необходимо отключить.
Если выполняется настройка двойной записи для одной камеры многоканального кодера, система следит за тем, чтобы все камеры этого кодера были настроены на один и тот же получатель записи.

Двойную запись можно настроить путем назначения кодеров, запись которых обеспечивается основным диспетчером VRM, вторичному VRM. Это может быть полезно, если требуется назначить только часть кодеров, запись которых обеспечивается основным VRM.
Вторичный VRM должен быть уже настроен.

Настройка

1. Щелкните  правой кнопкой мыши, затем щелкните **Добавить кодер с первичного VRM**.
   Отображается диалоговое окно **Добавить кодеры**.
2. Выберите необходимые кодеры.
   При выборе пула или VRM автоматически выбираются все дочерние элементы.
3. Нажмите **ОК**.
   Выбранные кодеры будут добавлены во вторичный VRM.

См.
- *Настройка двойного режима записи в Таблице камер, Страница 314*
- *Настройка функции ANR, Страница 314*
- *Двойная / резервная запись, Страница 30*

14.24 Страница «Кодер/декодер Bosch»

Сведения о настройке кодера/декодера Bosch см. в разделе *Страница «Кодер/декодер/камера Bosch», Страница 224*.

14.25 Страница устройства iSCSI

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните 

Можно добавить либо устройство iSCSI серии E, либо другое поддерживаемое устройство iSCSI.

См.
- *Добавление устройства iSCSI вручную, Страница 198*
- *Добавление устройства iSCSI DSA E-Series вручную, Страница 199*
- *Настройка устройства iSCSI, Страница 201*
- *Добавление устройства LUN, Страница 205*
- *Форматирование LUN, Страница 206*

14.25.1 Пул хранения iSCSI

Пул хранилищ может использоваться для логического сегментирования системы. Например, для приведения в соответствие с сетевой топологией системы Video Recording Manager. Например, если есть два здания, в каждом из которых есть свое хранилище и устройства, то можно исключить маршрутизацию сетевого трафика из одного здания в другое.

Пулы хранилищ также можно использовать для группировки камер и систем хранения по определенному важному полю обзора. Пусть, к примеру, система содержит несколько очень важных камер и большое число менее важных. В этом случае можно сгруппировать камеры в два пула хранилищ: один с большим количеством функций резервирования, а второй — с меньшей степенью резервирования.

Для пула хранилищ можно настроить следующие свойства балансировки нагрузки:

- Настройки видеозаписи (**Автоматически** или **При отказе**).
- Использование вторичного целевого объекта.
  Вторичный целевой объект используется в режиме **При отказе** в случае сбоя назначенного первичного целевого объекта. Если эта функция отключена, при сбое первичного целевого объекта видеозапись со всех назначенных ему устройств прекращается.
  В режиме **Автоматический**: если происходит сбой одного целевого объекта, VRM Server выполняется автоматическое переназначение соответствующих устройств другим хранилищам. Если VRM Server отключен во время отказа целевого объекта, запись с устройств, в этот момент выполняющих запись на отказавший целевой объект, прекращается.
- Резервирование блоков на время простоя
- Период проверки работоспособности

Каждый пул можно настроить таким образом, чтобы он допускал использование устройств LUN больше 2 ТБ.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:

- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMSне позволяет выполнять следующие действия:

- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

Если основной VRM имеет пул, поддерживающий использование больших устройств LUN, соответствующий зеркальный VRM наследует этот параметр, и вы не можете установить или снять флажок **Разрешить LUN более 2 ТБ** в соответствующем пуле зеркального VRM. После добавления устройства iSCSI с большим устройствами LUN к зеркальному VRM вы не можете снять флажок **Разрешить LUN более 2 ТБ** в соответствующем пуле основного VRM.

См.

- *Страница "Пул", Страница 187*

14.25.2 Добавление устройства iSCSI вручную

Главное окно > **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство iSCSI** > диалоговое окно **Добавить устройство iSCSI**
Позволяет добавить устройство iSCSI в VRM.

Добавление устройства iSCSI:

1. Щелкните правой кнопкой мыши  и выберите команду **Добавить устройство iSCSI**.
   Откроется диалоговое окно **Добавить устройство iSCSI**.
2. Введите требуемое имя для отображения, сетевой адрес устройства iSCSI и тип устройства и нажмите **OK**.
   Устройство iSCSI добавляется к выбранному пулу VRM.
   При необходимости добавьте целевые объекты и устройства LUN.

Диалоговое окно Добавить устройство iSCSI

Имя
Введите отображаемое имя для устройства.

Сетевой адрес
Введите действительный сетевой адрес устройства.

Тип устройства iSCSI
Выберите соответствующий тип устройства.

Имя пользователя
Введите имя пользователя для проверки подлинности.

Пароль
Введите пароль для проверки подлинности.

Вкл. мониторинг
Если устройство DIVAR IP выбрано в качестве устройства типа iSCSI и поддерживается какой-либо мониторинг SNMP (Simple Network Management Protocol) для данного типа устройств DIVAR IP, то включен флажок **Вкл. мониторинг**.
Установите флажок, чтобы разрешить мониторинг состояния устройства DIVAR IP. Теперь BVMS автоматически принимает и подавляет ловушки SNMP устройства DIVAR IP и активирует события и аварийные предупреждения мониторинга состояния (например, ЦП, ЗУ, вентилятор...). По умолчанию срабатывает только критически важные аварийные предупреждения.
Примечание: Сначала обязательно настройте SNMP на устройстве DIVAR IP.
Примечание: Эта настройка доступна только для поддерживаемых устройств.
Дополнительную информацию о настройке SNMP на устройстве DIVAR IP можно найти в соответствующих документах DIVAR IP.

Дополнительная информация

– *Добавление устройств VRM путем поиска, Страница 177*

См.

– *Страница SNMP, Страница 159*
– *Настройка мониторинга SNMP, Страница 98*

14.25.3 Добавление устройства iSCSI DSA E-Series вручную

Главное окно > **Устройства** >  > разверните  > 

Вы можете добавить устройство iSCSI серии E-Series, которое уже инициализировано, или устройство iSCSI серии E-Series, которое не инициализировано.

вы можете добавить устройства LUN больше 2 ТБ, если пул настроен для использования больших устройств LUN.

Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:

- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMSне позволяет выполнять следующие действия:

- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

для добавления инициализированного устройства iSCSI:

1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.
   Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
2. Введите IP-адрес управления и пароль.
3. Нажмите **Подключиться**
   . Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполнятся.
4. Нажмите **ОК**.
   Устройство будет добавлено в систему.
   Автоматически сканируются доступные целевые объекты, и отображаются устройства LUN.
   Вы можете использовать устройство iSCSI.
   Если пул настроен для использования больших устройств LUN и для устройства iSCSI настроены большие устройства LUN, в столбце **Большой LUN** отображается флажок для соответствующих устройств LUN.

Чтобы добавить не инициализированное устройство iSCSI:

1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить устройство серии DSA E-Series**.
   Отображается диалоговое окно **Добавить устройство серии DSA E-Series**.
2. Введите IP-адрес управления и пароль.

3. Нажмите **Подключиться**
   . Если подключение установлено, поля в группе **Контроллер** и/или в группе **2-й контроллер** заполнятся.
4. Нажмите **ОК**.
   Устройство будет добавлено в систему.
5. Нажмите  , затем нажмите  .
6. Перейдите на вкладку **Базовая конфигурация**.
7. Введите требуемый объем устройства LUN.
   Если вы введете значение больше 2 ТБ, потребуется настроить пул для использования устройств LUN больше 2 ТБ.
8. Нажмите кнопку **Инициализировать**.
   Создаются устройства LUN.
9. Нажмите **Закрыть**.
10. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.
    Устройства LUN отображаются с неизвестным состоянием.
11. Сохраните и активируйте конфигурацию.
12. Форматирование всех устройств LUN.
13. После добавления устройства iSCSI с двойным контроллером удалите требуемые устройства LUN из первого контроллера, правой кнопкой мыши щелкните второй контроллер и выберите **Сканировать целевой объект** для добавления этих устройств LUN.

Диалоговое окно Добавить устройство серии DSA E-Series

Главное окно > **Устройства** >  > разверните  > щелкните правой кнопкой мыши  > **Добавить устройство серии DSA E-Series** > диалоговое окно **Добавить устройство серии DSA E-Series**

Позволяет добавить устройство iSCSI DSA E-Series. IP-адрес управления этого типа устройства отличается от IP-адреса хранилища iSCSI. Этот IP-адрес управления используется для автоматического обнаружения и настройки устройства.

Имя

Введите отображаемое имя устройства.

Адрес управления

Введите IP-адрес для автоматической настройки устройства.

Пароль:

Введите пароль для данного устройства.

Тип DSA E-Series

Отображает тип устройства.

Сетевой адрес канала iSCSI

Отображает IP-адрес или порт iSCSI устройства. При наличии можно выбрать другой IP-адрес.

Адрес управления

Отображает IP-адрес для автоматической конфигурации второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

Сетевой адрес канала iSCSI
Отображает IP-адрес порта iSCSI второго контроллера при его наличии. При наличии можно выбрать другой IP-адрес.

Подключиться
Нажмите, чтобы определить параметры устройства.
Если подключение установлено, поля в группе **Контроллер** и в группе **Второй контроллер** заполнятся.

См.
- *Страница "Базовая конфигурация", Страница 202*
- *Форматирование LUN, Страница 206*

14.25.4 Настройка устройства iSCSI

Главное окно > **Устройства** > разверните  > разверните  > 
После добавления устройств VRM, устройств iSCSI и кодеров выполните следующие действия для обеспечения того, чтобы все видеоданные сохранялись на устройствах iSCSI и видеоданные можно было получить с этих устройств iSCSI.
- Активируйте конфигурацию по умолчанию, чтобы создать номера LUN на каждом целевом объекте устройства iSCSI.
  Это действие не является обязательным. Его не обязательно выполнять на устройстве iSCSI с предварительно настроенными номерами LUN.
- Просканируйте устройство iSCSI, чтобы добавить целевые объекты и номера LUN в логическое дерево после активации конфигурации по умолчанию.

Примечание
Не все устройства iSCSI поддерживают конфигурацию по умолчанию и автоматическое сопоставление IQN.

Предварительные условия:
Устройство iSCSI должно быть сконфигурировано с действительными IP-адресами.

Чтобы выполнить базовую конфигурацию устройства DSA E-Series iSCSI:

- разверните соответствующее устройство  и  , щелкните соответствующее устройство iSCSI  .

1. Перейдите на вкладку **Базовая конфигурация**.
2. Введите требуемый объем устройства LUN.
   Если вы введете значение больше 2 ТБ, потребуется настроить пул для использования устройств LUN больше 2 ТБ.
3. Нажмите кнопку **Инициализировать**.
   Создаются устройства LUN.
4. Нажмите **Закрыть**.
5. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.
   Устройства LUN отображаются с неизвестным состоянием.
6. Сохраните и активируйте конфигурацию.
7. Форматирование всех устройств LUN.

8. После добавления устройства iSCSI с двойным контроллером удалите требуемые устройства LUN из первого контроллера, правой кнопкой мыши щелкните второй контроллер и выберите **Сканировать целевой объект** для добавления этих устройств LUN.

Чтобы выполнить базовую конфигурацию на других устройствах iSCSI:

1. перейдите на вкладку **Базовая конфигурация**.
2. Введите необходимое количество устройств LUN.
3. Нажмите **Установить**.
   Создаются устройства LUN.
4. Нажмите **Закрыть**.
5. Щелкните правой кнопкой мыши значок устройства iSCSI и выберите команду **Сканировать целевой объект**.
   Устройства LUN отображаются с неизвестным состоянием.
6. Сохраните и активируйте конфигурацию.
7. Форматирование всех устройств LUN.

Для выполнения сопоставления IQN для других устройств iSCSI:

1. Разверните соответствующее устройство  и  , щелкните соответствующее устройство iSCSI  .
2. Щелкните правой кнопкой мыши  и нажмите **Сопоставить IQN**. Отображается диалоговое окно
   iqn-Mapper, и процесс запускается.
   Кодеры, назначенные выбранному устройству VRM, анализируются, а их имена IQN добавляются к данному устройству iSCSI.
3. Нажмите  , чтобы сохранить настройки.
4. Нажмите  для активации конфигурации.

См.

- *Страница "Базовая конфигурация", Страница 202*
- *Диалоговое окно "Распределение нагрузки", Страница 204*
- *Диалоговое окно iqn-Mapper, Страница 207*
- *Форматирование LUN, Страница 206*

14.25.5 Страница "Базовая конфигурация"

Главное окно > **Устройства** > Разверните  > Разверните  > Разверните  > Нажмите  > Вкладка **Базовая конфигурация**

Отображаемые параметры могут зависеть от используемого типа системы хранения iSCSI.

Позволяет выполнить базовую настройку устройства iSCSI. На жестком диске iSCSI создаются и форматируются устройства LUN.

Отображается, только если устройство представляет собой систему хранения iSCSI, поддерживаемую Bosch, например DSA или DLS 1x00.

Замечание!
После базовой настройки серии E-Series для инициализации системы требуется много часов (или даже дней). На этом этапе полная производительность недоступна, а на этапе 1,5 возможен сбой форматирования.

Физическая емкость (ГБ)
Информация об общей емкости системы хранения.

Количество логических устройств
Можно изменить количество устройств LUN.

Замечание!
При изменении количества устройств LUN вся система iSCSI будет реорганизована, а все сохраненные в системе видеопоследовательности будут утрачены.
Поэтому прежде чем вносить изменения, проверьте записи и сделайте резервные копии всех важных видеопоследовательностей.

Емкость для новых логических устройств (ГБ)
Поскольку 256 - это максимальное количество LUN массива хранения, размер LUN не должен устанавливаться на слишком низкое значение. В противном случае в будущем при установке дополнительных полок дополнительные LUN не создаются.

Целевые свободные диски
Количество свободных дисков, которые пользователь хочет оставить в системе.

Фактическое кол-во свободных дисков
Количество свободных дисков, присутствующих в системе в настоящий момент. Это число может отличаться от указанного выше числа, например, если система хранения перенастроена вручную или часть дисков неисправна.

Состояние инициализации (%)
Дополнительные сведения отображаются при инициализации. По завершении инициализации (100 %) будет еще одна возможность удалить все устройства LUN.

RAID-DP (обеспечение надежности)
Активируйте этот параметр, если вы не хотите использовать указанный тип RAID — RAID-4, а предпочитаете использовать более надежный RAID-DP.

RAID 6 (приоритет надежности)
Выберите этот вариант, если вы не хотите использовать указанный тип RAID — RAID 5, а предпочитаете использовать более надежный RAID 6.

Дополнительная информация
Служит для отображения дополнительной информации, например, сведений о том, что система хранилища настроена неправильно и по этой причине настройка невозможна.

См.
– *Добавление устройства iSCSI DSA E-Series вручную, Страница 199*

14.25.6 Диалоговое окно "Распределение нагрузки"

Главное окно > **Устройства** > разверните > разверните > разверните > щелкните правой кнопкой мыши > команда **Балансировка нагрузки...** > диалоговое окно **Балансировка загрузки**

Предварительные условия: настройка режима записи **Автоматически**.

Установка верхних пределов допустимой скорости передачи и количества одновременных подключений iSCSI для каждой системы iSCSI. Если эти пределы превышены, данные перестают записываться в систему iSCSI и будут утеряны.

Для поддерживаемых систем (например, Bosch RAID, NetApp, DLA) используйте значения по умолчанию. В случае использования других устройств см. соответствующую документацию. Начинайте тестирование с малых значений.

14.25.7 Перемещение системы iSCSI в другой пул («Изменение пула...»)

Главное окно > **Устройства** > разверните > разверните > разверните >

Устройство можно переместить из одного пула в другой в пределах одного устройства VRM без потерь записи.

Для перемещения:

1. Щелкните правой кнопкой мыши / / и выберите команду **Изменить пул...**.
   Откроется диалоговое окно **Изменить пул**.
2. В списке **Новый пул:** выберите необходимый пул.
3. Нажмите **ОК**.
   Устройство перейдет к выбранному пулу.

14.25.8 Страница устройств LUN

Главное окно > **Устройства** > разверните > разверните > разверните > разверните >

Позволяет добавлять, удалять или форматировать устройства LUN, а также просматривать информацию об устройствах LUN.

Добавить

Нажмите для отображения диалогового окна **Добавить LUN**.

Удалить

Нажмите, чтобы удалить выбранные строки. Для выбора строки нажмите заголовок строки с левой стороны. Каждая строка представляет LUN.

Отображается окно сообщения.

Форматировать LUN

Нажмите для форматирования выбранного устройства LUN. Отображается окно сообщения.

Формат

Установите флажок, чтобы выбрать устройство LUN, и нажмите кнопку **Форматировать LUN**.

Логическое устройство
Отображает имя устройства LUN.

Размер [ГБ]
Отображает максимальную емкость устройства LUN.

Большой LUN
Каждая ячейка отображает, является ли это устройство LUN устройством больше 2 ТБ.

Состояние
Отображает состояние устройства LUN.

Ход выполнения
Отображает ход выполнения процесса форматирования.

См.
- *Страница "Пул", Страница 187*
- *Добавление устройства LUN, Страница 205*
- *Добавление устройств VRM путем поиска, Страница 177*

14.25.9 Добавление устройства LUN

Главное окно > **Устройства** > разверните  > разверните  > 
Обычно нужные устройства iSCSI с их получателями и номерами LUNs добавляются в результате сканирования сети автоматически. Если сканирование сети не приводит к нужным результатам или требуется настройка устройства iSCSI в автономном режиме перед его интегрированием в сеть, следует настроить получателя в устройстве iSCSI, а в этом получателе настроить один или несколько номеров LUN.
вы можете добавить устройства LUN больше 2 ТБ, если пул настроен для использования больших устройств LUN.
Устройства LUN больше 2 ТБ («большие устройства LUN») не поддерживаются следующими устройствами:
- Устройства VRM версии ниже 3.60
- Устройства VSG с версией микропрограммного обеспечения ниже 6.30
- Кодеры с версией микропрограммного обеспечения ниже 6.30

BVMSне позволяет выполнять следующие действия:
- Добавлять или перемещать устройства с версией микропрограммного обеспечения ниже 6.30 в пул, допускающий использование больших устройств LUN.
- Добавлять или перемещать устройства, которые в данный момент не подключены к сети, к пулу, допускающему использование больших устройств LUN.
- Добавлять или перемещать устройство iSCSI, содержащее большие устройства LUN, в пул, который не поддерживает использование больших устройств LUN.
- Разрешать использование больших устройств LUN в пуле, содержащем устройства с версией микропрограммного обеспечения ниже 6.30.
- Отключать использование больших устройств LUN в пуле с устройством iSCSI, содержащим большие устройства LUN.

Переместите устройства с версией микропрограммного обеспечения ниже 6.30 в пул, не поддерживающий большие устройства LUN.

Для добавления выполните следующие действия.
1. При необходимости выберите **Разрешить LUN более 2 ТБ**.
2. Щелкните 

правой кнопкой мыши и выберите **Сканировать целевой объект**.

Целевой объект  добавлен.

3. Выберите целевой объект.
   Отобразится страница **Устройства LUN**.
4. Нажмите **Добавить**.
   Откроется диалоговое окно **Добавить LUN**.
5. Введите нужный номер LUN и нажмите кнопку **OK**.
   Номер LUN будет добавлен в новой строке таблицы.
   Повторите эти действия для каждого выбранного LUN.

Примечания

– Чтобы удалить LUN, нажмите **Удалить**.
  Видеоданные не удаляются с этого LUN.
– Чтобы отформатировать LUN, нажмите **Форматировать LUN**.
  Все данные с этого LUN будут удалены!

Диалоговое окно Добавить LUN

Главное окно > **Устройства** > развернуть  > развернуть  > развернуть  > развернуть  >  > нажмите **Добавить**

Позволяет добавить LUN.

Id

Введите идентификатор требуемого LUN.

См.

– *Страница "Пул", Страница 187*
– *Страница устройств LUN, Страница 204*

14.25.10 Форматирование LUN

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  > 

Устройство LUN форматируется для подготовки к первому использованию.

Замечание!

После форматирования все данные на устройстве LUN удаляются.

Настройка

1. Выберите нужное устройство LUN и установите флажок в столбце **Формат**.
2. Нажмите **Форматировать LUN**.
3. Внимательно прочтите появившееся сообщение и подтвердите его.
   Выбранное устройство LUN будет отформатировано. Все данные с этого LUN будут удалены.

См.

– *Страница устройств LUN, Страница 204*

14.25.11 Диалоговое окно iqn-Mapper

Главное окно > **Устройства** > Разверните > Разверните > Разверните > Правой кнопкой мыши щелкните > **Сопоставить IQN**

Позволяет начать процесс сопоставления IQN.

См.

- *Добавление устройств VRM путем поиска, Страница 177*
- *Настройка устройства iSCSI, Страница 201*

14.26 Страница устройства Video Streaming Gateway

Главное окно > **Устройства** > Разверните > Разверните > Разверните >

В данном разделе содержится информация о настройке устройства VSG в системе.

Позволяет добавлять и настраивать следующие типы кодеров.

- Кодеры Bosch
- Кодеры ONVIF
- Кодеры JPEG
- Кодеры RTSP

Добавление устройств VSG путем поиска.

1. Щелкните правой кнопкой мыши и выберите команду **Поиск шлюзов Video Streaming Gateway**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые устройства VSG, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.
   В столбце **Состояние** успешные входы в систему обозначены значком .
   Неудачные попытки входа обозначены значком .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

При добавлении нового VSG версии 7.0 или выше флажок **Безопасное соединение** устанавливается по умолчанию.

Чтобы изменить безопасное или небезопасное соединение, используйте команду **Изменить шлюз Video Streaming Gateway** и установите или снимите флажок **Безопасное соединение**.

См.

- *Изменение шлюза Video Streaming Gateway, Страница 209*
- *Страница "ONVIF", Страница 245*

14.26.1 Добавление Video Streaming Gateway вручную

Главное окно > **Устройства** > Разверните  > 

Можно добавлять устройства VSG в пул VRM.

Для добавления устройства VSG вручную выполните следующие действия.

1. Щелкните правой кнопкой мыши  и щелкните **Добавить шлюз Video Streaming Gateway**.
   Откроется диалоговое окно **Добавить шлюз Video Streaming Gateway**.
2. Задайте необходимые параметры для устройства VSG.
3. Нажмите **Добавить**.

⇨ Устройство VSG будет добавлено в систему. Изображения с камер, назначенных этому устройству VSG, будут записываться.

Диалоговое окно Добавить шлюз Video Streaming Gateway

Щелкните правой кнопкой мыши  > **Добавить шлюз Video Streaming Gateway** > диалоговое окно **Добавить шлюз Video Streaming Gateway**

Имя

Введите необходимое отображаемое имя для устройства.

Имя пользователя

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

Сетевой адрес / порт

Введите IP-адрес устройства.

Если флажок **Безопасное соединение** установлен, порт автоматически меняется на порт HTTPS.

Можно изменить номер порта, если порты по умолчанию не используются или если экземпляры VSG настроены в другом порядке.

Порты по умолчанию

Экземпляр VSG	Порт RCPP	Порт HTTPS
1	8756	8443
2	8757	8444
3	8758	8445
4	8759	8446
5	8760	8447
6	8761	8448
7	8762	8449

Пароль

Введите действующий пароль для аутентификации на устройстве.

Show password
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Безопасность
По умолчанию флажок **Безопасное соединение** установлен, если поддерживается протокол HTTPS.
Начиная с VSG версии 7.0, VSG поддерживает безопасное соединение.

Замечание!
При переходе к версии BVMS 10.0 и выше флажок **Безопасное соединение** не установлен по умолчанию, а соединение не защищено (RCPP).

Чтобы изменить безопасное или небезопасное соединение, используйте команду **Изменить шлюз Video Streaming Gateway** и установите или снимите флажок **Безопасное соединение**.

Тест
Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

См.
– *Изменение шлюза Video Streaming Gateway, Страница 209*

14.26.2 Изменение шлюза Video Streaming Gateway

Главное окно > **Устройства** > Разверните > Разверните > Разверните > 

Чтобы изменить безопасное/небезопасное соединение:

1. Щелкните правой кнопкой мыши .
2. Нажмите **Изменить шлюз Video Streaming Gateway**.
   Откроется диалоговое окно **Изменить шлюз Video Streaming Gateway**.
3. Установите флажок **Безопасное соединение**.
   Используемый порт автоматически меняется на порт HTTPS.
   Или
   снимите флажок **Безопасное соединение**.
   Используемый порт автоматически меняется на порт RCPP.

Замечание!
После обновления до новой версии рекомендуется изменить включить безопасное соединение.

См.
– *Добавление Video Streaming Gateway вручную, Страница 208*

14.26.3 Добавление камеры в VSG

Главное окно > **Устройства** > Разверните > Разверните > Разверните >

В VSG можно добавить следующие устройства.

- Кодеры Bosch
- Камеры ONVIF
- Камеры JPEG
- Кодеры RTSP

После добавления кодеров VSG в автономном режиме можно обновить их состояние.

Порядок добавления:

1. Щелкните правой кнопкой мыши, наведите указатель на **Добавить кодер/камеру** и нажмите требуемую команду.
2. Задайте необходимые параметры в диалоговом окне для добавления устройства.
3. Нажмите **OK**.

Устройство добавляется.

Обновление:

- Щелкните правой кнопкой необходимый кодер и выберите **Обновить состояние**. Извлекаются свойства устройства.

См.

- *Диалоговое окно "Добавить кодер Bosch", Страница 210*
- *Диалоговое окно "Добавить кодер ONVIF", Страница 211*
- *Диалоговое окно "Добавить камеру JPEG", Страница 213*
- *Диалоговое окно "Добавить кодер RTSP", Страница 214*

14.26.4 Диалоговое окно "Добавить кодер Bosch"

Главное окно > **Устройства** > разверните > разверните > разверните >

щелкните правой кнопкой мыши > **Добавить кодер/камеру** > команда **Кодер Bosch**

Можно добавить кодер Bosch для устройства VSG.

Имя

Введите необходимое отображаемое имя для устройства.

Сетевой адрес

Введите сетевой адрес устройства.

Тип

Отображает определенный тип устройства, если он поддерживается.

Имя пользователя

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

Пароль

Введите действующий пароль для аутентификации на устройстве.

Show password
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Тест
Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

Свойства
Нажмите для включения необходимых функций, доступных для этого устройства.

Аудио	Выберите этот пункт, чтобы включить звук, если он доступен для этого устройства.
PTZ	Выберите этот пункт, чтобы включить режим PTZ, если он доступен для этого устройства.
Протокол камеры	TCP Используется для передачи в Интернете и (или) для передачи данных без потерь. Обеспечивает отсутствие потерь пакетов данных. Могут предъявляться высокие требования к полосе пропускания. Используйте, если устройство защищено брандмауэром. Не поддерживает многопотоковую передачу. UDP Используется при облегченной передачи данных без соединения в частных сетях. Пакеты данных могут теряться. Требования к пропускной способности могут быть низкими. Поддерживает многоадресную передачу.
Используйте видеовход 1 - **Используйте видеовход 4**	Нажмите для выбора видеовходов, если выполняется настройка многоканального устройства.

См.
– *Добавление камеры в VSG, Страница 210*

14.26.5 Диалоговое окно "Добавить кодер ONVIF"

Главное окно > **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > **Добавить кодер/камеру** > команда **Добавить кодер ONVIF**
или

Главное окно > **Устройства** > щелкните правой кнопкой мыши  > команда **Добавить кодер ONVIF**

Можно добавить кодер ONVIF к устройству VSG или как кодер, работающий только в режиме реального времени.
Необходимо настроить используемый профиль для видеозаписи и видео в режиме реального времени в таблице камер.

Начиная с версии BVMS 10.0 события кодера ONVIF можно получить непосредственно от VSG или кодера ONVIF. При добавлении нового кодера ONVIF флажок **Извлекать события ONVIF из VSG (Profile S, T)** устанавливается по умолчанию, а Profile T поддерживается.
Следующие возможности поддерживаются, только если кодер ONVIF добавлен в систему через устройство VSG:

– Если события кодера ONVIF извлекаются из VSG, настроенные по умолчанию события ONVIF уже сопоставлены.
– Оператор может включать и выключать реле в Operator Client.

Замечание!
Получение событий ONVIF из VSG доступно только начиная с VSG версии 7.0. При переходе на BVMS версии 10.0 существующие события кодера ONVIF извлекаются непосредственно из кодера ONVIF. Необходимо обновить VSG до версии 7.0.

Имя
Введите необходимое отображаемое имя для устройства.

Сетевой адрес
Введите сетевой адрес устройства. При необходимости измените номер порта.

Имя пользователя
Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

Пароль
Введите действующий пароль для аутентификации на устройстве.

Show password
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Тест
Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

Безопасное соединение
Можно активировать безопасное подключение для видео в режиме реального времени, передаваемого кодером ONVIF на ваше устройство VSG.

Примечание.
Если эта функция включена, пользователь Operator Client не может переключить поток на протокол UDP или многоадресный протокол UDP.
Когда эта функция включена, ANR не работает на подверженных устройствах.
При активации этой функции воспроизведение с помощью кодера в кодерах с микропрограммой до версии 6.30 не поддерживается.

Замечание!
Порт 443 выбран по умолчанию. Вы можете изменить номер порта в соответствии с настроенным портом HTTPS кодера.
Настроенный номер порта не будет сохранен.

Свойства

Тип устройства	Отображает полученный тип устройства.
Производитель	Отображает полученное название производителя.
Модель	Отображает полученное название модели.
Версия микропрограммы	Отображает полученную версию микропрограммного обеспечения.
Дополнительные команды	Если флажок установлен, вспомогательные команды поддерживаются.
Число входных видеоканалов	Введите необходимое количество видеовходов.
Число входных аудиоканалов	Введите необходимое количество аудиовходов.
Число тревожных входов	Введите необходимое количество тревожных входов.
Число реле	Введите необходимое количество реле.
Назначенные каналы шлюза	Введите необходимо количество каналов шлюза.
Протокол камеры	Выберите необходимый протокол камеры.
Использовать видеовход {0}	Установите флажок, чтобы использовать соответствующий видеовход.
Профиль ONVIF	Выберите профиль (если поддерживается), который нужно настроить.

Замечание!
Параметры **Настройки Video Streaming Gateway** недоступны для кодеров ONVIF, которые добавлены в качестве кодеров, работающих только в режиме реального времени.

См.

– *Добавление камеры в VSG, Страница 210*

14.26.6 Диалоговое окно "Добавить камеру JPEG"

Главное окно > **Устройства** > разверните > разверните > разверните > щелкните правой кнопкой мыши > **Добавить кодер/камеру** > команда **Камера JPEG**

Можно добавить камеру JPEG для устройства VSG.

Имя

Введите необходимое отображаемое имя для устройства.

URL

Введите URL-адрес камеры JPEG или камеры RTSP.
Для камеры JPEG производства Bosch введите следующую строку:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

Для камеры RTSP производства Bosch введите следующую строку:

`rtsp://<ip-address>/rtsp_tunnel`

Имя пользователя

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

Пароль

Введите действующий пароль для аутентификации на устройстве.

Show password

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Тест

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

Свойства

Число входных видеоканалов	Введите количество доступных видеовходов (если они есть).
Частота кадров [кадр/с]	Введите необходимую частоту кадров.

См.

– *Добавление камеры в VSG, Страница 210*

14.26.7 Диалоговое окно "Добавить кодер RTSP"

Главное окно > **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > **Добавить кодер/камеру** > команда **Камера RTSP**

Можно добавить кодер RTSP для устройства VSG.

Имя

Введите необходимое отображаемое имя для устройства.

URL

Введите URL-адрес камеры JPEG или камеры RTSP.

Для камеры JPEG производства Bosch введите следующую строку:

`http://<ip-address>/snap.jpg?jpegCam=<channel_no.>`

Для камеры RTSP производства Bosch введите следующую строку:

`rtsp://<ip-address>/rtsp_tunnel`

Имя пользователя

Введите имя пользователя, используемое для аутентификации на устройстве. Обычно: service

Пароль

Введите действующий пароль для аутентификации на устройстве.

Show password

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Тест

Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

Свойства

Число входных видеоканалов	Введите количество доступных видеовходов (если они есть).

См.

– *Добавление камеры в VSG, Страница 210*

14.26.8 Перемещение VSG в другой пул («Изменение пула»)

Главное окно > **Устройства** > разверните > разверните > > Устройство можно переместить из одного пула в другой в пределах одного устройства VRM без потерь записи.

Для перемещения:

1. Щелкните правой кнопкой мыши / / и выберите команду **Изменить пул...**.
   Откроется диалоговое окно **Изменить пул**.
2. В списке **Новый пул:** выберите необходимый пул.
3. Нажмите **ОК**.
   Устройство перейдет к выбранному пулу.

14.26.9 Настройка многоадресной передачи (вкладка «Многоадресная передача»)

Главное окно > **Устройства** > развернуть > развернуть > развернуть >

Для каждой камеры, назначенной устройству Video Streaming Gateway, можно настроить адрес многоадресной передачи и порт.

Порядок настройки многоадресной передачи:

1. Установите требуемый флажок для включения многоадресной передачи.
2. Введите правильный адрес многоадресной передачи и номер порта.
3. При необходимости настройте непрерывный поток многоадресной передачи.

Вкладка Многоадресная передача

Главное окно > **Устройства** > разверните > разверните > разверните >

> вкладка **Сеть** > вкладка **Многоадресная передача**

Позволяет настроить многоадресную передачу для назначенных камер.

Включить

Нажмите, чтобы активировать многоадресную передачу для данной камеры.

Адрес многопотоковой передачи

Вставьте допустимый адрес многоадресной передачи (в диапазоне от 224.0.0.0 до 239.255.255.255).

Введите `1.0.0.0`. Уникальный адрес многоадресной передачи вставляется автоматически в зависимости от MAC-адреса устройства.

Порт
Если используется брандмауэр, введите номер порта, который не блокируется в брандмауэре.

Поток
Нажмите, чтобы активировать непрерывную многоадресную потоковую передачу на коммутатор. Это означает, что многоадресному соединению не будет предшествовать регистрация RCP+. Кодер всегда будет передавать на коммутатор все данные. Коммутатор, в свою очередь (если не поддерживается или не настроена многоадресная фильтрация IGMP), будет передавать эти данные на все порты, то есть через коммутатор будет непрерывно проходить полный поток.
Потоковая передача необходима для получения многоадресного потока при использовании устройства другой компании (не Bosch).

14.26.10 Настройка ведения журналов (вкладка «Дополнительно»)

Главное окно > **Устройства** > Разверните  > Разверните  > Разверните  >  > Вкладка **Обслуживание** > Вкладка **Дополнительно**

Позволяет активировать регистрация для шлюза потокового видео.
Файлы журнала обычно хранятся в следующем каталоге:

```
C:\Program Files (x86)\Bosch\Video Streaming Gateway\log
```

Начиная с VSG версии 7.0 файлы журнала обычно хранятся в следующем каталоге:

```
C:\ProgramData\Bosch\VSG\log
```

Примечание. При обновлении до VSG 7.0 или более новой версии предыдущие файлы журнала автоматически перемещаются в этот каталог.
Файлы журнала старых версий VSG обычно хранятся в следующем каталоге:

```
C:\Program Files (x86)\Bosch\Video Streaming Gateway\log
```

Вкладка Дополнительно

Регистрация RCP+
Нажмите, чтобы включить функцию ведения журнала RCP+.

Регистрация данных отладки
Нажмите, чтобы включить функцию ведения журнала отладки.

Регистрация RTP
Нажмите, чтобы включить функцию ведения журнала RTP.

Срок хранения (в днях)
Выберите требуемое количество дней.

Полный дамп-файл памяти
Устанавливайте этот флажок только в случае необходимости, например, если в службе технической поддержки потребуют полную сводку состояния основной памяти.

Поддержка Telnet
Устанавливайте этот флажок, если требуется поддержка доступа по протоколу Telnet. Устанавливать только в случае необходимости.

Замечание!
Для интенсивной регистрации в журналах необходимы значительные ресурсы центрального процессора и емкость жесткого диска.
Не пользуйтесь интенсивной регистрацией постоянно.

14.26.11 Запуск ONVIF Camera Event Driver Tool из Configuration Client

Главное окно > **Устройства** > Разверните  > Разверните  > Разверните  >

ONVIF Camera Event Driver Tool для выбранного VSG можно запустить непосредственно из Configuration Client.
Примечание. Данный инструмент также можно запустить из меню «Пуск» Windows.
ONVIF Camera Event Driver Tool позволяет сопоставлять события ONVIF с событиями BVIP VSG. Можно подключаться к камерам ONVIF и извлекать события ONVIF для сопоставления.

Для запуска ONVIF Camera Event Driver Tool из Configuration Client:
1. Щелкните правой кнопкой мыши соответствующий VSG.
2. Нажмите **Запустите ONVIF Camera Event Driver Tool**.
   Отобразится ONVIF Camera Event Driver Tool.

Замечание!
ONVIF Camera Event Driver Tool поддерживает только безопасное подключение к VSG.

Для использования ONVIF Camera Event Driver Tool:
См. видео пояснения

14.27 Страница Режим реального времени и локальное хранилище

Главное окно > **Устройства** > разверните  > 
Позволяет добавлять и настраивать кодеры, работающие только в режиме реального времени. Вы можете добавить кодеры Bosch и сетевые видеопередатчики ONVIF.

Сведения о добавлении, изменении и настройке кодеров ONFIV, работающих только в режиме реального времени, см. в разделе *Страница "ONVIF", Страница 245*.

См.
- *Добавление кодера, работающего только в режиме реального времени, Страница 227*
- *Поиск устройств, Страница 76*
- *Страница «Кодер/декодер/камера Bosch», Страница 224*
- *Страница "ONVIF", Страница 245*
- *Настройка многоадресной передачи, Страница 243*

14.27.1 Добавление устройств, работающих только в режиме реального времени, путем поиска

Для добавления устройств Bosch, работающих только в реальном времени, путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши и выберите команду **Поиск кодеров, работающих только в реальном времени**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

   В столбце **Состояние** успешные входы в систему обозначены значком .

   Неудачные попытки входа обозначены значком .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

14.27.2 Добавление кодера вручную

Главное окно > **Устройства** > Развернуть > Развернуть > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Развернуть > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить декодер** > Диалоговое окно **Добавить кодер**
Позволяет добавить кодер вручную. Это особенно полезно, если необходимо добавить какое-либо IP-видеоустройство производства Bosch (только для VRM).

Внимание.
Если добавляется IP-видео кодер Bosch с выбранным параметром **<Автоопределение>**, это устройство должно быть доступно в сети.

Добавление IP-видеоустройства производства Bosch:

1. Разверните , разверните , щелкните правой кнопкой мыши .
   Или
   щелкните правой кнопкой мыши .
   Или
   щелкните правой кнопкой мыши .
2. Нажмите **Добавить кодер**.
   Откроется диалоговое окно **Добавить кодер**.
3. Введите соответствующий IP-адрес.
4. В списке выберите **<Автоопределение>**, введите пароль устройства и нажмите **Проверить подлинность.**
   Или
   В списке выберите конкретный тип кодера или **<Камера с одним заполнителем>**.
5. Нажмите **ОК**.
   Устройство добавляется в систему.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

Диалоговое окно Добавить кодер

Сетевой адрес
Введите действительный IP-адрес.

Тип кодера
Для устройства с известным типом выберите соответствующий элемент. Устройство не обязательно должно быть доступно в сети.
Если требуется добавить какое-либо IP-видеоустройство производства Bosch, выберите **<Автоопределение>**. Это устройство должно быть доступно в сети.
Если вы хотите добавить камеру для конфигурирования в автономном режиме, выберите **<Камера с одним заполнителем>**.

Имя пользователя
Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль
Введите действующий пароль для аутентификации на устройстве.

Отобразить пароль
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Проверить подлинность
Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

14.27.3 Предоставление пароля пункта назначения декодеру («Проверка подлинности...»)

Главное окно > **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Аутентификация...** > диалоговое окно **Введите пароль**
Для предоставления доступа к защищенному паролем кодеру для декодера необходимо ввести пароль уровня авторизации пользователя кодера в качестве пароля пункта назначения в декодере.

Предоставление.

1. В списке **Введите имя пользователя** выберите destination password.
2. В поле **Введите пароль для пользователя** введите новый пароль.
3. Нажмите **ОК**.

⇨ Пароль на устройстве изменяется незамедлительно.

См.

– *Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»), Страница 148*

14.28 Страница Локальное хранилище

Главное окно > **Устройства** > Развернуть  > 
Позволяет добавлять и настраивать кодеры с локальным хранилищем.

Для добавления кодеров локального хранилища путем поиска выполните следующие действия.

1. В дереве устройств щелкните  правой кнопкой мыши и выберите **Поиск кодеров локального хранилища**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

   В столбце **Состояние** успешные входы в систему обозначены значком  .

   Неудачные попытки входа обозначены значком  .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

См.
- *Настройка многоадресной передачи, Страница 243*
- *Добавление кодера локального хранилища, Страница 227*
- *Страница «Кодер/декодер/камера Bosch», Страница 224*
- *Поиск устройств, Страница 76*

14.29 Страница Unmanaged Site

Главное окно > **Устройства** > разверните  > 

Можно добавить сетевое видеоустройство в элемент **Unmanaged Sites** дерева устройств. Предполагается, что все unmanaged сетевые устройства unmanaged site находятся в одном часовом поясе.

Имя объекта

Отображает имя объекта, введенное во время создания этого элемента.

Описание

Введите описание этого объекта site.

Часовой пояс

Выберите соответствующий часовой пояс для этого unmanaged site.

См.
- *Unmanaged site, Страница 27*
- *Добавление объекта unmanaged site вручную, Страница 221*
- *Импорт unmanaged sites, Страница 221*
- *Настройка часового пояса, Страница 223*

14.29.1 Добавление объекта unmanaged site вручную

Главное окно > **Устройства** > 

Создание

1. Щелкните  правой кнопкой мыши и выберите пункт **Добавить Unmanaged Site**. Отображается диалоговое окно **Добавить Unmanaged Site**.
2. Введите имя и описание объекта.
3. В списке **Часовой пояс** выберите нужный элемент.
4. Нажмите **ОК**.
   В систему будет добавлен новый unmanaged site.

См.
- *Unmanaged site, Страница 27*
- *Страница Unmanaged Site, Страница 221*

14.29.2 Импорт unmanaged sites

Главное окно > **Устройства** > 

Вы можете импортировать файл CSV, содержащий конфигурацию видеорегистратора или другой системы BVMS, которую вы хотите импортировать в вашу систему BVMS как unmanaged site.

Импорт:

1. Щелкните  правой кнопкой мыши, а затем нажмите **Импорт Unmanaged Sites**.
2. Выберите нужный файл и нажмите кнопку **Открыть**.
   В систему будет добавлен один или несколько новых участков unmanaged site.
   Теперь можно добавить эти участки unmanaged sites в логическое дерево.
   Примечание. Если возникает ошибка и файл импортировать невозможно, появится соответствующее сообщение об ошибке.

14.29.3 Страница «Unmanaged Site»

Имя объекта

Отображает имя объекта, введенное во время создания этого элемента.

Описание

Введите описание этого объекта site.

Часовой пояс

Выберите соответствующий часовой пояс для этого unmanaged site.

14.29.4 Добавление unmanaged сетевого устройства

Главное окно > **Устройства** >  > 

1. Щелкните правой кнопкой мыши этот элемент и выберите команду **Добавить unmanaged сетевое устройство**.
   Откроется диалоговое окно **Добавить unmanaged сетевое устройство**.
2. Выберите необходимый тип устройства.
3. Введите допустимый IP-адрес или имя узла и учетные данные для этого устройства.
4. Нажмите **OK**.
   В систему будет добавлен новое **Unmanaged сетевое устройство**.
   Теперь можно добавить этот объект unmanaged site в логическое дерево.
   Обратите внимание, что в логическом дереве виден только объект, но не относящиеся к нему сетевые устройства.
5. Введите действующее имя пользователя для этого сетевого устройства при его наличии.
6. Введите действующий пароль, если есть.

Диалоговое окно Добавить unmanaged сетевое устройство

главное окно > **Устройства** > развернуть  > щелкните правой кнопкой мыши  > нажмите **Добавить unmanaged сетевое устройство**

Тип устройства:

Выберите запись, применимую для данного устройства.

Доступные записи:

- **DIVAR AN / DVR**
- **DIVAR IP (AiO), BVMS**
- **IP-камера/кодер Bosch**

Сетевой адрес:

Введите IP-адрес или имя узла. При необходимости измените номер порта.

Примечание: при использовании подключения SSH введите адрес в следующем формате:

ssh://IP или servername:5322

Безопасность
Флажок **Безопасное соединение** установлен по умолчанию.

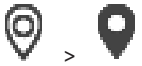
Замечание!
При добавлении цифрового видеорегистратора с установленным флажком **Безопасное соединение**, подключения команд и управления защищены. Потоковая передача видеоданных не защищена.

Имя пользователя:
Введите действующее имя пользователя для этого сетевого устройства при его наличии. Подробную информацию см. в разделе *Unmanaged site, Страница 27*.

Пароль:
Введите действующий пароль при наличии. Сведения об учетных данных пользователя см. в разделе *Unmanaged site, Страница 27*.

См.
– *Unmanaged site, Страница 27*

14.29.5 Настройка часового пояса

Главное окно > **Устройства** > разверните > 
Вы можете настроить часовой пояс unmanaged site. Это полезно, когда пользователь Operator Client имеет намерение получить доступ к unmanaged site с помощью компьютера с Operator Client, расположенного в другом часовом поясе, чем этот unmanaged site.

Чтобы настроить часовой пояс:
- в списке **Часовой пояс** выберите нужный элемент.

См.
– *Страница Unmanaged Site, Страница 221*

15 Страница «Кодер/декодер/камера Bosch»

В данном разделе содержится информация о настройке кодеров и декодеров в системе.

Замечание!
BVMS Viewer не поддерживает устройства декодирования.

Подробные сведения о параметрах кодера, декодера или камеры (например, Video Content Analysis (VCA)) или о параметрах сети см. в руководстве по соответствующему устройству.
Количество элементов под записью отображается в квадратных скобках.

Для настройки кодера выполните следующие действия.

Главное окно > **Устройства** > Развернуть > Развернуть > >

или

Главное окно > **Устройства** > Развернуть > Развернуть > Развернуть >

или

Главное окно > **Устройства** > >

или

Главное окно > **Устройства** > >

Для настройки декодера выполните следующие действия.

Главное окно > **Устройства** > Развернуть > Развернуть > >

Дополнительные сведения о страницах см. в интерактивной справке.

Для настройки камеры:

Главное окно > **Устройства** > Развернуть > Развернуть > > >

Главное окно > **Устройства** > Развернуть > Развернуть > > > >

или

Главное окно > **Устройства** > Развернуть > Развернуть > Развернуть > > >

или

Главное окно > **Устройства** > > > >

или

Главное окно > **Устройства** > > > >

– Нажмите  для сохранения настроек.

– Нажмите  для отмены последней настройки.

– Нажмите  для активации конфигурации.

Большинство параметров на страницах кодера / декодера / камеры вступают в силу сразу же после нажатия  . При переходе на другую вкладку без нажатия  после внесения изменений отображаются два окна сообщений. Для сохранения изменений следует подтвердить изменения в обоих окнах.

Чтобы изменить пароли кодера, щелкните правой кнопкой мыши значок устройства и выберите команду **Изменить пароль...**.

Чтобы открыть устройство в веб-браузере, щелкните значок устройства правой кнопкой мыши и выберите команду **Показать страницу в браузере**.

Примечание.

В зависимости от выбранного кодера или камеры не все описанные здесь страницы будут доступны для каждого устройства. Используемые здесь формулировки, описывающие названия полей, зависят от используемого вами программного обеспечения.

- Щелкните вкладку для перехода к соответствующей странице свойств.

Добавление кодеров путем поиска:

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**. Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.
   В столбце **Состояние** успешные входы в систему обозначены значком  .
   Неудачные попытки входа обозначены значком  .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

См.

– *Поиск устройств, Страница 76*

15.1 Добавление кодера вручную

Главное окно > **Устройства** > Развернуть > Развернуть > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить кодер** > Диалоговое окно **Добавить кодер**
или

Главное окно > **Устройства** > Развернуть > Щелкнуть правой кнопкой мыши > Щелкнуть **Добавить декодер** > Диалоговое окно **Добавить кодер**
Позволяет добавить кодер вручную. Это особенно полезно, если необходимо добавить какое-либо IP-видеоустройство производства Bosch (только для VRM).

Внимание.
Если добавляется IP-видео кодер Bosch с выбранным параметром **<Автоопределение>**, это устройство должно быть доступно в сети.

Добавление IP-видеоустройства производства Bosch:

1. Разверните , разверните , щелкните правой кнопкой мыши .
   Или
   щелкните правой кнопкой мыши .
   Или
   щелкните правой кнопкой мыши .
2. Нажмите **Добавить кодер**.
   Откроется диалоговое окно **Добавить кодер**.
3. Введите соответствующий IP-адрес.
4. В списке выберите **<Автоопределение>**, введите пароль устройства и нажмите **Проверить подлинность.**
   Или
   В списке выберите конкретный тип кодера или **<Камера с одним заполнителем>**.
5. Нажмите **ОК**.
   Устройство добавляется в систему.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

Диалоговое окно Добавить кодер
Сетевой адрес
Введите действительный IP-адрес.

Тип кодера
Для устройства с известным типом выберите соответствующий элемент. Устройство не обязательно должно быть доступно в сети.
Если требуется добавить какое-либо IP-видеоустройство производства Bosch, выберите **<Автоопределение>**. Это устройство должно быть доступно в сети.
Если вы хотите добавить камеру для конфигурирования в автономном режиме, выберите **<Камера с одним заполнителем>**.

Имя пользователя
Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль
Введите действующий пароль для аутентификации на устройстве.

Отобразить пароль
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Проверить подлинность
Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

15.2 Добавление кодера в пул VRM

Сведения о добавлении кодеров в пул VRM см. в разделе *Добавление кодеров путем поиска, Страница 185*.

См.
– *Добавление устройства, Страница 129*

15.3 Добавление кодера, работающего только в режиме реального времени

Сведения о добавлении кодера, работающего только в режиме реального времени, путем поиска см. в разделе *Добавление устройств, работающих только в режиме реального времени, путем поиска, Страница 218*.

См.
– *Добавление устройства, Страница 129*
– *Страница Режим реального времени и локальное хранилище, Страница 217*

15.4 Добавление кодера локального хранилища

Сведения о добавлении кодеров локального хранилища путем поиска см. в разделе *Страница Локальное хранилище, Страница 220*.

См.
– *Добавление устройства, Страница 129*
– *Страница Локальное хранилище, Страница 220*

15.5 Добавление одной камеры-заполнителя

Если необходимо добавить и настроить камеру, которая в данный момент находится в автономном режиме, можно вместо этого добавить одну камеру-заполнитель. Вы можете добавить одну камеру-заполнитель в логическое дерево, в карты и настроить события и тревоги.

Для добавления одной камеры-заполнителя:

1. Щелкните правой кнопкой мыши дерево устройств, в котором необходимо добавить камеру-заполнитель.
2. Нажмите **Добавить кодер**.
   Откроется диалоговое окно **Добавить кодер**.
3. Введите соответствующий IP-адрес, который в данный момент находится оффлайн.
4. Выберите тип кодера **<Камера с одним заполнителем>**.
5. Настройте все необходимые параметры для камеры-заполнителя.

Для замены одной камеры-заполнителя:

1. Щелкните правой кнопкой мыши соответствующую камеру-заполнитель.
2. Нажмите **Изменить кодер**.
   Откроется диалоговое окно **Изменить кодер**.
3. Введите сетевой адрес новой камеры.
4. Введите правильный пароль для новой камеры.
5. Нажмите **OK**.
   Откроется диалоговое окно **Обновление имен устройств**.
6. Нажмите **OK**.

Примечание: если возможности устройства новой камеры актуальны, необходимо проверить настройки, которые вы сделали в таблице камер и записей.

15.6 Импорт камер из файла CSV

Главное окно > **Устройства** > разверните  > разверните 

Из файла CSV можно импортировать большее количество камер. Можно указать имена кодеров или камер, узлы логического дерева и группы пользователей, у которых есть доступ к добавленным камерам.

CSV шаблон

Шаблон MassConfigurationTemplate.csv можно использовать в: C:\Program Files\Bosch\VMS\Samples.

Примечание. Используйте запятую в качестве разделителя столбцов файла CSV.

Столбец	Информация
NetworkAddress	IP-адрес кодера. Поле не может быть пустым, а его значение не может дублироваться.
EncoderName	Название кодера. Поле значения не может быть пустым.
CameraNames	Имена камер текущего кодера. Поле значения не может быть пустым. Разделяйте имена камер точкой с запятой.
UseName	Имя пользователя для аутентификации на кодере. Поле может быть пустым.

Столбец	**Информация**
Password	Пароль для аутентификации на кодере. Поле может быть пустым.
LogicalTree	Пути к части логического дерева, в которую вы добавляете камеры. Разделяйте пути точкой с запятой. Если поле значения пусто, камеры не добавлены в логическое дерево, и назначить группы пользователей невозможно. Пути логического дерева начинаются с "/". Знак "/" обязательно использовать только для корневого узла, для других папок это необязательно. Имя корневого узла можно не добавлять в путь папки. Если путь не существует, он будет создан.
Permissions	Группы пользователей с разрешением на доступ. Разделяйте группы пользователей точкой с запятой. Если поле значения пусто, доступ к камерам разрешен для всех групп. У группы администраторов есть разрешение на доступ ко всем камерам. Даже если доступ не предоставляется ни одной группе, необходимо добавить группу администраторов. Если группа пользователей не существует, камера не будет импортирована. **Примечание.** Enterprise User Groups не поддерживаются, только Enterprise Accounts.

Примеры:
NetworkAddress,EncoderName,CameraNames,UseName,Password,LogicalTree,Permissions
1.1.1.1,Encoder1,Camera1,service,pwd,/Folder1/Folder2;/Folder3,Admin Group
2.2.2.2,Multichannel2,Camera21;Camera22,service,pwd,/Folder1/Folder2,Admin Group;Operator

Перед запуском импорта необходимо предоставить следующие разрешения:
- **Изменение свойств устройства**
- **Изменение логического дерева**
- **Настройка групп пользователей/Enterprise Accounts**

Примечание. Пользователь-администратор может выполнить импорт в любом случае.

Импорт камер из файла CSV:

1. Щелкните правой кнопкой мыши  , затем нажмите **Импортировать камеры из файла CSV...**.
   Откроется проводник.
2. Выберите нужный файл CSV и нажмите **Открыть**.
   Примечание. Обработка файла CSV может занять некоторое время. Можно импортировать до 250 камер.

3. В диалоговом окне **Импортировать камеры из файла CSV** отображается вся необходимая информация об импорте камер.
   Чтобы просмотреть невыполненные процессы импорта камер, нажмите **Только функции дисплея**.
4. Чтобы закрыть диалоговое окно, нажмите **Закрыть**. Чтобы экспортировать и сохранить файл журнала, нажмите **Экспортировать журнал**.

15.7 Редактирование кодера

15.7.1 Шифрование видео в режиме реального времени («Изменение кодера»)

Главное окно > **Устройства** > разверните  > разверните  > разверните  > нажмите  > диалоговое окно **Изменить кодер**

Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > диалоговое окно **Изменить кодер**

Главное окно > **Устройства** > разверните  > нажмите  > диалоговое окно **Изменить кодер**

Вы можете активировать защищенное подключенное для видео в реальном времени, передаваемого с кодера следующим устройствам, если на кодере настроен порт HTTPS 443:

- Компьютер с Operator Client
- Компьютер с Management Server
- Компьютер с Configuration Client
- Компьютер с VRM
- Декодер

Примечание.
Когда эта функция включена, ANR не работает на данных устройствах.
При активации этой функции воспроизведение с помощью кодера в кодерах с микропрограммой до версии 6.30 не поддерживается.
Защищенный протокол UDP поддерживаются только кодерами с версией микропрограммного обеспечения 7.0 или выше. Если в этом случае включено безопасное соединение, пользователь Operator Client может переключиться поток на UDP и на multicast UDP.

Для активации выполните следующие действия:

1. Установите флажок **Безопасное соединение**.
2. Нажмите **ОК**.
   Для этого кодера включено безопасное соединение.

См.

- *Настройка многоадресной передачи, Страница 243*
- *Диалоговое окно «Изменить кодер / Изменить декодер», Страница 231*

15.7.2 Обновление возможностей устройства («Изменение кодера»)

Главное окно **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или
Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или
Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или
Главное окно > **Устройства** > Развернуть  > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Изменить декодер** > Диалоговое окно **Изменить декодер**

После замены устройства можно обновить его функциональные возможности. Текст сообщения информирует о том, соответствуют ли полученные возможности устройства возможностям, сохраненным в BVMS.

Для обновления:

1. Нажмите кнопку **ОК**.
   Отображается окно сообщения со следующим текстом:
   Если применить данные возможности устройства, могут измениться настройки записи и событий для данного устройства. Проверьте эти настройки.

2. Нажмите кнопку **ОК**.
   Выполняется обновление возможностей устройства.

См.

– *Диалоговое окно «Изменить кодер / Изменить декодер», Страница 231*

15.7.3 Диалоговое окно «Изменить кодер / Изменить декодер»

Главное окно **Устройства** > разверните  > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или
Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**
или
Главное окно > **Устройства** > разверните  > щелкните правой кнопкой мыши  > нажмите **Изменить кодер** > диалоговое окно **Изменить кодер**

или

Главное окно > **Устройства** > Развернуть  > Развернуть  > Щелкнуть правой кнопкой мыши  > Щелкнуть **Изменить декодер** > Диалоговое окно **Изменить декодер**

Позволяет проверить и обновить возможности устройства. Устройство подключается при открытии этого диалогового окна. Запрашивается пароль, и возможности устройства сравниваются с возможностями устройства, сохраненными вBVMS.

Имя

Отображает имя устройства. При добавлении IP-видеоустройства производства Bosch имя устройства генерируется системой. При необходимости измените значение.

Сетевой адрес

Введите сетевой адрес устройства. При необходимости измените номер порта.

Имя пользователя

Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль

Введите действующий пароль для аутентификации на устройстве.

Отобразить пароль

Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

Проверить подлинность

Нажмите для аутентификации на устройстве с использованием введенных выше учетных данных.

Безопасность

Флажок **Безопасное соединение** установлен по умолчанию.
Если безопасное подключение невозможно, отображается соответствующее сообщение.
Нажмите, чтобы снять флажок.

Следующие декодеры поддерживают безопасное соединение:

- VJD 7000
- VJD 8000
- VIP XD HD

Замечание!

Соединение между декодером и кодером безопасно, только если они настроены с использованием безопасного соединения.

Поток видео

UDP: обеспечивает зашифрованную многоадресную потоковую передачу для поддерживаемых устройств декодирования.
TCP: обеспечивает зашифрованную одноадресную потоковую передачу для поддерживаемых устройств декодирования.
Примечание: если для кодера не настроен адрес многоадресной передачи, декодер извлекает поток через одноадресную передачу.

Замечание!
BVMS не поддерживает камеры Bosch, подключенные к VSG.
BVMS поддерживает только шифрование UDP для платформ старше CPP13.

Возможности устройства
Отображаемые возможности устройства можно упорядочивать по категориям или по алфавиту.
Текст сообщения информирует о том, соответствуют ли автоматически определенные возможности устройства возможностям данного устройства.
Нажмите **ОК** для применения изменений возможностей устройства после обновления устройства.

См.
- *Шифрование видео в режиме реального времени («Изменение кодера»), Страница 230*
- *Обновление возможностей устройства («Изменение кодера»), Страница 231*

15.8 Управление проверкой подлинности

Для активации проверки подлинности на кодере необходимо выполнить следующие действия:
- настройте проверку подлинности на кодере.
- загрузить сертификат кодера.
- установить этот сертификат кодера на рабочую станцию, используемую для проверки подлинности.

См.
- *Проверка подлинности , Страница 233*

15.8.1 Проверка подлинности

Пользователь клиента Operator Client может проверить подлинность записей.
Подлинность экспортов проверяется автоматически.
Администратору следует выполнить следующие действия для обеспечения непрерывности цепочки сертификатов. Для крупных систем (> 30 камер) рекомендуется выполнить следующие действия:
- Разрешить сертифицирующему органу (CA) создать сертификат для каждого кодера.
- Загрузить созданный сертификат (включая закрытый ключ) надежным способом на каждом кодере.
- Установить сертификат на Operator Client рабочих станций, где требуется выполнить проверку подлинности.

Для небольших систем (< 30 камер) рекомендуется выполнить следующие действия:
- Загрузить сертификат `сервера HTTPS` от каждого кодера.
- Установить эти сертификаты на Operator Client рабочих станций, где требуется выполнить проверку подлинности.

За подробной информацией обратитесь в службу IT-поддержки вашей компании.
Для активации надежной проверки подлинности администратор должен выполнить следующие действия:
- Активировать проверку подлинности на каждой выбранной камере.
- Для крупных систем: загрузить и назначить соответствующий сертификат для каждой выбранной камеры.

– Для небольших систем: загрузить сертификат от каждого кодера. Установить сертификаты, позволяющие выполнять проверку на рабочей станции.

Ограничения

Требуется версия микропрограммного обеспечения 6.30 или более поздней версии.
Не рекомендуется выполнять проверку подлинности более 4 камер одновременно.
Пользователь Operator Client не может проверить подлинность видеоизображения в реальном времени.
Примечание: не следует осуществлять замену сертификата, когда выполняется запись. Если необходимо изменить сертификат, сначала остановите запись, затем измените сертификат и запустите запись еще раз.
Для проверки подлинности записи эта запись будет воспроизводиться в фоновом режиме с максимальной скоростью. В сетях с низкой пропускной способностью воспроизведение может быть замедленным. В этом случае продолжительность проверки может быть равна продолжительности выбранного отрезка записи. Пример: выбран период времени, равный 1 часу. Процесс проверки может длиться до 1 часа.
Пользователь может проверить лишь факт подлинности записи. Если процесс проверки подлинности завершился неудачей, это не всегда означает, что видео было изменено. Неудача может быть вызвана множеством причин, например, удалением вручную.
Пользователь Operator Client не может отличить намеренное изменение видео от мошеннического изменения.
Проверка подлинности связана только с методами проверки подлинности видео. Проверка подлинности видео никаким образом не связана с передачей видео или данных.
Функция водяного знака для проверки подлинности в более ранних версиях BVMS заменена. Новая проверка подлинности автоматически становится доступной после обновления до самой последней версии BVMS. Проверки подлинности, успешно проведенные в прошлом, теперь не могут быть подтверждены, так как эти записи не содержат необходимой расширенной информации.
Проверка подлинности не поддерживается в следующих случаях:
– Транскодирование
– Локальная запись
– VSG
– Цифровой видеорегистратор
– Bosch Recording Station
– ANR

См.

– *Настройка проверки подлинности, Страница 234*
– *Отправка сертификата, Страница 235*
– *Загрузка сертификата, Страница 235*
– *Установка сертификатов на рабочей станции, Страница 236*

15.8.2 Настройка проверки подлинности

Главное окно > **Устройства** > разверните  > разверните  > разверните  >

или

Главное окно > **Устройства** > разверните  > 

Вы можете активировать проверку подлинности для кодера.

Настройка

1. Нажмите **Камера**, затем нажмите **Видеовход**.
2. В списке **Проверка подлинности видео** выберите пункт **SHA-256**.
3. В списке **интервалы подписи** выберите необходимое значение.
   Небольшое значение повышает степень защиты, большое значение снижает нагрузку кодера.
4. Нажмите .

15.8.3 Отправка сертификата

Главное окно > **Устройства** > разверните > разверните > разверните >

или

Главное окно > **Устройства** > разверните >

Вы можете отправить производный сертификат на кодер.

Для отправки:

1. нажмите **Обслуживание**, затем **Сертификаты**.
2. Нажмите **Отправка сертификата**.
3. Выберите соответствующий файл с сертификатом для данного кодера. Этот файл должен содержать закрытый ключ, например, *.pem.
   Убедитесь, что передача данных защищена.
4. Нажмите **Открыть**.
5. В списке**Использование** выберите **HTTPS-сервер**, чтобы назначить отправленный сертификат элементу **HTTPS-сервера**.
6. Нажмите .

15.8.4 Загрузка сертификата

Главное окно > **Устройства** > разверните > разверните > разверните >

или

Главное окно > **Устройства** > разверните >

Вы можете загрузить сертификат с кодера.

Для загрузки:

1. нажмите **Обслуживание**, затем **Сертификаты**.
2. Выберите требуемый сертификат и нажмите значок `Save`.
3. Выберите соответствующий каталог для сохранения файла сертификата.
4. Переименуйте расширение файла сертификата на `*.cer`.

Теперь можно установить этот сертификат на рабочей станции, на которой необходимо проверить подлинность.

15.8.5 Установка сертификатов на рабочей станции

Можно установить сертификат, загруженный с кодера, на рабочую станцию, на которой требуется выполнить проверку подлинности.

1. Запустите `Microsoft Management Console` на рабочей станции.
2. Добавьте `Сертификаты`в отправку на данном компьютере с выбранным параметром `Учетная запись компьютера`.
3. Разверните `Сертификаты (локальный компьютер)`, разверните `Доверенный корневой орган сертификации`.
4. Щелкните правой кнопкой мыши `Сертификаты`, поместите указатель мыши на `Все задачи` и нажмите`Импорт...`.
   Отобразится `Мастер импорта сертификатов`.
   Параметр `локального компьютера` является выбранным заранее, и его нельзя изменить.
5. Нажмите `Далее`.
6. Выберите файл сертификата, который вы загрузили с кодера.
7. Нажмите `Далее`.
8. Оставьте параметры без изменений и нажмите кнопку `Далее`.
9. Оставьте параметры без изменений и нажмите кнопку `Завершить`.

15.9 Предоставление пароля пункта назначения декодеру («Проверка подлинности...»)

Главное окно > **Устройства** > разверните  > разверните  > щелкните правой кнопкой мыши  > нажмите **Аутентификация...** > диалоговое окно **Введите пароль**

Для предоставления доступа к защищенному паролем кодеру для декодера необходимо ввести пароль уровня авторизации пользователя кодера в качестве пароля пункта назначения в декодере.

Предоставление.

1. В списке **Введите имя пользователя** выберите destination password.
2. В поле **Введите пароль для пользователя** введите новый пароль.
3. Нажмите **ОК**.

⇨ Пароль на устройстве изменяется незамедлительно.

См.

– *Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»), Страница 236*

15.10 Изменение пароля кодера и декодера («Изменить пароль»/«Введите пароль»)

Главное окно > **Устройства** > Развернуть  > Развернуть  >  > 

или

Главное окно > **Устройства** >  > 

или

Главное окно > **Устройства** >  > 

или

Главное окно > **Устройства** > разверните > разверните >

Определите или измените отдельный пароль для каждого уровня. Введите пароль (не более 19 символов; без специальных символов) для выбранного уровня.

Для изменения пароля выполните следующие действия.

1. щелкните правой кнопкой мыши и нажмите **Изменить пароль...**.
   Откроется диалоговое окно **Введите пароль**.
2. Из списка **Введите имя пользователя** выберите пользователя, для которого необходимо изменить пароль.
3. В поле **Введите пароль для пользователя** введите новый пароль.
4. Нажмите **ОК**.

⇨ Пароль на устройстве изменится незамедлительно.

Пароль препятствует несанкционированному доступу к устройству. Для ограничения доступа могут быть использованы различные уровни авторизации.
Надлежащая защита паролем обеспечивается только в тех случаях, когда все более высокие уровни авторизации также защищены паролем. Таким образом, всегда следует начинать с самого высокого уровня авторизации при назначении паролей.
Можно задать и изменить пароль для каждого уровня авторизации, если вы вошли в учетную запись пользователя «service».
Устройство имеет три уровня авторизации: service, user и live.

– service представляет собой высший уровень авторизации. Ввод правильного пароля дает доступ ко всем функциям и позволяет изменять все параметры конфигурации.
– user представляет собой средний уровень авторизации. На этом уровне можно эксплуатировать устройство, воспроизводить записи и управлять камерой, однако невозможно изменять конфигурацию.
– live представляет собой низший уровень авторизации. На этом уровне можно только просматривать видеоизображения в реальном времени и переключаться между различными экранами изображений в реальном времени.

Для декодера уровень авторизации live заменяется следующим уровнем авторизации:

– destination password (доступно только для декодеров)
  Используется для доступа к кодеру.

См.

– *Предоставление пароля пункта назначения декодеру («Проверка подлинности...»), Страница 236*

15.11 Перемещение кодера в другой пул («Изменение пула»)

Главное окно > **Устройства** > Разверните > Разверните > >

Главное окно > **Устройства** > разверните > разверните > разверните > развернite

Главное окно > **Устройства** > Разверните > Разверните > Разверните >

Устройство можно переместить из одного пула в другой в пределах одного устройства VRM без потерь записи.

Для перемещения:

1. Щелкните правой кнопкой мыши / / и выберите команду **Изменить пул...**.
   Откроется диалоговое окно **Изменить пул**.
2. В списке **Новый пул:** выберите необходимый пул.
3. Нажмите **OK**.
   Устройство перейдет к выбранному пулу.

Диалоговое окно Изменить пул

Позволяет изменить назначенный устройству пул.

Текущий пул:

Отображает номер пула, к которому в данный момент соотносится выбранное устройство.

Новый пул:

Выберите требуемый номер пула.

15.12 Восстановление записей с замененного кодера (диалоговое окно «Связать с записями предшествующего устройства»)

Главное окно > **Устройства** > разверните > разверните > >

В случае замены неисправного кодера записи замененного кодера будут доступны на новом кодере при выборе нового кодера в Operator Client.

Замечание!

Кодер может быть заменен только на кодер с тем же количеством каналов.

Для восстановления записей с замененного кодера

Замечание!

Не используйте команду **Изменить кодер**.

1. Щелкните правой кнопкой мыши по > команде **Связать с записями предшественника...**.
2. Отображается диалоговое окно **Связать с записями предшественника...**.
3. Введите сетевой адрес и действительный пароль для нового устройства.
4. Нажмите **OK**.
5. Нажмите , чтобы сохранить настройки.
6. Нажмите для активации конфигурации.

Диалоговое окно Связать с записями предшественника...
Позволяет восстановить записи с замененного кодера. После настройки параметров в диалоговом окне записи замененного кодера доступны для нового кодера при выборе нового кодера в Operator Client.

Сетевой адрес / порт
Введите сетевой адрес устройства.

Имя пользователя
Отображает имя пользователя, используемое для аутентификации на устройстве.

Пароль
Введите действующий пароль для аутентификации на устройстве.

Проверить подлинность
Нажмите для проверки подлинности на устройстве с использованием введенных выше учетных данных.

15.13 Настройка кодеров/декодеров

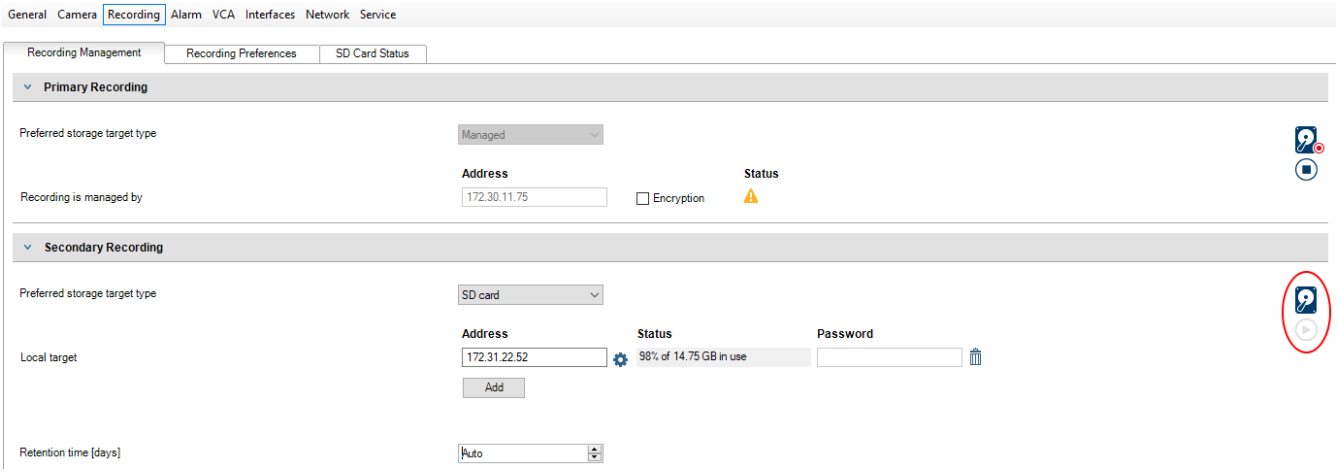
15.13.1 Настройка носителей данных кодера

Главное окно > **Устройства** > разверните > разверните > > > **Дополнительные параметры** > **Управление записями**

Примечание. Убедитесь, что требуемые камеры этого кодера добавлены в Логическое дерево.

Для использования функции ANR необходимо настроить носитель данных кодера.

Примечание. Если необходимо настроить носитель данных кодера, который уже добавлен в систему и записан с помощью VRM, убедитесь, что остановлена вторичная запись:



Функция ANR работает только на кодерах с версией микропрограммного обеспечения 5.90 и выше. Не все типы кодеров поддерживают ANR, даже если установлена верная версия микропрограммного обеспечения.

Настройка носителя данных кодера

1. В разделе **Вторичная запись** в списке **Предпочитаемый тип целевого хранилища** выберите носитель данных. В зависимости от типа устройства будут доступны разные носители.

2. При необходимости нажмите кнопку ..., чтобы отформатировать носитель данных. После успешного форматирования носитель данных будет готов к использованию с функцией ANR.
3. Настройте функцию ANR для этого кодера на странице **Камеры и запись**.

См.
- *Страница "Управление записью", Страница 242*
- *Настройка функции ANR, Страница 314*

15.13.2 Настройка нескольких кодеров / декодеров

Главное окно

Вы можете одновременно изменить следующие свойства нескольких кодеров и декодеров:
- Пароли устройств
- IP-адреса
- Краткие имена
- Маска подсети
- Идентификатор шлюза
- Версии микропрограмм

Чтобы выбрать несколько устройств:

▸ Выберите нужные устройства, нажав клавишу CTRL или SHIFT.

Чтобы выбрать все доступные устройства:

▸ Нажмите команду **Выделить все**.

Чтобы изменить пароль для нескольких устройств:

1. В главном окне **Устройства** нажмите команду **Изменить пароли устройств**.
   Или
   в меню **Аппаратное обеспечение** нажмите **Изменить пароли устройств...**
   Откроется диалоговое окно **Изменить пароли устройств**.
2. Выберите требуемые устройства.
3. Щелкните правой кнопкой мыши выбранные устройства.
4. Нажмите **Изменить пароль...**. Откроется диалоговое окно **Изменение паролей**.
5. Установите необходимые параметры.

Замечание!
Вы можете выбрать только те типы паролей, которые доступны для всех выбранных устройств.

Чтобы настроить несколько кратких имен:

1. В меню **Аппаратное обеспечение** нажмите **Изменить IP-адрес устройства и сетевые параметры...**.
   Отображается диалоговое окно **Изменить IP-адрес и сетевые параметры устройства**.
2. Выберите требуемые устройства.

3. Щелкните правой кнопкой мыши выбранные устройства.
4. Нажмите **Задать краткие имена...**.
   Отображается диалоговое окно **Задать краткие имена**.
5. Установите необходимые параметры.

Чтобы настроить несколько IP-адресов:

Замечание!
Изменение IP-адреса может сделать IP-устройство недоступным.

1. В меню **Аппаратное обеспечение** нажмите **Изменить IP-адрес устройства и сетевые параметры...**.
   Отображается диалоговое окно **Изменить IP-адрес и сетевые параметры устройства**.
2. Выберите требуемые устройства.
3. Щелкните правой кнопкой мыши выбранные устройства.
4. Нажмите **Задать IP-адреса...**.
   Откроется диалоговое окно **Установить IP-адреса**.
5. Установите необходимые параметры.

Чтобы изменить маску подсети/идентификатор шлюза для нескольких устройств:

1. Нажмите нужную поле одного из устройств, значение которого требуется изменить.
2. Введите соответствующее значение.
3. Выберите все требуемые устройства.
4. Щелкните правой кнопкой мыши нужное поле устройства, значение которого вы уже изменили.
5. Выберите команду и команду **Копировать ячейку в** и команду **Выделение в столбце** .
   Или нажмите команду **Заполнить столбец,** если это необходимо.

Замечание!
Вы можете также скопировать полные строки для изменения IP-адресов, кратких имен, масок подсети и идентификаторов шлюза для нескольких устройств.

Чтобы обновить микропрограммы для нескольких устройств:

1. В меню **Аппаратное обеспечение** выберите пункт **Обновить микропрограмму устройства...**.
   Отображается диалоговое окно **Обновить микропрограмму устройства**.
2. Выберите требуемые устройства.
3. Нажмите команду **Обновить микропрограмму**.
4. Выберите файл с обновлением.
5. Нажмите **OK**.

Результат операции
Отображает соответствующее состояние затрагиваемых устройств.

15.13.3 Настройка резервного режима записи на кодере

Главное окно > **Устройства** > Развернуть  > Развернуть  >  > 

требования: на странице **Пул** в списке **Режим настроек записи**выберите**При отказе**.

Если выбран **Автоматически** режим, параметры настраиваются автоматически, и изменить их нельзя.

Если вы хотите использовать вторичный целевой объект как для автоматического, так и для резервного режима: на странице **Пул** в списке **Использование вторичной цели** выберите**Вкл.**.

Рекомендуется настроить хотя бы два устройства iSCSI для резервного режима.

Для настройки:

1. Нажмите **Дополнительные параметры**.
2. Нажмите **Очередность записи**.
3. В разделе **Главная цель** выберите запись для нужного объекта. Все системы хранения, введенные на вкладке **Хранение**, будут перечислены в списке.
4. В разделе **Второстепенная цель** выберите запись для нужного объекта. Все системы хранения, указанные в разделе **Хранение**, отображаются в списке.
   Изменения вступают в силу немедленно. Активация не требуется.

Дополнительная информация

– *Настройка автоматического режима записи в пуле, Страница 188*

15.13.4 Страница "Управление записью"

Активные записи обозначаются значком  .

Наведите курсор на значок. Откроется окно с подробной информацией об активных записях.

Записи, управляемые вручную

Управление записями на данном кодере осуществляется локально. Все необходимые параметры настраиваются вручную. Кодер или IP-камера действует как устройство только в режиме реального времени. Его нельзя удалять из VRM автоматически.

Запись 1 управляется диспетчером VRM

Управление записями кодера осуществляется системой VRM.

Двойной VRM

Запись 2 данного кодера управляется вторичным VRM.

Вкладка Носитель iSCSI

Нажмите, чтобы отобразить доступные хранилища iSCSI, подключенные к данному кодеру.

Вкладка Локальный носитель

Нажмите, чтобы отобразить доступное локальное хранилище на данном кодере.

Добавить

Нажмите, чтобы добавить устройство хранения в список управляемых носителей данных.

Удалить

Нажмите, чтобы удалить устройство хранения из данного списка управляемых носителей данных.

См.

– *Настройка носителей данных кодера, Страница 239*

15.13.5 Страница "Параметры записи"

Страница **Параметры записи** отображается для каждого кодера. Эта страница появляется только в том случае, если устройство добавлено в систему VRM.

Главная цель

Отображается, только если список **Режим настроек записи** на странице **Пул** настроен как **При отказе**.

Выберите запись для необходимого целевого объекта.

Второстепенная цель

Отображается, только если список **Режим настроек записи** на странице **Пул** настроен как **При отказе** и если список **Использование второстепенной цели** настроен как **Вкл**.

Выберите запись для необходимого целевого объекта для настройки резервного режима.

См.

– *Страница "Пул", Страница 187*

15.14 Настройка многоадресной передачи

Для каждой назначенной камеры можно настроить адрес многоадресной передачи и порт.

Порядок настройки многоадресной передачи:

1. Установите требуемый флажок для включения многоадресной передачи.
2. Введите правильный адрес многоадресной передачи и номер порта.
3. При необходимости настройте непрерывный поток многоадресной передачи.

Вкладка Многоадресная передача

Главное окно > **Устройства** >  > 

или

Главное окно > **Устройства** >  > 

или

Главное окно > **Устройства** > Развернуть  > Развернуть  >  > 

> вкладка **Сеть** > вкладка **Многоадресная передача**

Позволяет настроить многоадресную передачу для назначенных камер.

Включить

Нажмите, чтобы активировать многоадресную передачу для данной камеры.

Адрес многопотоковой передачи

Вставьте допустимый адрес многоадресной передачи (в диапазоне от 224.0.0.0 до 239.255.255.255).

Введите `1.0.0.0`. Уникальный адрес многоадресной передачи вставляется автоматически в зависимости от MAC-адреса устройства.

Порт

Если используется брандмауэр, введите номер порта, который не блокируется в брандмауэре.

Поток

Нажмите, чтобы активировать непрерывную многоадресную потоковую передачу на коммутатор. Это означает, что многоадресному соединению не будет предшествовать регистрация RCP+. Кодер всегда будет передавать на коммутатор все данные. Коммутатор, в свою очередь (если не поддерживается или не настроена многоадресная фильтрация IGMP), будет передавать эти данные на все порты, то есть через коммутатор будет непрерывно проходить полный поток.
Потоковая передача необходима для получения многоадресного потока при использовании устройства другой компании (не Bosch).

Замечание!
Многоадресные потоки могут быть защищены, только если в кодере установлена микропрограмма версии 7.0 или более поздней и установлен флажок **Безопасное соединение**.

См.

– *Шифрование видео в режиме реального времени («Изменение кодера»), Страница 230*

16 Страница "ONVIF"

Главное окно > **Устройства** > разверните >
или

Главное окно > **Устройства** > разверните > разверните > разверните > разверните >

См.
- *Страница устройства Video Streaming Gateway, Страница 207*
- *Страница Режим реального времени и локальное хранилище, Страница 217*

16.1 Добавление устройства ONVIF, работающего только в режиме реального времени, путем сканирования

Для добавления устройств ONVIF, работающих только в реальном времени:

1. Щелкните правой кнопкой мыши, затем щелкните **Поиск кодеров ONVIF, работающих только в реальном времени**.
   Отображается диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**. Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.
   В столбце **Состояние** успешные входы в систему обозначены значком .
   Неудачные попытки входа обозначены значком .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

16.2 Страница "Кодер ONVIF"

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Кодер ONVIF**
или

Главное окно > **Устройства** > разверните > > вкладка **Кодер ONVIF**
Отображает сведения о кодере ONVIF, работающем только в режиме реального времени, добавленном к BVMS.

Имя
Отображает имя устройства ONVIF. Его можно переименовать непосредственно в дереве устройств.

Сетевой адрес
Отображает IP-адрес устройства.

Производитель
Отображает название производителя.

Модель
Отображает название модели.

Видеовходы
Введите количество камер, подключенных к этому кодеру.

Аудиовходы
Введите количество аудиовходов, подключенных к этому кодеру.

Тревожные входы
Введите количество тревожных входов, подключенных к этому кодеру.

Реле
Введите количество реле, подключенных к этому кодеру.

См.
- *Страница "События кодера ONVIF", Страница 246*
- *Добавление кодера, работающего только в режиме реального времени, Страница 227*
- *Настройка таблицы сопоставления ONVIF, Страница 250*

16.3 Страница "События кодера ONVIF"

Начиная с версии BVMS 10.0 события кодера ONVIF можно получить непосредственно от VSG или кодера ONVIF. При добавлении нового кодера ONVIF флажок **Извлекать события ONVIF из VSG (Profile S, T)** устанавливается по умолчанию, а Profile T поддерживается.
Следующие возможности поддерживаются, только если кодер ONVIF добавлен в систему через устройство VSG:
- Если события кодера ONVIF извлекаются из VSG, настроенные по умолчанию события ONVIF уже сопоставлены.
- Оператор может включать и выключать реле в Operator Client.

Замечание!
Получение событий ONVIF из VSG доступно только начиная с VSG версии 7.0. При переходе на BVMS версии 10.0 существующие события кодера ONVIF извлекаются непосредственно из кодера ONVIF. Необходимо обновить VSG до версии 7.0.

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **События кодера ONVIF**
или
Главное окно > **Устройства** > разверните > > вкладка **События кодера ONVIF**

Если события кодера ONVIF извлекаются непосредственно из кодера ONVIF, вам необходимо сопоставить события ONVIF с событиями BVMS. За счет этого в дальнейшем можно настраивать события ONVIF как тревоги BVMS.

Замечание!
Если события кодера ONVIF извлекаются из VSG, события ONVIF по умолчанию уже сопоставлены.

Таблица сопоставлений
Можно создать или изменить таблицу сопоставления.

Нажмите  , чтобы открыть диалоговое окно **Добавление таблицы сопоставлений**.

Нажмите  для отображения диалогового окна **Изменение имени таблицы сопоставлений**.

Нажмите  , чтобы удалить таблицу сопоставления и все входящие в нее строки.

Нажмите  или  , чтобы импортировать или экспортировать таблицу сопоставления ONVIF.

События и тревоги
Выберите событие BVMS для сопоставления с событием ONVIF.

Добавить строку
Нажмите, чтобы добавить строку в таблицу сопоставления.
Если доступно несколько строк, событие происходит, когда верно условие в одной строке.

Удалить строку
Нажмите, чтобы удалить выбранную строку из таблицы сопоставления.

Тема ONVIF
Введите или выберите текстовую строку, например:

```
tns1:VideoAnalytics/tnsaxis:MotionDetection
```

Имя данных ONVIF
Введите или выберите текстовую строку.

Тип данных ONVIF
Введите или выберите текстовую строку.

Значение данных ONVIF
Введите или выберите текстовую строку или число.

Если события ONVIF извлекаются из VSG, по умолчанию сопоставлены следующие события с VSG:

- **Глобальное изменение — обнаружено**
- **Глобальное изменение — не обнаружено**
- **Обнаружение движения** - **Обнаружено движение**
- **Обнаружение движения** - **Движение остановлено**
- **Проверка контрольного изображения** - **Настройки отменены**

- **Проверка контрольного изображения** - **Настроено**
- **Потеря видеоизображения** - **Видеосигнал утерян**
- **Потеря видеоизображения** - **Видеосигнал в порядке**
- **Потеря видеоизображения** - **Состояние видеосигнала неизвестно**
- **Видеосигнал слишком размытый — Видеосигнал в порядке**
- **Видеосигнал слишком размытый — Видеосигнал не в порядке**
- **Видеосигнал слишком яркий** - **Видеосигнал в порядке**
- **Видеосигнал слишком яркий** - **Видеосигнал не в порядке**
- **Видеосигнал слишком темный** - **Видеосигнал в порядке**
- **Видеосигнал слишком темный** - **Видеосигнал не в порядке**
- **Видеосигнал с большими помехами** - **Видеосигнал в порядке Видеосигнал не в порядке**
- **Состояние реле** - **Реле открыто**
- **Состояние реле** - **Реле закрыто**
- **Состояние реле** - **Ошибка реле**
- **Состояние входа** - **Вход открыт**
- **Состояние входа** - **Вход закрыт**
- **Состояние входа** - **Ошибка ввода**

См.
- *Запуск ONVIF Camera Event Driver Tool из Configuration Client, Страница 217*
- *Сопоставление событий ONVIF, Страница 42*
- *Настройка таблицы сопоставления ONVIF, Страница 250*

16.3.1 Добавление и удаление профиля ONVIF

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **События кодера ONVIF**

или

Главное окно > **Устройства** > разверните > > вкладка **События кодера ONVIF**

Можно добавить, удалить или изменить профили ONVIF для выбранного кодера.

Добавление:
1. Нажмите кнопку **Добавить...**.
2. В диалоговом окне **Добавить профиль** введите название нового профиля.
3. Нажмите кнопку **Далее >**.
4. В следующем диалоговом окне выберите нужную камеру.
5. Нажмите кнопку **Далее >**.
6. В следующем диалоговом окне выберите нужный профиль кодера не для записи.
7. Нажмите кнопку **Сохранить**.
   Новый профиль будет сохранен.
   Параметры этого профиля заполняются значениями из выбранного профиля кодера. При необходимости можно изменить эти значения.

Удаление:
- Выберите профиль в списке и нажмите кнопку **Удалить**.

Изменение:
1. Выберите профиль в списке.

2. Измените необходимые параметры.

16.3.2 Экспорт файла таблицы сопоставления ONVIF

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF**
или

Главное окно > **Устройства** > разверните  >  > вкладка **События кодера ONVIF**

Можно экспортировать таблицу сопоставления ONVIF в виде файла (файл-OMF). Таблица сопоставления сохраняется для выбранной модели кодера.

Экспорт:

1. Нажмите  .
2. Введите имя файла и нажмите кнопку **Сохранить**.
   Таблица сопоставления ONVIF экспортируется как OMF-файл для выбранной модели кодера.

См.

– *Страница "События кодера ONVIF", Страница 246*

16.3.3 Импорт файла таблицы сопоставления ONVIF

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF**
или

Главное окно > **Устройства** > разверните  >  > вкладка **События кодера ONVIF**

Можно импортировать таблицу сопоставления ONVIF в виде файла (OMF-файл).
Выпущенные файлы сопоставления ONVIF хранятся в следующем каталоге Configuration Client:

– `%programdata%\Bosch\VMS\ONVIF`

Если уже импортирована таблица сопоставления с таким же именем, выводится сообщение об ошибке.
Если импортирована более новая версия этого файла, выводится предупреждение.
Нажмите кнопку **ОК**, если нужно импортировать этот файл. В противном случае нажмите кнопку **Отмена**.

Импорт:

1. Нажмите  .
2. Выберите нужный файл и нажмите кнопку **Открыть**.
   Откроется диалоговое окно **Импорт таблицы сопоставлений**.
3. Настройте необходимые параметры.
4. Нажмите **ОК**.

Диалоговое окно Импорт таблицы сопоставлений

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF** > 
или

Главное окно > **Устройства** > разверните  >  > вкладка **События кодера ONVIF** > 

Производитель
Отображает имя производителя, для которого действует эта таблица сопоставления.

Модель
Отображает имя модели, для которой действует эта таблица сопоставления.

Описание
Отображает дополнительные сведения: например, протестированные модели камер.

Имя таблицы сопоставления
Отображает имя таблицы сопоставления. Измените это имя, если оно уже используется в BVMS.
Можно выбрать один из следующих параметров, чтобы указать, к каким кодерам ONVIF следует применить таблицу сопоставления.

Применить только к выбранному кодеру ONVIF

Применить ко всем кодерам ONVIF перечисленных моделей

Применить ко всем кодерам ONVIF данного производителя
Существующее сопоставление событий ONVIF продолжает действовать. Нельзя импортировать OMT-файлы из более ранних версий BVMS.

16.3.4 Настройка таблицы сопоставления ONVIF

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF**
или

Главное окно > **Устройства** > разверните  >  > вкладка **События кодера ONVIF**
Таблицы сопоставления настраиваются для сопоставления событий ONVIF с событиями BVMS.
Таблица сопоставления настраивается для всех кодеров ONVIF одной модели или всех кодеров ONVIF одного производителя.

Нажмите  , чтобы обновить кодеры ONVIF, добавленные в автономном режиме, и настроить для них сопоставление событий уже добавленного кодера ONVIF того же производителя или с тем же названием модели.
Для многоканальных кодеров можно настроить источники событий, например определенную камеру или реле.

Создание таблицы сопоставления:

1. Нажмите  .
   Отображается диалоговое окно **Добавление таблицы сопоставлений**.
2. Введите имя для таблицы сопоставления.
3. При необходимости в списках **Производитель** и **Модель** выберите записи.
   Если вы выбрали **<нет>** в обоих списках, сопоставление событий действительно только для данного устройства.
   Если вы выбрали **<нет>** в списке **Модель** и название производителя в списке **Производитель**, сопоставление событий действительно для всех устройств одного и того же производителя.
   Если вы выбрали доступные записи в обоих списках, сопоставление событий действительно для всех устройств одного и того же производителя и одной и той же модели.
4. Нажмите кнопку **ОК**.
   Теперь можно отредактировать таблицу сопоставления, например добавить строку к событию **Обнаружено движение**.

Изменение таблицы сопоставления:

1. Нажмите  .
   Отображается диалоговое окно **Изменение имени таблицы сопоставлений**.
2. Измените необходимые записи.

Добавление и удаление сопоставлений событий:

1. В списке **Таблица сопоставлений** выберите необходимое имя.
2. Добавление строки: нажмите **Добавить строку**.
3. В строке выберите необходимые записи.
   Если доступно несколько строк, событие создается, когда верно условие только в одной строке.
4. Удаление строки: нажмите **Удалить строку**.

Удаление таблицы сопоставления:

1. В списке **Таблица сопоставлений** нажмите имя сопоставлений событий, которые необходимо удалить.
2. Нажмите  .

Настройка источника событий:

1. Разверните  и нажмите  ,  или  .
2. Перейдите на вкладку **Источник событий ONVIF**.
3. В столбце **Активирующее событие** включите событие, настроенное в данной строке.
4. Выберите необходимые определения события.

Диалоговое окно «Добавить/переименовать таблицу сопоставления ONVIF»

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **События кодера ONVIF** >  или 
или

Главное окно > **Устройства** > разверните > > вкладка **События кодера ONVIF** > или

Позволяет добавить таблицу сопоставления. Если эта таблица сопоставления будет использоваться как шаблон для следующих кодеров ONVIF того же производителя и такой же модели, выберите соответствующие записи.

Имя таблицы сопоставления
Введите удобное имя.

Производитель
При необходимости выберите запись.

Модель
При необходимости выберите запись.

См.
- *Включение журнала для событий ONVIF, Страница 392*
- *Сопоставление событий ONVIF, Страница 42*
- *Страница "События кодера ONVIF", Страница 246*
- *Страница "Источник событий ONVIF", Страница 266*

16.4 Страница конфигурации ONVIF

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF**
или

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF**
Можно выбрать несколько кодеров ONVIF и изменить настройки на странице **Профиль видеокодера**. Измененные настройки действуют для всех выбранных устройств.
Эта страница доступна только для кодеров ONVIF.

Замечание!
Ограничения для конфигурации ONVIF
Параметры, настраиваемые на этих страницах, могут не реализовываться правильно, так как они не поддерживаются вашей камерой. Поддерживаемые камеры ONVIF были протестированы только с параметрами по умолчанию.

16.4.1 Доступ к устройству

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Доступ к устройству**
или

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Доступ к устройству**

Производитель
Отображает название производителя выбранного кодера.

Модель
Отображает название модели выбранного кодера.
Примечание. Если вы хотите экспортировать какие-либо сопоставления событий в файл сопоставления ONVIF, выберите имя этой модели как имя файла.

ID аппаратного обеспечения
Отображает идентификатор оборудования выбранного кодера.

Версия ПО
Отображает версию микропрограммного обеспечения выбранного кодера.
Примечание. По списку совместимости с BVMS убедитесь, что используется правильная версия микропрограммы.

Серийный номер
Отображает серийный номер выбранного кодера.

MAC-адрес
Отображает MAC-адрес выбранного кодера.

Версия ONVIF
Отображает версию ONVIF выбранного кодера.
Для BVMS требуется версия ONVIF 2.0.

16.4.2 Дата / время

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Дата/Время**
или
Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Дата/Время**

Часовой пояс
Выберите часовой пояс, в котором находится система.
Если в вашей системе или сети функционируют несколько устройств, необходимо осуществить их внутреннюю синхронизацию. Например, идентификация и правильная оценка одновременных записей возможна только в том случае, если часы всех устройств синхронизированы.

1. Введите текущую дату. Поскольку время устройства управляется внутренними часами, нет необходимости вводить день недели — он будет добавлен автоматически.
2. Введите текущее время или нажмите **Синхр. ПК**, чтобы применить системное время вашего компьютера к устройству.

Примечание
Важно, чтобы дата и время при записи были выставлены правильно. Неверная установка параметров даты и времени может привести к неправильному функционированию записи.

16.4.3 Управление пользователями

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Управление пользователями**
или

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Управление пользователями**

Эти пользовательские параметры используются для сторонних приложений, таких как прямой доступ к кодерам через веб-клиент.

Для доступа через сторонние приложения поддерживаются следующие роли пользователей:

- **Анонимный**: у этой роли есть неограниченный доступ только к устройствам, на которых не зарегистрированы пользователи с другими ролями (**Пользователь**, **Оператор**, **Администратор**). Если на устройстве есть хотя бы один из указанных выше пользователей, анонимный пользователь имеет право только смотреть параметры времени.
- **Администратор**(не поддерживается клиентом Configuration Client): у этой роли есть доступ ко всем разделам и функциям приложения, права для перезагрузки устройства, сброса настроек и обновления микропрограммы, а также полномочия создавать других пользователей с различными правами доступа.

Первый созданный на устройстве пользователь должен быть **Администратор**.

Различия в правах доступа оператора и пользователя по умолчанию (роли **Оператор** и **Пользователь**) см. в следующей таблице.

Раздел конфигурации или функция ONVIF	Оператор	Пользователь
Идентификация	ПРОСМОТР	СКРЫТО
Параметры времени	ПРОСМОТР	ПРОСМОТР
Параметры сети	ПРОСМОТР	ПРОСМОТР
Пользователи	СКРЫТО	СКРЫТО
Параметры реле	ИЗМЕНЕНИЕ	ПРОСМОТР
Видеоизображение в реальном времени (включая связь RTSP)	ИЗМЕНЕНИЕ	ИЗМЕНЕНИЕ
Потоковая передача видео	ИЗМЕНЕНИЕ	ПРОСМОТР
Профили	ИЗМЕНЕНИЕ	ПРОСМОТР

ИЗМЕНЕНИЕ: изменение текущих и создание новых параметров.
ПРОСМОТР: параметры не скрыты, но изменять и создавать их нельзя.
СКРЫТО: некоторые параметры или даже целые разделы скрыты.

Пользователи

Список доступных пользователей устройства.

Пароль

Введите действующий пароль.

Подтверждение пароля
Подтвердите введенный пароль.

Роль
Выберите требуемую роль для выбранного пользователя. Права доступа изменяются соответствующим образом.

16.4.4 Страница "Профиль видеокодера"

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль видеокодера**
или
Главное окно > **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль видеокодера**
Профили достаточно сложны и включают ряд взаимодействующих друг с другом параметров, поэтому, как правило, рекомендуется использовать предустановленные профили. Изменение профиля допускается только в том случае, если вы полностью ознакомились со всеми параметрами конфигурации.

Профили
Выберите нужное имя.

Замечание!
Настроенные здесь профили можно выбирать в клиенте Configuration Client.

В главном окне последовательно нажмите **Камеры и запись** и  или  .
Параметр по умолчанию <Automatic> можно изменить на один из перечисленных и настроенных профилей
Примечание. Обратите внимание, что при активном использовании нескольких профилей на одном устройстве применяются некоторые ограничения производительности; при перегрузке камера может автоматически ограничить качество потока.

Имя
Здесь можно ввести новое имя для профиля. Это имя будет отображаться в списке доступных профилей в поле «Активный профиль».

Кодирование
Выберите необходимый кодек.

Разрешение
Здесь можно выбрать необходимое разрешение для видеоизображения.

Качество
Этот параметр позволяет уменьшить нагрузку на канал, снизив разрешение изображения. Этот параметр задается с помощью ползунка: самое левое положение соответствует максимальному разрешению, самое правое — минимальной нагрузке на видеоканал.

Ограничение по частоте кадров
Частота кадров (кадров в секунду) указывает, какое количество кадров в секунду записывается видеокамерой, подключенной к устройству. Этот параметр отображается только для информации.
Если указан интервал кодирования, итоговая частота кадров после кодирования уменьшается на заданный коэффициент.

Ограничение скорости передачи
Чем меньше скорость передачи данных, тем меньше конечный размер видеофайла. При значительном снижении скорости передачи данных программе придется использовать более сильные алгоритмы сжатия, из-за чего снижается качество видеоизображения. Выберите максимальную выходную скорость передачи данных в кбит/сек. Эта максимальная скорость передачи не превышается ни при каких обстоятельствах. В зависимости от настроек качества видеоизображения для I-кадров и P-кадров это может привести к пропуску отдельных изображений.
Введенное здесь значение должно быть по крайней мере на 10 % больше, чем стандартная целевая скорость передачи данных.

Интервал кодировки
Интервал кодирования (количество кадров) обозначает частоту, с которой кодируются кадры, поступающие из камеры. Например, если интервал кодирования составляет 25, это означает, что 1 кадр из 25, записанных в секунду, кодируется и передается пользователю. Максимальное значение снижает нагрузку на канал, но может привести к пропуску информации от некодированных кадров. Уменьшение интервала кодирования увеличивает частоту обновлений изображения, а также нагрузку на канал.

Длина группы видеокадров
Длину группы видеокадров можно изменить, только если используется кодер H.264 или H.265. Этот параметр обозначает длину группы изображений между двумя ключевыми кадрами. Чем выше это значение, тем меньше нагрузка на сеть, но тем ниже и качество видео.
Значение 1 означает, что I-кадры генерируются непрерывно. Значение 2 означает, что каждое второе изображение является I-кадром, 3 — что только каждое третье и т. д. Кадры между ними кодируются как P-кадры или B-кадры.

Истекло время таймаута
Истекло время ожидания сеанса RTSP для соответствующего потока видеоданных. Время ожидания сеанса предоставляется как подсказка для поддержания сеанса RTSP устройством.

Многоадресная передача - IP-адрес
Для работы в режиме многоадресной передачи (дублирование потоков данных в сети) введите правильный адрес многоадресной передачи.

При установке параметра в значение 0.0.0.0 кодер соответствующего потока работает в режиме много-/одноадресной передачи (копирование потоков данных в устройстве). Камера поддерживает много-/одноадресные соединения для пяти одновременно подключенных приемников.

Копирование данных существенно загружает ЦП и при определенных условиях может приводить к ухудшению качества изображения.

Многоадресная передача - Порт
Выберите порт назначения многоадресной передачи RTP. Устройство может поддерживать RTCP. В этом случае значение порта должно быть четным, чтобы обеспечить сопоставление соответствующего потока RTCP со следующим более высоким номером порта назначения (нечетным), как указано в спецификации RTSP.

Многоадресная передача — TTL
Вы можете ввести значение для указания того, в течение какого времени пакеты для многоадресной передачи будут активны в сети. Если многоадресная передача осуществляется через маршрутизатор, это значение должно быть больше единицы.

Замечание!
Многоадресная передача возможна только при использовании протокола UDP.
Протокол TCP не поддерживает многоадресные соединения.
Если устройство защищено брандмауэром, то в качестве протокола передачи выберите протокол TCP (порт HTTP). Для работы в локальной сети выберите UDP.

16.4.5 Профиль аудиокодера

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль аудиокодера**
или
Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Профиль аудиокодера**
Профили достаточно сложны и включают ряд взаимодействующих друг с другом параметров, поэтому, как правило, рекомендуется использовать предустановленные профили. Изменение профиля допускается только в том случае, если вы полностью ознакомились со всеми параметрами конфигурации.

Кодирование
Выберите необходимое кодирование для аудиоисточника при наличии:
- **G.711 [ITU-T G.711]**
- **G.726 [ITU-T G.726]**
- **AAC [ISO 14493-3]**

Скорость передачи данных
Выберите необходимую скорость передачи данных звуковых сигналов, например 64 кбит/сек.

Частота дискретизации
Введите частоту дискретизации на выходе в кГц, например 8 кбит/сек.

Истекло время таймаута
Истекло время ожидания сеанса RTSP для соответствующего потока аудиоданных. Время ожидания сеанса предоставляется как подсказка для поддержания сеанса RTSP устройством.

16.4.6 Обработка изображений, общие данные

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Обработка изображений, общие данные**

или

Главное окно > **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Камера** > вкладка **Обработка изображений, общие данные**

Яркость

Настройте яркость изображения в соответствии с условиями эксплуатации.

Насыщенность цвета

Откорректируйте насыщенность цвета, чтобы обеспечить максимально реалистичную цветопередачу на мониторе.

Контраст

Можно настроить контрастность видеоизображения в соответствии с вашими условиями эксплуатации.

Резкость

Откорректируйте резкость изображения.

При низком значении изображение становится менее резким. При повышении резкости отображается больше деталей. Повышение резкости может улучшить детализацию номерных знаков, черт лица и краев некоторых поверхностей, но это может увеличить требования к полосе пропускания.

Отключение ИК-фильтра

Выберите состояние ИК-фильтра.

Состояние АВТО позволяет алгоритму экспозиции принимать решение о моменте переключения ИК-фильтра.

16.4.7 Компенсация фоновой засветки

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Компенс. фоновой засветки**

или

Главное окно > **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Компенс. фоновой засветки**

В зависимости от модели устройства здесь можно настроить параметры компенсации фоновой засветки.

Режим

Выберите пункт **Выключено**, чтобы выключить компенсацию фоновой засветки.

Выберите пункт **Включено**, чтобы обеспечить детализацию в условиях высокого контраста и очень большой разницы между яркими и темными участками.

Уровень

Введите или выберите необходимое значение.

16.4.8 Экспозиция

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Экспозиция**
или

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Экспозиция**
В зависимости от модели устройства здесь можно настроить параметры экспозиции.

Режим
Выберите **Авто**, чтобы включить алгоритм экспозиции на устройстве. Алгоритм использует значения в следующих полях:
- **Приоритет**
- **Окно**
- **Мин. время экспозиции**
- **Макс. время экспозиции**
- **Мин. усиление**
- **Макс. усиление**
- **Мин. диафрагма**

Выберите **Вручную**, чтобы отключить алгоритм экспозиции на устройстве. Алгоритм использует значения в следующих полях:
- **Время экспозиции**
- **Усиление**
- **Диафрагма**

Приоритет
Настройте режим приоритета экспозиции (низкое отношение шум/частота кадров).

Окно
Определите прямоугольную маску экспозиции.

Мин. время экспозиции
Настройте минимальную продолжительность экспозиции [мкс].

Макс. время экспозиции
Настройте максимальную продолжительность экспозиции [мкс].

Мин. усиление
Настройте минимальный диапазон усиления датчика [дБ].

Макс. усиление
Настройте максимальный диапазон усиления датчика [дБ].

Мин. диафрагма
Настройте минимальное затухание падающего света за счет диафрагмы [дБ]. 0 дБ соответствует полностью открытой диафрагме.

Макс. диафрагма
Настройте максимальное затухание падающего света за счет диафрагмы [дБ]. 0 дБ соответствует полностью открытой диафрагме.

Время экспозиции
Задайте время фиксированной экспозиции [мкс].

Усиление

Настройте фиксированное усиление [дБ].

Диафрагма
Настройте фиксированное затухание падающего света за счет диафрагмы [дБ]. 0 дБ соответствует полностью открытой диафрагме.

16.4.9 Фокусировка

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Фокус**
или

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Фокус**

В зависимости от модели устройства здесь можно настроить параметры фокусировки. На этой странице можно перемещать объектив в абсолютных и относительных координатах, а также непрерывно. Корректировка фокусного расстояния с помощью этой функции отключает автофокус. Устройство с поддержкой удаленного управления фокусировкой обычно поддерживает управление через эту операцию перемещения. Положение фокуса отображается определенным числовым значением. Возможны следующие состояния фокуса:

ПЕРЕМЕЩЕНИЕ
ОК
НЕИЗВЕСТНО
Кроме того, могут отображаться сведения об ошибке, например ошибка позиционирования, о которой сообщает оборудование.

Режим
Выберите **Авто**, чтобы включить автоматическую фокусировку объектива в любой момент в соответствии с объектами в сцене. Алгоритм использует значения в следующих полях:

- **Ближний предел**
- **Дальний предел**

Выберите **Вручную**, чтобы вручную регулировать фокусировку. Алгоритм использует значения в следующих полях:

- **Скорость по умолчанию**

Скорость по умолчанию
Настройте скорость перемещения фокуса по умолчанию (если нет параметра скорости).

Дальний предел
Настройте ближний предел фокусировки объектива [м].

Дальний предел
Настройте дальний предел фокусировки объектива [м].

16.4.10 Широкий динамический диапазон

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Широкий динамический диапазон**

или

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Широкий динамический диапазон**
В зависимости от модели устройства здесь можно настроить параметры широкого динамического диапазона.

Режим
Введите или выберите необходимое значение.

Уровень
Введите или выберите необходимое значение.

16.4.11 Баланс белого

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Баланс белого**
или

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Основные параметры** > вкладка **Баланс белого**
В зависимости от модели устройства здесь можно настроить параметры баланса белого.

Режим
Автоматический режим позволяет камере постоянно выполнять корректировки, чтобы обеспечить оптимальную цветопередачу с использованием метода средней отражательной способности или в условиях с естественными источниками света.
В режиме «Вручную» усиление красного, зеленого и синего можно установить в желаемое положение вручную.
Смещение белой точки необходимо изменять только в особых условиях:
- источники света в помещениях и цветная светодиодная подсветка;
- источник света с натриевыми лампами (уличное освещение);
- любой доминирующий в изображении цвет, например зеленый на футбольном поле или на игровом столе.

Усиление красного
В режиме баланса белого «Вручную» отрегулируйте ползунок усиления красного, чтобы сместить стандартную установку белой точки (уменьшение красного приводит к увеличению голубого).

Усиление синего
В режиме баланса белого «Вручную» отрегулируйте ползунок усиления синего, чтобы сместить стандартную установку белой точки (уменьшение синего приводит к увеличению желтого).

16.4.12 Доступ к сети

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Доступ к сети**
или

Главное окно > **Устройства** > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Доступ к сети**

Здесь можно настроить различные сетевые параметры.

Ethernet IPv4

DHCP

Если для динамического назначения IP-адресов в сети используется DHCP-сервер, можно активировать принятие IP-адресов, автоматически назначенных кодеру. BVMS использует IP-адрес для уникального назначения кодера. DHCP-сервер должен поддерживать привязку IP-адреса к MAC-адресу, а также должен быть правильно настроен, чтобы после назначения IP-адреса он сохранялся при каждой перезагрузке компьютера.

Маска подсети

Введите соответствующую маску подсети для установленного IP-адреса.
Если включен DHCP-сервер, маска подсети назначается автоматически.

Шлюз по умолчанию

Если вы хотите, чтобы модуль установил соединение с удаленным пунктом в другой подсети, введите IP-адрес шлюза. В противном случае оставьте это поле пустым (0.0.0.0).

Ethernet IPv6

DHCP

Введите или выберите необходимое значение.

IP-адрес

Отображает адрес IPv6 устройства, предоставленный DHCP-сервером.

Длина префикса

Отображает длину префикса устройства, предоставляемого DHCP-сервером.

Шлюз по умолчанию

Отображает шлюз устройства по умолчанию, предоставленный DHCP-сервером.

Имя сервера

Введите или выберите необходимое значение.

DNS

DNS-сервер позволяет устройству найти адрес, указанный как имя. Введите здесь IP-адрес DNS-сервера.

NTP-серверы

Введите IP-адрес необходимого сервера времени или предоставьте это DHCP-серверу. Кодер может принимать сигнал времени с сервера времени с использованием различных протоколов сервера времени, а затем использовать его для установки внутренних часов. Модуль запрашивает сигнал времени автоматически каждую минуту. Введите IP-адрес сервера времени. Он поддерживает высокий уровень точности и необходим для работы специальных приложений.

Порты HTTP

При необходимости выберите другой порт HTTP-браузера. Порт HTTP по умолчанию — 80. Чтобы разрешить безопасные соединения по протоколу HTTPS, необходимо отключить порт HTTP.

Примечание. Не поддерживается системой BVMS.

Порты HTTPS

Примечание. Не поддерживается системой BVMS.

Если вы хотите предоставить доступ в сеть через безопасное соединение, при необходимости выберите порт HTTPS. Порт HTTPS по умолчанию — 443. Выберите параметр **Выкл**, чтобы отключить порты HTTPS; будут возможны только небезопасные соединения.

Шлюз по умолчанию

Введите или выберите необходимое значение.

Порты RTSP

При необходимости выберите другой порт для обмена данными RTSP. Стандартный порт RTSP — 554. Выберите **Выкл**, чтобы отключить функцию RTSP.

Адрес нулевой конфигурации

Включите или отключите обнаружение нулевой конфигурации выбранной камеры. Нулевая конфигурация — это альтернативный способ назначения IP-адресов камер, не использующий DHCP и DNS-серверов. Он автоматически создает работающий сетевой IP-адрес без конфигурации или специальных серверов.

Примечание. В стандарте ONVIF используется только обнаружение службы нулевой конфигурации.

Если нулевая конфигурация не используется, сеть должны предоставить службы, такие как DHCP или DNS.

В противном случае необходимо вручную настроить сетевые параметры всех IP-камер.

Режим обнаружения ONVIF

Если функция включена, можно отсканировать камеру в сети. Это включает ее возможности.

Если эта функция отключен, камера не отправляет сообщения обнаружения, чтобы избежать атак отказа в обслуживании.

Рекомендуется отключить обнаружение после добавления камеры в конфигурацию.

Введите или выберите необходимое значение.

Включить DynDNS

Позволяет включить DynDNS.

Динамическая служба доменных имен (DNS) позволяет выбрать устройство через Интернет по имени хоста, не указывая текущий IP-адрес устройства. Для этого необходимо иметь учетную запись у одного из поставщиков услуг динамического DNS и зарегистрировать требуемое имя узла для устройства на этом сайте.

Примечание.

Информацию об этой службе, процессе регистрации и доступных именах узлов см. на сайте поставщика услуг DynDNS по адресу dyndns.org.

Тип

Введите или выберите необходимое значение.

Имя

Введите имя учетной записи пользователя DynDNS.

TTL

Введите или выберите необходимое значение.

16.4.13 Области

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  >  > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Области**

или

Главное окно > **Устройства** > разверните  > > вкладка **Конфигурация ONVIF** > вкладка **Сеть** > вкладка **Области**

Вы можете добавлять характеристики устройства ONVIF или удалить их с использованием URI, имеющих следующий формат:

```
onvif://www.onvif.org/<path>
```

В следующем примере показано использование значения характеристики. Это просто пример, а не полное описание параметров характеристики, входящих в конфигурацию кодера. В данном примере предполагается, что на кодере настроены следующие характеристики:

```
onvif://www.onvif.org/location/country/china
onvif://www.onvif.org/location/city/bejing
onvif://www.onvif.org/location/building/headquarter
onvif://www.onvif.org/location/floor/R5
onvif://www.onvif.org/name/ARV-453
```

Можно присвоить устройству подробное местоположение и имя устройства, чтобы идентифицировать его в списке устройств.

В таблице показаны основные возможности и другие свойства устройства, которые являются стандартными:

Категория	Определенные значения	Описание
тип	video_encoder	Устройство является устройством сетевого видеокодера.
	PTZ	Устройство является устройством PTZ.
	audio_encoder	Устройство поддерживает аудиокодер.
	video_analytics	Устройство поддерживает видеоаналитику.
	Network_Video_Transmitter	Устройство является сетевым видеопередатчиком.
	Network_Video_Decoder	Устройство является сетевым видеодекодером.
	Network_Video_Storage	Устройство является сетевым устройством хранения видео.
	Network_Video_Analytic	Устройство является сетевым устройством видеоаналитики.
местонахождение	Любая строка символов или значение пути.	Не поддерживается системой BVMS.

Категория	Определенные значения	Описание
оборудование	Любая строка символов или значение пути.	Строка или значение пути, описывающие оборудование устройства. В список характеристик устройства должна входить как минимум одна запись оборудования.
имя	Любая строка символов или значение пути.	Доступное для поиска имя устройства. Это имя отображается в дереве устройств и в логическом дереве.

Имя характеристики, модель, производитель влияют на то, как устройство отображается в дереве устройств и на идентификацию кодера ONVIF и основные параметры.

16.4.14 Реле

Главное окно > **Устройства** > разверните > разверните > разверните > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Интерфейсы** > вкладка **Реле**

Главное окно > **Устройства** > разверните > > вкладка **Конфигурация ONVIF** > вкладка **Интерфейсы** > вкладка **Реле**

Состояние физического бездействия релейного выхода можно настроить, задав состояние бездействия **разомкнуто** или **замкнуто** (инверсия поведения реле).

Доступные цифровые выходы устройства отображаются вместе с именем, например:

- **AlarmOut_0**
- **AlarmOut_1**

Для любого сопоставления событий реле в пределах системы BVMS следует использовать указанные здесь имена.

Режим

Реле может работать в двух режимах:

- **Бистабильный**. После изменения состояния реле остается в этом состоянии.
- **Моностабильный**. После изменения состояния реле возвращается в состояние бездействия после заданного времени задержки.

Свободное состояние

Выберите **Разомкнуто** , если хотите, чтобы реле работало как нормально разомкнутый контакт, или **Замкнуто**, если реле должно работать как нормально замкнутый контакт.

Время задержки

Установите время задержки. После этого периода времени реле переключается обратно в состояние бездействия, если это настроено в **Моностабильном** режиме.

Если вы хотите проверить конфигурации, связанные с изменения состояния реле, нажмите **Активировать** или **Отключить** для переключения реле. Можно проверить правильную работу настроенных событий реле камеры: отображение состояния значка реле в логическом дереве, события в списке тревожных сигналов и журнале событий.

Активировать

Нажмите для переключения реле в настроенное состояние бездействия.

Отключить

Нажмите для переключения реле в настроенное активное состояние.

16.5 Страница "Источник событий ONVIF"

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  > разверните  >  > вкладка **Источник событий ONVIF**

или

Главное окно > **Устройства** > разверните  > разверните  >  > вкладка **Источник событий ONVIF**

или

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  > разверните  >  > вкладка **Источник событий ONVIF**

или

Главное окно > **Устройства** > разверните  > разверните  >  > вкладка **Источник событий ONVIF**

или

Главное окно > **Устройства** > разверните  > разверните  > разверните  > разверните  > разверните  >  > вкладка **Источник событий ONVIF**

или

Главное окно > **Устройства** > разверните  > разверните  >  > вкладка **Источник событий ONVIF**

Можно настроить события ONVIF источника (видеоканал, вход или реле). Определение активированного события добавляется в таблицу сопоставления кодера.
Например, для многоканального кодера выполняется выбор камеры, для которой создается событие **Обнаружено движение**.

Активирующее событие
Активировать это событие.

Тема ONVIF
Введите или выберите текстовую строку.

Имя источника ONVIF
Введите или выберите текстовую строку.

Тип источника ONVIF
Введите или выберите текстовую строку.

Значение источника ONVIF
Введите или выберите текстовую строку.

См.

- *Сопоставление событий ONVIF, Страница 42*
- *Настройка таблицы сопоставления ONVIF, Страница 250*

16.6 Назначение профиля ONVIF

Главное окно > **Камеры и запись** > 

Можно назначить ключ медиапрофиля ONVIF камере ONVIF.

Ключ можно назначить либо для видео в реальном времени, либо для записи.

Назначение ключа для видео в реальном времени.

- В столбце **Видеоизображение в реальном времени** – **Профиль** выберите необходимый элемент.

Назначение ключа для записи.

- В столбце **Запись** – **Профиль** выберите необходимый элемент.

См.

– *Страница Камеры, Страница 297*

17 Вкладка Карты и структура

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

Количество элементов под записью отображается в квадратных скобках.
Главное окно > **Карты и структура**
Разрешения могут быть утрачены. При перемещении группы устройств они утрачивают свои параметры разрешений. Необходимо снова установить разрешения на странице **Группы пользователей**.
Отображает дерево устройств, логическое дерево и окно **Глобальная карта**.
Позволяет создать структуру всех устройств системы BVMS. Структура отображается в логическом дереве.
Позволяет выполнять следующие действия:
- Настройка полного логического дерева
- Управление ресурсами
- Создание командных сценариев
- Создание последовательностей
- Создание окон просмотра карт
- Создание реле сигнализации о неисправностях
- Добавление карт мест и создание активных точек

Возможные активные точки на картах:
- Камеры
- Входы
- Реле
- Командные сценарии
- Последовательности
- Документы
- Ссылки на другие карты объектов
- VRM
- iSCSI
- Считыватели системы контроля и управления доступом
- Панели охранной сигнализации
- Сервер управления Enterprise Systems

Файлами ресурсов могут быть:
- Файлы карт
- Файлы документов
- Ссылки на внешние URL-адреса
- Аудиофайлы
- Ссылка на внешние приложения

Значки

	Отображает диалоговое окно управления файлами ресурсов.
	Отображает диалоговое окно для добавления командного сценария в логическое дерево или управления им.

	Отображает диалоговое окно для добавления или изменения файла последовательности камер.
	Создает папку в логическом дереве.
	Отображает диалоговое окно для добавления файлов ресурсов карт.
	Создает окно просмотра карт в логическом дереве.
	Отображает диалоговое окно для добавления файла с документом.
	Отображает диалоговое окно для добавления ссылки на внешнее приложение.
	Отображает диалоговое окно для добавления реле сигнализации о неисправностях.

Символы

	Устройство добавлено в логическое дерево.

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

18 Настройка карт и логического дерева

В данном разделе содержится информация о настройке логического дерева и управлении файлами ресурсов, например, картами.

Замечание!
При перемещении группы устройств в логическом дереве, устройства утрачивают параметры разрешений. Необходимо снова установить разрешения на странице **Группы пользователей**.

– Нажмите  для сохранения настроек.

– Нажмите  для отмены последней настройки.

– Нажмите  для активации конфигурации.

См.
- *Диалоговое окно Диспетчер ресурсов, Страница 273*
- *Диалоговое окно Выбрать ресурс, Страница 274*
- *Диалоговое окно Конструктор последовательностей, Страница 276*
- *Диалоговое окно Добавить последовательность, Страница 278*
- *Диалоговое окно Добавить шаг последовательности, Страница 279*
- *Диалоговое окно Добавить URL-адрес, Страница 275*
- *Диалоговое окно Выбрать карту для ссылки, Страница 280*
- *Диалоговое окно "Реле сигнализации о неисправностях", Страница 287*
- *Диалоговое окно Ссылка на внешнее приложение, Страница 275*

18.1 Настройка логического дерева

Главное окно > **Карты и структура** > вкладка **Логическое дерево**

Предусмотрена возможность добавления устройств, файлов ресурсов, окон просмотра карт, последовательностей, сценариев команд клиента и папок в логическое дерево. Устройства перечислены в дереве устройств, и вы можете перетащить любой уровень дерева устройств в логическое дерево.

Файлом ресурса может быть, например, карта объекта, документ, веб-файл, аудиофайл или командный сценарий.

- Карта объекта представляет собой файл, который можно добавить в логическое дерево. При добавлении карты объекта в логическое дерево создается папка карт, в которой вы можете организовать логические устройства, относящиеся к данной карте.
- Окно просмотра карт — это область глобальной карты с конкретным центром и уровнем масштабирования.
- Папка позволяет вам осуществлять дальнейшую организацию устройств в логическом дереве.

При первом запуске Configuration Client логическое дерево пусто.

Если у группы пользователей нет разрешения на доступ к устройству (например, камере), то устройство не будет отображаться на карте объекта, в окне просмотра карт и логическом дереве.

Вы можете добавлять на карту следующие элементы дерева устройств или логического дерева в качестве активных точек:

- Камеры
- Входы
- Реле
- Командные сценарии
- Последовательности
- Документы
- Ссылки на другие карты объектов
- VRM
- iSCSI
- Считыватели системы контроля и управления доступом
- Панели охранной сигнализации
- Сервер управления Enterprise Systems

Добавление элемента на карту объекта создает на ней активную точку.
При добавлении элемента в папку карты в логическом дереве он также будет отображаться в левом верхнем углу карты. При добавлении элемента в карту он также будет добавлен в соответствующий узел карты в логическом дереве модуля Operator Client.
Вы можете добавлять на глобальную карту следующие элементы дерева устройств:

- Камеры

Чтобы настроить логическое дерево, необходимо выполнить некоторые или все указанные действия несколько раз.

Чтобы переименовать логическое дерево:

1. Выберите корневой элемент логического дерева.
2. Нажмите  .
3. Введите новое имя.

Это имя видят все пользователи в логическом дереве Operator Client.

См.

- *Вкладка Карты и структура, Страница 268*

18.2 Добавление устройства в логическое дерево

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Для добавления устройства:

- Перетащите элемент из дерева устройств в нужное место логического дерева. Можно перетащить весь узел с подчиненными элементами из дерева устройств в логическое дерево. Можно выбрать несколько устройств, нажав клавишу CTRL или SHIFT.

См.

- *Вкладка Карты и структура, Страница 268*

18.3 Удаление элемента дерева

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Чтобы удалить элемент из логического дерева:

- Щелкните элемент в логическом дереве правой кнопкой мыши и выберите команду **Удалить**. Если выбранный элемент имеет подчиненные элементы, на экране появляется окно сообщения. Чтобы подтвердить выбор, нажмите кнопку **ОК**.

Элемент будет удален из системы.
При удалении элемента из папки карт логического дерева он одновременно удаляется с карты.

См.
– *Вкладка Карты и структура, Страница 268*

18.4 Управление файлами ресурсов

Главное окно > **Карты и структура** > > Вкладка **Логическое дерево** > 
или

Главное окно > **Тревожные сигналы** > 

Можно импортировать файлы ресурсов следующих форматов:
– Файлы DWF (двумерные файлы ресурсов карты)
– PDF
– JPG
– PNG
– Файлы HTML
– MP3 (аудиофайлы)
– Файлы TXT (командные сценарии или последовательности камер)
– Файлы MHT (веб-архивы)
– Файлы URL (ссылки на веб-страницы)
– Файлы URL-адресов HTTPS (ссылки на виджеты Intelligent Insights)
– WAV (аудиофайлы)

Импортируемые файлы ресурсов заносятся в базу данных. Они не связаны с исходными файлами.

Замечание!
По окончании каждого из следующих действий:
Нажмите  , чтобы сохранить настройки.

Чтобы импортировать файл ресурса:

1. Нажмите  .
   Откроется диалоговое окно **Импортировать ресурс**.
2. Выберите один или несколько файлов.
3. Нажмите **Открыть**.
   Выбранные файлы будут добавлены в список.
   Если файл уже был импортирован, на экране появляется окно сообщения.
   Если вы решили повторно импортировать уже импортированный файл, в список будет добавлена новая запись.

Чтобы удалить файл ресурса:

1. Выберите файл ресурса.
2. Нажмите  .
   Выбранный файл ресурса будет удален из списка.

Чтобы переименовать файл ресурса:

1. Выберите файл ресурса.
2. Нажмите  .
3. Введите новое имя.
   Исходное имя файла и дата создания сохраняются.

Чтобы заменить содержимое файла ресурса:

1. Выберите файл ресурса.
2. Нажмите  .
   Откроется диалоговое окно **Заменить ресурс**.
3. Выберите файл с подходящим содержимым и нажмите **Открыть**.
   Имя ресурса будет сохранено, а исходное имя файла будет заменено новым.

Чтобы экспортировать файл ресурса:

1. Выберите файл ресурса.
2. Нажмите  .
   Отображается диалоговое окно для выбора каталога.
3. Выберите нужный каталог и нажмите **ОК**.
   Исходный файл будет экспортирован.

См.

– *Диалоговое окно Выбрать ресурс, Страница 274*

18.4.1 Диалоговое окно Диспетчер ресурсов

Главное окно > **Карты и структура** >  > диалоговое окно **Диспетчер ресурсов**

Позволяет осуществлять управление файлами ресурсов.

Вы можете осуществлять управление файлами следующих форматов:

– Файлы DWF (файлы ресурсов карты)
  Для использования в Operator Client эти файлы конвертируются в растровый формат.
– PDF
– JPG
– PNG
– Файлы HTML (документы HTML, например планы действий)
– MP3 (аудиофайлы)
– Файлы TXT (текстовые файлы)
– Файлы URL (содержат ссылки на веб-страницы или виджеты Intelligent Insights)
– Файлы MHT (веб-архивы)
– WAV (аудиофайлы)
– EXE

 Нажмите для отображения диалогового окна импорта файла ресурса.

 Нажмите для отображения диалогового окна **Добавить URL-адрес**.

 Нажмите для отображения диалогового окна **Ссылка на внешнее приложение**.

 Нажмите для удаления выбранного файла ресурсов.

 Нажмите для переименования выбранного файла ресурсов.

 Нажмите для отображения диалогового окна для замены выбранного файла ресурсов другим.

 Нажмите для отображения диалогового окна для экспорта выбранного файла ресурсов.

18.4.2 Диалоговое окно Выбрать ресурс

Главное окно > **Карты и структура** > 

Позволяет добавлять файл карты в формате DWF, PDF, JPG или PNG в Логическое дерево.

Выберите файл ресурса:

Для выбора файла карты нажмите на имени файла. Содержимое выбранного файла отображается на панели предварительного просмотра.

Управление...

Нажмите для отображения диалогового окна **Диспетчер ресурсов**.

См.

- *Добавление карты, Страница 279*
- *Назначение карты папке., Страница 280*
- *Добавление документа, Страница 274*

18.5 Добавление документа

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

В качестве документов можно добавить текстовые файлы, файлы HTML (в том числе MHT), файлы URL (содержащие интернет-адрес) или файлы URL HTTPS (например, содержащие виджет Intelligent Insights). Кроме того, можно добавить ссылку на другое приложение.

Перед добавлением документа необходимо иметь импортированные файлы документов. Информация по импорту файлов документа содержится в *Управление файлами ресурсов, Страница 272*.

Чтобы добавить файл документа карты или виджет Intelligent Insights**:**

1. Убедитесь, что файл документа, который вы хотите добавить, уже импортирован.
2. Выберите папку, в которую нужно добавить новый документ.
3. Нажмите  . Отображается диалоговое окно **Выбрать ресурс**.
4. Выберите файл из списка. Если необходимые файлы отсутствуют в списке, нажмите **Управление...** для отображения диалогового окна **Диспетчер ресурсов** для импорта файлов.
5. Нажмите **ОК**. Новый документ будет добавлен в выбранную папку.

См.

- *Диалоговое окно Выбрать ресурс, Страница 274*
- *Управление файлами ресурсов, Страница 272*

18.5.1 Диалоговое окно Добавить URL-адрес

Главное окно > **Карты и структура** >  > 

Позволяет добавить в систему Интернет-адрес HTTP (URL) или Интернет-адрес HTTPS, например виджеты Intelligent Insights. Вы можете добавить этот URL-адрес в логическое дерево в качестве документа. Пользователь может отобразить интернет-страницу или виджет Intelligent Insights в своем Operator Client.

Имя
Введите отображаемое имя для URL-адреса.

URL
Введите URL-адрес.

Только для безопасного подключения
Пользователь
Введите имя пользователя для URL-адреса HTTPS.
Пароль:
Введите пароль для URL-адреса HTTPS.

Отобразить пароль
Нажмите, чтобы отобразить введенный пароль. Следите за тем, чтобы никто не мог подсмотреть этот пароль.

См.
– *Добавление документа, Страница 274*

18.6 Диалоговое окно Ссылка на внешнее приложение

Главное окно > **Карты и структура** > **Логическое дерево** вкладка >  > **Диспетчер ресурсов** диалоговое окно >  > **Ссылка на внешнее приложение** диалоговое окно
Позволяет добавить ссылку на внешнее приложение. Ссылка должна быть действительна на рабочей станции, на которой она используется.

Замечание!
Внешнее приложение, которое запускается с экрана с заставкой, будет работать неправильно.
Внешнее приложение, которое имеет совместные функции с Operator Client, не будет работать правильно, и в редких случаях его использование может привести к сбою клиента Operator Client.

Имя
Введите имя для ссылки, которая отображается в логическом дереве.

Путь
Введите имя внешнего приложения или выберите путь к нему. Путь к внешнему приложению должен быть действительным на рабочей станции, на которой пользователь клиентаOperator Client использует эту ссылку.

Аргументы
При необходимости введите аргументы в команду, которая выполняет внешнее приложение.

18.7 Добавление командного сценария

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Перед тем, как добавить командный сценарий, необходимо иметь импортированные или созданные файлы командного сценария.

Более подробные сведения см. в *Настройка командных сценариев, Страница 92*.

Чтобы добавить файл командного сценария:

1. Выберите папку, в которую вы хотите добавить новый командный сценарий.
2. Нажмите  . Отображается диалоговое окно **Выбрать клиентский сценарий**.
3. Выберите файл из списка.
4. Нажмите **ОК**.
   Новый командный сценарий будет добавлен в выбранную папку.

См.

– *Диалоговое окно Выбрать ресурс, Страница 274*

18.8 Добавление последовательности камер

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Можно добавить последовательность камер в корневой каталог или папку логического дерева.

Для добавления последовательности камер выполните следующие действия.

1. В логическом дереве выберите папку, в которую вы хотите добавить новую последовательность камер.
2. Нажмите  . Откроется диалоговое окно **Конструктор последовательностей**.
3. Выберите последовательность камер из списка.
4. Нажмите **Добавить в Логическое дерево**. Новая последовательность  будет добавлена в выбранную папку.

См.

– *Диалоговое окно Конструктор последовательностей, Страница 276*

18.8.1 Диалоговое окно Конструктор последовательностей

Главное окно > **Карты и структура** > 

Позволяет осуществлять управление последовательностями камер.

Значки

	Нажмите для отображения диалогового окна **Добавить последовательность**.
	Нажмите для переименования последовательности камер.
	Нажмите для удаления выбранной последовательности камер.

Добавить шаг

Нажмите для отображения диалогового окна **Добавить шаг последовательности**.

Удалить шаг
Нажмите, чтобы удалить выбранные шаги.

Шаг
Отображает номер шага. Все камеры определенного шага имеют одинаковое время задержки.

Переключение
Позволяет устанавливать время задержки (в секундах).

Номер камеры
Щелкните ячейку для выбора камеры в соответствии с логическим номером.

Камера
Щелкните ячейку для выбора камеры в соответствии с именем.

Функция камеры
Щелкните ячейку для изменения функции камеры в данной строке.

Данные
Введите время, в течение которого будет выполняться данная функция камеры. Чтобы настроить этот параметр, следует выбрать запись в столбце **Камера** и запись в столбце **Функция камеры**.

Единица данных
Выберите единицу времени, например секунды. Чтобы настроить этот параметр, следует выбрать запись в столбце **Камера** и запись в столбце **Функция камеры**.

Добавить в Логическое дерево
Нажмите для добавления выбранной последовательности камер в логическое дерево и для закрытия диалогового окна.

См.
– *Управление предварительно настроенными последовательностями камер, Страница 277*

18.9 Управление предварительно настроенными последовательностями камер

Главное окно > **Карты и структура** > **Логическое дерево** вкладка
Доступны следующие задачи для управления последовательностями камер:
– Создавать последовательность камер
– Добавлять к существующей последовательности камер шаг с новым периодом переключения
– Удалять шаг из последовательности камер
– Удалять последовательность камер

Замечание!
При изменении и активации конфигурации последовательность камеры (предварительно настроенная или автоматическая) обычно продолжается после перезапуска Operator Client.
Однако в следующих случаях последовательность не продолжается:
Монитор, на котором последовательность настроена на отображение, был удален.
Режим монитора (один экран/четыре экрана), на котором последовательность настроена на отображение, был изменен.
Логический номер монитора, на котором последовательность настроена на отображение, был изменен.

Замечание!
По окончании каждого из следующих действий:
Нажмите для сохранения настроек.

Чтобы создать последовательность камер:
1. В логическом дереве выберите папку, в которой вы хотите создать новую последовательность камер.
2. Нажмите .
   Откроется диалоговое окно **Конструктор последовательностей**.
3. В диалоговом окне **Конструктор последовательностей** нажмите .
   Откроется диалоговое окно **Добавить последовательность**.
4. Введите соответствующие значения.
5. Нажмите **OK**.

   Новая последовательность камер будет добавлена.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

Чтобы добавить к последовательности камер шаг с новым периодом переключения:
1. Выберите нужную последовательность камер.
2. Нажмите **Добавить шаг**.
   Откроется диалоговое окно **Добавить шаг последовательности**.
3. Установите необходимые параметры.
4. Нажмите **OK**.
   Новый шаг будет добавлен к последовательности камер.

Чтобы удалить шаг из последовательности камер:
- Щелкните правой кнопкой мыши нужную последовательность камер правой кнопкой мыши и нажмите **Удалить шаг**.
  Шаг с наибольшим номером будет удален.

Чтобы удалить последовательность камер:
1. Выберите нужную последовательность камер.
2. Нажмите . Выбранная последовательность камер будет удалена.

См.
– *Диалоговое окно Конструктор последовательностей, Страница 276*

18.9.1 Диалоговое окно Добавить последовательность

Главное окно > **Карты и структура** > > диалоговое окно **Конструктор последовательностей** >

Позволяет настроить параметры последовательности камер.

Имя последовательности:
Введите соответствующее имя новой последовательности камер.

Логический номер:
При использовании клавиатуры Bosch IntuiKey введите логический номер для последовательности.

Период переключения:
Введите соответствующий период переключения.

Камер на шаг:
Введите количество камер на каждый шаг.

Шаги:
Введите соответствующее количество шагов.

18.9.2 Диалоговое окно Добавить шаг последовательности

Главное окно > **Карты и структура** >  > кнопка **Добавить шаг**
Позволяет добавить к существующей последовательности камер шаг с новым периодом переключения.

Период переключения:
Введите соответствующий период переключения.

18.10 Добавление папки

Главное окно > **Карты и структура** > **Логическое дерево** вкладка
Для добавления папки выполните следующие действия.

1. Выберите папку, в которую нужно добавить новую папку.
2. Нажмите  . Новая папка будет добавлена в выбранную папку.
3. Нажмите  , чтобы переименовать папку.
4. Введите новое имя и нажмите клавишу ВВОД.

См.
– *Вкладка Карты и структура, Страница 268*

18.11 Добавление карты

Главное окно > **Карты и структура** > **Логическое дерево** вкладка
Чтобы можно было добавить карту, необходимо предварительно импортировать файлы ресурса карты.
Информация по импорту файла ресурса карты содержится в *Управление файлами ресурсов, Страница 272*.
Чтобы добавить карту:

1. Убедитесь, что файл ресурса карты, который вы хотите добавить, уже импортирован.
2. Выберите папку, в которую нужно добавить новую карту.
3. Нажмите  . Отображается диалоговое окно **Выбрать ресурс**.
4. Выберите файл из списка.
   Если необходимые файлы отсутствуют в списке, нажмите **Управление...** для отображения диалогового окна **Диспетчер ресурсов** для импорта файлов.

5. Нажмите **ОК**.

   Новая карта  будет добавлена в выбранную папку.
   Карта будет отображаться.
   В верхнем левом углу карты будут отображаться все устройства, находящиеся в данной папке.

См.

– *Диалоговое окно Выбрать ресурс, Страница 274*

18.12 Добавление ссылки на другую карту

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

После добавления двух и более карт вы можете создать ссылку для перехода с одной карты на другую, чтобы пользователь мог переходить с одной карты на другую одним нажатием мыши.

Чтобы добавить ссылку:

1. Нажмите на папку карт  в логическом дереве.
2. Щелкните правой кнопкой мыши по карте и нажмите **Создать ссылку**.
   Откроется диалоговое окно **Выбрать карту для ссылки**.
3. В диалоговом окне выберите карту  .
4. Нажмите **Выбрать**.
5. Перетащите элемент в нужное место на карте.

18.12.1 Диалоговое окно Выбрать карту для ссылки

Главное окно > **Карты и структура** > Выберите папку карты  в логическом дереве > На карте щелкните правой кнопкой мыши и выберите **Создать ссылку**

Позволяет выбрать карту для создания ссылки на другую карту.

 Щелкните другую карту, чтобы выбрать.

Выбрать

Нажмите для вставки ссылки в выбранную карту.

18.13 Назначение карты папке.

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Чтобы можно было назначить карты, необходимо предварительно импортировать файлы ресурса карты.

Более подробные сведения см. в *Управление файлами ресурсов, Страница 272*.

Чтобы назначить файл ресурса карты:

1. Щелкните правой кнопкой мыши папку и нажмите **Назначить карту**.
   Отображается диалоговое окно **Выбрать ресурс**.
2. Выберите файл ресурса карты из списка.
3. Нажмите **ОК**. Выбранная папка будет отображаться как  .
   Карта будет отображаться в окне карт.
   В верхнем левом углу карты будут отображаться все элементы, находящиеся в данной папке.

См.

- *Вкладка Карты и структура, Страница 268*
- *Диалоговое окно Выбрать ресурс, Страница 274*

18.14 Управление устройствами на карте объектов

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Перед тем, как начать управление устройствами на карте объектов, необходимо добавить карту или назначить карту папке и добавить устройства в данную папку.

Замечание!

По окончании каждого из следующих действий:

Нажмите  для сохранения настроек.

Чтобы поместить элемент на карту объектов:

1. Выберите папку карт.
2. Перетащите устройства из дерева устройств в папку карт.
   Устройства папки карт расположены в левом верхнем углу карты объектов.
3. Перетащите элементы в нужные места на карте объектов.

Чтобы удалить элемент логического дерева только с карты объектов:

1. Щелкните элемент на карте правой кнопкой мыши и выберите пункт **Невидимый**.
   Элемент будет удален с карты объектов.
   Элемент останется в логическом дереве.
2. Чтобы элемент снова отображался, щелкните устройство правой кнопкой мыши в логическом дереве и выберите пункт **Видимый на карте**.

Чтобы удалить элемент с карты объектов и из всего логического дерева:

- Щелкните элемент в логическом дереве правой кнопкой мыши и выберите пункт **Удалить**.
  Элемент будет удален с карты объектов и из логического дерева.

Чтобы сменить значок ориентации камеры:

- Щелкните элемент правой кнопкой мыши, выберите команду **Изменить изображение** и нажмите необходимый значок.
  Значок изменяется.

Чтобы изменить цвет элемента:

- Щелкните элемент правой кнопкой мыши и выберите команду **Изменить цвет**.
  Выберите необходимый цвет.
  Значок изменится.

Для активации / деактивации режима обхода устройства на карте объектов:

1. Щелкните правой кнопкой мыши по определенному устройству на карте объектов.
2. Нажмите **Обход** / **Отменить обход**.

Замечание!

Имеется возможность фильтрации устройств в режиме обхода в текстовом поле поиска.

См.

- *Настройка обхода устройств, Страница 287*
- *Вкладка Карты и структура, Страница 268*

18.15 Настройка глобальной карты и окон просмотра карт

Главное окно > **Карты и структура** > **Глобальная карта** вкладка

Для использования онлайн-карт или Map-based tracking assistant в Operator Client необходимо добавить и настроить камеры на глобальной карте.

Вы можете настроить окна просмотра карт на глобальной карте. Окно просмотра карт — это область глобальной карты с конкретным центром и уровнем масштабирования. Окно просмотра карт может отображаться в области изображений Operator Client.

Если вы хотите создать окно просмотра карт или использовать Map-based tracking assistant в Operator Client, сначала сделайте следующее:

1. Выберите тип фоновой карты на глобальной карте.
2. Перетащите камеры на глобальную карту.
3. Настройте направление и угол обзора камер на глобальной карте.

Если вы хотите создать окна просмотра карт или использовать Map-based tracking assistant в Operator Client **на нескольких этажах**, сначала сделайте следующее:

1. Выберите тип фоновой карты на глобальной карте.
2. Добавьте карту на глобальную карту.
   Примечание:карта первого этажа будет добавлена первой. Если Вы выбираете тип фоновой карты в автономном режиме, **Нет** первой картой, которую вы добавляете, будет фоновая карта.
3. Добавьте этажи к первому этажу или фоновой карте.
4. Выберите нужный этаж.
5. Перетащите камеры на карту этажа.
6. Настройте направление и конус просмотра своих камер.

18.15.1 Настройка глобальной карты

Можно задавать типы фоновых карт для глобальной карты и искать камеры, места и адреса.

Для изменения типа фоновой карты для глобальной карты:

1. Перейдите в главное окно и выберите **Настройки** меню > команда **Параметры...**.
2. Выберите нужный вариант.
   Примечание: При наличии доступа к Интернету можно выбрать онлайн тип фоновой карты (Here карты). Если у вас нет доступа к Интернету, выберите тип фоновой карты для автономного режима **Нет**.
   Для использования онлайн карт необходимо приобрести лицензию.
3. Если вы выбрали онлайн тип фоновой карты, введите свой ключ API, для указанного клиента.
4. Нажмите **Тест** для проверки API соединения.
5. Нажмите **ОК**.

Замечание!

При переключении типа фоновой карты с онлайн (Here карты) на автономный (**Нет**) или наоборот теряются все активные точки положения камер и окна просмотра карт.

Для глобальной карты можно задать только один фон. Этот фон применим ко всем окнам просмотра карт.

Для поиска камер или местоположений на глобальной карте:

1. Введите в поле поиска имя камеры, месторасположение или адрес.
   Как только вы начнете вводить, появится раскрывающееся меню со списком соответствующих вариантов.

2. Выберите из списка соответствующий вариант:
   на несколько секунд камера, месторасположение или адрес отобразятся с флажком
   
   .

См.

– *Диалоговое окно «Параметры» (меню «Настройки»), Страница 124*

18.15.2 Для настройки камеры на глобальной карте:

Для настройки камеры на глобальной карте:

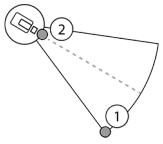
Примечание: если на картах установлено несколько этажей, убедитесь, что выбран правильный этаж, на котором вы хотите настроить свои камеры.

1. Выберите вкладку **Глобальная карта**.
2. Чтобы перейти в положение, в котором вы хотите разместить камеру, введите адрес или место в поле поиска.

   Вы также можете увеличивать и уменьшать с помощью кнопок  и или колесика мыши.
3. Перетащите камеру из дерева устройств в соответствующую область глобальной карты.
4. Щелкните камеру, чтобы выбрать ее.
5. Настройте направление и угол обзора камеры.
   Примечание: При выборе купольной камеры можно увидеть возможный угол обзора и фактический угол обзора. Символ предупреждения указывает на то, что фактический угол обзора купольной камеры необходимо откалибровать по горизонтали и по вертикали. Чтобы откалибровать купольную камеру, откройте предварительный просмотр видео в режиме реального времени.
6. Нажмите  , чтобы просмотреть видео с выбранной камеры в режиме реального времени.
   Предварительный просмотр видео может помочь вам настроить направление и угол обзора.
7. Нажмите  , чтобы скрыть предварительный просмотр видео с выбранной камеры.

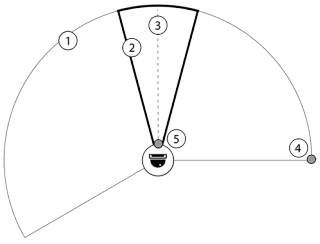
Примечание: При добавлении на глобальную карту камеры, которая еще не добавлена в логическое дерево, эта камера автоматически добавляется в конец логического дерева.

Для настройки направления и угла обзора камеры:



1. Перетащите для настройки угла обзора.
2. Чтобы развернуть и настроить направление, перетащите.

Для настройки горизонтального направления и угла обзора камеры PTZ (платформа CPP4 или выше):



1. Возможный угол обзора – это теоретически досягаемая область обзора.
2. Фактический угол обзора – это фактическое положение угла обзора объектива камеры PTZ
3. Угол панорамирования 0.
4. Перетащите для настройки угла обзора.
5. Чтобы развернуть и настроить направление, перетащите.

Замечание!
Для оптимального использования Map-based tracking assistant также необходимо отрегулировать вертикальное положение камеры PTZ. Мы рекомендуем регулировать вертикальное положение при предварительном просмотре в режиме реального времени видео с хорошо известного положения на участке, например, сравнивая с оригинальной видеозаписью. После этого Map-based tracking assistant будет всегда использовать настроенную вертикальную позицию.

Для отображения или скрытия предварительного просмотра камеры:

1. Нажмите , чтобы просмотреть видео с выбранной камеры в режиме реального времени.
   или
   правой кнопкой мыши щелкните камеру и выберите **Показать предварительный просмотр**.
   Предварительный просмотр видео может помочь вам настроить направление и конус просмотра.
2. Щелкните , чтобы скрыть предварительный просмотр видео с выбранной камеры.
   Или
   правой кнопкой мыши щелкните камеру и выберите **Скрыть предварительный просмотр**.

Для удаления камеры с глобальной карты:

- Щелкните камеру правой кнопкой мыши и выберите **Удалить**.

Для того, чтобы сделать камеру видимой на всех этажах:

- Щелкните правой кнопкой активную точку камеры и выберите **Видно на всех этажах**.
  При выборе другого этажа эта камера будет всегда видна.

Группирование активных точек камеры
Если уменьшить глобальную карту, на которой уже настроено несколько камер, то активные точки камеры сгруппируются в группы активных точек. Отобразится количество отдельных активных точек в группе активных точек. Выбранная камера не отображается как часть группы.

18.15.3 Добавление карт на глобальную карту

Вы можете добавить собственные файлы карт здания в верхней части глобальной карты. После этого операторы BVMS могут получить более детализированный просмотр с определенных мест расположения камер.

Для добавления карты на глобальную карту:

1. Выберите вкладку **Глобальная карта**.
2. Чтобы перейти в положение, в котором вы хотите разместить карту, введите адрес или место в поле поиска.

   Вы также можете увеличивать и уменьшать с помощью кнопок + и − или колесика мыши.
3. Нажмите  .
   Откроется окно **Выбрать ресурс**.
4. Выберите карту и нажмите **ОК**.
5. Нажмите и перетащите ↻, чтобы развернуть карту.
6. Нажмите и перетащите +, чтобы передвинуть карту.
7. Используйте точки переноса для регулировки размера карты.
8. Нажмите × , чтобы удалить карту.

Примечание: если необходимо добавить несколько этажей, карта первого этажа будет добавлена первой. Первый этаж обозначают цифрой 0 в поле 

.

Для добавления большего количества этажей к первому:

1. Щелкните цифру 0 в поле 

.

   Откроется поле .
2. Выберите этаж, где вы хотите добавить карту.
3. **Примечание:** для добавления карты можно выбрать только следующий более высокий или низкий этаж.
4. Нажмите  .
   Откроется окно **Выбрать ресурс**.
5. Выберите карту и нажмите **ОК**.
6. Измените добавленную карту этажа, чтобы настроить ее положение по отношению к карте первого этажа.

Для того, чтобы сделать этаж видимым на всех этажах:

1. Щелкните правой кнопкой мыши на любом значке настройки на соответствующей карте этажа ↻, + или ×.
2. Выберите **Видно на всех этажах**.
   Этот этаж теперь всегда виден при выборе другого этажа.

Примечание: если у вас нет доступа к Интернет и вы выбрали тип фоновой карты в автономном режиме, **Нет**, вы можете добавить карту в качестве фоновой. Рекомендуем сделать фоновую карту видимой на всех этажах. В таком случае при выборе другого этажа фоновая карта всегда будет видна.

18.16 Добавление окна просмотра карт

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Чтобы добавить окно просмотра карт**:**

1. Нажмите  , чтобы добавить окно просмотра карт.
2. Введите имя окна просмотра карт.
3. Чтобы перейти в расположение, где вы хотите создать свое окно просмотра карт, введите адрес или местоположение в поле поиска на глобальной карте.
   Если вы не знаете адрес или местоположение, то можно увеличивать и уменьшать с помощью кнопок  и или колесика мыши.
4. Нажмите  , чтобы сохранить конфигурацию.

Замечание!
Если окно просмотра карт содержит разные этажи, то при его открытии оператором в Operator Client отображается тот этаж, который был выбран при сохранении конфигурации. Далее в области изображения оператор может изменить этаж, отображаемый в окне просмотра карт.

18.17 Включение Map-based tracking assistant

Map-based tracking assistant позволяет отслеживать движущиеся объекты с нескольких камер. Соответствующие камеры должны быть предварительно настроены на глобальной карте. Если в области тревожных событий или в записи появляется интересные движущиеся объекты, пользователь может запустить Map-based tracking assistant, который автоматически покажет все соседние камеры.

Чтобы включить Map-based tracking assistant:

1. Перейдите в главное окно и выберите **Настройки** меню > команда **Параметры...**.
2. Установите флажок **Включить функцию системы**.
3. Нажмите **ОК**.

18.18 Добавление реле сигнализации о неисправностях

Главное окно > **Карты и структура** > **Логическое дерево** вкладка >  > **Реле сигнализации о неисправностях** диалоговое окно

Назначение
Реле сигнализации неисправности переключается в случае какой-либо серьезной системной ошибки, приводя в действие внешнее сигнальное устройство (стробоскоп, сирену и т. п.).
Пользователь должен вручную сбросить реле.
Функцию реле сигнализации неисправности может выполнять одно из следующих устройств:

- реле кодера или декодера BVIP;
- реле ADAM;
- выход охранной панели.

Пример
В случае какого-либо события, серьезно влияющего на работу системы (например, сбой жесткого диска), или происшествия, которое представляет угрозу для объекта (например, сбой при проверке контрольного изображения), срабатывает реле сигнализации неисправности. Оно может, например, активировать звуковую сигнализацию или автоматически закрыть двери.

Описание принципа действия
Можно настроить одно реле для выполнения функции реле сигнализации неисправности. Реле сигнализации неисправности автоматически активируется, когда происходит событие из заданного пользователем набора событий. Активация реле означает, что на реле подается команда замыкания контакта. Последующее событие «Реле замкнуто» не привязано к команде. Оно происходит и регистрируется, только если состояние реле изменяется физически! Например, ранее замкнутое реле не создает это событие.
За исключением того факта, что реле сигнализации неисправности автоматически срабатывает по событию из заданного пользователем набора событий, во всем остальном оно работает так же, как и все остальные реле. В частности, пользователь может отключить реле сигнализации неисправности в Operator Client. Веб-клиент также позволяет отключить реле сигнализации неисправности. Поскольку на реле сигнализации неисправности также распространяются разрешения регулярного доступа, всем клиентам требуется учитывать разрешения, имеющиеся у вошедшего в систему пользователя.

Порядок добавления:
1. В списке **Реле сигнализации о неисправностях** выберите нужное реле.
2. Нажмите **События...**
   Отображается диалоговое окно **Выбор событий для реле сигнализации о неисправностях**.
3. Выберите необходимые события, которые могут вызвать срабатывание реле сигнализации о неисправностях.
4. Нажмите **ОК**.
   Реле сигнализации о неисправностях добавляется в систему.

18.18.1 Диалоговое окно "Реле сигнализации о неисправностях"

Главное окно > **Карты и структура** > **Логическое дерево** вкладка >  > **Реле сигнализации о неисправностях** диалоговое окно
Можно добавить в систему реле сигнализации о неисправностях. Вы определяете, какое реле будет использоваться в качестве реле сигнализации о неисправностях, и настраиваете события, которые могут привести к срабатыванию реле сигнализации о неисправностях.
Это реле уже должно быть настроено в Логическом дереве.

Реле сигнализации о неисправностях
В списке выберите требуемое реле.

События...
Нажмите, чтобы открыть диалоговое окно **Выбор событий для реле сигнализации о неисправностях**.

18.19 Настройка обхода устройств

Главное окно > **Карты и структура** > **Логическое дерево** вкладка

Вы можете настроить обход определенных кодеров, камер, входов и реле, например, во время строительных работ. При настроенном обходе кодера, камеры, входа или реле запись остановлена, BVMSOperator Client не отображает никакие события или тревоги, при этом последние не регистрируются в журнале.
Камеры в режиме обхода по-прежнему отображают видео в режиме реального времени в Operator Client и оператор по-прежнему имеет доступ к старым записям.

Замечание!
Если кодер находится в режиме обхода, никакие тревоги и события не создаются для всех камер, реле и входов этого кодера. Если определенные отдельные камера, реле или вход находятся в режиме обхода и определенное устройство будет отключено от кодера, такие тревоги по-прежнему создаются.

Для активации / деактивации режима обхода устройства в логическом дереве или дереве устройств:

1. в логическом дереве или дереве устройств правой кнопкой мыши щелкните по определенному устройству.
2. Нажмите **Обход** / **Отменить обход**.

Для активации / деактивации режима обхода устройства на карте:
см. *Управление устройствами на карте объектов, Страница 281*

Замечание!
Имеется возможность фильтрации устройств в режиме обхода в текстовом поле поиска.

См.

– *Управление устройствами на карте объектов, Страница 281*

19 Страница Расписания

Главное окно >
Позволяет настроить расписания записей и расписания задач.

 Нажмите для переименования выбранного расписания записей или задач.

Расписания записей
Отображает дерево расписаний записей. Выберите элемент для настройки.

Расписания задач
Отображает дерево расписаний задач. Выберите элемент для настройки.

Добавить
Нажмите для добавления нового расписания задач.

Удалить
Нажмите для удаления выбранного расписания задач.

См.
– *Настройка расписаний, Страница 292*

19.1 Страница Расписания записей

Главное окно > > Выбрать элемент в дереве расписания записей
Позволяет настроить расписания записей.

Рабочие дни
нажмите для отображения расписания для рабочих дней. Отображаются временные интервалы для всех настроенных расписаний записей.
Перетащите указатель для выделения периодов времени в выбранном расписании. Все выделенные ячейки будут отображаться тем же цветом, что и выбранное расписание. 24 часа в сутках отображаются по горизонтали. Каждый час разделен на 4 ячейки. Одна ячейка представляет собой 15 минут.

Выходные дни
Нажмите для отображения расписания на выходные.

Дни исключений
Нажмите для отображения расписания на дни исключений.

Добавить
Нажмите, чтобы отобразить диалоговое окно для добавления выходных и дней исключений.

Удалить
Нажмите, чтобы отобразить диалоговое окно для удаления выходных и дней исключений.

См.
– *Настройка расписания записей, Страница 292*
– *Добавление выходных дней и дней исключений, Страница 294*
– *Удаление выходных дней и дней исключений, Страница 295*
– *Переименование расписания, Страница 295*

19.2 Страница Расписания задач

Главное окно > > Выбрать элемент в дереве расписания записей

Позволяет настроить доступные расписания задач. Вы можете настроить стандартную или повторяющуюся схему.

Стандарт
Нажмите, чтобы отобразить таблицу для настройки стандартных расписаний задач. Если вы настраиваете стандартную схему, повторяющаяся схема недоступна для выбранного расписания.

Повторение
Нажмите, чтобы отобразить таблицу настройки схемы повторения для выбранного расписания задач. Например, вы можете настроить расписание на каждый второй четверг каждого месяца или на 4 июля каждого года. Если вы настраиваете повторяющуюся схему, стандартная схема недоступна для выбранного расписания задач.

Рабочие дни
нажмите для отображения расписания для рабочих дней.
Перетащите указатель для выделения периодов времени в выбранном расписании. Выделенные ячейки будут отображаться тем же цветом, что и выбранное расписание. 24 часа в сутках отображаются по горизонтали. Каждый час разделен на 4 ячейки. Одна ячейка представляет собой 15 минут.

Выходные дни
Нажмите для отображения расписания на выходные.

Дни исключений
Нажмите для отображения расписания на дни исключений.

Очистить все
Нажмите, чтобы очистить временные интервалы для всех доступных дней (рабочих, выходных, дней исключений).

Выделить все
Нажмите, чтобы выделить временные интервалы для всех доступных дней (рабочих, выходных, дней исключений).

Добавить...
Нажмите, чтобы отобразить диалоговое окно для добавления выходных и дней исключений.

Удалить...
Нажмите, чтобы отобразить диалоговое окно для удаления выходных и дней исключений.

Схема повторения
Выберите частоту, с которой должны повторяться задачи расписания (Ежедневно, Еженедельно, Ежемесячно, Ежегодно), после чего выберите соответствующие параметры.

Схема дней
Перетащите указатель для выделения периодов времени в схеме повторения.

См.
- *Добавление расписания задач, Страница 293*
- *Настройка стандартного расписания задач, Страница 293*
- *Настройка повторяющегося расписания задач, Страница 293*
- *Удаление расписания задач, Страница 294*
- *Добавление выходных дней и дней исключений, Страница 294*

- *Удаление выходных дней и дней исключений, Страница 295*
- *Переименование расписания, Страница 295*

20 Настройка расписаний

Главное окно > **Расписания**

Имеется два типа расписаний:

– Расписания записей
– Расписания задач

Вы можете настроить до 10 различных расписаний записей в таблице расписаний записей. В этих сегментах камеры могут функционировать по-разному. Например, они могут иметь разную частоту кадров и параметры разрешения (настраиваются на странице **Камеры и запись**). В каждый момент времени действует только одно расписание записей. В нем отсутствуют какие-либо пробелы или накладки.

Настраиваются расписания задач для планирования различных событий в системе (настройка производится на странице **События**).

Определения терминов "Расписание записей" и "Расписания задач" см. в глоссарии.

Расписания также используются на других страницах Configuration Client:

– Страница **Камеры и запись**
  Используется для настройки записи.
– Страница **События**
  Используется для определения времени, когда события заносятся в журнал, вызывают тревожные сигналы или выполнение командных сценариев.
– Страница **Группы пользователей**
  Используется для определения времени, когда члены пользовательской группы могут войти в систему.

– Нажмите  для сохранения настроек.

– Нажмите  для отмены последней настройки.

– Нажмите  для активации конфигурации.

См.

– *Страница Расписания записей, Страница 289*
– *Страница Расписания задач, Страница 289*

20.1 Настройка расписания записей

Главное окно > **Расписания**

В любое расписание записей можно добавить дни исключений. Данные установки корректируют обычные недельные параметры.

Последовательность уменьшения приоритета такова: дни исключений, выходные дни, будни.

Максимальное число расписаний записей составляет 10. Первые три записи настраиваются по умолчанию. Вы можете изменить эти настройки. Записи с серым значком  не имеют настроенного периода времени.

Рабочие дни для всех расписаний записей одинаковы.

Для каждого стандартного расписания задач существуют собственные шаблоны рабочих дней.

Чтобы настроить расписание записей:

1. В дереве **Расписания записей** выберите расписание.
2. Перейдите на вкладку **Рабочие дни**.

3. В поле **Расписание** перетащите указатель для выделения периодов времени в выбранном расписании. Выделенные ячейки будут отображаться тем же цветом, что и выбранное расписание.

Примечания:

– Временной интервал рабочего дня в расписании записей может быть отмечен цветом из другого расписания записей.

См.

– *Страница Расписания записей, Страница 289*

20.2 Добавление расписания задач

Главное окно > **Расписания**

Чтобы добавить расписание задач:

1. Нажмите **Добавить**.
   Будет добавлена новая запись.
2. Введите соответствующее имя.
3. Нажмите **Стандарт** для создания стандартного расписания задач или **Повторение** для создания повторяющегося расписания задач.
   При изменении настроек отображается окно сообщения. Нажмите **OK**, если вы хотите изменить тип расписания.
   Стандартное расписание задач отображается как  , повторяющееся расписание задач отображается как  .
4. Установите соответствующие параметры для выбранного расписания.

См.

– *Страница Расписания задач, Страница 289*

20.3 Настройка стандартного расписания задач

Главное окно > **Расписания**

Для каждого стандартного расписания задач существуют собственные шаблоны рабочих дней.

Чтобы настроить стандартное расписание задач:

1. в дереве **Расписания задач** выберите стандартное расписание задач.
2. Перейдите на вкладку **Рабочие дни**.
3. В поле **Расписание** перетащите указатель для выделения периодов времени в выбранном расписании.

См.

– *Страница Расписания задач, Страница 289*

20.4 Настройка повторяющегося расписания задач

Главное окно > **Расписания**

Для каждого повторяющегося расписания задач существуют собственная схема дней.

Чтобы настроить повторяющееся расписание задач:

1. В дереве **Расписания задач** выберите повторяющееся расписание задач  .
2. В поле **Схема повторения** выберите частоту, с которой должны повторяться задачи расписания (**Ежедневно**, **Еженедельно**, **Ежемесячно**, **Ежегодно**), после чего выберите соответствующие параметры.

3. Выберите подходящую начальную дату из списка **Начальная дата:**.
4. В поле **Схема дней** перетащите указатель для выбора соответствующего периода времени.

См.

– *Страница Расписания задач, Страница 289*

20.5 Удаление расписания задач

Главное окно > > Выбрать элемент в дереве **Расписания задач**

Чтобы удалить расписание задач:

1. В дереве **Расписания задач** выберите элемент.
2. Нажмите **Удалить**.
   Расписание задач будет удалено. Все задачи, имевшиеся в этом расписании, удаляются и не будут выполнены.

См.

– *Страница Расписания задач, Страница 289*

20.6 Добавление выходных дней и дней исключений

Главное окно >**Расписания**

Замечание!
Список дней исключений и выходных можно оставить пустым. Дни исключений и выходных заменяют расписание для соответствующего дня недели.
Пример:
Старая конфигурация:
Расписание рабочего дня должно быть активно с 9:00 до 10:00
Расписание дня исключений должно быть активно с 10:00 до 11:00
Результат: активность с 10:00 до 11:00
То же самое работает и для выходных дней.

Вы можете добавлять выходные дни и дни исключений в расписание записей и в расписание задач.
Выходные дни и дни исключений одинаковы для всех расписаний записей.
Для каждого стандартного расписания задач существуют собственные шаблоны выходных дней и дней исключений.

Чтобы добавить в расписание выходные дни и дни исключений:

1. В дереве **Расписания записей** или **Расписания задач** выберите расписание.
2. Перейдите на вкладку **Выходные дни**.
3. Нажмите **Добавить**.
   Откроется диалоговое окно **Добавить выходные**.
4. Выберите один или несколько выходных дней и нажмите **OK**.
   Выбранные выходные дни будут добавлены в расписание.
5. Перетащите указатель для выбора соответствующего периода времени (это невозможно осуществить для расписаний записей).
   Выделенные ячейки будут очищены и наоборот.
6. Перейдите на вкладку **Дни исключений**.
7. Нажмите **Добавить**.
   Откроется диалоговое окно **Добавить дни исключений**.

8. Выберите один или несколько специальных дней и нажмите **OK**.
   Выбранные дни исключений будут добавлены в расписание.
9. Перетащите указатель для выбора соответствующего периода времени (это невозможно для расписаний записей).
   Выделенные ячейки будут очищены и наоборот.
   Сортировка добавленных выходных дней и дней исключений осуществляется в хронологическом порядке.

Примечания:

– Временной интервал выходного дня или дня исключений в расписании записей может быть отмечен цветом из другого расписания записей.

См.

– *Страница Расписания записей, Страница 289*
– *Страница Расписания задач, Страница 289*

20.7 Удаление выходных дней и дней исключений

Главное окно > **Расписания**

Из расписания видеозаписи и расписания задач можно удалить выходные дни и дни исключений.

Чтобы удалить выходные дни и дни исключений из расписания задач:

1. В дереве **Расписания записей** или **Расписания задач** выберите расписание.
2. Перейдите на вкладку **Выходные дни**.
3. Нажмите **Удалить**.
   Откроется диалоговое окно **Выберите выходные для удаления**.
4. Выберите один или несколько выходных дней и нажмите **OK**.
   Выбранные выходные дни будут удалены из расписания.
5. Перейдите на вкладку **Дни исключений**.
6. Нажмите **Удалить**.
   Откроется диалоговое окно **Выберите дни исключений для удаления.**
7. Выберите один или несколько дней исключений и нажмите **OK**.
   Выбранные дни исключений будут удалены из расписания.

См.

– *Страница Расписания записей, Страница 289*
– *Страница Расписания задач, Страница 289*

20.8 Переименование расписания

Главное окно >

Чтобы переименовать расписание:

1. В дереве **Расписания записей** или **Расписания задач** выберите элемент.
2. Нажмите  .
3. Введите новое имя и нажмите клавишу ВВОД. Элемент будет переименован.

См.

– *Страница Расписания записей, Страница 289*
– *Страница Расписания задач, Страница 289*

21 Страница Камеры и запись

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

Главное окно > **Камеры и запись**
Отображает страницу с таблицей камер или страницу с таблицей записей.
Позволяет настроить различные свойства камеры и параметры записи.
Позволяет отфильтровать камеры, отображаемые в соответствии с их типом.

Значки

	Нажмите для копирования настроек записи из одного расписания записей в другое.
	Нажмите для отображения диалогового окна **Параметры качества потока**.
	Нажмите для отображения диалогового окна **Настройки записи по расписанию**.
	нажмите, чтобы отобразить диалоговое окно настройки выбранной камеры PTZ.
	Отображает все доступные камеры, независимо от их устройства хранения.
	Нажмите для изменения Таблицы камер в соответствии с выбранным устройством хранения.
	Отображает соответствующую таблицу камер. Настройки записи недоступны, поскольку запись с этих камер не осуществляется в BVMS.
	Щелкните, чтобы выбрать столбцы, которые должны быть видимы в таблице **Камеры**.

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

21.1 Страница Камеры

Главное окно > **Камеры и запись** > Нажмите значок, чтобы изменить страницу «Камеры» в соответствии с требуемым устройством хранения, например 

Отображает различную информацию о камерах, доступных в BVMS.

Позволяет изменять следующие свойства камеры:

- Название камеры
- Назначение источника аудиосигнала
- Логический номер
- Управление PTZ, если есть
- Качество режима реального времени (VRM и Режим реального времени / Локальное хранилище)
- Профиль параметров записи
- Минимальное и максимальное время хранения
- Область интереса (Region of Interest)
- Automated Network Replenishment
- Двойная запись

Для настройки таблицы Камеры:

1. Щелкните  , чтобы выбрать столбцы, которые должны быть видимы в таблице **Камеры**.
2. Щелкните заголовок столбца, чтобы отсортировать таблицу по этому столбцу.

Камера - Кодер

Отображает тип устройства.

Камера - Камера

Отображает название камеры.

Камера - Сетевой адрес

Отображает IP-адрес камеры.

Камера - Местонахождение

Отображает местонахождение камеры. Если камера еще не назначена логическому дереву, отображается надпись **Неназначенное местоположение**.

Камера - Серия устройств

Отображает название семейства устройств, к которому относится выбранная камера.

Камера - Номер

Щелкните ячейку для изменения логического номера, автоматически получаемого камерой при ее обнаружении. Если введен номер, который уже используется, появляется соответствующее сообщение об ошибке.

Логический номер "освобождается" после удаления камеры.

Аудио

Нажмите ячейку, чтобы назначить камере источник аудиосигнала.

Если срабатывает тревожное событие с низким приоритетом и камерой с настроенным аудиосигналом, этот аудиосигнал воспроизводится даже в том случае, когда на экране отображается тревожное событие с более высоким приоритетом. Это происходит только в том случае, если для тревожного события с более высоким приоритетом не настроен аудиосигнал.

Потоки / Ограничения потоков

В этом столбце представлены данные только для чтения, там также указаны ограничения потока для соответствующей камеры.

Примечание: ограничения потока отображаются только для камер CPP13 и CPP14.

Замечание!
Вы не можете редактировать ограничения потока в BVMS. Их можно редактировать на веб-сайте кодера или в Configuration Manager. После редактирования ограничений потока на веб-сайте или в Configuration Manager необходимо обновить возможности устройства в BVMS. Если вы не обновите возможности устройства, BVMS вернет обновленные ограничения потока к старым настройкам, которые отображались при последнем обновлении возможностей устройства.

Поток 1 - Кодек / Поток 2 - Кодек
Щелкните ячейку для выбора необходимого кодека для кодирования потока.

Поток 3 - Кодек
Щелкните ячейку для выбора нужного разрешения видео.
Значения разрешения видео загружаются из кодера. Отображение этих значений может занять некоторое время.
Примечание: только камеры CPP13 и CPP14 поддерживают третий поток. Этот столбец отображается только тогда, когда есть хотя бы одна настроенная камера, которая поддерживает третий поток.

Поток 1 - Качество / Поток 2 - Качество / Поток 3 - Качество
Выберите требуемое качество потока, используемое при записи или трансляции в режиме реального времени. Параметры качества можно настроить в диалоговом окне **Параметры качества потока**.

Поток 1 - Активная платформа / Поток 2 - Активная платформа / Поток 3 - Активная платформа
Отображает название параметров платформы в диалоговом окне **Параметры качества потока**. Этот столбец доступен только для чтения и указывает, какие параметры профиля будут записываться на кодер.

Замечание!
Поток 3 можно использовать только для отображения в режиме реального времени. Запись невозможна.

Видеоизображение в реальном времени - Поток (только VRM и режим реального времени, и локальное хранилище)
Нажмите ячейку для выбора потока для VRM или кодера, работающего только в режиме реального времени или локального хранилища.

Видеоизображение в реальном времени - Профиль (доступно только для камер ONVIF)
Нажмите ячейку для выбора доступных токенов профиля реального режима этой камеры ONVIF.
Если выбирается элемент **<Автоматически>**, автоматически используется поток наивысшего качества.
Примечание: если вы выбрали устройство Video Streaming Gateway для извлечения видео в режиме реального времени на рабочей станции, настройка **Видеоизображение в реальном времени** - **Профиль** станет устаревшей. Вместо этого для видеоизображения в реальном времени также будет использоваться параметр **Запись** - **Профиль**.

Видеоизображение в реальном времени - Область интереса ""
Нажмите, чтобы включить Region of Interest (ROI). Это возможно, только если в столбце **Качество** выбран элемент H.264 MP SD ROI или H.265 MP SD ROI для потока 2, а поток 2 назначен для передачи видео в режиме реального времени.
Примечание. Если поток 1 используется для режима реального времени для конкретной рабочей станции, клиент оператора, запущенный на этой рабочей станции, не может включить функцию ROI этой камеры.

 автоматически включается в таблице  .

Запись - Параметр
Нажмите ячейку для выбора требуемых параметров записи. Доступные параметры качества можно настроить в диалоговом окне **Настройки записи по расписанию**.

Запись - Профиль (доступно только для камер ONVIF)
Нажмите ячейку для выбора доступных ключей профиля записи этой камеры ONVIF. Выберите требуемый элемент.

Запись - ANR
Установите флажок для включения функции ANR. Эту функцию можно включить, только если кодер имеет соответствующую версию микропрограммного обеспечения и соответствующий тип устройства.

Запись - Максимальная длительность до тревожного сигнала
Отображает расчетную максимальную длительность записи до включения тревожного сигнала для этой камеры. Это значение может помочь в вычислении необходимого пространства для хранения на локальном носителе данных.

Замечание!
Если зеркальный диспетчер VRM уже настроен для кодера, невозможно изменить какие-либо настройки для этого кодера в столбцах **Вторичная запись**.

Вторичная запись — Параметр (доступно, только если настроен вторичный VRM)
Нажмите ячейку для назначения параметров записи по расписанию двойной записи этого кодера.
В зависимости от конфигурации при некоторых обстоятельствах настроенное качество потока для вторичной записи может не быть действительным. В таком случае вместо него используется качество потока, настроенное для основной записи.

Вторичная запись - Профиль (доступно только для камер ONVIF)
Нажмите ячейку для выбора доступных ключей профиля записи этой камеры ONVIF.

 (отображается только после нажатия  **Все**)
Установите флажок для активации управления панорамированием, наклоном и увеличением камеры.

Примечание.
Сведения о параметрах порта см. в . COM1.

Порт (отображается только после нажатия  **Все**)

Щелкните ячейку, чтобы выбрать нужный последовательный порт кодера для управления панорамированием/наклоном/увеличением камеры. Для камеры PTZ, подключенной к системе Bosch Allegiant, можно выбрать **Allegiant**. Для такой камеры магистральная линия не требуется.

Протокол (отображается только после нажатия **Все**)
Щелкните ячейку, чтобы выбрать нужный протокол для управления панорамированием/наклоном/увеличением камеры.

Адрес PTZ (отображается только после нажатия **Все**)
Введите адрес для управления панорамированием/наклоном/увеличением камеры.

Запись — Мин. время хранения [дни]
Вторичная запись — Мин. время хранения [дни] (только VRM и локальное хранилище)
Щелкните ячейку и введите минимальное количество дней, в течение которых будут сохраняться видеоданные с этой камеры. Видеоизображения, записанные в течение этого периода времени, не будут автоматически удаляться.

Запись — Макс. время хранения [дни]
Вторичная запись — Макс. время хранения [дни] (только VRM и локальное хранилище)
Щелкните ячейку и введите максимальное количество дней, в течение которых будут сохраняться видеоданные с этой камеры. Автоматически будут удаляться только те видеоизображения, которые записаны ранее этого указанного периода времени. 0 = без ограничений.

См.
- *Настройка двойного режима записи в Таблице камер, Страница 314*
- *Настройка предустановленных положений и дополнительных команд, Страница 311*
- *Настройка параметров портов PTZ, Страница 311*
- *Настройка параметров качества потока, Страница 303*
- *Копирование и вставка в таблицы, Страница 302*
- *Настройка функции ANR, Страница 314*
- *Экспорт таблицы камер, Страница 303*
- *Назначение профиля ONVIF, Страница 315*
- *Настройка функции ROI, Страница 313*

21.2 Панели параметров записи

Главное окно > **Камеры и запись** > > Нажмите вкладку "Расписание записей" (например,)
Позволяет задать настройки записи.
Настройка отображения Расписания записи выполняется через **Расписания**.
Описаны только те столбцы, которые не являются частью таблицы камер.

- Щелкните заголовок столбца, чтобы отсортировать таблицу по этому столбцу.

Непрерывная запись
Нажмите ячейку в столбце **Качество**, чтобы отключить запись или выбрать качество потока 1.

В столбце установите флажок для активации аудиосигнала.

Запись в режиме реального времени/перед событием
Нажмите на ячейку в столбце **Качество**, чтобы выбрать качество потока в режиме реального времени (необходимого для мгновенного воспроизведения) и выполнения записи перед событием (требуется для записи по движению и записи по тревоге) в потоке 2. Если на кодере включена двухпотоковая передача данных, то можно выбрать поток 1 и использовать запись в режиме реального времени или запись перед событием.

В столбце установите флажок для активации аудиосигнала.

Запись движения
Нажмите ячейку в столбце **Качество**, чтобы отключить запись или выбрать качество потока 1.

В столбце нажмите ячейку для активации аудиосигнала.
Нажмите ячейку в столбце **Перед событием [с]**, чтобы выбрать время записи перед движением в секундах.
Нажмите ячейку в столбце **После события [с]**, чтобы выбрать время записи после движения в секундах.

Запись по тревоге
В столбце **Качество** нажмите на ячейку для выбора качества записи потока 1.
Чтобы активировать запись по тревоге, нужно настроить соответствующее тревожное событие.

В столбце установите флажок для активации аудиосигнала.
Нажмите ячейку в столбце **Перед событием [с]**, чтобы выбрать время перед тревожным сигналом в секундах.
Нажмите ячейку в столбце **После события [с]**, чтобы выбрать время после тревожного сигнала в секундах.

См.
– *Копирование и вставка в таблицы, Страница 302*

22 Настройка камер и параметров записи

Замечание!
В данном документе описываются некоторые функции, недоступные для BVMS Viewer. Подробные сведения о различных редакциях BVMS см. www.boschsecurity.com и BVMS Руководство по быстрому выбору: Руководство по быстрому выбору BVMS.

Главное окно > **Камеры и запись**
В данном разделе содержится информация о конфигурировании устройств в BVMS.
Вы можете настроить различные свойства камеры и параметры записи.

– Нажмите  для сохранения настроек.
– Нажмите  для отмены последней настройки.
– Нажмите  для активации конфигурации.

См.
– *Страница Камеры, Страница 297*
– *Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище), Страница 308*
– *Диалоговое окно Параметры качества потока, Страница 304*
– *Диалоговое окно «Предустановленные положения и дополнительные команды», Страница 313*

22.1 Копирование и вставка в таблицы

Можно одновременно настраивать многие объекты в таблице камер, таблице настройки событий или таблице настройки тревог.
Вы можете скопировать настраиваемые значения из табличной строки в другие строки:
– Копировать все значения из строки в другие строки.
– Копировать только одно значение из строки в другую строку.
– Копировать значение из одной ячейки в целый столбец.
Вы можете копировать значения двумя способами:
– Копирование значения в буфер обмена с последующей вставкой из него.
– Непосредственное копирование и вставка.
Вы можете выбрать, в какие строки вставлять скопированные значения:
– Вставка во все строки.
– Вставка в выделенные строки.

Чтобы скопировать все настраиваемые значения из одной строки в другую:
1. Щелкните правой кнопкой мыши нужные значения и выберите **Копировать строку**.
2. Щелкните заголовок строки, которую вы хотите изменить.
   Для выбора нескольких строк нажмите и удерживайте клавишу CTRL.
3. Щелкните таблицу правой кнопкой мыши и нажмите **Вставить**.
   Значения будут скопированы.

Чтобы скопировать одно значение из одной строки в другую:
1. Щелкните правой кнопкой мыши нужные значения и выберите **Копировать строку**.
2. Щелкните правой кнопкой мыши ячейку, которую вы хотите изменить, выберите **Вставить ячейку в** и нажмите **Текущая ячейка**.
   Значение будет скопировано.

Чтобы скопировать все настраиваемые значения непосредственно:

1. Щелкните заголовок строки, которую вы хотите изменить.
   Для выбора нескольких строк нажмите и удерживайте клавишу CTRL.
2. Щелкните правой кнопкой мыши нужные значения и выберите **Копировать строку в** и нажмите **Выбранные строки**.
   Значения будут скопированы.

Чтобы скопировать одно значение непосредственно:

1. Щелкните заголовок строки, которую вы хотите изменить.
   Для выбора нескольких строк нажмите и удерживайте клавишу CTRL.
2. Щелкните правой кнопкой мыши ячейку с нужным значением, выберите **Копировать ячейку в** и нажмите **Выделение в столбце** .
   Значение будет скопировано.

Чтобы скопировать значение из одной ячейки во все остальные ячейки в данном столбце:

- Щелкните правой кнопкой мыши ячейку с нужным значением, выберите **Копировать ячейку в** и нажмите **Заполнить столбец**.
  Значение будет скопировано.

Чтобы скопировать строку:

- Щелкните строку правой кнопкой мыши и нажмите **Добавить повторяющуюся строку**.
  Строка будет добавлена ниже под новым именем.

См.

- *Страница Камеры, Страница 297*
- *Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище), Страница 308*
- *Страница События, Страница 316*
- *Страница Тревожные сигналы, Страница 321*

22.2 Экспорт таблицы камер

Главное окно > **Камеры и запись**
или
Главное окно > **Камеры и запись** > нажмите значок, чтобы изменить страницу "Камеры" в соответствии с требуемым устройством хранения, например 
Отображает различную информацию о камерах, доступных в BVMS.
Таблицу камер можно экспортировать в файл CSV.

Порядок выполнения экспорта:

1. Щелкните в любом месте Таблицы камер правой кнопкой мыши и нажмите **Экспортировать таблицу...**.
2. В диалоговом окне введите соответствующее имя файла.
3. Нажмите **Сохранить**.
   Выбранная Таблица камер экспортируется в файл CSV.

22.3 Настройка параметров качества потока

Чтобы добавить элемент с параметрами качества потока:

1. Нажмите  для добавления нового элемента в список.
2. Введите имя.

Чтобы удалить элемент с параметрами качества потока:

- Выберите элемент из списка и нажмите  для его удаления.
  Вы не можете удалить стандартные элементы.

Чтобы переименовать элемент с параметрами качества потока:

1. Выберите элемент из списка.
2. Введите новое имя в поле **Имя**.
   Вы не можете переименовать стандартные элементы.
3. Нажмите **ОК**.

Чтобы настроить параметры качества потока:

1. Выберите элемент из списка.
2. Установите необходимые параметры.

22.3.1 Диалоговое окно Параметры качества потока

Главное окно > **Камеры и запись** > 

Позволяет настраивать профили качества потока, которые затем можно назначить камерам на странице **Камеры и запись** или в диалоговом окне **Настройки записи по расписанию**.

Качество потока включает в себя разрешение видео, частоту кадров, максимальную полосу пропускания и сжатие видео.

Качество потока

 Выберите предварительно заданное качество потока и нажмите  , чтобы добавить новое качество потока на основании предварительно заданного качества. При выборе одного потока и нажатии  настройка качества этого потока копируется как узел верхнего уровня без дочерних элементов.

 Нажмите для удаления выбранного качества потока. Невозможно удалить параметры качества потока.

В этом списке приводятся все доступные предварительно заданные параметры качества потока. Рекомендуется назначать качество потока с таким же именем, что и у платформы камеры.

Для различных настроек качества потока доступны следующие профили:

Image optimized: параметры оптимизируются для обеспечения качества изображения. Это может увеличить нагрузку на сеть.

Bit rate optimized: параметры оптимизируются согласно низкой пропускной способности сети. Это может снизить качество изображения.

Balanced: эти параметры представляют собой компромисс между оптимальным качеством потока и оптимальной нагрузкой на сеть.

Доступны следующие профили для различных настроек качества потока, начиная с BVMS 9.0 для поддержки функции Intelligent Streaming камер Bosch:

Cloud optimized 1/8 FR: параметры оптимизируются для низкой полосы пропускания одинаково для всех типов камер.

PTZ optimized: параметры оптимизируются для камер PTZ.

Image optimized quiet / standard / busy

Bit rate optimized quiet / standard / busy

Balanced quiet / standard / busy

Категории типов сцен:
quiet: параметры оптимизируются для изображений с низкой активностью. 89 % — статичная сцена, 10 % — обычная сцена, 1 % — оживленная сцена.
standard: параметры оптимизируются для изображений со средней активностью. 54 % — статичная сцена, 35 % — обычная сцена, 11 % — оживленная сцена.
busy: параметры оптимизируются для изображения с высокой активностью. 30% статичная сцена, 55% оживленная сцена, 15% сцена со скоплением людей.
Значения в процентах указывают на распределение в течение дня.

По умолчанию назначен профиль Balanced standard.

Замечание!
Для каждой комбинации платформы камеры (CPP3-CPP7.3) и для каждого доступного разрешения существует отдельный параметр, позволяющий установить необходимую скорость передачи данных для камер.
Профиль и соответствующий тип сцены необходимо выбрать вручную для каждой камеры.

Замечание!
При обновлении установки новые профили необходимо выбрать вручную для их активации. Прежние профили сохраняются.

Имя
Отображает имя качества потока. При добавлении нового качества потока можно изменить имя.

Разрешение SD-видео
Этот параметр применим, только если для кодека потока установлено разрешение SD.

Выберите нужное разрешение видео. Для качества HD задается качество SD для потока 2.

Примечание. Это не влияет на разрешение, если для кодека настроено разрешение HD или UHD (любое значение выше SD). Разрешение камеры, например HD, невозможно уменьшить до SD с помощью этого параметра.

Интервал кодирования изображений
Переместите ползунок или введите соответствующее значение.
Система помогает вычислить соответствующее значение кадров/сек.
При помощи значения **Интервал кодирования изображений** настраивается интервал, с которым изображения кодируются и передаются. Если введено значение 1, кодируются все изображения. Значение 4 означает, что кодируется только каждое четвертое изображение, а следующие три пропускаются — это может оказаться особенно полезным при низкой пропускной способности. Чем ниже пропускная способность, тем выше должно быть это значение для обеспечения видеоизображений наилучшего качества.

Например, датчик передает на вход механизма кодирования 30 кадров. На выходе для просмотра видео в реальном времени или в записи необходимо получить 15 кадров.
Для этого:

- Установите параметр **Интервал кодирования изображений** в значение 2.
  Кодер будет пропускать каждый второй кадр с датчика и выдавать закодированный поток H.264 с лишь 15 кадрами.

Интервал кодирования изображений:
– 1= полная частота кадров, указанная в параметрах кодека
– 2= 50 % частоты кадров, указанной в параметрах кодека
Для быстрого расчета частоты кадров используется следующая формула: кадр/с = режим датчика / интервал кодирования изображений

Структура группы видеокадров (GOP)
Выберите требуемую структуру для группы изображений (GOP). В зависимости от того, чему отдается больший приоритет — минимально возможной задержке (только для IP-кадров) или использованию минимально возможной пропускной способности, — можно выбрать IP, IBP или IBBP. (Выбор GOP недоступен на некоторых камерах.)

Примечание:
B-кадры поддерживаются только камерами с разрешением до 1080 пикселей и микропрограммой версии 6.40 и новее.
Избегайте использования B-кадров при просмотре в реальном времени и для PTZ, поскольку они приводят к задержке видео в реальном времени.

Оптимизация скорости передачи
Оптимизация по скорости передачи данных связана с приоритетом в пользу качества изображения или сокращения скорости передачи данных.
При выборе параметров **Высокое качество** или **Максимальное качество** экономия скорости передачи данных мала или отсутствует при хорошем или превосходном качестве изображения. Параметры
Низкая скорость передачи данных и **Средний** позволяют сэкономить полосу пропускания, однако полученное изображение будет менее детальным.
Если оптимизация по скорости передачи данных отключена, ожидается средняя скорость передачи данных 24 ч (выше целевой скорости передачи данных).

Объектная скорость передачи [кбит/с]
Переместите ползунок или введите соответствующее значение.
Можно ограничить скорость передачи данных для encoder, чтобы оптимизировать использование пропускной способности сети. Необходимая скорость передачи данных должна устанавливаться в соответствии с требуемым качеством изображения для стандартных сцен без излишнего движения.
Для сложных изображений или частых смен изображения в результате частого движения этот предел может быть временно увеличен до значения, которое можно ввести в поле **Максимальная скорость передачи [кбит/с]**.

Максимальная скорость передачи [кбит/с]
Переместите ползунок или введите соответствующее значение.
Посредством данного значения вы устанавливаете максимальную скорость передачи, которая не может быть превышена.
Ограничение скорости устанавливается для того, чтобы иметь возможность надежного определения необходимого дискового пространства для хранения видеоданных.
В зависимости от настроек качества изображения для I-кадра и P-кадра это может привести к пропуску отдельных изображений.

Введенное здесь значение должно быть по крайней мере на 10% выше значения, указанного в поле **Объектная скорость передачи [кбит/с]**. Слишком низкое значение, введенное для этого параметра, будет автоматически изменено на допустимое.

Расстояние между I-кадрами
Данный параметр позволяет установить интервалы, с которыми будут кодироваться I-кадры.
Значение 1 означает, что I-кадры генерируются непрерывно. Значение 10 означает, что только каждое десятое изображение является I-кадром, значение 60 означает, что только каждое шестидесятое изображение является I-кадром и т. д. Все изображения, находящиеся между ними, кодируются как P-кадры.
Примечание. При использовании очень длинных групп GOP (до 255) при низкой частоте кадров (1 кадр/с) временное расстояние между I-кадрами слишком велико, и воспроизведение изображения невозможно. Рекомендуется уменьшить длину группы GOP до 30.

Уровень качества кадра
Здесь можно установить значение между 0 и 100 для I-кадров и P-кадров. Самое низкое значение приводит к наивысшему качеству и самой низкой частоте обновления кадров. Самое высокое значение приводит к самому низкому качеству изображения и наивысшей частоте обновления кадров.
Чем ниже пропускная способность, тем выше должен быть уровень качества для сохранения высокого качества видеоизображений.

Примечание:
Если нет иных указаний от службы технической поддержки, настоятельно рекомендуется установить флажки **Авто**. В таком случае оптимальное соотношение между движением и резкостью изображения настраивается автоматически.

Параметры VIP X1600 XFM4
Позволяет настроить следующие параметры H.264 для модуля кодера VIP X 1600 XFM4.
Разблокирующий фильтр H.264 — выберите для повышения качества видеоизображения и эффективности прогнозирования путем сглаживания резких границ.
Кодирование CABAC — выберите для активации высокоэффективного сжатия. Использует большой объем вычислительной мощности.

См.
– *Настройка параметров качества потока, Страница 303*

22.4 Настройка свойств камеры

Главное окно > **Камеры и запись** > 

Чтобы изменить свойства камеры:
1. Выберите ячейку в столбце **Камера** и введите новое имя камеры.
   Это имя будет отображаться в других местах, в которых упоминается эта камера.
2. Установите соответствующие параметры в других столбцах.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

См.
– *Страница Камеры, Страница 297*

22.5 Настройка параметров записи (только VRM и Локальное хранилище)

Главное окно > > **Камеры и запись** 

Можно настроить параметры записи для всех устройств, которые добавлены к VRM в дереве устройств.

Примечание: при записи убедитесь, что соответствующий VRM или локальное хранилище настроены правильно.

VRM: **Устройства** > Разверните  > 

Локальное хранилище: **Устройства** > Разверните  > 

Добавление элемента, содержащего параметры записи.

1. Нажмите  для добавления нового элемента в список.
2. Введите имя.

Удаление элемента, содержащего параметры записи.

- Выберите элемент из списка и нажмите  для его удаления.
  Вы не можете удалить стандартные элементы.

Переименование элемента, содержащего параметры записи.

1. Выберите элемент из списка.
2. Введите новое имя в поле **Имя:**.
   Вы не можете переименовать стандартные элементы.
3. Нажмите **ОК**.

Чтобы настроить параметры записи:

1. Выберите элемент из списка.
2. Установите подходящие параметры и нажмите **ОК**.
3. Нажмите  или  .
4. В столбце **Запись** выберите необходимые параметры записи для каждого кодера.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.

– *Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище), Страница 308*

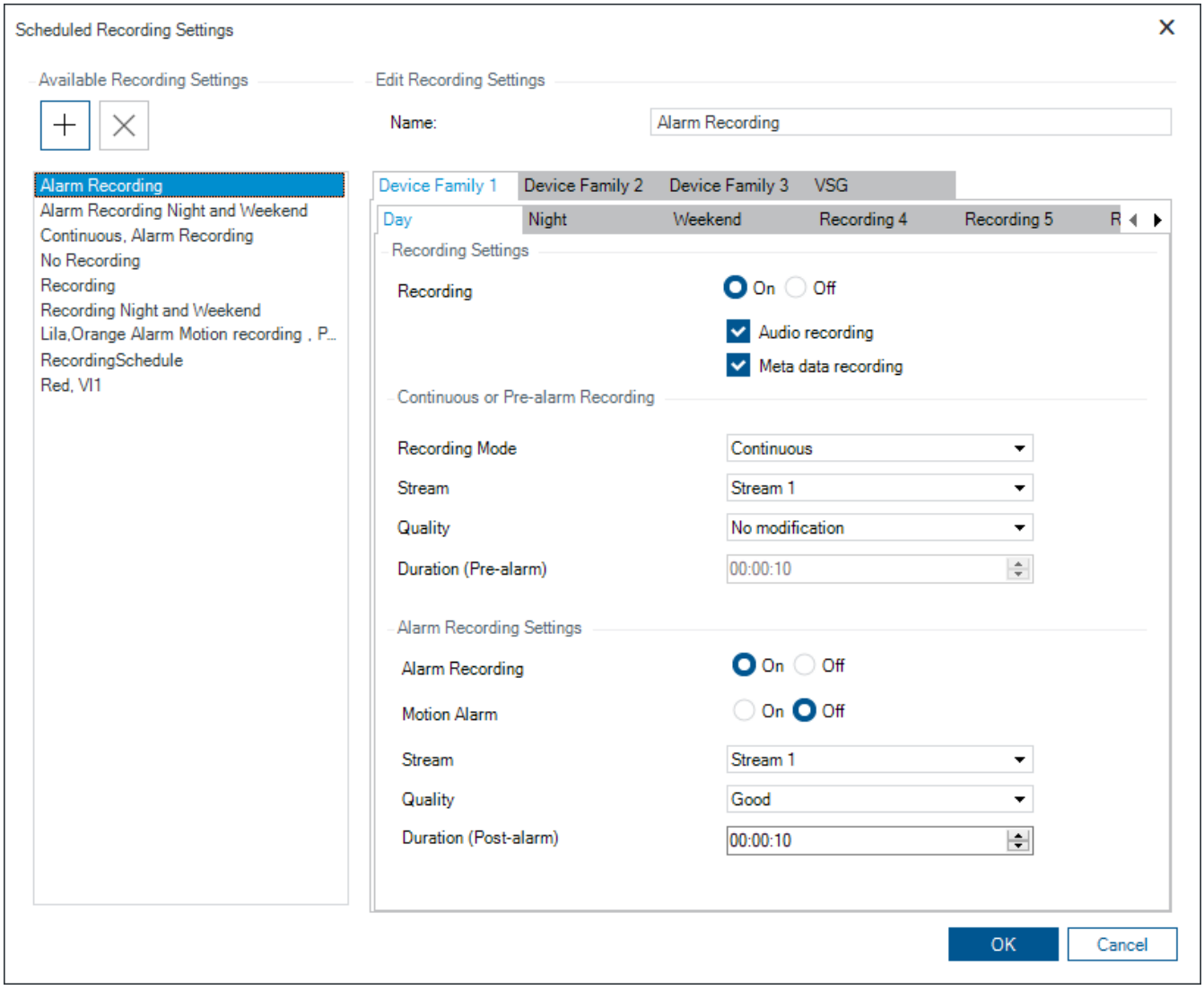
22.6 Диалоговое окно Настройки записи по расписанию (только VRM и локальное хранилище)

Главное окно > **Камеры и запись** > 

Позволяет настроить зависящие от расписания параметры записи для каждой доступной серии устройств. Серия устройств доступна, если в Дерево устройств добавлен хотя бы один кодер данной серии устройств. В таблице **Камеры** такие параметры записи назначаются каждой камере.

Используются Расписания записей, настроенные на странице **Расписания**.

Примечание. Включение или отключение обычной записи действительно для всех серий устройств.



Доступные настройки записи

Выберите предварительно заданную настройку записи для изменения ее параметров. Можно добавлять и удалять заданные пользователем настройки.

Имя:

Введите имя файла для новой настройки записи.

Вкладка «Серия устройств»

Выберите требуемое семейство устройств для настройки параметров записи, действительных для этого семейства устройств.

Вкладка «Расписание записей»

Для выбранного семейства устройств выберите расписание записи для настройки ее параметров.

Запись

Включите или отключите стандартную запись (непрерывную или до сигнала тревоги).

Запись аудио

Выберите, нужно ли записывать звук.

Запись метаданных

Выберите, нужно ли записывать метаданные.

Режим записи
Выберите требуемый режим записи.
Доступны следующие параметры:
– **Непрерывно**
– **До тревоги**

Поток
Выберите требуемый поток, используемый для стандартной записи.
Примечание. Доступность потоков зависит от серии устройства.

Качество
Выберите требуемое качество потока, используемое для стандартной записи. Параметры качества доступны для настройки в диалоговом окне **Параметры качества потока**.

Длительность (до тревоги)
Введите необходимое время записи до тревожного сигнала. Введите время в формате чч:мм:сс.
Примечание. Включено, только если выбран пункт **До тревоги**.

Замечание!
Для значений времени перед тревожным сигналом от 1 до 10 с данные до тревожного сигнала хранятся в ОЗУ кодера, если в ОЗУ достаточно места, в противном случае они передаются в хранилище.
Для значений времени перед тревожным сигналом более 10 с данные до тревожного сигнала передаются в хранилище.
Хранение данных до тревожного сигнала в ОЗУ кодера доступно только для версий микропрограммного обеспечения 5.0 и выше.

Настройки записи по тревоге
Позволяет включать и отключать запись по тревоге для этой камеры.

Тревожный сигнал движения
Позволяет включать и отключать запись по тревоге, запускаемую датчиком движения.

Поток
Выберите поток, который будет использоваться для записи по тревоге.
Примечание. Доступность потоков зависит от серии устройства.

Качество
Выберите требуемое качество потока, используемое для записи по тревоге. Параметры качества доступны для настройки в диалоговом окне **Параметры качества потока**.
Только для устройств, относящихся к семейству устройств 2 или 3: если выбран элемент **Без изменения**, для записи по тревоге используется такое же качество, как и для записи до срабатывания тревоги или непрерывной записи. Рекомендуется использовать значение **Без изменения**. При выборе качества потока для записи по тревоге изменяются только интервал кодирования изображений и скорость передачи в соответствии с параметрами качества данного потока. Используются другие параметры качества, которые настроены для профиля качества, назначенного непрерывной записи или записи до тревожного сигнала.

Длительность (после тревоги)
Введите необходимое время записи по тревоге. Введите время в формате чч:мм:сс.

См.
– *Копирование и вставка в таблицы, Страница 302*

– *Настройка параметров записи (только VRM и Локальное хранилище), Страница 308*

22.7 Настройка параметров портов PTZ

Главное окно > **Устройства** > Разверните > Разверните > > Вкладка **Интерфейсы** > Вкладка **Периферия**

Главное окно > **Устройства** > > > Вкладка **Интерфейсы** > Вкладка **Периферия**

Вы можете настраивать параметры порта только для кодера, на котором активировано управление камерой.

При замене кодера или камеры PTZ настройки порта не сохраняются. Их необходимо настроить снова.

После обновления микропрограммы проверьте настройки порта.

Чтобы настроить параметры порта кодера:

- Внесите необходимые изменения в настройки.
  Изменения в настройках вступают в силу сразу после их сохранения. Активировать конфигурацию нет необходимости.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

22.8 Настройка предустановленных положений и дополнительных команд

Главное окно > **Камеры и запись** >

Для PTZ-камер, камер с функцией ROI и панорамных камер можно заранее определять и сохранять положения камеры. Для PTZ-камер также можно определять дополнительные команды.

Примечание. Для настройки параметров PTZ-камеры сначала необходимо настроить параметры ее порта. В противном случае управление PTZ в данном диалоговом окне работать не будет.

Для настройки предустановленного положения:

1. В таблице **Камеры** выберите нужный кодер.
2. Только для PTZ-камер: чтобы активировать управление PTZ-камерой, установите флажок в столбце .
3. Нажмите кнопку .
   Отобразится диалоговое окно **Препозиции и вспомогательные команды**.
4. Можно определить требуемое количество предустановленных положений.
5. Выберите положение, которое нужно задать.
6. В окне предварительного просмотра с помощью мыши перейдите к положению, которое нужно настроить.
   Изображение можно увеличивать или уменьшать с помощью колесика мыши и можно перемещать путем перетаскивания.
7. При необходимости введите имя для настроенного положения.

8. Нажмите  , чтобы сохранить предустановленное положение.

   Примечание. Значок  нужно нажимать для каждого предустановленного положения. Иначе положение не сохранится.
9. Нажмите **OK**.

Чтобы отобразить уже настроенные предустановленные положения:

1. В таблице **Камеры** выберите нужный кодер.
2. Нажмите кнопку  .
   Отобразится диалоговое окно **Препозиции и вспомогательные команды**.
3. Выберите соответствующее положение.
4. Нажмите  .
   В окне предварительного просмотра отобразится предустановленное положение камеры.

Примечание.

В случае PTZ-камер и камер с функцией ROI предустановленные положения хранятся непосредственно в самой камере. Что касается панорамных камер, то предустановленные положения хранятся в системе BVMS.

PTZ-камеры физически перемещаются в предустановленное положение. Панорамные камеры и камеры с функцией ROI не перемещаются, а лишь отображают некоторый фрагмент полного изображения с камеры.

Для настройки дополнительных команд для PTZ-камер:

1. В таблице **Камеры** выберите нужный кодер.
2. Нажмите кнопку  .
   Отобразится диалоговое окно **Препозиции и вспомогательные команды**.
3. Откройте вкладку **Команды AUX**.
4. Задайте необходимые настройки.
5. Для сохранения предустановленных команд нажмите  .

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.

- *Диалоговое окно «Предустановленные положения и дополнительные команды», Страница 313*
- *Настройка параметров портов PTZ, Страница 311*
- *Настройка тревоги, Страница 335*
- *Диалоговое окно Выбрать содержимое Области изображений, Страница 323*
- *Диалоговое окно Параметры тревог, Страница 325*
- *Диалоговое окно «Выбрать содержимое области изображений» (MG), Страница 324*

22.9 Диалоговое окно «Предустановленные положения и дополнительные команды»

Главное окно > **Камеры и запись** >  > выберите PTZ-камеру, камеру с функцией ROI или панорамную камеру > 

Позволяет настроить PTZ-камеру, камеру с функцией ROI или панорамную камеру.
Для камер с функцией ROI и панорамных камер дополнительные команды недоступны.
Примечание. Для настройки параметров PTZ-камеры сначала необходимо настроить параметры ее порта. В противном случае управление PTZ в данном диалоговом окне работать не будет.

Значки

	Нажмите для перемещения камеры в предустановленное положение или для выполнения команды.
	Нажмите для сохранения предустановленного положения или команды.

Вкладка Препозиции
Нажмите для отображения таблицы предопределенных положений.

Номер
Отображает номер предопределенного положения.

Имя
Щелкните ячейку для изменения имени предопределенного положения.

Вкладка Команды AUX (только для камер PTZ)
Нажмите для отображения таблицы вспомогательных команд.
Примечание. Если кодер ONVIF поддерживает вспомогательные команды, они предоставляются непосредственно из кодера ONVIF.

Номер
Отображает номер вспомогательной команды.

Имя
Щелкните ячейку для изменения имени вспомогательной команды.

Код
Щелкните ячейку для редактирования кода команды.

См.
- *Настройка параметров портов PTZ, Страница 311*
- *Настройка предустановленных положений и дополнительных команд, Страница 311*

22.10 Настройка функции ROI

Главное окно > **Камеры и запись** > 

Можно включить функцию ROI для фиксированной камеры HD.
Необходимо настроить поток 2 для видео в реальном времени и необходимо настроить кодек H.264 MP SD ROI или H.265 MP SD ROI для потока 2.

Убедитесь, что поток 2 используется для видео в реальном времени на всех рабочих станциях, где будет использоваться ROI.

Включение функции ROI.

1. В столбце **Поток 2** - **Кодек** выберите необходимый кодек H.264 MP SD ROI или H.265 MP SD ROI.
2. В столбце **Видеоизображение в реальном времени** - **Поток** выберите **Поток 2**.
3. Установите флажок в столбце **Видеоизображение в реальном времени** - **Область интереса ""**.

Отключение функции ROI.

1. Снимите установленный флажок в столбце **Видеоизображение в реальном времени** - **Область интереса ""**.
2. В столбце **Поток 2** – **Кодек** выберите необходимый кодек.

См.

– *Страница Камеры, Страница 297*

22.11 Настройка функции ANR

Главное окно > **Камеры и запись** >

Перед включением функции ANR необходимо добавить носитель данных кодера требуемому кодеру и настроить этот носитель данных.

Для настройки функции ANR необходимо отключить двойную запись кодера.

Функция ANR работает только на кодерах с версией микропрограммного обеспечения 5.90 и выше. Не все типы кодеров поддерживают ANR, даже если установлена верная версия микропрограммного обеспечения.

Для включения:

- Установите флажок в строке требуемой камеры в столбце **ANR**.

См.

– *Настройка двойного режима записи в Таблице камер, Страница 314*
– *Страница Камеры, Страница 297*
– *Настройка носителей данных кодера, Страница 239*

22.12 Настройка двойного режима записи в Таблице камер

Главное окно > **Камеры и запись** >

Для настройки двойной записи функцию ANR необходимо отключить.

Если выполняется настройка двойной записи для одной камеры многоканального кодера, система следит за тем, чтобы все камеры этого кодера были настроены на один и тот же получатель записи.

Для настройки:

1. В столбце **Вторичная запись** - **Целевой объект** выберите ячейку требуемого кодера, а затем нажмите требуемый пул вторичного VRM.
   Все камеры соответствующего кодера автоматически настраиваются на запись в выбранный вторичный VRM.
2. В столбце **Параметр** выберите параметр записи по расписанию.

См.

– *Настройка двойного режима записи в Дереве устройств, Страница 195*

– *Настройка функции ANR, Страница 314*
– *Двойная / резервная запись, Страница 30*
– *Страница Камеры, Страница 297*

22.13 Управление шлюзом Video Streaming Gateway

См.
– *Страница устройства Video Streaming Gateway, Страница 207*
– *Диалоговое окно "Добавить кодер Bosch", Страница 210*
– *Диалоговое окно "Добавить кодер ONVIF", Страница 211*
– *Диалоговое окно "Добавить камеру JPEG", Страница 213*
– *Диалоговое окно "Добавить кодер RTSP", Страница 214*

22.13.1 Назначение профиля ONVIF

Главное окно > **Камеры и запись** > 

Можно назначить ключ медиапрофиля ONVIF камере ONVIF.
Ключ можно назначить либо для видео в реальном времени, либо для записи.

Назначение ключа для видео в реальном времени.

- В столбце **Видеоизображение в реальном времени** – **Профиль** выберите необходимый элемент.

Назначение ключа для записи.

- В столбце **Запись** – **Профиль** выберите необходимый элемент.

См.
– *Страница Камеры, Страница 297*

23 Страница События

Главное окно > **События**

Отображает дерево событий со всеми доступными событиями и таблицей настройки событий для каждого события. События сгруппированы по типу, например все события записи с камер, такие как непрерывная запись или запись по тревоге, сгруппированы по режиму записи.

Доступные события сгруппированы по соответствующим устройствам. Изменение состояния устройства отображается под значком  в виде  . Все другие события отображаются в зависимых от устройства группах в виде  .

Для каждого события могут быть настроены:

- Включение тревоги в соответствии с расписанием (доступно не для всех событий).
- Регистрация события в журнале в соответствии с расписанием. Если событие зарегистрировано в журнале, оно отображается в списке событий Operator Client.
- Выполнение командного сценария в соответствии с расписанием (доступно не для всех событий).
- Для событий типа  : добавление текстовых данных к записи.

Если событие происходит, ваши настройки выполняются.

При помощи логических выражений вы можете создать сложное событие, объединяющее несколько событий.

- Щелкните элемент дерева для отображения соответствующей таблицы настройки событий.

 Нажмите для дублирования события. Используйте это для генерирования нескольких тревожных сигналов для определенного события.

 Нажмите для удаления дублированного или сложного события.

 Нажмите для переименования выбранного сложного события.

 Нажмите, чтобы отобразить диалоговое окно для создания при помощи логических выражений сложного события, состоящего из других событий (максимум 10).

Сложные события добавляются в таблицу настройки события.

 Нажмите для редактирования выбранного сложного события.

 Нажмите, чтобы отобразить диалоговое окно для создания и редактирования командных сценариев.

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

См.

- *Настройка событий и тревог, Страница 330*
- *Настройка командных сценариев, Страница 92*
- *Диалоговое окно «Параметры» (меню «Настройки»), Страница 124*
- *Настройка мигающих активных точек, Страница 338*

23.1 Вкладка "Настройки задержки"

Примечание: для некоторых событий вкладка "Параметры задержки" недоступна из-за технических ограничений.
Позволяет настроить параметры задержки для выбранного события.

Время задержки
В течение указанного периода времени все дальнейшие события игнорируются.

Приоритет состояния события
Состоянию события можно назначить настройку приоритета.

Изменить приоритеты
Нажмите, чтобы отобразить диалоговое окно для настройки параметров приоритета.

Добавить параметр
Нажмите для добавления строки для настройки времени задержки, которое отличается от времени задержки всех устройств.

Удалить параметр
Нажмите, чтобы удалить выделенную строку. Для выбора строки нажмите левый заголовок строки.

23.2 Вкладка "Настройки" для расширенного отображения карты

Настройка цвета состояний на картах возможна, только если установлен флажок **Включено расширенное отображение состояния (выделение активных точек цветом на картах в зависимости от состояния)** или флажок **Включено расширенное отображение состояния (выделение активных точек цветом на картах в зависимости от тревоги)** в диалоговом окне **Параметры**.

Для каждого события или тревоги () можно настроить цвет фона и поведение активных точек (мигает или не мигает). Например, можно настроить событие или тревогу  устройства так, чтобы его значок устройства на карте начинал мигать при изменении состояния этого устройства.
Кроме того, можно настроить приоритет отображения для всех активных точек. Это необходимо, если для одного устройства возникают различные события. (1 = наивысший приоритет)
Настроенный цвет действует для всех активных точек с одинаковым приоритетом отображения. Можно изменить цвет, поведение и приоритет для любого события или тревоги  : изменение цвета и поведения используется для всех активных точек всех остальных событий или тревог  , имеющих такой же приоритет.

Включить цвет состояний на картах
Нажмите, чтобы активные точки устройств, принадлежащих этому событию, отображались с цветным фоном и могли мигать на картах.

Приоритет отображения на карте:
Щелкайте стрелки, чтобы изменять приоритет активных точек устройств, принадлежащих этому событию.

Цвет фона на карте:
Нажмите поле цвета, чтобы выбрать цвет фона, используемый для активных точек устройств, принадлежащих этому событию.
Примечание. Все события состояния всех устройств с одинаковым приоритетом имеют один и тот же цвет.

Мигание
Нажмите, чтобы включить мигание активных точек устройств, принадлежащих этому событию.

23.3 Вкладка "Настройки" для конфигурации событий

Устройство
Отображает имя устройства или расписания.

Сеть
Отображает IP-адрес соответствующего IP-устройства.

Активировать тревогу
Нажмите ячейку, чтобы выбрать расписание записей или задач для активации тревоги.
Выберите **Всегда**, если нужно, чтобы тревога была активирована независимо от момента времени.
Выберите **Никогда**, если не нужно активировать тревогу.

Журнал
Нажмите ячейку в столбце **Расписание**, чтобы выбрать расписание записей или задач для регистрации в журнале.
Выберите **Всегда**, если хотите, чтобы событие было зарегистрировано независимо от момента времени.
Выберите **Никогда**, если не нужно регистрировать событие.

Сценарий
Нажмите ячейку в столбце **Сценарий**, чтобы выбрать командный сценарий.
Нажмите ячейку в столбце **Расписание**, чтобы выбрать расписание записей или задач для выполнения командного сценария.
Выберите **Всегда**, если нужно, чтобы командный сценарий был выполнен независимо от момента времени.
Выберите **Никогда**, если не нужно выполнять командный сценарий.

Запись текстовых данных
Можно настроить добавление текстовых данных к непрерывной записи камеры.
Примечание. Этот столбец доступен только для событий, содержащих текстовые данные, например **Устройства ATM/POS** > **Вход ATM** > **Ввод данных**

23.4 Диалоговое окно Редактор командных сценариев

Главное окно > **События** > 
Позволяет создавать и редактировать командные сценарии.

 Нажмите для сохранения измененных настроек.

 Нажмите для восстановления сохраненных настроек.

Нажмите для проверки кода сценария.

Нажмите для создания файла команды.

Нажмите для удаления файла команды.

Нажмите, чтобы отобразить диалоговое окно для импорта файла сценария.

Нажмите, чтобы отобразить диалоговое окно для экспорта файла сценария.

Нажмите для преобразования существующего сценария в другой доступный язык сценария. Все существующие тексты сценариев удаляются.

Нажмите для отображения интерактивной справки BVMS Script API.

Нажмите для отображения интерактивной справки BVMS.

Нажмите для закрытия диалогового окна **Редактор командных сценариев**.

См.

– *Настройка командных сценариев, Страница 92*

23.5 Диалоговое окно Создать сложное событие / Редактировать сложное событие

Главное окно > **События** >

Позволяет создавать и изменять сложные события.

Чтобы искать элементы:

- Введите запрос в поле поиска и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

Имя события:

Введите нужное имя сложного события.

Состояния событий:

Выберите изменение состояния, которое должно стать частью сложного события.

Объекты:

Выберите один или несколько доступных объектов выбранного состояния события. Это состояние и выбранный объект отображаются в дереве сложных событий как непосредственный дочерний элемент корневого оператора.

Сложное событие:

Позволяет создавать сложные события в дереве сложных событий. Все непосредственные дочерние элементы логического оператора (AND, OR) объединяются этим оператором.

См.

– *Создание сложного события, Страница 333*
– *Редактирование сложного события, Страница 334*

23.6 Диалоговое окно Выберите язык сценария

Главное окно > **События** > 

Позволяет выбрать язык для вашего командного сценария.
Вы не можете изменить язык существующих командных сценариев.

Язык сценария:
Выберите нужный язык сценария.

См.

– *Настройка командных сценариев, Страница 92*

23.7 Диалоговое окно Изменение приоритетов типа события

Главное окно > **События** > вкладка **Параметры задержки** > **Изменить приоритеты** кнопка
Можно настроить приоритеты разных изменений состояния типа событий (если применимо), например "Виртуальных вход закрыт" и "Виртуальный вход открыт". Изменение состояния с более высоким приоритетом переопределяет время задержки другого изменения состояние с более низким приоритетом.

Название приоритета:
Введите название для данного параметра приоритета.

Значение состояния
Отображаются названия состояний выбранного события.

Приоритет состояния:
Введите требуемый приоритет. 1=наивысший приоритет, 10=самый низкий приоритет.

23.8 Диалоговое окно Выбор устройств

Главное окно > **События** >  или  > вкладка **Настройки задержки** > кнопка **Добавить параметр**

Выбрать
Установите данный флажок для требуемой записи и нажмите **ОК**, чтобы добавить строку в таблицу **Устройства со специальными параметрами задержки**.

23.9 Диалоговое окно "Запись текстовых данных"

Главное окно > **События** > в дереве событий выберите  **Ввод данных** (текстовые данные должны быть доступны, например **Устройства чтения кредитных карточек** > **Устройство чтения кредитных карточек** > **Карта отклонена**) > столбец **Запись текстовых данных** > ...
Можно настроить камеры, для которых к непрерывной записи камеры будут добавляться текстовые данные.

См.

– *Включение записи по тревоге с помощью текстовых данных, Страница 336*

24 Страница Тревожные сигналы

Главное окно > **Тревожные сигналы**

Отображает дерево событий таблицу настройки тревог для каждого события.

Отображаются только те события, которые настроены на странице **События**.

В таблицах вы можете настроить, каким образом будет отображаться тревожный сигнал, вызванный данным событием, а также, какие камеры будут вести запись и отображаться при срабатывании данного тревожного сигнала.

Некоторые события настроены как тревожные сигналы по умолчанию, например, системная ошибка.

Вы можете настроить тревожное событие для следующих событий:

- Изменение режима записи
- Изменение состояния тревожного события
- Большинство пользовательских действий, например, действия по управлению камерами PTZ

 Нажмите для отображения диалогового окна **Диспетчер ресурсов**.

 Отображает диалоговое окно настройки параметров тревоги, действующих на этом сервере Management Server.

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

- Щелкните элемент дерева для отображения соответствующей таблицы настройки тревожного сигнала.

Устройство

Отображает устройство условия события, выбранного в дереве событий.

Сетевой адрес

Отображает IP-адрес соответствующего IP-устройства.

Идентификатор тревоги

В столбце **Приоритет** нажмите в ячейке и введите приоритет тревоги для выбранной тревоги (**100** — низкий, **1** — высокий). В столбце **Название** нажмите в ячейке и введите название тревожного сигнала, которое будет отображаться в системе BVMS, например, в списке тревог. В столбце **Цвет** нажмите в ячейке, чтобы отобразить диалоговое окно для выбора цвета, которым будет отображаться тревожный сигнал в Operator Client, например, в списке тревог.

Области изображений тревог

В одном из столбцов **1-5** нажмите ячейку в ... для отображения диалогового окна выбора камеры.

Можно выбрать только ту камеру, которая была добавлена в логическое дерево на странице **Карты и структура**.

Можно настроить количество доступных областей изображений тревог в диалоговом окне **Настройки тревог**.
В столбце **Аудиофайл** нажмите ... в ячейке, чтобы отобразить диалоговое окно для выбора аудиофайла, который должен воспроизводиться в случае тревоги.

Параметры тревог
Нажмите ячейку в ... для отображения диалогового окна **Параметры тревог**.

См.
– *Обработка сигналов тревоги, Страница 39*

24.1 Диалоговое окно Настройки тревог

Главное окно > **Тревожные сигналы** > 

Вкладка Настройки тревог

Макс. количество областей изображений на тревогу:
Введите максимальное количество областей изображений тревог, которые будут отображаться в случае тревоги.
Примечание. Если используется система Enterprise System, применяется максимальное количество, установленное на подключенных серверах Management Servers.

Время автоматического отключения:
Введите время в секундах, через которое тревожное событие будет автоматически отключено.
Это относится только к тревожным сигналам, для которых на странице **Тревожные сигналы** задано значение **Автоотключение тревоги по истечении определенного времени (диалоговое окно 'Настройки тревог')**.

Многострочное отображение тревоги в окне изображений тревог
Установите флажок, чтобы включить отображение многострочных тревог окна тревожных событий.

Замечание!
Для существующих конфигураций тревог режим многострочных тревог активирован; для новый конфигураций тревог он отключен по умолчанию, при этом активирован одноэкранный режим.

Настроить лимит продолжительности записи тревог, вызванных состояниями:
Установите флажок, чтобы включить ограничение длительности записей по тревоге.
Введите длительность записи по тревоге в минутах. Запись по тревоге останавливается автоматически по истечении установленного времени.
Пользователь может ввести длительность от 1 до 1440 минут.
Когда тревожное событие инициирует запись с настроенным ограничением длительности:
– если тревожное событие повторно активируется до истечения времени ожидания, запись продолжается, а время ожидания начинается с 0;
– если тревогу отменяют до истечения времени ожидания, запись продолжается в течение настроенного времени ожидания после тревоги.

Вкладка Группы мониторов

Порядок отображения в случае одинакового приоритета тревог
Выберите нужное значение для сортировки сигналов тревоги с одним приоритетом в соответствии с их меткой времени.

Отобразить пустой экран
нажмите, чтобы на мониторе, не используемом в качестве экрана тревожных сигналов, не отображалось ничего.

Продолжить отображение в реальном времени
нажмите, чтобы на мониторе, не используемом в качестве экрана тревожных сигналов, отображалось изображение в реальном времени.

См.
– *Настройка параметров для всех тревог, Страница 335*

24.2 Диалоговое окно Выбрать содержимое Области изображений

Главное окно > **Тревожные сигналы** >  или  > **Столбец «Области изображений тревог»** > Нажмите ... в одном из столбцов **1-5**
Позволяет выбирать элемент логического дерева, который отображается и записывается (если элементом является камера) в случае возникновения выбранного тревожного события.

Замечание!
Изображение карты объекта в области тревожных изображений оптимизировано для отображения на экране и содержит только исходный вид оригинального файла карты.

Найти элемент
Введите текст для поиска элемента в логическом дереве.

Найти
Нажмите для поиска камеры по введенному тексту в ее описании.

Режим реального времени
Нажмите, чтобы указать, что в случае тревоги должно отображаться живое видео с камеры.

Немедленное воспроизведение
Нажмите, чтобы указать, что должно отображаться немедленное воспроизведение с камеры.
Время перемотки для тревоги при немедленном воспроизведении настраивается на странице **Функции оператора** (см. раздел *Страница Свойства оператора, Страница 349*).

Приостановить воспроизведение
Установите этот флажок для отображения приостановленного немедленного воспроизведения тревожного события с камеры. Пользователь при необходимости может запустить немедленное воспроизведение вручную.

Закольцованное воспроизведение
Установите этот флажок для отображения зацикленного немедленного воспроизведения тревожного события с камеры.

Продолжительность зацикленного немедленного воспроизведения в области тревожных изображений определяется как сумма: время перемотки + продолжительность состояния тревоги + плюс время перемотки.

Записать с данной камеры
Установите флажок, чтобы разрешить для данной камеры запись по тревоге. При срабатывании тревоги запись с этой камеры производится с качеством режима записи по тревоге. Продолжительность записи равна продолжительности состояния тревоги плюс время перед и после тревоги. Этот параметр непосредственно влияет на настройки записи по тревоге в диалоговом окне **Параметры тревог** и наоборот.
Примечание. Если для панорамной камеры выбрано предустановленное положение, сохраняется не только этот фрагмент изображения, но и полное круговое изображение.

Панорамная препозиция
В случае выбора панорамной камеры можно выбрать предустановленное положение камеры. После того как пользователь Operator Client подтверждает получение сигнала тревоги, отображается кадрированное тревожное изображение, соответствующее предустановленному положению.
В случае выбора **<нет>** тревожное изображение выводится в панорамном представлении.

См.
- *Страница Свойства оператора, Страница 349*
- *Настройка тревоги, Страница 335*

24.3 Диалоговое окно «Выбрать содержимое области изображений» (MG)

Главное окно >

Тревожные сигналы >  или  > столбец **Параметры тревог** > нажмите ... > диалоговое окно **Параметры тревог** > вкладка **Группа мониторов** > нажмите ... в одном из столбцов 1–10
Позволяет выбрать камеру в логическом дереве. Изображение с этой камеры будет отображаться на назначенном мониторе в случае возникновения выбранной тревоги.

Найти элемент
Введите текст для поиска элемента в логическом дереве.

Найти
Нажмите для поиска камеры по введенному тексту в ее описании.

Панорамная препозиция
В случае выбора панорамной камеры можно выбрать предустановленное положение камеры. После того как пользователь Operator Client подтверждает получение сигнала тревоги, отображается кадрированное тревожное изображение, соответствующее предустановленному положению.
Если выбрать **<нет>**, декодер отображает тревожное изображение в виде круга.

Камера не выбрана
Нажмите, чтобы удалить камеру из столбца группы мониторов.
Примечание.
Поле обзора в предустановленном положении панорамной камеры у Operator Client или Configuration Client и у декодера разное.

Замечание!
Для использования предустановленных положений, настроенных для панорамных камер, параметр **Положение установки** панорамной камеры должен иметь значение **Стена** или **Потолок**.

24.4 Диалоговое окно Параметры тревог

Главное окно > **Тревожные сигналы** >  или  > столбец **Параметры тревог** > ...
Позволяет настроить следующие параметры тревог:
- Камеры, начинающие запись в случае тревоги.
- Включение защиты этих записей по тревоге.
- Включение и настройка отличающихся параметров длительности тревоги.
- Включение команд управления камерами PTZ в случае тревоги.
- Уведомления, отправляемые в случае тревоги.
- Поток заданий, выполняемый в случае тревоги.
- Назначение камер, отображаемых в группах мониторов в случае тревоги.

Вкладка Камеры

Номер	Отображает номер камеры в соответствии с настройками на странице **Камеры и запись**.
Имя	Отображает название камеры в соответствии с настройками на странице **Камеры и запись**.
Местонахождение	Отображает местонахождение в соответствии с настройками на странице **Карты и структура**.
Запись	Установите флажок, чтобы запись по тревоге с данной камеры включалась в случае тревоги. При срабатывании тревоги запись с этой камеры производится с качеством режима записи по тревоге. Продолжительность записи равна продолжительности состояния тревоги плюс время перед и после тревоги. Этот параметр непосредственно влияет на настройки записи по тревоге в диалоговом окне **Выбрать содержимое Области изображений** и наоборот.
Защитить запись	Установите флажок, чтобы обеспечить защиту записи по тревоге с данной камеры. **Примечание:** Защищенные видео данные никогда не удаляются VRM автоматически. Учитывайте, что слишком много защищенных блоков может привести к заполнению хранилища и камера остановит запись.
Изменение настройки длительности тревоги	Этот флажок устанавливается автоматически при установке флажка **Запись**, и если камера поддерживает ANR.

Команды AUX	Щелкните ячейку для выбора вспомогательной команды, которая должна быть выполнена в случае тревоги. Записи в этом списке доступны только для камер PTZ.
Препозиция	Щелкните ячейку для выбора предопределенного положения, которое должно быть установлено в случае тревоги. Записи в этом списке доступны только для камер PTZ.

Примечание. Невозможно настроить сразу оба параметра **Команды AUX** и **Препозиция** для одной камеры и тревоги.

Вкладка Уведомления

Электронная почта	Установите флажок для отправки электронного сообщения в случае тревоги.
Сервер:	Выберите сервер электронной почты.
Получатели:	Введите адреса электронной почты получателей, разделяя их запятыми (пример: name@provider.com).
Текст:	Введите текст уведомления.
Информация:	Установите флажок для добавления соответствующей информации к тексту уведомления. **Примечание.** Для электронной почты используется дата часового пояса Management Server.

Вкладка Поток заданий

Записывать только тревогу	Установите флажок, для того чтобы в случае тревоги с данной камеры производилась запись, а изображение не отображалось. Этот флажок активен только в том случае, если установлен флажок **Запись** на вкладке **Камеры**.
Автоотключение тревоги по истечении определенного времени (диалоговое окно 'Настройки тревог')	Установите флажок, чтобы тревога автоматически отключалась.
Автоотключение тревоги при возвращении события в нормальное состояние	Установите этот флажок, чтобы тревога автоматически отключалась, когда событие, вызвавшее эту тревогу, изменяет свое состояние. Тревога не будет отключена автоматически, если она принята или не принята.
Запретить удаление тревог при сохранении состояния срабатывания	Установите флажок, чтобы предотвратить удаление тревоги до устранения причины тревоги.
Подавлять дублирующиеся тревоги в списке тревог	Установите флажок, чтобы избежать дублирования тревог для одного типа события и устройства в списке тревог BVMS Operator Client.

	Пока тревога активна (в состоянии тревоги **Активно** или **Принято**), никакие последующие тревоги для того же типа события или устройства не отображаются в списке тревог. **Примечание.** – События по-прежнему регистрируются в журнале. – Обратите внимание, что все возможные действия по этой тревоге (например, запуск записи по тревоге и т.д.) не запускаются повторно. После очистки тревоги и возникновения новой тревоги того же типа для того же устройства, новая тревога снова появляется в списке тревог и снова возникают все возможные действия по этой тревоге. – Этот флажок заранее установлен для тревог Person Identification.
Показать план действий	Установите флажок, чтобы обеспечить выполнение алгоритма реакции в случае тревоги.
Ресурсы...	Нажмите для отображения диалогового окна **Диспетчер ресурсов**. Выберите документ с описанием соответствующего потока заданий.
Показать поле комментариев	Установите флажок, чтобы обеспечить отображение поля комментариев в случае тревоги. В этом поле пользователь может ввести комментарии к тревоге.
Форсировать обработку потока заданий оператором	Установите флажок, чтобы форсировать обработку потока заданий пользователем. При установке данного флажка пользователь не может отключить тревогу, до тех пор пока не введет комментарий к тревоге.
Выполнить следующий клиентский сценарий после принятия тревоги:	выберите клиента Командный сценарий, который выполняется автоматически, когда пользователь принимает тревогу.

Вкладка Группа мониторов

1...10	Нажмите ячейку в столбце под номером. Откроется диалоговое окно **Выбрать содержимое Области изображений**. Выберите камеру в логическом дереве. Изображение с этой камеры будет отображаться на назначенном мониторе в случае тревоги. Выберите предустановленные положения камеры, если они настроены. Дополнительные сведения см. в описании диалогового окна **Выбрать содержимое Области изображений** (MG) в онлайн-справке.
Очистить таблицу	Нажмите для удаления всех назначений камер группам мониторов.

Название тревожного сигнала	Установите флажок, чтобы название тревоги отображалось на мониторах в виде экранного сообщения.
Время тревожного сигнала	Установите флажок, чтобы время тревоги отображалось на мониторах в виде экранного сообщения.
Дата тревоги	Установите флажок, чтобы дата тревоги отображалась на мониторах в виде экранного сообщения.
Имя тревожной камеры	Установите флажок, чтобы название тревожной камеры отображалось на мониторах в виде экранного сообщения.
Номер тревожной камеры	Установите флажок, чтобы номер тревожной камеры отображался на мониторах в виде экранного сообщения.
Только на первом мониторе	Установите флажок, чтобы время и название тревоги отображались в виде экранного сообщения только на первом мониторе группы мониторов.

Вкладка Изменение настройки длительности тревоги

Настройки на этой вкладке доступны, только если для этой камеры включена функция ANR.

Использовать настройки профиля	Нажмите, чтобы включить этот параметр. Для этой камеры используются параметры длительности до и после срабатывания тревоги, заданные в диалоговом окне **Настройки записи по расписанию**.
Переопределить настройки	Нажмите для включения следующих параметров длительности до и после срабатывания тревоги.
Длительность (до тревоги)	Доступно для всех событий.
Длительность (после тревоги)	Доступно только для событий  .

Вкладка **Уровень угрозы**

Повышение уровня угрозы до	Выберите уровень угрозы, при котором активируется эта тревога. Выберите **Сбросить уровень угрозы**, если эта тревога должна сбросить активный уровень угрозы. Клиент Operator Client прекратит сеанс, и пользователь сможет снова войти в систему.

См.

- *Диалоговое окно «Выбрать содержимое области изображений» (MG), Страница 324*
- *Включение записи по тревоге с помощью текстовых данных, Страница 336*
- *Настройка тревоги, Страница 335*
- *Настройка длительности до и после срабатывания тревожного сигнала, Страница 336*

24.5 Диалоговое окно Выбрать ресурс

Главное окно > **Тревожные сигналы**>  или  > **Столбец «Идентификатор тревоги»** > Столбец **Аудиофайл** > Нажмите ...

Позволяет выбрать аудиофайл, воспроизводимый в случае тревоги.

Воспроизведение

Нажмите для воспроизведения выбранного аудиофайла.

Пауза

Нажмите для приостановки воспроизведения выбранного аудиофайла.

Стоп

Нажмите для остановки воспроизведения выбранного аудиофайла.

Управление...

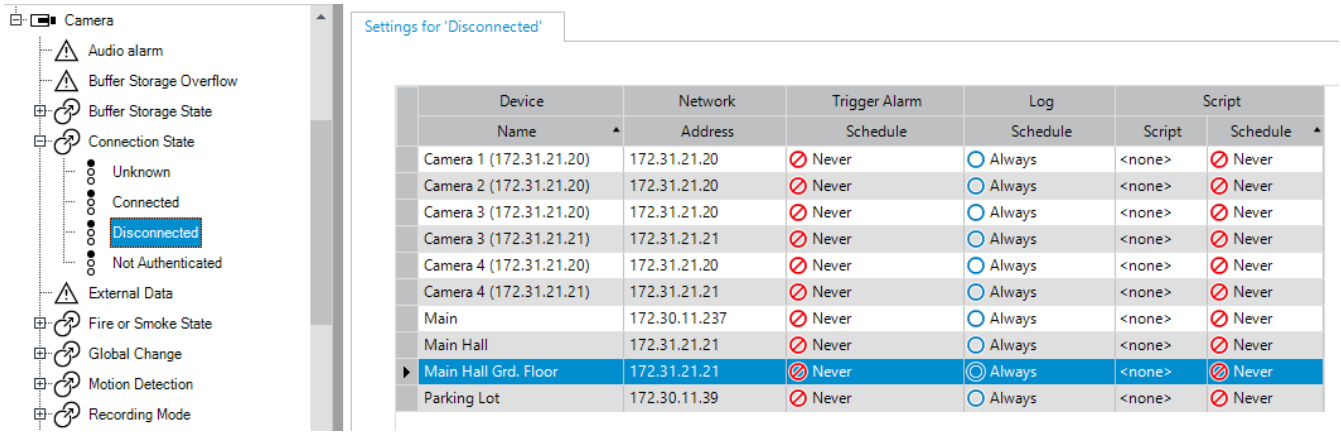
Нажмите для отображения диалогового окна **Диспетчер ресурсов**.

См.

- *Настройка тревоги, Страница 335*
- *Управление файлами ресурсов, Страница 331*

25 Настройка событий и тревог

Главное окно > **События**
или
Главное окно > **Тревожные сигналы**
В данном разделе содержится информация о настройке событий и тревог в системе.
Доступные события сгруппированы по соответствующим устройствам.
На странице **События** можно настроить, в каких ситуациях событие в BVMS будет активировать тревогу, выполнять командный сценарий и регистрироваться в журнале.
Пример (часть таблицы настройки событий):



Данный пример означает следующее:
При потере видеосигнала с выбранной камеры активируется тревожное событие, событие регистрируется в журнале, а сценарии не выполняются.
На странице **Тревожные сигналы** можно настроить способ отображения тревоги, а также указать камеры, изображения с которых будут воспроизводиться и записываться в случае тревоги.
Некоторые системные события по умолчанию сконфигурированы как тревоги.

- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

См.

- *Вкладка "Настройки задержки", Страница 317*
- *Вкладка "Настройки" для расширенного отображения карты, Страница 317*
- *Вкладка "Настройки" для конфигурации событий, Страница 318*
- *Диалоговое окно Редактор командных сценариев, Страница 318*
- *Диалоговое окно Создать сложное событие / Редактировать сложное событие, Страница 319*
- *Диалоговое окно Выберите язык сценария, Страница 320*
- *Диалоговое окно Изменение приоритетов типа события, Страница 320*
- *Диалоговое окно Выбор устройств, Страница 320*
- *Диалоговое окно "Запись текстовых данных", Страница 320*
- *Диалоговое окно Настройки тревог, Страница 322*
- *Диалоговое окно Выбрать содержимое Области изображений, Страница 323*

– *Диалоговое окно Параметры тревог, Страница 325*

25.1 Копирование и вставка в таблицы

Можно одновременно настраивать многие объекты в таблице камер, таблице настройки событий или таблице настройки тревог при помощи всего лишь нескольких щелчков мышью.
Подробные сведения см. в *Копирование и вставка в таблицы, Страница 302*.

25.2 Удаление строки из таблицы

Главное окно > **Тревожные сигналы**
Вы можете удалять только те строки, которые были добавлены вами или другим пользователем, т.е. вы можете удалять дублированные или сложные события.
Сложные события находятся в дереве событий в разделе **Системные устройства** > **Сложные события**.

Чтобы удалить строку из таблицы:

1. Выделите строку
2. Нажмите  .

См.

– *Страница События, Страница 316*

25.3 Управление файлами ресурсов

Подробные сведения см. в:

– *Управление файлами ресурсов, Страница 272*.

25.4 Настройка события

Главное окно > **События**

Настройка события:

1. Выберите в дереве событие или состояние события, например **Системные устройства** > **Идентификация** > **Аутентификация оператора отклонена**.
   Откроется соответствующая таблица настройки событий.
2. В столбце **Активировать тревогу** - **Расписание** нажмите ячейку и выберите соответствующее расписание.
   Расписание определяет, когда запускается тревожный сигнал.
   Выберите одно из расписаний записей или расписаний задач, настроенных на странице **Расписания**.
3. Выберите ячейку в столбце **Журнал** - **Расписание** и выберите соответствующее расписание.
   Расписание определяет время регистрации события.
4. Выберите ячейку в столбце **Сценарий** - **Сценарий** и выберите соответствующий командный сценарий.
5. В столбце **Сценарий** - **Расписание** нажмите ячейку и выберите соответствующее расписание.
   Расписание определяет, когда событие запускает командный сценарий.

См.

– *Страница События, Страница 316*

25.5 Дублирование события

Главное окно > **События**

Вы можете дублировать событие для активации нескольких тревожных сигналов для одного события.

Чтобы дублировать событие:

1. Выберите в дереве условие события. Отображается соответствующая таблица настройки событий.
2. Выберите строку таблицы.
3. Нажмите значок  . В таблицу будет добавлена новая строка. Она имеет параметры по умолчанию.

См.

– *Страница События, Страница 316*

25.6 Регистрация пользовательских событий

Главное окно > **События Системные устройства** > разверните **Действия пользователя**

Можно настроить способы регистрации в журнале некоторых действий пользователя отдельно для каждой доступной группы пользователей.

Пример:

Регистрация пользовательских событий:

1. Выберите пользовательское событие для настройки способа его регистрации, например **Вход оператора**.
   Откроется соответствующая таблица настройки событий.
   Каждая группа пользователей отображается в столбце **Устройство**.
2. В случае доступности: выберите ячейку в столбце **Активировать тревогу** - **Расписание** и выберите соответствующее расписание.
   Расписание определяет время активации уведомляющего пользователя тревожного сигнала.
   Можно выбрать одно из расписаний записей или расписаний задач, настроенных на странице **Расписания**.
3. Выберите ячейку в столбце **Журнал** - **Расписание** и выберите соответствующее расписание.
   Расписание определяет время регистрации события.
   В данном примере вход оператора группы администраторов и группы опытных пользователей не будет зарегистрирован, а вход оператора группы пользователей "Live" будет зарегистрирован по расписанию **День**.

См.

– *Страница События, Страница 316*

25.7 Настройка кнопок пользовательских событий

Главное окно > **События**

Вы можете настроить кнопки пользовательских событий Operator Client. Вы можете настроить Operator Client таким образом, чтобы одна или несколько кнопок пользовательских событий не отображались.

На странице **Группы пользователей** можно настроить систему таким образом, чтобы кнопки пользовательских событий отображались только в Operator Client соответствующей пользовательской группы.

Чтобы настроить кнопки пользовательских событий:

1. В дереве выберите **Системные устройства** > **Кнопки событий модуля Operator Client** > **Кнопка события нажата**.
   Отображается соответствующая таблица настройки событий.
2. Выберите кнопку пользовательского события для настройки режима ее работы.
3. Выберите ячейку в столбце **Активировать тревогу** - **Расписание** и выберите соответствующее расписание.
   Расписание определяет время активации тревожного сигнала, уведомляющего пользователя о событии.
4. Выберите ячейку в столбце **Журнал** - **Расписание** и выберите соответствующее расписание.
   Расписание определяет время регистрации события.
   При выборе **Никогда** кнопка пользовательского события становится недоступной в Operator Client для всех пользовательских групп, имеющих разрешение на кнопку пользовательского события.
5. Выберите ячейку в столбце **Сценарий** - **Сценарий** и выберите соответствующий командный сценарий.
6. Выберите ячейку в столбце **Сценарий** - **Расписание** и выберите соответствующее расписание.
   Расписание определяет время исполнения командного сценария.

См.

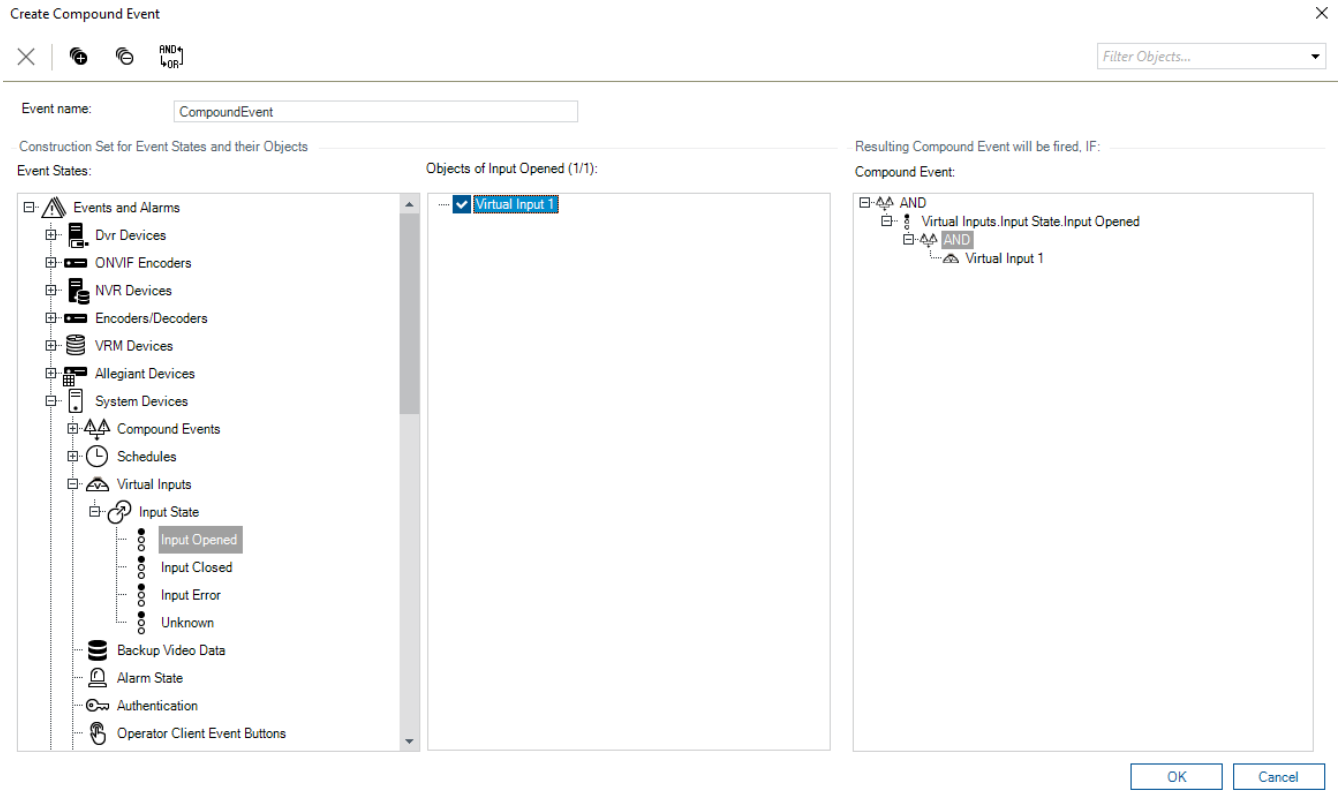
– *Страница События, Страница 316*

25.8 Создание сложного события

Главное окно > **События** > 

Необходимо создать Сложное событие. Вы можете объединять только изменения состояний и их объекты. Объектами могут быть, например, расписания или устройства. Вы можете объединять как изменения состояний, так и их объекты при помощи логических выражений AND и OR.

Пример: Вы объединяете состояния подключения IP-камеры и декодер. Сложное событие будет иметь место только в том случае, если оба устройства теряют подключение. В этом случае вы используете оператор AND для двух объектов (IP-камеры и декодера) и для двух состояний подключения **Видеосигнал утерян** и **Отключено**.



Создание сложного события.

1. В поле **Имя события:** введите имя для сложного события.
2. В поле **Состояния событий:** выберите состояние события.
   Доступные объекты отображаются в поле **Объекты:**.
3. В поле **Объекты:** выберите нужное устройство.
   Соответствующее событие и выбранные устройства добавляются в область "Составное событие".
4. В поле **Сложное событие:** щелкните правой кнопкой мыши логическую операцию и внесите необходимые изменения.
   Логическая операция определяет сочетание своих непосредственных дочерних элементов.
5. Нажмите **ОК**.
   Новое сложное событие будет добавлено в таблицу настройки событий. Его можно будет найти в дереве событий в разделе **Системные устройства**.

См.

– *Страница События, Страница 316*

25.9 Редактирование сложного события

Главное окно > **События**

Вы можете изменить ранее созданное сложное событие.

Чтобы изменить сложное событие:

1. В дереве событий разверните **Системные устройства** > **Состояние сложного события** > **Сложное событие верно**.
2. В столбце **Устройство** таблицы настройки событий щелкните правой кнопкой мыши нужное сложное событие и нажмите **Правка**.
   Отобразится диалоговое окно **Редактировать сложное событие**.

3. Внесите необходимые изменения.
4. Нажмите **OK**.
   Сложное событие будет изменено.

См.
– *Страница События, Страница 316*

25.10 Настройка тревоги

Главное окно > **Тревожные сигналы**
Перед настройкой тревоги нужно настроить активирующее ее событие в разделе **События**.
Для настройки сигнала тревоги:
1. Выберите тревогу в дереве, например **Системные устройства** > **Идентификация** > **Аутентификация оператора отклонена**.
   Отобразится соответствующая таблица настройки тревог.
2. В столбце **Приоритет** нажмите ... в ячейке и введите приоритет тревоги для выбранной тревоги (100 — низкий, 1 — высокий).
   В столбце **Название** нажмите ... в ячейке и введите название тревожного сигнала, которое будет отображаться в системе BVMS (например, в списке тревог).
   В столбце **Цвет** нажмите ... в ячейке, чтобы отобразить диалоговое окно для выбора цвета, которым будет отображаться тревожный сигнал в Operator Client (например, в списке тревог).
3. В столбцах 1-5 нажмите ... в ячейке для отображения диалогового окна **Выбрать содержимое Области изображений**.
   Задайте требуемые параметры.
4. В столбце **Аудиофайл** нажмите ... в ячейке, чтобы отобразить диалоговое окно для выбора аудиофайла, который должен воспроизводиться в случае тревоги.
5. В столбце **Параметры тревог** нажмите ... в ячейке для отображения диалогового окна **Параметры тревог**.
6. Задайте требуемые параметры.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.
– *Настройка события, Страница 331*
– *Страница Тревожные сигналы, Страница 321*
– *Диалоговое окно Выбрать содержимое Области изображений, Страница 323*
– *Диалоговое окно Параметры тревог, Страница 325*

25.11 Настройка параметров для всех тревог

Главное окно > **Тревожные сигналы**
Вы можете настроить следующие параметры тревоги, которые будут действительны для этого Management Server:
– Количество областей изображений на тревогу
– Время автоматического отключения
– Время записи по тревоге вручную
– Отображение тревог в нескольких строках в окне тревожных изображений
– Ограничение длительности записей по тревоге, активируемых в определенном состоянии
– Поведение всех групп мониторов

Чтобы настроить все тревоги:

1. Нажмите  .
   Откроется диалоговое окно **Настройки тревог**.
2. Задайте необходимые параметры.

▸ Нажмите **ОК**.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

См.

– *Диалоговое окно Настройки тревог, Страница 322*

25.12 Настройка длительности до и после срабатывания тревожного сигнала

Для настройки параметров длительности до и после срабатывания тревожного сигнала требуется камера, поддерживающая функцию ANR с установленным микропрограммным обеспечением версии 5.90 или выше.

Главное окно > **Камеры и запись** > 

▸ Для требуемой камеры включите функцию **ANR**.

Главное окно > **События**

▸ Настройте требуемое событие для камеры с включенной функцией ANR.

Главное окно > **Тревожные сигналы**

1. Настройте тревожное событие для этого события.
2. Выберите  или 
3. В столбце **Параметры тревог** нажмите ....
   Отображается диалоговое окно **Параметры тревог**.
4. Для включения записи по тревоге в столбце **Запись** установите флажок для камеры с включенной функцией ANR.
   Флажок в столбце **Изменение настройки длительности тревоги** устанавливается автоматически.
5. Перейдите на вкладку **Изменение настройки длительности тревоги**.
6. Настройте параметр длительности тревоги согласно необходимости.

См.

– *Диалоговое окно Параметры тревог, Страница 325*

25.13 Включение записи по тревоге с помощью текстовых данных

Главное окно > **Тревожные сигналы**

Можно включать запись по тревоге с помощью текстовых данных.

Перед настройкой тревоги необходимо настроить событие, содержащее текстовые данные.

Пример: **События** > выберите в дереве событий  (текстовые данные должны быть доступны, например, **Устройства чтения кредитных карточек** > **Устройство чтения кредитных карточек** > **Карта отклонена**)

Замечание!
Задайте для выбранного события время задержки 0.
Это необходимо, чтобы избежать потерь текстовых данных.

Настройка записи по тревоге:

1. Выберите тревогу в дереве, например **Устройства ATM/POS** > **Вход ATM** > **Ввод данных**.
   Отображается соответствующая таблица настройки тревог.
2. Установите требуемые параметры.
3. В столбце **Параметры тревог** щелкните ... в ячейке для отображения диалогового окна **Параметры тревог**.
4. Нажмите вкладку **Камеры** и установите флажок **Запись**.

См.

- *Диалоговое окно Параметры тревог, Страница 325*
- *Диалоговое окно "Запись текстовых данных", Страница 320*

25.14 Добавление текстовых данных к непрерывной записи

Главное окно > **События** > в дереве событий выберите **Ввод данных** (текстовые данные должны быть доступны, например **Устройства чтения кредитных карточек** > **Устройство чтения кредитных карточек** > **Карта отклонена**) > столбец **Запись текстовых данных** > ...
Можно добавлять текстовые данные к непрерывной записи.

25.15 Защита записи по тревоге

Главное окно > **Тревожные сигналы**
Перед настройкой тревоги необходимо настроить событие на странице **События**.

Замечание!
Если включить защиту записи по тревоге с какой-то камеры, то защищенные видео данные никогда не удаляются VRM автоматически. Учитывайте, что слишком много защищенных блоков может привести к заполнению хранилища и камера остановит запись. Защита видео-данных отключается вручную через Operator Client.

Настройка записи по тревоге:

1. Выберите тревогу в дереве, например **Устройства ATM/POS** > **Вход ATM** > **Ввод данных**.
   Отображается соответствующая таблица настройки тревог.
2. Установите требуемые параметры.
3. В столбце **Параметры тревог** щелкните ... в ячейке для отображения диалогового окна **Параметры тревог**.
4. Нажмите вкладку **Камеры** и установите флажок **Запись**.
1. Установите флажок **Защитить запись**.

См.

- *Диалоговое окно Параметры тревог, Страница 325*

25.16 Настройка мигающих активных точек

Замечание!
Мигающие активные точки можно настроить только для события или тревоги.

Главное окно > **События**
или
Главное окно > **Тревожные сигналы**

Для каждого события или тревоги ( ) можно настроить цвет фона и поведение активных точек (мигает или не мигает). Например, можно настроить событие или тревогу устройства так, чтобы его значок устройства на карте начинал мигать при изменении состояния этого устройства.
Кроме того, можно настроить приоритет отображения для всех активных точек. Это необходимо, если для одного устройства возникают различные события. (1 = наивысший приоритет)
Настроенный цвет действует для всех активных точек с одинаковым приоритетом отображения. Можно изменить цвет, поведение и приоритет для любого события или тревоги : изменение цвета и поведения используется для всех активных точек всех остальных событий или тревог , имеющих такой же приоритет.
Настройка цвета состояний на картах возможна, только если установлен флажок **Включено расширенное отображение состояния (выделение активных точек цветом на картах в зависимости от состояния)** или флажок **Включено расширенное отображение состояния (выделение активных точек цветом на картах в зависимости от тревоги)** в диалоговом окне **Параметры**.

Для настройки мигающей активной точки для события:

1. выберите в дереве состояние события ( ), например **Кодеры/Декодеры** > **Реле кодера** > **Состояние реле** > **Реле открыто**.
   Откроется соответствующая таблица настройки событий.
2. Нажмите **Включить цвет состояний на картах**.
3. Введите необходимый приоритет в поле **Приоритет отображения на карте:**.
4. Нажмите поле **Цвет фона на карте:**, чтобы выбрать необходимый цвет.
5. При необходимости щелчком включите функцию **Мигание**.

Для настройки мигающей активной точки для тревоги:
См. раздел *Идентификатор тревоги , Страница 321* на *Страница Тревожные сигналы, Страница 321*.

Замечание!
Активная точка мигает только в том случае, когда тревога содержится в списке тревог.

Значки устройств на карте мигают цветом, настроенным для тревоги или события.

См.

- *Страница События, Страница 316*
- *Диалоговое окно «Параметры» (меню «Настройки»), Страница 124*

25.17 События и тревоги для систем контроля и управления доступом

Дополнительная информация о событиях и тревогах для систем контроля и управления доступом.

Событие запроса доступа

Это событие позволяет оператору BVMS вручную предоставить доступ или отказать в доступе человеку с помощью системы контроля и управления доступом. Можно настроить запись по тревоге, запись текстовых данных или дополнительную информацию для данного события.

События запроса доступа передаются в систему BVMS, только если на каждом считывающем устройстве системы контроля и управления доступом включен параметр **Дополнительная проверка**. В конфигурации событий BVMS события **Доступ запрошен,** передаваемые считывающими устройствами, всегда активируют тревогу в BVMS.

Замечание!

Рекомендуется установить наивысший приоритет (1) для тревожных сигналов **Доступ запрошен**. В этом случае тревожные сигналы будут автоматически отображаться, привлекая внимание оператора.

25.18 События и тревоги для Person Identification (идентификации личности)

Главное окно > **События**

Дополнительная информация о событиях и тревогах для Person Identification.

Обнаружено неавторизованное лицо

Для каждой камеры можно настроить группу лиц, имеющих или не имеющих санкционированный доступ к определенной области.

Примечание: настройка групп лиц с санкционированным доступом и без него возможна только при наличии разрешения **Изменение настроек событий**.

Для настройки Обнаружено неавторизованное лицо:

1. Выберите соответствующую камеру в **Video Analytics**.
2. Выберите событие **Обнаружено неавторизованное лицо**.
3. Откройте вкладку **Обнаружено неавторизованное лицо**.
4. Щелкните ... в ячейке **Неавторизованные** или **Авторизованные**.
   Появится диалоговое окно **«Авторизация для камеры»**.
5. Перетащите и установите настроенные группы лиц в соответствующее поле.
6. Нажмите **ОК**.
   Настроенные группы лиц теперь отображаются в соответствующей камере как имеющие санкционированный доступ или без него.

26 Страница Пользовательские группы

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

Главное окно > **Группы пользователей**
Позволяет настроить группы пользователей, Enterprise User Groups и доступ Enterprise.
По умолчанию доступна следующая группа пользователей:
– Группа администраторов (с одним пользователем Admin).

Вкладка Группы пользователей
Нажмите, чтобы открыть страницы, доступные для настройки прав стандартной пользовательской группы.

Вкладка Enterprise User Groups
Нажмите, чтобы открыть страницы, доступные для настройки разрешений Enterprise User Group.

Вкладка доступ Доступ Enterprise
Нажмите, чтобы открыть страницы, доступные для добавления и настройки доступа Enterprise Access.

Параметры пользователей/пользовательских групп

Значок	Описание
	Нажмите, чтобы удалить выбранную запись.
	Нажмите, чтобы добавить новую группу или учетную запись.
	Нажмите, чтобы добавить нового пользователя к выбранной группе пользователей. При необходимости можно изменить имя пользователя по умолчанию.
	Нажмите, чтобы добавить новую группу с двойной авторизацией.
	Нажмите, чтобы добавить новую комбинацию для входа в систему при двойной авторизации.
	Открывает диалоговое окно для копирования разрешений из выбранной группы пользователей в другую группу пользователей.
	Нажмите, чтобы открыть страницы, доступные для настройки разрешений этой группы.
	Нажмите, чтобы открыть страницу, доступную для настройки свойств данного пользователя.
	Нажмите, чтобы открыть страницу, доступную для настройки свойств данной комбинации для входа в систему.

Значок	Описание
	Нажмите, чтобы открыть страницы, доступные для настройки разрешений данной пользовательской группы с двойной авторизацией.

Активация изменений имени пользователя и пароля

 Нажмите, чтобы активировать изменение пароля.

 Нажмите, чтобы активировать изменение имени пользователя.

Замечание!
Изменения имени пользователя и изменения пароля будут отменены и возвращены в исходное состояние после отката конфигурации.

Разрешения Enterprise System

Для Enterprise System можно настроить следующие права:

– Рабочие разрешения Operator Client, определяющие пользовательский интерфейс для работы в Enterprise System, например пользовательский интерфейс монитора тревожных сигналов.
  Воспользуйтесь Enterprise User Group. Настройте группу на Enterprise Management Server.
– Разрешения устройства, которые должны функционировать для работы в Enterprise Management Server, определяются на каждом Management Server.
  Используйте Enterprise Accounts. Настройте его на каждом Management Server.

Права на один Management Server

Для управления доступом к одному из Management Servers используйте стандартную группу пользователей. Все разрешения на этот Management Server можно настроить в этой группе пользователей.
Двойную авторизацию можно настроить для стандартных групп пользователей и Enterprise User Groups.

Тип	Содержит	Доступные параметры конфигурации	Где задается конфигурация?
Пользовательская группа	Пользователи	– Рабочие разрешения и использование устройств	– Management Server
Enterprise User Group	Пользователи	– Рабочие разрешения – На Management Server: имена соответствующих учетных записей доступа Enterprise с учетными данными	– Enterprise Management Server

Тип	Содержит	Доступные параметры конфигурации	Где задается конфигурация?
Enterprise Account	-	– Разрешения на использование устройств – Ключ учетной записи	– Management Server
Группа пользователей с двойной авторизацией	Группы пользователей	– См. группы пользователей	– См. группы пользователей
Enterprise двойная авторизация	Enterprise User Groups	– См. Enterprise User Groups	– См. Enterprise User Groups

Чтобы искать элементы:

- Введите запрос в поле поиска  и нажмите клавишу ENTER, чтобы отфильтровать отображаемые элементы.
  Отображаются только элементы, содержащие поисковой запрос, и соответствующие родительские элементы (только на деревьях). Кроме того, отображается количество отфильтрованных элементов и общее их количество.

Примечание. Для поиска точных фраз поисковые запросы следует заключать в кавычки, например, в случае запроса "Camera 1" отфильтровываются только камеры с таким именем, но не camera 201.

26.1 Страница Свойства пользовательской группы

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей**
Позволяет настроить следующие параметры выбранной группы пользователей:

– Расписание входа в систему
– Выбор связанной группы пользователей LDAP

Свойства группы пользователей

Описание:
Введите информативное описание пользовательской группы.

Язык
Выберите язык клиента Operator Client.

Расписание входа в систему
Выберите расписание записей или задач. Пользователи выбранной группы могут входить в систему только в то время, которое определено расписанием.

Свойства LDAP

Искать группы
Нажмите для отображения доступных пользовательских групп LDAP в списке **Связанная группа LDAP**. Чтобы выбрать связанную группу LDAP, необходимо сделать соответствующие настройки в диалоговом окне **Параметры сервера LDAP**.

Связанная группа LDAP
Выберите в списке группу LDAP **Связанная группа LDAP**, которую вы хотите использовать для своей системы.

См.
- *Выбор связанной группы LDAP, Страница 370*
- *Связывание группы LDAP, Страница 121*
- *Составление расписания разрешений на вход пользователей в систему, Страница 370*

26.2 Страница Свойства пользователей

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** > >
Позволяет настроить нового пользователя в стандартной группе пользователей или в Enterprise User Group.
Если изменить пароль пользователя или удалить пользователя, пока он зарегистрирован в системе, пользователь может продолжить работу с Operator Client и после изменения или удаления пароля. Если после изменения или удаления пароля соединение с Management Server прерывается (например, после активации конфигурации), пользователь не может автоматически повторно подключиться к Management Server без выхода/входа в Operator Client.

Учетная запись включена
Установите флажок, чтобы активировать учетную запись пользователя.
Примечание. По умолчанию все новые учетные записи пользователей отключены. Чтобы активировать учетную запись пользователя, необходимо установить пароль.

Имя
Введите полное имя пользователя.

Описание
Введите информативное описание пользователя.

Пользователь должен изменить пароль при следующем входе в систему
Установите флажок, чтобы обязать пользователя задать новый пароль при следующем входе.

Введите новый пароль
Введите пароль для нового пользователя.

Подтвердить пароль
Введите новый пароль еще раз.

Замечание!

Чтобы активировать изменения в этом диалоговом октаве, нажмите .

Замечание!
Мы настоятельно рекомендуем назначить конкретный пароль для всех новых пользователей и обязать пользователя изменить пароль при входе.

Замечание!
Клиенты Mobile Video Service, Web Client, приложения Bosch iOS и клиенты SDK не могут изменить пароль при входе.

Применить
Нажмите для применения настроек.

Нажмите  для активации пароля.

Дополнительная информация
После обновления до BVMS 9.0.0.x установятся следующие настройки **Свойства пользователей**:
- **Учетная запись включена** установлен.
- **Пользователь должен изменить пароль при следующем входе в систему** не установлен.

26.3 Страница Свойства комбинации для входа в систему

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > 

Создать группу с двойной авторизацией > 
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** > 

Создать группу Enterprise с двойной авторизацией > 
Позволяет изменить пару пользовательских групп к группе с двойной авторизацией. Пользователи первой пользовательской группы вводят свои данные в первом диалоговом окне входа в систему, пользователи второй пользовательской группы только подтверждают вход в систему.

Выбрать комбинацию для входа в систему
Выберите из каждого списка группу пользователей.

Форсировать двойную авторизацию
Установите флажок, чтобы каждый пользователь мог войти в систему только вместе с пользователем другой группы.

См.
- *Добавление комбинации для входа в систему к группе с двойной авторизацией, Страница 368*

26.4 Страница Разрешения камеры

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > вкладка **Разрешения устройств** > вкладка **Разрешения камеры**

или

Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise** >  > вкладка **Разрешения устройств** > вкладка **Разрешения камеры**

Позволяет устанавливать права доступа к функциям выбранной камеры или группы камер для выбранной пользовательской группы.
После добавления новых компонентов разрешения камеры должны быть сконфигурированы заново.
Можно отменить доступ к камере на странице **Камера**.

Камера
Отображает название камеры в соответствии с настройками на странице **Камеры и запись**.

Местоположение
Отображает местонахождение камеры, заданное на странице **Карты и структура**.

Доступ
Установите флажок для обеспечения доступа к камере.

Видео в реальном времени
Установите флажок, чтобы обеспечить просмотр изображений в реальном времени.

Аудио в реальном времени
Установите флажок, чтобы обеспечить прослушивание аудио в реальном времени.

Запись вручную
Установите флажок, чтобы разрешить запись вручную (запись по тревоге).
Можно установить или снять этот флажок только в том случае, если запись тревоги вручную активирована на странице **Функции оператора**.

Воспроизвести видео
Установите флажок для обеспечения возможности использования воспроизведения видеосигнала.
Можно установить или снять этот флажок только в том случае, если воспроизведение активировано на странице **Функции оператора**.

Воспроизвести аудио
Установите флажок для обеспечения возможности использования воспроизведения аудиосигнала.
Можно установить или снять этот флажок только в том случае, если воспроизведение активировано на странице **Функции оператора**.

Текстовые данные
Установите флажок для обеспечения отображения метаданных.
Можно установить или снять этот флажок только в том случае, если отображение метаданных активировано на странице **Функции оператора**.

Экспорт
Установите флажок для обеспечения экспорта видеоданных.
Можно установить или снять этот флажок только в том случае, если экспорт видеоданных активирован на странице **Функции оператора**.

PTZ/область интереса
Установите флажок, чтобы разрешить использование средств управления PTZ или функции ROI данной камеры.

Этот флажок можно установить или снять только в том случае, если управление PTZ или функция ROI этой камеры включена на странице **Функции оператора**. Кроме того необходимо настроить PTZ или ROI в Таблице камер.

Aux
Установите флажок, чтобы обеспечить возможность исполнения вспомогательных команд.
Можно установить или снять этот флажок только в том случае, если управление камерой PTZ активировано на странице **Функции оператора**.

Задать препозиции
Установите флажок, чтобы разрешить пользователю устанавливать предустановки данной камеры PTZ.
Также можно задать предварительные положения для функции области интереса, если она включена и разрешена.
Можно установить или снять этот флажок только в том случае, если управление камерой PTZ активировано на странице **Функции оператора**.

Контрольное изображение
Установите флажок для обеспечения возможности обновления контрольного изображения данной камеры.

Privacy overlay
Установите флажок, чтобы включить Privacy overlay для этой камеры в режимах реального времени и воспроизведения.

26.5 Страница Приоритеты управления

Главное окно > **Группы пользователей** > Вкладка **Группы пользователей** > > Вкладка **Разрешения устройств** > Вкладка **Приоритеты управления**
или

Главное окно > **Группы пользователей** > Вкладка **Доступ Enterprise** > > Вкладка **Разрешения устройств** > Вкладка **Приоритеты управления**

Приоритеты управления
Переместите соответствующий ползунок вправо для уменьшения приоритета получения доступа к управлению камерами PTZ магистральным линиям Bosch Allegiant.
Пользователь с более высоким приоритетом может заблокировать управление PTZ или управление магистральными линиями для пользователей с более низким приоритетом.
Время, по истечении которого блокировка PTZ прекращается, устанавливается в поле **Время ожидания в мин.**. По умолчанию используется значение 1 минута.

Время ожидания в мин.
Введите время в минутах.

См.
– *Настройка различных приоритетов, Страница 372*

26.6 Диалоговое окно Копировать разрешения пользовательской группы

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > 

или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > 

Позволяет выбрать разрешения группы пользователей для копирования в выбранные группы пользователей.

Копировать из:
Отображает выбранную пользовательскую группу. Ее разрешения копируются в другую пользовательскую группу.

Параметры для копирования
Установите флажок для выбора разрешений пользовательской группы, которые нужно скопировать.

Копировать в:
Установите флажок, чтобы указать пользовательскую группу, в которую следует скопировать разрешения.

См.
– *Копирование разрешений пользовательской группы, Страница 372*

26.7 Страница Разрешения декодера

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** вкладка >  > **Разрешения устройств** вкладка > **Разрешения декодера**

или

Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise** >  > вкладка **Разрешения устройств** > вкладка **Разрешения декодера**

Позволяет настроить декодеры, к которым имеют доступ пользователи данной группы.

Декодер
Отображает доступные декодеры.
Установить флажок для предоставления пользовательской группе доступа к данному декодеру.

Группа мониторов
Установите флажок для предоставления пользователям выбранной пользовательской группы доступа к данной группе мониторов.

26.8 Страница События и тревоги

Главное окно > **Группы пользователей** > Вкладка **Группы пользователей** >  > Вкладка **Разрешения устройств** > Вкладка **События и тревоги**

или

Главное окно > **Группы пользователей** > Вкладка **Доступ Enterprise** >  > Вкладка **Разрешения устройств** > Вкладка **События и тревоги**

Позволяет настроить разрешения для дерева событий, например, вы настраиваете события, которые группа пользователей может или не может использовать.

Вы не можете изменить эти настройки для пользовательской группы по умолчанию.

Для каждого события имеется по крайней мере одно устройство. Например, для события **Потеря видеоизображения** устройствами являются доступные камеры. Для события **Резервное копирование закончено** соответствующим устройством является **Резервное копирование по времени**. Таким образом, устройством может быть программный процесс.

1. Разверните элемент дерева и установите нужные флажки для активации событий. Установите флажок в столбце **Доступ** устройства, чтобы включить события этого устройства. Параметры доступа к устройствам настраиваются на странице **Камера** и на странице **Разрешения камеры**.
2. Для включения или выключения всех событий сразу установите или снимите флажок **События и тревоги**.

26.9 Страница Учетные данные

Главное окно > **Группы пользователей** > Вкладка **Доступ Enterprise** >  > Вкладка **Разрешения устройств** > Вкладка **Учетные данные**

Настройте учетные данные Enterprise Account на Management Server.

Вы можете настроить доступ Enterprise на каждом Management Server, входящем в Enterprise System. Enterprise Management Server использует эти учетные данные для предоставления доступа к устройствам этого Management Server Operator Client, выполняющему вход в систему как пользователь из Enterprise User Group.

Описание:

Введите описание требуемой учетной записи Enterprise Account.

Политика надежных ключей

Флажок **Политика надежных ключей** предварительно установлен для всех вновь созданных пользовательских групп.

Мы настоятельно рекомендуем сохранить этот параметр в целях обеспечения защиты вашего компьютера от несанкционированного доступа.

Применяются следующие правила:

- Минимальная длина ключа соответствует указанной на странице **Политики учетных записей** для соответствующих групп пользователей.
- Не используйте ключи повторно.
- Используйте по крайней мере одну букву в верхнем регистре (A–Z).
- Используйте по крайней мере одну цифру (0–9).
- Используйте по крайней мере один специальный символ (например, ! $ # %).

Введите новый ключ: / Подтвердите ключ:

Введите и подтвердите ключ для этого Management Server.

См.

- *Создание Enterprise Account, Страница 366*

26.10 Страница Логическое дерево

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > > вкладка **Разрешения устройств** > вкладка **Логическое дерево**
или

Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise** > > вкладка **Разрешения устройств** > вкладка **Логическое дерево**
Позволяет настроить логическое дерево для каждой группы пользователей.

Чтобы настроить разрешения:

- По необходимости установите или снимите флажки.
  Выбор дочернего элемента узла автоматически выбирает узел.
  Выбор узла автоматически выбирает все дочерние элементы.

Камера
Установите флажок для предоставления пользователям выбранной пользовательской группы доступа к соответствующим устройствам.
Можно отменить доступ к камере на странице **Разрешения камеры**.

Группа мониторов
Установите флажок для предоставления пользователям выбранной пользовательской группы доступа к данной группе мониторов.

См.
– *Настройка разрешений устройств, Страница 371*

26.11 Страница Свойства оператора

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > > вкладка **Рабочие разрешения** > вкладка **Функции оператора**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** > > вкладка **Рабочие разрешения** > вкладка **Функции оператора**

Позволяет настроить различные разрешения для выбранной пользовательской группы.

Управление купольными камерами PTZ
Установите флажок для активации управления камерой.
Приоритеты управленияВ поле **Приоритеты управления** можно установить приоритет для получения доступа к управлению камерой.

Магистральные линии Allegiant
Установите этот флажок для обеспечения доступа к магистральным линиям Bosch Allegiant.
Приоритеты управленияВ поле **Приоритеты управления** можно установить приоритет для получения магистралей Bosch Allegiant.

Печать и сохранение
Установите флажок для активации печати и сохранения видеоданных, карт и документов.

Обработка тревожных сигналов
Установите флажок для включения обработки тревожных сигналов.

Прервать отображение заставки Windows при поступлении тревожного сигнала
Установите этот флажок, чтобы входящий тревожный сигнал отображался даже в том случае, когда активна экранная заставка. Если для выхода из экранной заставки требуется ввод имени пользователя и пароля, этот параметр не используется.

Экран тревожных сигналов
Установите флажок для включения отображения тревожных сигналов. При выборе данного параметра одновременно отключается параметр **Обработка тревожных сигналов**.

Воспроизведение
Установите флажок, чтобы разрешить различные функции воспроизведения.

Экспортировать видео
Установите флажок, чтобы разрешить экспорт видеоданных.

Экспорт в другие форматы
Установите флажок, чтобы разрешить экспорт видеоданных в формате, отличном от собственного формата.

Защита видео
Установите флажок для обеспечения защиты видеоданных.

Отменить защиту видео
Установите флажок для активации и деактивации защиты видеоданных.

Ограничить доступ к видео (ограниченное видео могут просматривать только пользователи, имеющие это разрешение)
Установите флажок, чтобы разрешить ограничение доступа к видеоданным.

Отменить ограничение видео
Установите флажок для введения и снятия ограничения доступа к видеоданным.

Замечание!
VRM
Настройте пользовательские разрешения для настройки и снятия ограничений доступа к видеоматериалам BVMS при необходимости.
Только пользователь, у которого есть разрешение **Ограничить доступ к видео (ограниченное видео могут просматривать только пользователи, имеющие это разрешение)**, может видеть видео с ограниченным доступом на временной шкале Operator Client. В противном случае диапазон времени с ограничениями доступа отображается как **Без записи**.

Замечание!
DIVAR AN
Настройте пользовательские разрешения для введения и снятия ограничений с видео-данных на вашем устройстве DIVAR AN при необходимости. Соответствующим образом создайте пользователя в BVMS с теми же учетными данными и настройте разрешения для введения и снятия ограничений для видео-данных.
Это не влияет на отображение видео с ограниченным доступом, его необходимо отдельно настраивать на устройстве DIVAR AN.

Удалить видео
Установите флажок для обеспечения возможности удаления видеоданных.

Доступ к видео, записанному в то время, когда вход в систему для группы пользователей был запрещен
Установите флажок для обеспечения доступа к описанным видеоданным.

Доступ к журналу
Установите флажок для обеспечения доступа к журналу.

Удалить текстовые данные из записей журнала (для удаления данных, связанных с людьми)
Установите этот флажок, чтобы разрешить удаление текстовых данных из записей журнала.

Кнопки событий оператора
Установите флажок для активации кнопок пользовательских событий в Operator Client.

Закрыть модуль Operator Client
Установите флажок для обеспечения возможности закрытия Operator Client.

Свернуть Operator Client
Установите флажок для обеспечения возможности свертывания Operator Client.

Внутренняя аудиосвязь
Установите флажок, чтобы позволить пользователю говорить с использованием громкоговорителя кодера с функциями аудиовхода и аудиовыхода.

Запись тревожного сигнала вручную
Установите флажок, чтобы разрешить запись по тревоге вручную.

Доступ к монитору VRM
Установите этот флажок, чтобы разрешить доступ к программному обеспечению VRM Monitor.

Установить контрольное изображение
Установите этот флажок, чтобы разрешить обновление контрольного изображения в Operator Client.

Установить область для контрольного изображения
Установите флажок для обеспечения возможности выбора области в изображении с камеры для обновления контрольного изображения в Operator Client.

Изменить пароль
Установите этот флажок, чтобы разрешить пользователю использовать Operator Client для изменения пароля входа в систему.

Постановка на охрану областей тревожной панели
Установите флажок, чтобы пользователь Operator Client мог ставить на охрану области, настроенные на охранной панели, входящей в конфигурацию BVMS.

Принудительная постановка на охрану областей тревожной панели
Установите флажок, чтобы пользователь Operator Client мог принудительно ставить на охрану области, настроенные на охранной панели, входящей в конфигурацию BVMS.

Снятие с охраны областей тревожной панели
Установите флажок, чтобы пользователь Operator Client мог снимать с охраны области, настроенные на охранной панели, входящей в конфигурацию BVMS.

Отключение сирены для областей тревожной панели
Установите флажок, чтобы пользователь Operator Client мог отключать сигнальные сирены областей, настроенных на охранной панели, входящей в конфигурацию BVMS.

Обход точек тревожной панели
Установите флажок, чтобы пользователь Operator Client мог изменять состояние точки, настроенной на охранной панели, на **Выполнен обход точки**. Обойденная точка не может передавать тревожный сигнал. Когда состояние снова меняется на **Выполнен обход точки**, ожидающий тревожный сигнал, если он есть, отправляется.

Открывание дверей тревожной панели
Установите флажок, чтобы пользователь Operator Client мог открывать дверь, настроенную на охранной панели.

Блокировка и разблокировка дверей тревожной панели
Установите флажок, чтобы пользователь Operator Client мог блокировать и разблокировать дверь, настроенную на охранной панели.

Активация рабочего цикла дверей тревожной панели
Установите флажок, чтобы пользователь Operator Client мог включать рабочий цикл двери, настроенной на охранной панели.

Управление точками прохода
Установите флажок, чтобы разрешить пользователю Operator Client изменять состояние входной двери (заблокирована, заперта, не заперта).

Предоставление доступа
Установите флажок, чтобы разрешить пользователям Operator Client предоставлять доступ.

Управление людьми
Установите этот флажок, чтобы позволить пользователю Operator Client управлять лицами, связанными с тревогами Person Identification.

Сбросить уровень угрозы
Установите флажок, чтобы разрешить пользователям Operator Client сбрасывать уровень угрозы, если Operator Client находится в режиме угрозы.

Импортировать/экспортировать избранное и закладки
Установите флажок, чтобы разрешить пользователям Operator Client импортировать или экспортировать избранные элементы или закладки.

Порядок отображения в случае одинакового приоритета тревог
Выберите соответствующее значение для настройки порядка областей изображений тревог на экране тревожных сигналов Operator Client.

Время перемотки при немедленном воспроизведении:
Введите количество секунд, в течение которых должно осуществляться немедленное воспроизведение тревоги.

Повторять звук тревоги:
Установите флажок и введите количество секунд, по истечении которого будет повторяться звуковой сигнал тревоги.

Ограничить доступ к записанному видео до последних n минут:
Установите флажок, чтобы ограничить доступ к записанным видеоизображением. Введите в списке количество минут.

Принудительный автоматический выход оператора из системы после бездействия в течение:
Установите этот флажок для включения автоматического выхода из системы Operator Client по истечении заданного времени.

См.

– *Отключение при бездействии, Страница 43*

26.12 Страница Приоритеты

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > > вкладка **Рабочие разрешения** > вкладка **Приоритеты**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** > > вкладка **Рабочие разрешения** > вкладка **Приоритеты**
Позволяет настраивать время ожидания для явной блокировки PTZ. Можно установить приоритеты управления PTZ и отображения входящих тревожных сигналов.

Поведение автоматически всплывающих окон
Переместите ползунок для установки приоритетного значения для окна изображений в реальном времени и для окна воспроизведения. Это значение необходимо для определения того, будет ли входящий тревожный сигнал автоматически отображаться в окне тревожных сигналов.
Например: Если вы переместите ползунок для изображения в реальном времени на значение 50, а для окна воспроизведения на 70, а тревожный сигнал будет иметь приоритет 60, он будет автоматически отображен на экране только в том случае, если активным окном будет окно воспроизведения. Тревожный сигнал не будет автоматически отображаться, если активным окном будет окно изображения в реальном времени.

См.

– *Настройка различных приоритетов, Страница 372*

26.13 Страница Интерфейс пользователя

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > > вкладка **Рабочие разрешения** > вкладка **Интерфейс пользователя**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** > > вкладка **Рабочие разрешения** > вкладка **Интерфейс пользователя**
Позволяет настроить пользовательский интерфейс четырех мониторов, используемых Operator Client.
Вы можете настроить многомониторный режим с максимум 4 мониторами. Для каждого монитора можно определить, что будет на нем отображаться; например, что монитор 2 отображает только изображения в реальном времени или что монитор 1 и монитор 2 используют соотношение сторон 16:9 для камер HD.

Контрольный монитор
Выберите монитор, который будет использоваться в качестве монитора управления.

Макс. число строк областей изображений при воспроизведении
Выберите максимальное число строк областей изображений для отображения в окне воспроизведения изображений на мониторе управления.

Тревожный монитор
Выберите тревожный монитор, который может выполнять показ в режиме реального времени с содержимым тревоги или показывать только содержимое тревоги.

Монитор 1–4
Выберите нужный элемент из соответствующего списка каждого монитора.
- Для монитора управления запись **Управление** выбрана заранее и не может быть изменена.
- Для тревожного монитора можно выбрать одну из следующих записей:
  - **Видео в реальном времени и содержимое тревог**
  - **Только содержимое тревог**
- Для оставшихся мониторов можно выбрать одну из следующих записей:
  - **Только видео в реальном времени**
  - **Карта и документ**
  - **Две карты и документ**
  - **Видео в реальном времени на полный экран**
  - **Видео в реальном времени в квадрированном режиме**

Макс. число строк в областях изображений
Выберите максимальное число строк областей изображений для отображения в окне изображений на соответствующем мониторе.
Примечание: этот параметр доступен только для следующих режимов просмотра.
- **Управление**
- **Только содержимое тревог**
- **Видео в реальном времени и содержимое тревог**
- **Только видео в реальном времени**

Остальные режимы просмотра имеют фиксированные схемы с фиксированным количеством строк областей изображений и не могут быть изменены.

Соотношение сторон областей изображений
Выберите необходимое соотношение сторон для каждого монитора для первоначального запуска Operator Client. Для камер HD используйте соотношение 16:9.

Восстановить значения по умолчанию
Нажмите для восстановления на этой странице стандартных настроек. Все записи в списке восстанавливают свои исходные параметры.

26.14 Страница Доступ к серверу

Главное окно > **Группы пользователей** > Вкладка **Enterprise User Groups** >  > Вкладка **Доступ к серверу**
Доступ к серверу настраивается на Enterprise Management Server.
Необходимо ввести имя Enterprise Account и соответствующий пароль для каждого Management Server вашей системы Enterprise System. Эта учетная запись настраивается на каждом Management Server.

Management Server
Отображает имя Management Server, настроенного на этом Enterprise Management Server.

Сетевой адрес
Отображает частный IP-адрес или DNS-имя Management Server.

Номер сервера
Отображает номер Management Server. Этот номер используется клавиатурой Bosch IntuiKey для выбора нужного Management Server.

Доступ
Установите флажок, чтобы выбрать, когда предоставлять доступ к серверу Management Server. Этот Management Server теперь является Enterprise Management Server.

Enterprise Account
Введите имя учетной записи Enterprise Account, настроенной на Management Server.

Идентификация
Выберите соответствующий параметр аутентификации в диалоговом окне **Параметры аутентификации**.

Config API
Установите флажок, чтобы разрешить доступ к Config API в Management Server с помощью токена доступа.

Описание сервера
Отображает текст описания данного сервера.
Дополнительные столбцы отображаются, если они добавлены в список серверов.

См.
- *Создание группы или учетной записи, Страница 365*
- *Создание системы Enterprise, Страница 88*
- *Настройка списка серверов для корпоративной системы, Страница 88*
- *Проверка подлинности на основе токена, Страница 90*

26.15 Страница Разрешения конфигурации

Замечание!
В данном документе описываются некоторые функции, недоступные для BVMS Viewer. Подробные сведения о различных редакциях BVMS см. www.boschsecurity.com и BVMS Руководство по быстрому выбору: Руководство по быстрому выбору BVMS.

Главное окно > **Группы пользователей** > Вкладка **Группы пользователей** > > Вкладка **Рабочие разрешения** > Вкладка **Разрешения конфигурирования**
или

Главное окно > **Группы пользователей** > Вкладка **Enterprise User Groups** > > Вкладка **Рабочие разрешения** > Вкладка **Разрешения конфигурирования**
Позволяет настроить различные разрешения пользователей для Configuration Client. Разрешение для запуска Configuration Client подразумевает доступ только для чтения.

Дерево устройств
В этом разделе можно указать разрешения на стр. **Устройства**. Установите флажок для предоставления соответствующего разрешения.

Карты и структура
В этом разделе можно указать разрешения на стр. **Карты и структура**. Установите флажок соответствующего разрешения.

Расписания
В этом разделе можно указать разрешения на стр. **Расписания**. Установите флажок соответствующего разрешения.

Камеры и запись
В этом разделе можно указать разрешения на стр. **Камеры и запись**. Установите флажок соответствующего разрешения.

События
В этом разделе можно указать разрешения на стр. **События**. Установите флажок соответствующего разрешения.

Тревожные сигналы
В этом разделе можно указать разрешения на стр. **Тревожные сигналы**. Установите флажок соответствующего разрешения.

Группы пользователей
В этом разделе можно указать разрешения для настройки групп пользователей. Установите флажок соответствующего разрешения.

Замечание!
Флажок **Настройка групп пользователей/Enterprise Accounts** и флажок **Настроить пользователей** представляют собой взаимоисключающие параметры в целях безопасности.

Audit Trail
В этом разделе можно указать, может ли пользователь использовать функции Audit Trail и экспортировать данные Audit Trail.
Установите флажок соответствующего разрешения.

Команды меню
В этом разделе можно указать разрешения для настройки команд меню. Установите флажок соответствующего разрешения.

Отчеты
В этом разделе можно указать разрешения для настройки отчетов. Установите флажок соответствующего разрешения.

Замечание!
Если вы хотите использовать сервис Config API в Management Server, необходимо выбрать следующее: **Разрешения конфигурирования**:
- **Изменение свойств устройства**
- **Вызов диспетчера активации**

Замечание!
Если вы хотите настроить **Параметры доверенного сертификата**, необходимо выбрать разрешение **Настройка групп пользователей/Enterprise Accounts**.

26.16 Страница Разрешения групп пользователей

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > > вкладка **Рабочие разрешения** > вкладка **Разрешения группы пользователей**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** > > вкладка **Рабочие разрешения** > вкладка **Разрешения группы пользователей**
Позволяет установить, в какие группы пользователей пользователи определенной группы пользователей могут добавлять новых пользователей.

Замечание!
Вы можете назначать разрешения только для той группы пользователей, которой вы уже предоставили разрешение настраивать параметры пользователей. Вы можете назначить разрешение на странице **Разрешения конфигурирования** .

Замечание!
Пользователи из стандартной группы пользователей не имеют права добавлять новых пользователей в группу Admin. Этот флажок неактивен.

См.
– *Страница Разрешения конфигурации, Страница 355*

26.17 Страница политик учетной записи

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > > вкладка **Безопасность** > вкладка **Политики учетных записей**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** > > вкладка **Безопасность** > вкладка **Политики учетных записей**

Позволяет настроить параметры для пользователей и пароли.

Строгая политика паролей
Установите флажок, чтобы активировать политику требований к паролям.
Дополнительные сведения см. в разделе *Настройка пользователей, разрешений и корпоративного доступа, Страница 364*

Замечание!
Настройка **Строгая политика паролей** применяется только для пользователей, для группы которых установлен соответствующий флажок.
Мы настоятельно рекомендуем сохранить этот параметр в целях обеспечения защиты вашего компьютера от несанкционированного доступа.

Минимальная длина пароля
Этот параметр определяет минимальное количество символов, которые может содержать пароль к учетной записи пользователя.
Установите флажок, чтобы активировать параметр, и введите минимальное количество символов.

Максимальный срок использования пароля в днях
Этот параметр определяет период времени (в днях), в течение которого пароль может использоваться, прежде чем система потребует от пользователя изменить его.
Установите флажок, чтобы активировать параметр, и введите максимальное количество дней.

Число использованных паролей в журнале
Этот параметр определяет количество уникальных новых паролей, которые должны быть использованы для учетной записи, прежде чем пользователь сможет повторно использовать старый пароль.
Установите флажок, чтобы активировать параметр, и введите минимальное количество паролей.

Максимальное количество неудачных попыток входа
Этот параметр позволяет задать отключение учетной записи после определенного числа неудачных попыток входа.
Установите флажок, чтобы активировать параметр, и введите максимальное количество попыток.
Если флажок **Максимальное количество неудачных попыток входа** установлен, можно задать два следующих параметра:

Длительность блокировки учетной записи
Этот параметр определяет время (в минутах), по истечении которого отключенная учетная запись автоматически включается.
Установите флажок, чтобы активировать параметр, и введите количество минут.

Сброс счетчика блокировки учетной записи через
Этот параметр определяет время (в минутах), которое должно пройти после того, как пользователю не удалось выполнить вход, чтобы счетчик неудачных попыток входа был обнулен.
Установите флажок, чтобы активировать параметр, и введите количество минут.

Замечание!
Если максимальное число неудачных попыток входа будет превышено, учетная запись будет отключена.
Если флажок **Длительность блокировки учетной записи** не установлен, учетную запись нужно будет включить вручную.
Если флажок **Длительность блокировки учетной записи** установлен, учетная запись будет включена автоматически по истечении заданного периода времени.

Замечание!
Счетчик неудачных попыток входа обнуляется:
после успешного входа
или по истечении заданного времени, если установлен флажок **Сброс счетчика блокировки учетной записи через**.

Отключить автономный клиент
Установите флажок, чтобы отключить вход в клиент в автономном режиме.

Дополнительная информация
В случае версий BVMS 9.0 и выше по умолчанию применяются следующие параметры **Политики учетных записей**.
- Флажок **Строгая политика паролей** предварительно установлен.
- Флажок **Минимальная длина пароля** предварительно установлен. Значение по умолчанию — 10.
- Флажок **Максимальный срок использования пароля в днях** предварительно не установлен. Значение по умолчанию — 90.

– Флажок **Число использованных паролей в журнале** предварительно не установлен. Значение по умолчанию — 10.
– Флажок **Максимальное количество неудачных попыток входа** предварительно не установлен. Значение по умолчанию — 1.
– Флажок **Отключить автономный клиент** предварительно не установлен.

Начиная с версии BVMS 10.0.1, указанные ниже параметры **Политики учетных записей** выбираются по умолчанию для всех групп пользователей:

– **Максимальное количество неудачных попыток входа**
– **Длительность блокировки учетной записи**
– **Сброс счетчика блокировки учетной записи через**

26.17.1 Operator Client в автономном режиме

Функция Operator Client в автономном режиме обеспечивает следующие варианты использования:

– Operator Client продолжает работу в режиме трансляции, воспроизведения и экспорта без подключения к компьютеру Management Server.
– Если рабочая станция однажды была подключена к компьютеру Management Server, она может в любой момент войти в систему в автономном режиме для любого пользователя.

Для использования автономного режима необходима версия BVMS 3.0 или выше.
Если рабочая станция Operator Client отключена от компьютера Management Server, можно продолжать работу. Доступны некоторые основные функции, например трансляция и воспроизведение видео.
В версии BVMS V5.5 рабочая станция Operator Client может работать автономно с конфигурацией BVMS V5.0.5.

Замечание!
Если смена пароля на Management Server происходит в то время, когда Operator Client находится в автономном режиме, смена пароля не распространяется на данный Operator Client.
Если Operator Client находится в режиме онлайн, пользователю следует войти в систему с использованием нового пароля.
Если Operator Client находится в автономном режиме, пользователю следует воспользоваться старым паролем для входа в систему. Пароль останется прежним до активации и переноса новой конфигурации на рабочую станцию Operator Client.

Замечание!
Если изображение с камеры выводится на дисплеи группы мониторов с помощью подключенной к рабочей станции клавиатуры Bosch Intuikey, а рабочая станция находится в автономном режиме, клавиатура не издает сигналов об ошибке.

26.17.1.1 Работа в автономном режиме

Если клиент Operator Client отключен от сервера Management Server, соответствующий значок  накладывается на отключенный Management Server в логическом дереве.
Можно продолжать работать с клиентом Operator Client, даже если отключение продолжается долго, однако некоторые функции недоступны.
После восстановления соединения с сервером Management Server отображается соответствующий значок.

Если включена новая конфигурация Management Server, соответствующий значок отобразится в логическом дереве поверх значка сервера Management Server, на который влияет изменение, и на несколько секунд откроется диалоговое окно. Примите новую конфигурацию или отклоните ее.
Если ваш экземпляр Operator Client должен выйти из системы в определенное время, выход выполняется, даже если соединение с сервером Management Server в этот момент не восстановлено.
Когда пользователь Operator Client входит в систему с использованием Поиска сервера в автономном режиме, отображается список серверов при последнем успешном входе в систему. Автономный режим в данном случае означает, что у рабочей станции Operator Client нет сетевого подключения к серверу, содержащему список серверов.

Функции, недоступные при отключении
При отсутствии подключения к серверу Management Server в клиенте Operator Client недоступны следующие функции.

- Список тревожных сигналов.
  Список включает обработку тревожных сигналов. Список тревожных сигналов пуст; он заполняется автоматически при восстановлении соединения.
- Allegiant.
  Недоступно управление магистральной линией. В предыдущих версиях камеры Allegiant автоматически закрывались с выводом сообщения при отсутствии доступа к управлениюмагистральной линией. С версии BVMS V3.0 отображается более удобная область изображений, информирующая пользователя о том, что отобразить данные с этой камеры сейчас невозможно.
- Группа мониторов.
  Невозможно перетаскивать камеры на элемент управления MG. Элемент управления отключен и включается автоматически при восстановлении соединения.
- Приоритеты PTZ.
  При отсутствии подключения к Management Server клиент Operator Client в автономном режиме может подключаться к камере PTZ, если сама камера PTZ не заблокирована. Приоритеты купольных камер обновляются автоматически при восстановлении соединения.
- Вход.
  Невозможно переключить вход.
- Журнал.
  Журнал недоступен, открыть его невозможно. Открытое окно поиска в журнале не закрывается автоматически. Можно использовать и экспортировать существующие результаты поиска.
- Комплект разработчика ПО Operator Client.
  Функции комплекта разработчика ПО Operator Client с IServerApi не обрабатываются.
  Невозможно создать RemoteClientApi.
  Не работают некоторые методы, доступные только через API клиента, например ApplicationManager (попробуйте GetUserName()).
- Изменение пароля.
  Оператор не может сменить свой пароль.
- Реле.
  Невозможно переключать реле.
- Серверный сценарий.

Серверные методы интерфейса IServerApi обрабатываются, но не отправляются на клиент. К ним относятся следующие методы:
- AlarmManager
- AnalogMonitorManager
- CameraManager
- CompoundEventManager
- DecoderManager
- DeviceManager
- DomeCameraManager
- EventManager
- InputManager
- LicenseManager
- Журнал
- MatrixManager
- RecorderManager
- RelayManager
- ScheduleManager
- SendManager
- SequenceManager
- VirtualInputManager

– Наложения состояний.
Недоступны наложения состояний камер, входов и реле.

Наложение состояний устройства

Состояния устройства (точка записи, слишком много помех, слишком темно и т. д.) обрабатываются сервером Management Server. При потере соединения между клиентом и сервером состояния клиента не обновляются. О недоступности всех состояний устройства оператора уведомляет новое графическое наложение состояний. Если клиент восстановил подключение к серверу, наложения состояний обновляются автоматически.

– Состояние неизвестно
Наложение состояний устройства в логическом дереве или на карте в ситуации, когда клиент отключен от компьютера Management Server.

Причины отключения

Возможные причины потери соединения между клиентом Operator Client и сервером Management Server:
- нарушено физическое соединение;
- в автономном режиме изменился пароль пользователя, выполнившего вход в систему;
- сервер Management Server передал свободную лицензию рабочей станции другому клиенту Operator Client, подключившемуся, пока текущий клиент Operator Client был в автономном режиме;
- разные версии Operator Client и Management Server (версия Management Server ниже 5.5).

26.18 Разрешения для входа в систему на странице типа приложения

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > вкладка **Разрешения приложений** > вкладка **Разрешения для входа по типам приложений**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Разрешения приложений** > вкладка **Разрешения для входа по типам приложений**

Позволяет настроить различные разрешения пользователей для разных приложений.

Operator Client или Cameo SDK (непосредственно в Management Server)
Установите флажок, чтобы разрешить прямой вход на сервер Management Server клиента Operator Client или приложения Cameo SDK.

Operator Client (в Unmanaged Site)
Установите флажок, чтобы разрешить прямой вход в приложение Operator Client посредством подключения к unmanaged site.

Configuration Client
Установите флажок, чтобы разрешить вход в приложение Configuration Client.

Конфигурация API
Установите флажок, чтобы разрешить вход в **Конфигурация API**.

Мобильный доступ с помощью браузера
Установите флажок, чтобы разрешить мобильный доступ через браузер.

Мобильный доступ с помощью Video Security Client
Установите флажок, чтобы разрешить мобильный доступ через Video Security Client.

BVMS Server SDK / Server API
Установите флажок, чтобы разрешить вход в серверное приложение SDK системы BVMS.

BVMS Client SDK (разрешает подключение к Operator Client)
Установите флажок, чтобы разрешить вход в клиентское приложение Client SDK для определенных групп пользователей.

26.19 Страница параметров управления угрозами

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > вкладка **Управление угрозами** > вкладка **Настройки**

Позволяет настроить зависимость членства в группе от уровня угрозы.

Примечание. В случае тревоги определенного уровня текущий пользователь клиента Operator Client автоматически выйдет из системы, а Operator Client — перезапустится. Пользователь должен будет снова выполнить вход в Operator Client в режиме действующего уровня угрозы. В зависимости от настроек группы пользователей, соответствующий пользователь получит разрешения установленной группы пользователей для активного уровня угрозы.

Чтобы настроить уровень угрозы для группы пользователей:

1. Выберите соответствующую группу пользователей.
2. В соответствующем раскрывающемся меню уровня угрозы выберите группу пользователей, которую следует активировать при этом уровне угрозы.

27 Настройка пользователей, разрешений и корпоративного доступа

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

Главное окно > **Группы пользователей**

В этой главе описано, как настраивать группы пользователей, групп Enterprise User Group и доступ Enterprise.

Вы можете настроить все разрешения на использование устройств и рабочие разрешения для группы пользователей, а не для отдельного пользователя.

Применяются следующие правила:

- Пользователь BVMS может быть членом только одной группы пользователей BVMS или Enterprise User Group. Пользователь LDAP может быть членом нескольких групп пользователей LDAP.
- Настройки пользовательской группы по умолчанию изменять нельзя.
- Эта группа пользователей имеет доступ ко всем устройствам полного логического дерева, и ей назначено расписание **Всегда**.
- Для доступа к пользовательским группам домена Windows используются пользовательские группы LDAP.
- Нажмите  для сохранения настроек.
- Нажмите  для отмены последней настройки.
- Нажмите  для активации конфигурации.

Строгая политика паролей

Для повышения эффективности защиты компьютера от несанкционированного доступа рекомендуется использовать надежные пароли учетных записей пользователей.

В этих целях для всех вновь созданных групп пользователей по умолчанию активирована политика строгих требований к паролям. Это относится как к пользовательской группе Admin, так и стандартным пользовательским группам, группам Enterprise User Group и доступу Enterprise.

Применяются следующие правила:

- Минимальная длина пароля соответствует указанной на странице **Политики учетных записей** для соответствующих групп пользователей.
- Не используйте один из предыдущих паролей.
- Используйте по крайней мере одну букву в верхнем регистре (A–Z).
- Используйте по крайней мере одну цифру (0–9).
- Используйте по крайней мере один специальный символ (например, ! $ # %).

Когда пользователь-администратор впервые запускает Configuration Client, отображается диалоговое окно **Нарушение политики паролей** с предложением установить пароль для учетной записи администратора. Мы настоятельно рекомендуем сохранить этот параметр и задать надежный пароль для учетной записи администратора в соответствии с требованиями политики паролей.

При создании новой группы пользователей в Configuration Client строгие требования политики паролей применяются по умолчанию. Если не задать пароли для новых учетных записей пользователей соответствующих пользовательских групп, вы не сможете активировать конфигурацию. Отобразится диалоговое окно **Нарушение политики паролей**, содержащее список всех пользователей, для которых пароль еще не задан.
Для активации конфигурации необходимо задать недостающие пароли.

См.
- *Страница политик учетной записи, Страница 357*
- *Страница Свойства пользовательской группы, Страница 342*
- *Страница Свойства пользователей, Страница 343*
- *Страница Свойства комбинации для входа в систему, Страница 344*
- *Страница Разрешения камеры, Страница 344*
- *Страница Приоритеты управления, Страница 346*
- *Диалоговое окно Копировать разрешения пользовательской группы, Страница 347*
- *Страница Разрешения декодера, Страница 347*
- *Страница События и тревоги, Страница 347*
- *Диалоговое окно «Настройки LDAP сервера» (меню «Настройки»), Страница 119*
- *Страница Учетные данные, Страница 348*
- *Страница Логическое дерево, Страница 349*
- *Страница Свойства оператора, Страница 349*
- *Страница Приоритеты, Страница 353*
- *Страница Интерфейс пользователя, Страница 353*
- *Страница Доступ к серверу, Страница 354*

27.1 Создание группы или учетной записи

Главное окно > **Группы пользователей**
Вы можете создать стандартную группу пользователей, группу Enterprise User Group или Enterprise Account.
Чтобы разрешения группы пользователей соответствовали вашим требованиям, создайте новую группу и измените ее настройки.

27.1.1 Создание стандартной группы пользователей

Главное окно > **Группы пользователей**

Чтобы создать стандартную группу пользователей:
1. перейдите на вкладку **Группы пользователей**.
2. Нажмите  .
   Откроется диалоговое окно **Создать группу пользователей**.
3. Введите имя и описание.
4. Нажмите кнопку **ОК**.
   Новая группа добавляется в соответствующее дерево.
5. Щелкните по новой пользовательской группе правой кнопкой мыши и выберите **Переименовать**.
6. Введите нужное имя и нажмите клавишу ВВОД.

См.
- *Страница Свойства пользовательской группы, Страница 342*
- *Страница Свойства оператора, Страница 349*

– *Страница Приоритеты, Страница 353*
– *Страница Интерфейс пользователя, Страница 353*

27.1.2 Создание Enterprise User Group

Главное окно > **Группы пользователей**

Вы выполняете задачу создания Enterprise User Group для Enterprise System на Enterprise Management Server.

Вы создаете Enterprise User Group с пользователями для настройки их рабочих разрешений. Эти рабочие разрешения отображаются в Operator Client, подключенном к Enterprise Management Server . Примером рабочего разрешения является пользовательский интерфейс тревожного монитора.

Чтобы создать Enterprise User Group:

1. Нажмите вкладку **Enterprise User Groups**.
   Примечание. Вкладка **Enterprise User Groups** доступна только при наличии соответствующей лицензии и при условии, что один или несколько компьютеров Management Server настроены в **Устройства** > **Система Enterprise** > **Список серверов / адресная книга**.
2. Нажмите  .
   Откроется диалоговое окно **Создать группу пользователей Enterprise User Group**.
3. Введите имя и описание.
4. Нажмите кнопку **OK**.
   Enterprise User Group добавлена в соответствующее дерево.
5. Щелкните правой кнопкой по новой группе Enterprise и выберите **Переименовать**.
6. Введите нужное имя и нажмите клавишу ВВОД.
7. На странице **Рабочие разрешения** требуемым образом настройте рабочие разрешения и доступ к серверу для настроенных компьютеров Management Server.

См.

– *Страница Свойства пользовательской группы, Страница 342*
– *Страница Свойства оператора, Страница 349*
– *Страница Приоритеты, Страница 353*
– *Страница Интерфейс пользователя, Страница 353*
– *Страница Доступ к серверу, Страница 354*

27.1.3 Создание Enterprise Account

Главное окно > **Группы пользователей**

Замечание!
Прежде чем вы сможете добавить Enterprise Account, необходимо задать конфигурацию по меньшей мере одного устройства в дереве устройств.

Вы выполняете задачу создания Enterprise Account на Management Server. Повторите те же действия на каждом Management Server, являющемся элементом вашей Enterprise System.

Вы создаете Enterprise Account для настройки разрешений для устройств Operator Client с помощью Enterprise System.

Чтобы создать Enterprise Account:

1. Перейдите на вкладку **Доступ Enterprise**.

2. Нажмите  .
   Откроется диалоговое окно **Создать учетную запись Enterprise Account**.
3. Введите имя и описание.
4. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей.
   Введите ключ в соответствии с требованиями к ключам и подтвердите его.
5. Нажмите кнопку **OK**.
   Новая учетная запись Enterprise Account добавлена в соответствующее дерево.
6. Щелкните правой кнопкой по новой Enterprise Account и выберите **Переименовать**.
7. Введите нужное имя и нажмите клавишу ВВОД.
8. На странице **Разрешения устройств** настройте, если требуется, учетные данные, а также разрешения устройств.

См.
- *Строгая политика паролей , Страница 364*
- *Страница Учетные данные, Страница 348*
- *Страница Логическое дерево, Страница 349*
- *Страница События и тревоги, Страница 347*
- *Страница Приоритеты управления, Страница 346*
- *Страница Разрешения камеры, Страница 344*
- *Страница Разрешения декодера, Страница 347*

27.2 Создание пользователя

Главное окно > **Группы пользователей** > вкладка **Группы пользователей**
или
Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups**
Пользователь создается как новый член существующей стандартной группы пользователей или группы Enterprise User Group.

Замечание!
Имя и пароль пользователя, желающего работать с клавиатурой Bosch IntuiKey, подключенной к декодеру, должны состоять исключительно из цифр. Имя пользователя должно содержать не менее 3 цифр, а пароль — не менее 6 цифр.

Чтобы создать пользователя:

1. Выберите группу и нажмите  или щелкните правой кнопкой по необходимой группе и выберите **Новый пользователь**.
   Новый пользователь будет добавлен в дерево **Группы пользователей**.
2. Щелкните правой кнопкой мыши по новому пользователю и выберите **Переименовать**.
3. Введите нужное имя и нажмите клавишу ВВОД.
4. На странице **Свойства пользователей** введите имя пользователя и описание.
5. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей пользователей.
   Введите пароль в соответствии с требованиями политики и подтвердите его.
6. Нажмите **Применить**, чтобы применить настройки.

7. Установите флажок **Учетная запись включена**, чтобы активировать учетную запись пользователя.
8. Нажмите  , чтобы активировать пароль.
9. Нажмите  , чтобы активировать конфигурацию.

Примечание. После добавления нового пользователя нужно всегда активировать конфигурацию.

См.
- *Страница Свойства пользователей, Страница 343*
- *Строгая политика паролей , Страница 364*
- *Страница Пользовательские группы, Страница 340*

27.3 Создание группы с двойной авторизацией

Главное окно > **Группы пользователей** > вкладка **Группы пользователей**
или
Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups**
Вы можете создать двойную авторизацию для стандартной группы пользователей или для Enterprise User Group.
Для доступа Enterprise двойная авторизация недоступна.
Вы выбираете две пользовательских группы. Члены этих групп пользователей становятся членами новой группы с двойной авторизацией.

Чтобы создать группу с двойной авторизацией:

1. Нажмите кнопку  .
   Откроется диалоговое окно **Создать группу с двойной авторизацией** или диалоговое окно **Создать группу Enterprise с двойной авторизацией** соответственно.
2. Введите имя и описание.
3. Нажмите **ОК**.
   Новая группа с двойной авторизацией будет добавлена в соответствующее дерево.
4. Щелкните правой кнопкой мыши новую группу с двойной авторизацией и нажмите **Переименовать**.
5. Введите нужное имя и нажмите клавишу ВВОД.

См.
- *Добавление комбинации для входа в систему к группе с двойной авторизацией, Страница 368*
- *Страница Свойства пользовательской группы, Страница 342*
- *Страница Свойства оператора, Страница 349*
- *Страница Приоритеты, Страница 353*
- *Страница Интерфейс пользователя, Страница 353*

27.4 Добавление комбинации для входа в систему к группе с двойной авторизацией

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > 
Создать группу с двойной авторизацией

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  **Создать группу Enterprise с двойной авторизацией**

Чтобы добавить комбинацию для входа в систему к группе с двойной авторизацией:

1. выберите требуемую группу с двойной авторизацией и нажмите кнопку  или щелкните правой кнопкой по группе и выберите **Новая комбинация для входа в систему**.
   Отображается соответствующее диалоговое окно.
2. Выберите группу пользователей из каждого списка.
   Пользователи первой группы пользователей вводят свои данные в первом диалоговом окне входа в систему, а пользователи второй группы пользователей подтверждают вход в систему.
   Вы можете выбрать одну и ту же группу в обоих списках.
3. Для каждой группы выберите **Форсировать двойную авторизацию** при необходимости.
   Когда этот флажок установлен, каждый пользователь из первой группы может входить в систему только вместе с пользователем из второй группы.
   Когда этот флажок не установлен, каждый пользователь из первой группы может войти систему отдельно, при этом пользуясь только правами доступа своей группы.
4. Нажмите кнопку **ОК**.
   Новая комбинация для входа в систему будет добавлена в соответствующую группу с двойной авторизацией.
5. Щелкните правой кнопкой мыши по новой комбинации для входа в систему и нажмите кнопку **Переименовать**.
6. Введите нужное имя и нажмите клавишу ВВОД

См.

- *Создание группы с двойной авторизацией, Страница 368*
- *Страница Свойства комбинации для входа в систему, Страница 344*

27.5 Настройка группы администраторов

Главное окно > **Группы пользователей** > вкладка **Группы пользователей**  группа администраторов
Позволяет добавлять новых пользователей, переименовывать существующих пользователей и удалять их из группы администраторов.

Чтобы добавить нового пользователя в группу администраторов:

1. Нажмите кнопку  или нажмите правой кнопкой мыши на группу администраторов и нажмите **Добавить нового пользователя**.
   В группу администраторов будет добавлен новый пользователь.
2. На странице **Свойства пользователей** введите имя пользователя и описание.
3. Флажок **Пользователь должен изменить пароль при следующем входе в систему** предварительно установлен для всех вновь созданных учетных записей.
   Введите пароль в соответствии с требованиями к паролям и подтвердите его.
4. нажмите **Применить** для применения настроек.

5. Нажмите  для активации пароля.

Чтобы переименовать пользователя-администратора:

1. Щелкните правой кнопкой мыши нужного пользователя-администратора и нажмите кнопку **Переименовать**.
2. Введите нужное имя и нажмите клавишу ВВОД.
3. Нажмите  , чтобы активировать изменение имени пользователя.

Чтобы удалить пользователя из группы администраторов:

- Щелкните правой кнопкой мыши нужного пользователя и нажмите кнопку **Удалить**. Пользователь будет удален из группы администраторов.

Примечание.

Вы можете удалить пользователя из группы администраторов только в том случае, если существуют другие пользователи-администраторы.
Если в группе администраторов всего один пользователь, его невозможно удалить.

См.

- *Страница Пользовательские группы, Страница 340*
- *Страница Свойства пользователей, Страница 343*
- *Строгая политика паролей , Страница 364*

27.6 Выбор связанной группы LDAP

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей Enterprise User Group**

Настройка групп LDAP осуществляется в стандартных группах пользователей или в Enterprise User Groups.

Чтобы выбрать связанную группу LDAP:

1. Нажмите кнопку **Искать группы**.
2. Выберите соответствующий тип в списке **Связанная группа LDAP** .

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

См.

- *Диалоговое окно «Настройки LDAP сервера» (меню «Настройки»), Страница 119*
- *Страница Свойства пользовательской группы, Страница 342*

27.7 Составление расписания разрешений на вход пользователей в систему

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей**
или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей Enterprise User Group**

Вы можете запретить членам определенной пользовательской группы или Enterprise User Group входить в систему с их компьютеров в определенные периоды времени. Вы не можете изменить эти настройки для пользовательской группы по умолчанию.

Составление расписания входа в систему

1. Перейдите на вкладку **Свойства группы пользователей**.
2. В списке **Расписание входа в систему** выберите расписание.

27.8 Настройка рабочих привилегий

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей**

или

Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups** >  > вкладка **Рабочие разрешения** > вкладка **Свойства группы пользователей Enterprise User Group**

- Вы можете настроить рабочие разрешения, такие как доступ к журналу событий Logbook и параметры пользовательского интерфейса.
- Вы не можете изменить эти параметры для группы пользователей по умолчанию.
- Рабочие разрешения настраиваются в стандартных группах пользователей или группах Enterprise User Group.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

См.

- *Страница Свойства пользовательской группы, Страница 342*
- *Страница Свойства оператора, Страница 349*
- *Страница Приоритеты, Страница 353*
- *Страница Интерфейс пользователя, Страница 353*
- *Страница Доступ к серверу, Страница 354*

27.9 Настройка разрешений устройств

Главное окно > **Группы пользователей** > вкладка **Группы пользователей** > вкладка **Разрешения устройств**

или

Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise** > вкладка **Разрешения устройств**

Разрешения для всех устройств логического дерева можно задавать отдельно.

После перемещения разрешенных устройств в папку, не имеющую разрешений для данной группы пользователей, следует установить разрешения для этой папки, чтобы обеспечить доступ к устройствам.

- Вы не можете изменить эти параметры для группы пользователей по умолчанию.

– Разрешения устройств настраиваются в стандартных группах пользователей или корпоративных учетных записях.

Для получения подробной информации о различных полях см. интерактивную справку по соответствующему окну приложения.

Для получения подробной информации о различных полях щелкните ссылку на соответствующее окно приложения ниже.

См.

– *Страница Логическое дерево, Страница 349*
– *Страница События и тревоги, Страница 347*
– *Страница Приоритеты управления, Страница 346*
– *Страница Разрешения камеры, Страница 344*
– *Страница Разрешения декодера, Страница 347*

27.10 Настройка различных приоритетов

Главное окно > **Группы пользователей** > вкладка **Группы пользователей**
или
Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups**
или
Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise**

Можно настроить следующие приоритеты:

– Стандартные группы пользователей и **Enterprise User Groups**: можно настроить приоритеты тревожных сигналов для режимов живого просмотра и воспроизведения.
– Для стандартных групп пользователей и **Доступ Enterprise**: можно настроить приоритеты для получения управления PTZ и магистральных линий Bosch Allegiant. Можно задать период времени для блокировки PTZ, т. е. пользователь с более высоким приоритетом может забрать управление камерой у пользователя с более низким приоритетом и заблокировать доступ на это время.

Настройка приоритетов для режима реального времени и воспроизведения:

1. Выберите стандартную пользовательскую группу или Enterprise User Group.
2. Нажмите кнопку **Рабочие разрешения**.
3. Перейдите на вкладку **Приоритеты**.
4. В поле **Поведение автоматически всплывающих окон** переместите ползунок в нужное положение.

Настройка приоритетов для PTZ и магистральных линий Bosch Allegiant:

1. Выберите стандартную пользовательскую группу или Enterprise Account.
2. Перейдите на вкладку **Разрешения устройств**.
3. Перейдите на вкладку **Приоритеты управления**.
4. В поле **Приоритеты управления** переместите ползунок в нужное положение.
5. Выберите нужный элемент из списка **Время ожидания в мин.**.

См.

– *Страница Приоритеты управления, Страница 346*
– *Страница Приоритеты, Страница 353*

27.11 Копирование разрешений пользовательской группы

Главное окно > **Группы пользователей** > вкладка **Группы пользователей**
или
Главное окно > **Группы пользователей** > вкладка **Enterprise User Groups**

или

Главное окно > **Группы пользователей** > вкладка **Доступ Enterprise**

Разрешения для одной группы или учетной записи можно копировать для другой.

Необходимо настроить по крайней мере 2 группы или учетные записи.

Копирование разрешений:

1. Выберите в дереве пользовательских групп группу или учетную запись.
2. Нажмите  .
   Откроется диалоговое окно **Копировать разрешения пользовательской группы**.
3. Выберите соответствующие разрешения и соответствующую группу или учетную запись.
4. Нажмите **ОК**. Разрешения данной группы будут скопированы в другую группу или учетную запись. Диалоговое окно закроется.

28 Страница Audit Trail

Замечание!
В BVMS Viewer доступны только основные функции. Дополнительные функции доступны в BVMS Professional. Подробные сведения о различных BVMS редакциях см. www.boschsecurity.com и BVMS краткое руководство по выбору: Краткое руководство по выбору BVMS.

Главное окно > **Audit Trail**

Функция Audit Trail позволяет отслеживать все изменения конфигурации системы и экспортировать данные в файл CSV.

Требования

1. Установите базу данных Audit Trail, выбрав ее в настройках BVMS (дополнительная функция настроек).
2. У вас есть следующее разрешение: **Показать страницу Audit Trail**.
3. Чтобы включить Audit Trail, перейдите в **Параметры** > **Параметры...** > **Параметры Audit Trail**.

Рекомендации:

- Не включайте функцию Audit Trail с самого начала, поскольку это приведет к регистрации большого объема данных.
- Сначала выполните первоначальную конфигурацию системы, создайте отчеты по вводу в эксплуатацию, а затем включите функцию Audit Trail для регистрации дальнейших изменений.
- Кроме того, отключайте функцию Audit Trail при импорте конфигураций.

Чтобы развернуть / свернуть данные Audit Trail:

1. Нажмите , чтобы развернуть один узел данных.
2. Нажмите , чтобы свернуть один узел данных.
3. Нажмите **Развернуть все** / **Свернуть все**, чтобы развернуть / свернуть все загруженные узлы данных.

Чтобы загрузить данные Audit Trail:

- Нажмите **Загрузить еще**.

Примечание. При нажатии кнопки **Загрузить еще** можно загрузить только десять узлов данных за раз.

Чтобы экспортировать данные Audit Trail:

- Нажмите **Экспортировать**, чтобы сохранить загруженные данные как файл CSV.

Примечание. Будет выполнен экспорт только загруженных данных.

См.

- *Диалоговое окно «Параметры» (меню «Настройки»), Страница 124*
- *Страница Разрешения конфигурации, Страница 355*

28.1 Регистрация сведений для Audit Trail

Примечание. При нехватке места в базе данных самые старые записи будут удаляться автоматически. По истечении срока хранения эти записи будут автоматически удалены.

Таблица Audit Trail содержит следующие столбцы:

Действие	Инициированное пользователем изменение.
Создано	В конфигурацию BVMS добавлен новый объект, например камера или пользователь.
Изменено	Изменен имеющийся в конфигурации объект, например отображаемое имя камеры.
Удалено	Удален имеющийся в конфигурации объект.
Добавлен элемент списка	Объект добавлен в список, например камера добавлена в пул VRM.
Элемент списка удален	Объект удален из списка, например камера удалена из пула VRM или VSG.
Тип объекта	Тип измененного объекта конфигурации.
Объект	Измененный объект, например камера, пользователь или расписание.
Сетевой адрес	Сетевой адрес объекта (если доступен).
Контекст объекта 1 / **Контекст объекта 2**	Контекст измененного пункта, обычно предок объекта. Например: добавлен целевой объект устройства iSCSI. Контекст устройства 1 — это родительское устройство iSCSI, а контекст 2 — система VRM, к которой относится устройство iSCSI.
Свойство	Имя измененного свойства.
Старое значение	Старое значение до изменения.
Новое значение	Новое значение, заданное при изменении.
Контекст 1 / **Контекст 2**	Дополнительный контекст, описывающий изменение. Например: если вы измените настройки камеры в параметрах тревоги, эта камера будет добавлена в качестве контекста.

28.2 Диалоговое окно фильтров Audit Trail

Диалоговое окно фильтров позволяет фильтровать или искать определенную информацию в базе данных Audit Trail.
Диалоговое окно содержит следующие предварительно настроенные фильтры:

- Категория
- Действие
- Период времени

Если выбрать в диалоговом окне фильтров несколько категорий или действий, все соответствующие разделы будут включены в поиск.

Кроме того, в поле свободного поиска текста можно вводить запросы, позволяющие, например, отфильтровать определенные параметры, устройства или пользователей. При вводе нескольких терминов для поиска результат должен содержать все введенные слова.
Для терминов, содержащих пробел, можно использовать кавычки. Например: "Camera 1".

Пример:
Вы выбираете категории **Устройства** и **Карты и структура**, а затем вводите имя камеры “Cam1” и имя пользователя “X” в поле свободного поиска текста.
Результат: в базе данных Audit Trail будут найдены все изменения, внесенные пользователем “X” в объекты конфигурации камеры “Cam1”, включенной в разделы **Устройства** или **Карты и структура**.

Чтобы использовать фильтр Audit Trail:
1. Нажмите **Фильтр**.
   Отроется диалоговое окно Audit Trail.
2. После конфигурации фильтра нажмите **Применить**.
3. Нажмите  , чтобы удалить один объект фильтра.
4. Нажмите **Сбросить все фильтры**, чтобы сбросить конфигурацию фильтра.

29 Настройка обнаружения пожара с помощью видео

Чтобы настроить обнаружение пожара с помощью видео, необходимо выполнить следующие действия.

1. Настройте обнаружение пожара на камере, поддерживающей эту функцию.
   Это делается на веб-странице камеры.
   Подробную информацию о настройке камеры для обнаружения пожара см. в разделе
   – *Настройка камеры для обнаружения пожара, Страница 377*
2. Добавьте эту камеру для обнаружения пожара в систему. Можно добавить камеру для обнаружения пожара в пул VRM, как кодер, работающий только в режиме реального времени, или как кодер с локальным хранилищем.
   Подробную информацию о добавлении камеры см. в разделе
   – *Добавление кодера в пул VRM, Страница 227*
   – *Добавление кодера, работающего только в режиме реального времени, Страница 227*
   – *Добавление кодера локального хранилища, Страница 227*
3. Настройте событие пожара для этой камеры.
   – *Настройка события пожара, Страница 380*
4. Настройте тревожный сигнал для события пожара.
   – *Настройка тревожного сигнала пожара, Страница 380*

См.

– *Добавление кодера в пул VRM, Страница 378*
– *Добавление кодера, работающего только в режиме реального времени, Страница 227*
– *Добавление кодера локального хранилища, Страница 227*
– *Настройка события пожара, Страница 380*
– *Настройка тревожного сигнала пожара, Страница 380*

29.1 Настройка камеры для обнаружения пожара

Главное окно > **Устройства** > разверните > разверните > разверните > разверните >

или

Главное окно > **Устройства** > разверните > разверните > разверните > разверните >

или

Главное окно > **Устройства** > >

или

Главное окно > **Устройства** > >

Чтобы настроить обнаружение пожара с помощью видео, сначала необходимо настроить обнаружение пожара на соответствующей камере.
Подробные сведения см. в руководстве по эксплуатации камеры для обнаружения пожара.

Настройка

1. Щелкните правой кнопкой мыши значок устройства и выберите команду **Показать страницу в браузере**.
2. Нажмите **Конфигурация**.
3. На панели навигации разверните узел **Тревога** и выберите пункт **Обнаружение пожара**.
4. Введите требуемые параметры.

29.2 Добавление кодера в пул VRM

Сведения о добавлении кодеров в пул VRM см. в разделе *Добавление кодеров путем поиска, Страница 185*.

См.

– *Добавление устройства, Страница 129*

29.3 Добавление кодеров путем поиска

Для добавления кодеров путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Выберите необходимые кодеры, выберите необходимый пул VRM и нажмите **Назначить**, чтобы назначить их пулу VRM.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

   В столбце **Состояние** успешные входы в систему обозначены значком  .

   Неудачные попытки входа обозначены значком  .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

29.4 Добавление устройств, работающих только в режиме реального времени, путем поиска

Для добавления устройств Bosch, работающих только в реальном времени, путем поиска выполните следующие действия.

1. Щелкните правой кнопкой мыши  и выберите команду **Поиск кодеров, работающих только в реальном времени**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку в столбец**.

   В столбце **Состояние** успешные входы в систему обозначены значком  .

   Неудачные попытки входа обозначены значком  .
5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

Значок ⚠ указывает на ошибку, которую необходимо принять во внимание. См. подсказки для получения дополнительной информации о конкретной ошибке.

29.5 Добавление кодеров локального хранилища путем поиска

Главное окно > **Устройства** > Развернуть  >
Позволяет добавлять и настраивать кодеры с локальным хранилищем.

Для добавления кодеров локального хранилища путем поиска выполните следующие действия.

1. В дереве устройств щелкните  правой кнопкой мыши и выберите **Поиск кодеров локального хранилища**.
   Откроется диалоговое окно **BVMS Scan Wizard**.
2. Установите флажки для устройств, которые необходимо добавить.
3. Нажмите **Далее >>**.
   Откроется диалоговое окно мастера **Проверки подлинности устройств**.
4. Введите пароль для каждого устройства, защищенного паролем.
   Проверка пароля выполняется автоматически через несколько секунд после прекращения ввода символов в поле или при нажатии вне поля пароля.
   Если пароли всех устройств совпадают, введите этот пароль в первое поле **Пароль**.
   Щелкните это поле правой кнопкой мыши и выберите команду **Копировать ячейку**

в столбец.

В столбце **Состояние** успешные входы в систему обозначены значком .

Неудачные попытки входа обозначены значком .

5. Нажмите **Готово**.
   Устройство добавлено в дерево устройств.

29.6 Настройка события пожара

Главное окно > **События**

Настройка

1. В дереве выберите **Кодеры/Декодеры > Камера > Состояние пожара или задымления** > **Пожар или задымление обнаружены**.
   Откроется соответствующая таблица настройки событий.
2. В столбце **Активировать тревогу** - **Расписание** нажмите ячейку и выберите соответствующее расписание.
   Расписание определяет, когда запускается тревожный сигнал.
   Выберите одно из расписаний записей или расписаний задач, настроенных на странице **Расписания**.
3. Установите требуемые параметры.

Примечание. Эту процедуру можно использовать для других доступных событий пожара.

29.7 Настройка тревожного сигнала пожара

Главное окно > **Тревожные сигналы**

Настройка

1. В дереве выберите **Кодеры/Декодеры > Камера > Состояние пожара или задымления** > **Пожар или задымление обнаружены**.
   Отображается соответствующая таблица настройки тревог.
2. Установите требуемые параметры.

30 Настройка MIC IP 7000, подключенного к VIDEOJET 7000 connect

Для правильной работы камеры MIC IP 7000, подключенной к VIDEOJET 7000 connect, необходимо установить следующую конфигурацию.

Перед добавлением камеры MIC IP в систему BVMS выполните следующие действия:

1. Восстановите на камере MIC IP 7000 и устройстве VIDEOJET 7000 connect заводские параметры по умолчанию (это делается на веб-страницах устройств).
2. Установите для камеры MIC IP 7000 вариант использования **MIC IP Starlight 7000 HD-VJC-7000**.
3. Настройте камеру MIC IP 7000 и устройство VIDEOJET 7000 connect в соответствии с документацией, которая входит в комплект поставки устройств.
4. Если вы хотите использовать ANR, запустите сервисную программу установки ANR для устройства VIDEOJET 7000 connect.

   Выполните эту задачу на компьютере, входящем в ту же сеть, что и устройство VIDEOJET 7000 connect.

   Сервисную программу установки ANR можно найти на странице каталога продуктов для устройства VIDEOJET 7000 connect.

Выполните следующую процедуру, чтобы добавить камеру MIC IP 7000 в систему BVMS и настроить ее:

1. В дерево устройств добавьте только камеру MIC IP 7000.

   Устройство VIDEOJET 7000 connect нельзя добавить в систему BVMS.
2. Щелкните добавленную камеру правой кнопкой мыши и выберите команду **Изменить кодер**.

   Откроется диалоговое окно **Изменить кодер**.

   Возможности устройства загружаются автоматически в соответствии с выбранным выше вариантом.
3. При необходимости настройте ANR на странице **Камеры и запись**.

31 Устранение неполадок

В данном разделе содержится информация об устранении неполадок при использовании BVMS Configuration Client.

Проблемы, возникающие при установке

Проблема	Причина	Решение
Программа установки отображает неверные символы.	Неверные языковые настройки Windows.	*Настройка языка в Windows, Страница 384*
Программа установки прерывается с сообщением о невозможности установить .	Файлы сервера OPC невозможно заменить.	Удалите OPC Core Components Redistributable и запустите программу установки BVMS еще раз.
Программное обеспечение не может быть удалено с помощью Настройки.		Запуск Control Panel > Add/ Remove Programs и удаление BVMS.

Проблемы, возникающие сразу после запуска приложения.

Проблема	Причина	Решение
BVMS отображается не на том языке.	В настройках Windows не установлен нужный язык	*Настройка языка Configuration Client, Страница 75* или *Настройка языка Operator Client, Страница 75*
Окно входа в систему Operator Client отображается не на том языке.	Несмотря на установку языка Operator Client в Configuration Client, язык окна входа в систему Operator Client зависит от языка Windows.	*Настройка языка в Windows, Страница 384*

Проблемы с отображением языка

Проблема	Причина	Решение
Отдельные тексты в Configuration Client или Operator Client отображаются на иностранном языке, чаще всего английском.	Язык операционной системы компьютера, на котором установлен Management Server, часто является английским. Поэтому когда на этом компьютере создается база данных BVMS, многие тексты также создаются на английском языке. Они остаются неизменными, независимо от языка Windows на компьютере с	Не изменяйте этого.

Проблема	Причина	Решение
	Operator Client. Чтобы избежать подобных языковых противоречий, установите программное обеспечение Management Server на компьютере с нужным языком интерфейса Windows.	

Проблемы с клавиатурой Bosch IntuiKey

Проблема	Причина	Решение
Клавиатура Bosch IntuiKey вызывает тревожный сигнал, а на дисплее отображается сообщение Off Line.	Прервано соединение с рабочей станцией. Поврежден или отключен кабель либо перезапущена рабочая станция.	*Повторная установка соединения с клавиатурой Bosch IntuiKey, Страница 384*

Проблемы с настройкой панели управления звуковой картой

Проблема	Причина	Решение
Обратная связь возникает при использовании микрофона в системе внутренней связи.	На панели управления звуковой картой должен быть выбран только микрофон, а не стереомикшер (или что-либо иное). Operator Client проверяет файл конфигурации при запуске и соответствующим образом изменяет настройки панели управления. В данном файле конфигурации имеется стандартный параметр, который может не соответствовать данной системной конфигурации. Этот параметр восстанавливается при каждом запуске Operator Client.	Измените параметр в файле конфигурации Operator Client на микрофон.

Аварийное завершение Configuration Client

Проблема	Причина	Решение
Configuration Client аварийно завершает работу.	При большом количестве камер, настроенных в файле Allegiant и не подключенных к Bosch	См. *Сокращение количества камер Allegiant, Страница 384*.

Проблема	Причина	Решение
	Video Management System, следует сократить это количество. Это позволяет избежать дополнительной нагрузки на систему.	

31.1 Настройка языка в Windows

Если нужно изменить язык отображения программы установки BVMS, нужно изменить язык в Windows. Для активации языковых настроек компьютер следует перезапустить после выполнения следующих действий.

Чтобы настроить нужный язык.

1. Нажмите кнопку **Пуск**, выберите **Панель управления** и дважды щелкните **Язык и региональные стандарты**.
2. Перейдите на вкладку **Дополнительно** и выберите нужный язык в поле **Язык программ, не поддерживающих Юникод**.
3. Нажмите **ОК**.
4. В каждом следующем окне сообщения нажмите **Да**.
   Компьютер будет перезагружен.

31.2 Повторная установка соединения с клавиатурой Bosch IntuiKey

1. Подключите кабель или дождитесь, пока рабочая станция войдет в оперативный режим.
   Отображается сообщение Off Line.
2. Нажмите программную клавишу Terminal для входа в BVMS.

31.3 Сокращение количества камер Allegiant

Для редактирования файла Allegiant требуется программное обеспечение Master Control Software.

Для сокращения количества камер Allegiant:

1. Запустите Master Control Software.
2. Откройте файл Allegiant.
3. Перейдите на вкладку Camera.
4. Отметьте камеры, использование которых не является необходимым.
5. В меню Edit выберите пункт Delete.
6. Сохраните файл. Размер файла остается неизменным.
7. Повторите последнее действие для мониторов, использование которых не является необходимым. Перейдите на вкладку Monitors.
8. Импортируйте этот файл в Bosch Video Management System (см. *Добавление устройства, Страница 129*).

31.4 Используемые порты

В этом разделе перечислены все компоненты портов BVMS, которые должны быть открыты в локальной сети. Не открывайте эти порты для доступа через Интернет! Для доступа через Интернет используйте безопасные соединения, такие как VPN.
В каждой таблице перечислены локальные порты, которые должны быть открыты на компьютере, где установлено серверное ПО, или на маршрутизаторе/коммутаторе уровня 3, подключенном к оборудованию.

В брандмауэре Windows настройте правило входящих подключений для каждого открытого порта.
Разрешите все исходящие подключения для всех приложений BVMS.

Порты Management Server / Enterprise Management Server

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Management Server	UDP	123	Кодер	TimeServer NTP
Management Server	TCP	5322	Operator Client,	Подключение SSH
Management Server	TCP	5389	Устройство ONVIF	Прокси ONVIF, уведомления о событиях
Management Server	TCP	5390	Operator Client, Configuration Client	Удаленное использование .NET
Management Server	TCP	5391	Клиенты Operator Client, Configuration Client, NVR	Порт удаленного взаимодействия для всех служб NVR
Management Server	TCP	5392	Operator Client, Configuration Client, Mobile Video Service, Приложение BVMS SDK	WCF, gateway.push.apple.com
Management Server	TCP	5393	Operator Client, VRM, MVS	Data-Access-Service
Management Server	TCP	5394	Operator Client	Порт удаленного взаимодействия для Operator Client
Management Server	TCP	5395	Configuration Client, Operator Client	Настройки пользователя, передача файлов
Management Server	TCP	5396	Клиенты Configuration Client, WCF	Точка входа Mex (обычно отключена)
Management Server	TCP	5397	Operator Client для автоматического развертывания	Порт автоматического развертывания
Management Server	TCP	5398	Клиент конфигурации API	Внутренняя связь между компонентом AKKA.Net и CS
Management Server	UDP	12544	Клиент SNMP	Получение порта BVMS SNMP
Management Server	TCP	162	SNMP	

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Management Server	TCP	5389 - 5396	Порты BVMS	
Management Server	TCP, UDP	135	BRS DCOM	BRS
Management Server	TCP	808	Веб-служба BRS (DIBOS)	Центральный сервер подключается к DIBOS через этот порт, когда используется WCF
Management Server	TCP	1756 / 1757	RCP	1757 для вторичного VRM

Дополнительные центральные компоненты

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Configuration Client	UDP	1024 - 65535	Кодер, VRM	Потоковая передача видео
Конфигурация API	TCP	5399	Клиент REST API	Конфигурация API
Management Server	TCP	5443	PID	Подключение PID, доступ через HTTPS
Мониторинг рабочих станций	TCP	5410	Operator Client, Management Server	
Мониторинг рабочих станций	TCP	5411	Служба GRPC	

Порты Video Recording Manager

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
VRM	TCP	554 / 555	Клиент RTSP	Извлечение первичного/ вторичного потока RTSP
VRM	TCP	40023	Клиент Telnet	Telnet (локальный узел только из VRM 4.x)

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
VRM	TCP	40080 / 40081	Клиент VRM	HTTP-порт vj_generic.dll
VRM	TCP	41080 / 41081	Клиент VRM	HTTP vj_generic.dll (только локальный узел)
VRM	TCP	1756 / 1757	Management Server, Configuration Client	через RCP+, (1757 для вторичного клиента VRM RCP+)
VRM	UDP	1757	Management Server, Operator Client	Сканировать целевой объект широковещательной передачи
VRM	UDP	1758	Management Server, Configuration Client	Отклик сканирования
VRM	UDP	1759	Management Server, Configuration Client	Обнаружение сетевых ресурсов, сканировать целевой объект многоадресной передачи
VRM	UDP	1760		
VRM	UDP	1800 / 1900	Management Server, Operator Client	Сканировать целевой объект многоадресной передачи
VRM	TCP	80	Operator Client	Воспроизведение первичного VRM через http
VRM	TCP	443	Operator Client	Воспроизведение первичного VRM через https
VRM	TCP	81	Operator Client	Воспроизведение вторичного VRM через http
VRM	TCP	444	Operator Client	Воспроизведение вторичного VRM через https

Порты Bosch Video Streaming Gateway

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Bosch Video Streaming Gateway	TCP	8080 - 8086	VRM, Management Server, Configuration Client, Operator Client	HTTP
Bosch Video Streaming Gateway	TCP	8443 - 8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	TCP	8756 - 8762	VRM, Management Server, Configuration Client	RCP +
Bosch Video Streaming Gateway	TCP	8443-8449	VRM, Management Server, Configuration Client, Operator Client	HTTPS
Bosch Video Streaming Gateway	UDP	1757	Клиент VRM	Сканировать целевой объект широковещательной передачи
Bosch Video Streaming Gateway	UDP	1758	Клиент VRM	Отклик сканирования
Bosch Video Streaming Gateway	UDP	1759	Клиент VRM	Обнаружение сетевых ресурсов, сканировать целевой объект многоадресной передачи
Bosch Video Streaming Gateway	UDP	1800, 1900	VRM Configuration Client	Обнаружение сетевых ресурсов, сканировать целевой объект многоадресной передачи
Bosch Video Streaming Gateway	UDP	1064-65535	Кодер, VRM	Потоковая передача видео

Порты Mobile Video Service

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Mobile Video Service	TCP	80	Management Server, Operator Client, Configuration Client, HTML-клиент, мобильные приложения	Воспроизведение первичного VRM через HTTP
Mobile Video Service	TCP	443	Management Server, Operator Client, Configuration Client, HTML-клиент, мобильные приложения	Воспроизведение первичного VRM через HTTPS
Mobile Video Service	TCP	2195	Push-уведомление Apple	Mac iOS
Mobile Video Service	UDP	1064-65535	Кодер, VRM	Потоковая передача видео
Транскодер Mobile Video Service	TCP	5382	Мобильный провайдер Mobile Video Service	Поток медиа
Провайдер Mobile Video Service BVMS	TCP	5383	Operator Client	Поток медиа
Провайдер Mobile Video Service BVMS	TCP	5384	HTML-клиент, мобильные приложения	Поток медиа
Транскодер Mobile Video Service	TCP	5385	Мобильный провайдер Mobile Video Service	Поток медиа

Порты системы хранения iSCSI

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Система хранения iSCSI	TCP	3260	Кодер, VRM, Configuration Client, Operator Client	Система хранения iSCSI

Порты DVR

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
DVR	TCP	80	Management Server, Configuration Client, Operator Client	Доступ через HTTP
DVR	TCP	443	Management Server, Configuration Client, Operator Client	Доступ через HTTPS

Порты камеры ONVIF/камеры/кодера

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Кодер	TCP	80	Management Server, VSG, Configuration Client, Operator Client	Доступ через HTTP
Кодер	TCP	443	Management Server, VSG, Configuration Client, Operator Client	Доступ через HTTPS
Кодер	UDP	123	Management Server, VRM	SNTP
Кодер	UDP	161	Management Server, VRM	SNMP
Кодер	TCP	554	Operator Client, приложение BVMS SDK, VSG	Потоковая передача данных RTSP
Кодер	TCP	3260	Кодер (исходящий)	Запись iSCSI
Кодер	TCP	1756	Декодер, Management Server, Operator Client	Исходящие подключения для камер Bosch
Кодер	UDP	1757	Декодер, Management Server, Operator Client	Сканировать целевой объект широковещательной передачи
Кодер	UDP	1758	Декодер, Management Server, Operator Client	Отклик сканирования
Кодер	UDP	1800	Декодер, Management Server, Operator Client	Обнаружение сетевых ресурсов, сканировать целевой объект многоадресной передачи

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Кодер	UDP	1900		SSDP (дополнительный порт кодера)
Кодер	UDP	21		FTP (дополнительный порт кодера)
Кодер	UDP	3702		UPNP (дополнительный порт кодера)
Кодер	UDP	9554		SRTSP (дополнительный порт кодера)
Кодер	UDP	15344 / 15345		Отправка RTSP (дополнительный порт кодера)

Порты декодера BVMS

Настройте перенаправление портов на подключенном маршрутизаторе для этого устройства.

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Декодер	TCP	1756	Management Server, Operator Client, Configuration Client, приложение BVMS SDK	Исходящие подключения для камер Bosch
Декодер	UDP	1757	Management Server, Operator Client	Сканировать целевой объект широковещательной передачи
Декодер	UDP	1758	Management Server, Operator Client	Отклик сканирования
Декодер	UDP	1800	Management Server, Operator Client	Обнаружение сетевых ресурсов, сканировать целевой объект многоадресной передачи
Декодер	TCP	80	Operator Client	Доступ через HTTP
Декодер	TCP	443	Operator Client	Доступ через HTTPS
Декодер	UDP	1024-65535	Кодер	Порты потоковой передачи
Декодер	UDP	123	Management Server, VRM	SNTP

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Декодер	UDP	161	Management Server, VRM	SNMP

Порты BVMS Operator Client / Cameo SDK

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Operator Client	TCP	5394	Приложение BVMS SDK, BIS	WCF
Operator Client	UDP	1024-65535	Кодер, VRM	Потоковая передача видео
Operator Client	TCP	40082		
Operator Client	TCP	41756		

Порты адаптеров устройств LPR, BVMS

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
Адаптер устройства BVMS	TCP	31000	Клиент камеры LPR	VRC

Порты AMS, Access Management System

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
AMS	TCP	62904	Management Server	Доступ через HTTPS

Транскодер

Сервер (принимающий)	Протокол	Входящие порты	Клиент (отправляющий запрос)	Комментарий
	UDP	5080		
	UDP	5443		
	UDP	5756		

31.5 Включение журнала для событий ONVIF

Замечание!

Следует помнить, что эта функция срабатывает в конце срока использования.

Воспользуйтесь ONVIF Camera Event Driver Tool для простого ONVIF сопоставления событий.

См. *Запуск ONVIF Camera Event Driver Tool из Configuration Client, Страница 217*.

Можно включить запись событий ONVIF в журнал, если, например, возникают проблемы с получением событий BVMS. Запись в журнал помогает найти проблему.

Включение записи в журнал:

1. Откройте файл `%programfiles%\Bosch\VMS\AppData\Server\CentralServer\BVMSLogCfg.xml` в подходящем редакторе, например Notepad. Запустите приложение Notepad в качестве администратора.
2. Перейдите к строке, содержащей следующий текст:
   `Add logging for onvif events of a device by network address`
   Строки, ограниченные символами комментариев, содержат кратное описание.
3. Введите имя средства записи журналов `OnvifEvents.<Networkaddress>`.
   Введите только `OnvifEvents`, чтобы записывать в журнал события для всех устройств ONVIF.
4. Введите значение переменной `DEBUG` для всех входящих и исходящих событий.
   Введите `INFO` для всех исходящих событий.
   Введите `WARN` или `ERROR` для отключения.

Примечание. При активации может потребоваться перезапуск центрального сервера. В строках кода ниже дан пример записи всех исходящих и входящих событий с устройства 172.11.122.22:

```
<logger name="OnvifEvents.172.11.122.22" additivity="false">
<level value = "DEBUG"/>
<appender-ref ref="OnvifRollingFileAppender"/>
</logger>
```

Поддержка

Получить **услуги поддержки** можно по адресу www.boschsecurity.com/xc/en/support/.
Bosch Security and Safety Systems предоставляет поддержку в следующих областях:

- Приложения и инструменты
- Информационное моделирование здания
- Гарантия
- Устранение неисправностей
- Ремонт и обмен
- Безопасность продуктов

Bosch Building Technologies Academy

Посетите сайт Bosch Building Technologies Academy для доступа к **учебным курсам, видеоучебникам** и **документам**: www.boschsecurity.com/xc/en/support/training/

См.

- *Запуск ONVIF Camera Event Driver Tool из Configuration Client, Страница 217*
- *Настройка таблицы сопоставления ONVIF, Страница 250*
- *Сопоставление событий ONVIF, Страница 42*

Глоссарий

Allegiant

Семейство аналоговых матричных коммутаторов компании Bosch.

ANR

Автоматическая компенсация сети. Интегрированный процесс, в ходе которого отсутствующие видеоданные копируются с видеопередатчика на сетевой видеорегистратор после сбоя сети. Скопированные видеоданные в точности заполняют пропуск, возникший в результате сбоя сети. По этой причине передатчику необходимо локальное устройство хранения любого типа. Объем этого локального хранилища рассчитывается по следующей формуле: (пропускная способность сети x предполагаемое время простоя сети + запас надежности) x (1 + 1/скорость резервного копирования). Получаемый объем требуется в связи с тем, что во время процесса копирования процесс непрерывной записи должен продолжаться.

ATM

Банкомат

BIS

Building Integration System

B-кадр

Двунаправленный кадр. Часть способа сжатия видео.

DNS

Система доменных имен DNS-сервер конвертирует URL-адрес (например, www.myDevice.com) в IP-адрес в сетях, использующих протокол TCP/IP.

DTP

Устройство DTP (процессор преобразования данных) преобразует последовательные данные устройств ATM в заданный формат данных и отправляет эти данные через соединение Ethernet системе BVMS. Необходимо проследить за тем, чтобы на устройстве DTP был настроен фильтр трансформации. Эта задача выполняется отдельным ПО производителя устройства DTP.

DWF

Design Web Format. Используется для отображения технических чертежей на мониторе компьютера.

DynDNS

Динамическая система доменных имен Главный узел DNS, содержащий IP-адреса, готовые в базе данных. Динамическая система DNS позволяет подключаться к устройству через Интернет, используя имя главного узла устройства. См. DNS.

GSM

Global System for Mobile Communication. Стандарт цифровой мобильной связи.

H.264

Стандарт кодирования (сжатия) цифрового видео и аудио для мультимедийных приложений. Данный стандарт включает различные профили, которые могут зависеть от производителя. Доступны следующие профили: Baseline, Baseline+, Main Profile. Baseline (не используется в Bosch Video Management System) поддерживает 2 CIF. Baseline+ поддерживает 4 CIF и обеспечивает более высокое качество изображения, чем Baseline. Main Profile поддерживает 4 CIF и обеспечивает высокоэффективный алгоритм сжатия, называемый CABAC (Контекстно-адаптивное двоичное арифметическое кодирование). Он служит для высококачественного кодирования для хранения.

H.265

H.265 — это стандарт сжатия видеосигнала, заданный ISO2 и ITU3 и принятый 29 октября 2014. Он рассматривается как преемник MPEG-4 AVC (Advanced Video Codec), также называемый H.264, и призван осуществлять сжатие разрешения от 4K и ultra HD до 36 МП.

IQN

iSCSI Qualified Name (уточненное имя iSCSI). Имя инициатора в формате IQN используется для предоставления адресов как инициаторам, так и получателям iSCSI. При сопоставлении IQN создается группа инициаторов,

управляющая доступом к устройствам LUN на получателе iSCSI, а имена инициаторов каждого кодера и диспетчера видеозаписи записываются в данную группу инициаторов. Только тем устройствам, имена инициаторов которых добавлены в группу инициаторов, разрешен доступ к LUN. См. LUN и iSCSI.

iSCSI

Internet Small Computer System Interface. Протокол, обеспечивающий хранение через сеть TCP/IP. iSCSI обеспечивает доступ к сохраненным данным из любого места сети. Особенно с появлением Gigabit Ethernet стало возможным подключение серверов хранения iSCSI как обычных удаленных жестких дисков к компьютерной сети. В терминологии iSCSI сервер, обеспечивающий ресурсы хранения, называется "получателем iSCSI", а клиент, подключающийся к серверу и пользующийся его ресурсами, называется "инициатором iSCSI".

I-кадр

Ключевой кадр. Часть способа сжатия видео. Содержит информацию об изображении целиком, в отличие от P- или B-кадров, содержащих информацию об изменениях по отношению к предыдущему или последующему кадру.

JPEG

Joint Photographic Expert Group (объединенная группа экспертов по фотографии)

JPEG

Joint Photographic Expert Group (объединенная группа экспертов по фотографии). Процесс кодирования для фотографий.

LDAP

Lightweight Directory Access Protocol; облегченный протокол службы каталогов. Сетевой протокол, работающий под управлением TCP / IP, обеспечивающий доступ к каталогам. Каталогом может быть, например, список пользовательских групп и их прав доступа. Bosch Video Management System использует этот протокол для получения доступа к тем же группам, что и MS Windows или другая система управления пользователями для учреждений.

LUN

Logical Unit Number (Логический номер устройства) Используется в окружении iSCSI для адресации отдельного диска или виртуального раздела (тома). Раздел является частью дискового массива RAID (получатель iSCSI).

MHT

Другое название - веб-архивы. Формат файла, в котором могут сохраняться все файлы HTML и файлы изображений Интернет-сайта. Чтобы избежать проблем, рекомендуется создавать файлы MHT только при помощи Internet Explorer 7.0 или выше.

OID

Object Identifier; идентификатор объекта. Термин в окружении SNMP. Определяет переменные MIB.

ONVIF

Открытый форум по интерфейсу сетевого видео (Open Network Video Interface Forum). Глобальный стандарт для сетевых видеопродуктов. Устройства, соответствующие стандарту ONVIF, могут в режиме реального времени обмениваться видео- и аудиоданными, метаданными и информацией управления и обеспечивать автоматическое обнаружение и подключение к сетевым приложениям (например, к системам управления видео).

Operator Client

Компонент Bosch Video Management System, который предоставляет пользовательский интерфейс для мониторинга и эксплуатации системы.

PID

Person Identification Device. Оно извлекает характеристики человека из изображения, например его лица. Оно запускает специальные алгоритмы, способные идентифицировать человека в видеопотоке.

POS

Point of sale; точка продажи.

P-кадр

Предикативный кадр. Часть способа сжатия видео.

RAID

Избыточный массив независимых дисков. Используется для организации двух или нескольких жестких дисков, как если бы они были одним диском. На таком диске данные используются совместно или дублируются. Это необходимо для достижения большей емкости, надежности и скорости.

RCP

Протокол дистанционного управления

RTP

Сокращение от "Real-Time Transport Protocol"; протокол для передачи видео и аудио в реальном времени

RTSP

Real Time Streaming Protocol. Сетевой протокол, позволяющий управлять непрерывной передачей аудио- и видеоданных или программного обеспечения по IP-сетям.

SNMP

Простой протокол сетевого управления. Протокол, основанный на IP, позволяющий получать информацию от сетевых устройств (GET), устанавливать параметры сетевых устройств (SET) и получать уведомления об определенных событиях (EVENT).

TCP

Transmission Control Protocol (протокол управления передачей)

TCP/IP

Transmission Control Protocol / Internet Protocol; протокол TCP/IP. Другое название – пакет интернет-протоколов. Набор протоколов связи, используемых для передачи данных по IP-сети.

UDP

User Datagram Protocol; Протокол без установления соединения, используемый для обмена данными по IP-сети. Протокол UDP более эффективен для передачи видеоданных, чем протокол TCP по причине более низких потерь.

unmanaged site

Элемент дерева устройств в системе BVMS, который может содержать сетевые видеоустройства, например цифровые видеорегистраторы. Эти устройства не управляются сервером Management Server вашей системы. Пользователь Operator Client может подключаться к устройствам объекта unmanaged site по требованию.

URI

Универсальный идентификатор ресурса (Uniform Resource Identifier). Строка для определения сетевого ресурса. Каждый URI содержит схему, права, путь, запрос и фрагмент. Для Mobile Video Service обязательны только схема и фрагмент. Пример: http:<схема>// example.com<полномочия>/over/therepath>? name=ferret<запрос>#nose<фрагмент>

URL

Сокращение от "Uniform Resource Locator"; URL-адрес, унифицированный указатель ресурсов

VCA

Анализ видеоданных: компьютерный анализ видеопотоков, позволяющий определить, что происходит в контролируемом кадре. См. также Intelligent Video Analytics

VRM

Video Recording Manager (Диспетчер видеозаписи) Пакет программного обеспечения в Bosch Video Management System, который управляет сохранением видео (MPEG-4 SH++, H.264 и H.265) с аудиоданными и метаданными на устройства iSCSI в сети. VRM ведет базу данных, в которой содержится информация об источнике записи и список соответствующих устройств iSCSI. VRM реализуется как служба, запущенная на компьютере в сети Bosch Video Management System. Диспетчер видеозаписи не сохраняет видеоданные, а распределяет объем памяти на устройствах iSCSI по кодерам при одновременном распределении нагрузки между несколькими устройствами iSCSI. Диспетчер видеозаписи передает поток воспроизведения от iSCSI на модули Operator Client.

Активная точка

Значок на карте, реагирующий на щелчок мышью. Активные точки настраиваются в ПО Configuration Client. Активными точками могут быть, например, камеры, реле, входы. Оператор использует их для локализации и выбора устройства в здании. При соответствующих настройках активные точки могут мигать цветом фона, когда возникает определенное событие состояния или тревога.

Анализ видеоданных

Видеоаналитика — программный процесс, который сравнивает изображение с камеры с сохраненным изображением определенных людей или объектов. В случае соответствия программное обеспечение создает тревожный сигнал.

Бесконтактное развертывание

Способ автоматической загрузки, установки и запуска приложений .NET без изменения реестра или совместно используемых компонентов системы. В системе Bosch Video Management System автоматическое развертывание используется для обновления клиентов Operator Client с сервера Management Server. Обновление происходит, если на сервере Management Server хранится новая версия, и при каждом входе пользователя в систему на клиенте Operator Client. Если вы работаете с одним клиентом Operator Client и несколькими компьютерами Management Server, автоматическое развертывание использует только версию программного обеспечения, хранящуюся на сервере Management Server, к которому клиент Operator Client в последний раз успешно подключился. При попытке подключения к другому серверу Management Server с другой версией приложения он отображает Management Server как отключенный, поскольку версии ПО не совпадают.

Виртуальный вход

Используется для пересылки событий из внешних систем в систему Bosch Video Management System.

время задержки

Временной период, который начинается с момента возникновения некоторого события. В течение этого временного периода обычно не принимаются никакие другие события того же типа. Например, это предотвращает создание датчиком переключения большого количества событий. Для событий с несколькими состояниями можно настроить разные приоритеты для каждого состояния. Приведенные ниже примеры поясняют концепцию времени задержки. В примере 1 рассматриваются события создания одного состояния: возникает событие "Информация о системе" и начинается отсчет настроенного времени задержки. В это время возникает другое событие "Информация о системе". Такое событие "Информация о системе" не принимается как новое событие. В примере 2 рассматриваются события создания разных состояний с одинаковым приоритетом: возникает событие "Обнаружено движение" и начинается отсчет настроенного времени задержки. В это время возникает событие "Движение остановлено" с таким же приоритетом. Такое событие "Движение остановлено" не принимается как новое событие. В примере 3 также рассматриваются события создания разных состояний с одинаковым приоритетом: активно состояние виртуального входа. Приоритеты состояний для обоих изменений состояний идентичны. В конкретный момент времени виртуальный вход выключается и начинается отсчет времени задержки. В течение этого времени задержки виртуальный вход включен. Это изменение состояния не принимается как новое событие, так как у него такой же приоритет. После истечения времени задержки виртуальный вход находится в другом состоянии. При включении задается метка времени завершения времени задержки, и новое время задержки не начинает отсчитываться. В примере 4 рассматриваются события с разными приоритетами создания разных состояний: возникает событие "Обнаружено движение" и начинается отсчет настроенного времени задержки. В это время возникает событие "Движение остановлено" с более

высоким приоритетом. Событие "Движение остановлено" принимается как новое событие, но новый отсчет времени задержки не начинается. В примере 5 также рассматриваются события с разными приоритетами создания разных состояний: состояние виртуального входа — выкл. Приоритет состояния "включено" — "5", для "выключено" — "2". В конкретный момент времени виртуальный вход включается (приоритет "5") и начинается отсчет времени задержки. В течение этого времени задержки виртуальный вход выключен (приоритет "2"). Это изменение состояния принимается как новое событие, так как у него более высокий приоритет. Продолжается отсчет времени задержки первого включения. В течение этого времени задержки дальнейшие изменения состояния не принимаются.

Время перемотки

Количество секунд, через которые область изображений переключается на немедленное воспроизведение.

Вторичный VRM

Программное обеспечение в среде BVMS. Обеспечивает выполнение записи, производимой одним или несколькими основными диспетчерами видеозаписи, дополнительно и одновременно на другой целевой объект iSCSI. Настройки записи могут отличаться от настроек основного диспетчера видеозаписи.

группа мониторов

Несколько мониторов, подключенных к декодеру. Группа мониторов может быть использована для обработки тревожных сигналов в определенной физической области. Например, три изолированных друг от друга центра управления могут иметь три группы мониторов. Мониторы в группе мониторов логически объединены в строки и столбцы, их можно настроить на отображение с различной схемой расположения, например в квадрированном или полноэкранном режиме.

Группа пользователей Enterprise

Enterprise User Group — пользовательская группа, настроенная на Enterprise Management Server. Enterprise User Group — это группа пользователей, которые могут получить доступ одновременно к нескольким компьютерам Management Server. Определяет рабочие разрешения, доступные для этих пользователей.

двойная авторизация

Политика безопасности, требующая входа в систему Operator Client двух отдельных пользователей. Оба пользователя должны быть членами обычной пользовательской группы Bosch Video Management System. Эта группа (или группы, если пользователи принадлежат к разным пользовательским группам) должна входить в группу с двойной авторизацией. Группа с двойной авторизацией имеет свои собственные права в системе Bosch Video Management System. Эта группа с двойной авторизацией должна иметь более широкие права доступа, чем обычная пользовательская группа, к которой принадлежат пользователи. Пример: Пользователь A является членом пользовательской группы с именем Группа A. Пользователь B является членом Группы B. Кроме того, создана группа с двойной авторизацией, в состав которой входят Группа A и Группа B. Для пользователей Группы A двойная авторизация факультативна, для пользователей Группы B она обязательна. При входе в систему пользователя A появляется второе диалоговое окно для подтверждения регистрационных данных. В этом диалоговом окне может зарегистрироваться второй пользователь, если он доступен. Если нет, пользователь A может продолжать и запустить Operator Client. В этом случае он имеет права доступа только группы A. После входа в систему пользователя B опять отображается второе диалоговое окно для регистрации. В этом диалоговом окне должен зарегистрироваться второй пользователь. В противном случае пользователь B не может запустить Operator Client.

Двухпотоковая передача данных

Двухпотоковая передача обеспечивает одновременное кодирование потока входящих данных в соответствии с двумя различными, индивидуально настраиваемыми профилями. При этом создается два потока данных: один для записи в реальном времени и записи

перед тревожным сигналом, второй для непрерывной записи, записи движения и записи по тревоге.

декодер

Преобразует цифровой поток в аналоговый.

Дерево устройств

Иерархический список всех доступных устройств системы.

Документ

BVMS поддерживает следующие форматы документов: HTM, URL, MHT, HTML, TXT.

Доступ Enterprise

Доступ Enterprise — это компонент системы BVMS, который состоит из одного или нескольких учетных записей Enterprise Account. Каждая учетная запись Enterprise Account содержит разрешения устройств для определенного сервера Management Server.

дуплекс

Этот термин используется для определения направления передачи данных между двумя сторонами. Полудуплекс обеспечивает передачу данных в двух направлениях, но не одновременно Полный дуплекс обеспечивает одновременную передачу данных.

Журнал

Хранилище записей обо всех событиях в системе Bosch Video Management System.

Запрос

Термин в окружении SNMP для незапрошенного сообщения, отправляемого устройством (агент), мониторинг которого осуществляется системой мониторинга сети (диспетчер), о событии в этом устройстве.

Зеркальный VRM

Программное обеспечение в среде BVMS. Особый случай вторичного диспетчера видеозаписи. Обеспечивает выполнение записи, производимым основным диспетчером видеозаписи, дополнительно и одновременно на другой целевой объект iSCSI с теми же параметрами записи.

Кадр./сек

Количество кадров в секунду. Количество видеоизображений, передаваемых или записываемых за секунду.

Камера PTZ

Камера с функциями панорамирования, наклона и увеличения.

Кодировщик

Превращает аналоговый поток в цифровой, например, для интегрирования аналоговых камер в цифровую систему, например, Bosch Video Management System. Некоторые кодеры могут быть оснащены локальным устройством хранения данных, например, флэш-картой, жестким диском USB, или могут сохранять видеоданные на устройствах iSCSI. IP-камеры оснащены встроенным кодером.

Командный сценарий

Макрос, который может создать администратор для автоматического выполнения определенных действий, например, установки положения камеры PTZ или отправки сообщений электронной почты. Bosch Video Management System предоставляет для этого специальный набор команд. Командные сценарии подразделяются на клиентские и серверные. Клиентские сценарии используются на клиентских рабочих станциях для выполнения определенных действий, которые могут быть осуществлены на клиентской рабочей станции. Серверные сценарии автоматически запускаются событием, происшедшим в системе. Они получают аргументы события, например, дату и время. Командный сценарий может состоять из нескольких команд. Вы можете создать командный сценарий при помощи следующих языков составления сценариев: C#, VB.Net. Командные сценарии выполняются в ответ на события или тревожные сигналы автоматически в соответствии с расписанием, вручную из логического дерева или вручную при помощи значков или карт.

Контрольное изображение

Контрольное изображение постоянно сравнивается с текущим видеоизображением. Если текущее видеоизображение в отмеченных

областях отличается от контрольного изображения, включается сигнал тревоги. Это позволяет обнаружить попытки несанкционированного доступа, которые иначе не были бы обнаружены (например, при повороте камеры).

Логический номер

Логический номер представляет собой уникальный идентификатор, присваиваемый каждому устройству системы для облегчения его идентификации. Логические номера уникальны только в пределах определенного типа устройств. Примером типичного использования логических номеров являются командные сценарии.

Логическое дерево

Дерево с настроенной структурой всех устройств. Логическое дерево используется клиентом оператора для выбора камер и других устройств. Полное логическое дерево настраивается в клиенте настроек (на странице Карты и структура) и приспосабливается для каждой группы пользователей (на странице Пользовательские группы).

Магистральная линия

Аналоговые выходы или аналоговый матричный коммутатор, подключенный к устройству кодирования. Таким образом, матричные источники видеосигнала могут использоваться в системе Bosch Video Management System.

многопутевой ввод-вывод

Метод хранения на компьютере, предполагающий указание множества физических путей, по которым сервер данных подключается к целевому объекту хранилища (с использованием различных контроллеров, шин, коммутаторов и т.п) в качестве решения для отработки отказа и распределения нагрузки (обеспечивает резервирование и эффективность).

Многопутевой ввод-вывод

Использование метода многопутевого хранения на компьютере.

Мониторинг сети

Измерение относящихся к сети значений и соотнесение этих значений с настраиваемыми пороговыми значениями.

Немедленное воспроизведение

Воспроизведение записанного изображения с выбранной камеры в области изображений на экране реального времени. Можно настроить время начала воспроизведения (указать количество секунд в прошлом, или время обратной перемотки).

области

Область — это термин, используемый при работе с камерами ONVIF. Это параметр используется для проверки устройства ONVIF. Обычно параметр содержит URI следующим образом: onvif: / / www.onvif.org/<path>. Параметр < путь > может быть, например, video_encoder или audio_encoder. Одно устройство ONVIF может иметь несколько областей. Этот URI обозначает область задач устройства.

область

Группа устройств обнаружения, подключенных к системе безопасности.

Область изображений

Используется для отображения с одной камеры видео в режиме реального времени или в записи, карты объекта, документа, последовательности, группы мониторов, внешнего приложения или окна просмотра карт.

Область интереса

Область интереса. Область интереса предназначена для сохранения пропускной способности сети при масштабировании участка изображения с камеры с помощью фиксированной камеры HD. Этот участок ведет себя, как камера PTZ.

обход/отмена обхода

Режим обхода устройства означает, что все возможные тревоги будут проигнорированы, как правило, на время каких-либо смягчающих обстоятельств, таких как мероприятия по обслуживанию. Отмена обхода подразумевает прекращение игнорирования таких событий.

Окно изображений

Контейнер для областей изображений, расположенных в соответствии с узором областей изображений.

Окно просмотра карт

Область просмотра карты - это область экрана, используемая для отображения определенной части глобальной карты геолокации.

Окно тревожных сигналов

Окно изображений для отображения одной или нескольких областей тревожных сигналов.

Основной VRM

Синоним для VRM.

охранная панель управления

Универсальное имя для основного устройства в системе безопасности (системе защиты от взлома) производства Bosch. Клавиатуры, модули, детекторы и другие устройства подключаются к панели управления.

Панель области изображений

Панель инструментов области изображений.

Период переключения

Установленный промежуток времени, в течение которого камера отображается в окне изображений до отображения следующей камеры последовательности.

ПО Master Control Software

Программное обеспечение, используемое в качестве интерфейса между Bosch Video Management System и устройством Allegiant. Используется версия 2.8 или выше.

Пользовательская группа

Пользовательские группы используются для определения общих пользовательских атрибутов, например, разрешений, привилегий и приоритетов PTZ. Когда пользователь становится членом пользовательской группы, он автоматически наследует все атрибуты группы.

Порт

1) На компьютерах и устройствах телекоммуникации порт обычно представляет собой определенное место для физического подключения к другому устройству, обычно посредством гнезда и вилки. Обычно персональный компьютер имеет один или несколько последовательных портов и один параллельный порт. 2) В программировании порт представляет собой "логическое место соединения" и в частности, при использовании Интернет-протокола TCP/IP, способ, который использует клиентская программа для указания на определенную серверную программу на компьютере или в сети. Приложения высокого уровня, использующие TCP/IP, как веб-протокол, протокол передачи гипертекста, имеют порты с заранее назначенными номерами. Они известны как "известные порты", которые были назначены Комитетом по цифровым адресам в Интернете (IANA). Другим приложениям номер порта присваивается динамически при каждом соединении. Когда происходит первоначальный запуск серверной программы, говорят, что она привязывается к назначенному номеру порта. Когда клиентская программа имеет намерение использовать этот сервер, она также должна привязываться к назначенному порту. Номера портов находятся в диапазоне от 0 до 65535. Порты от 1 до 1023 зарезервированы для привилегированных служб. Для службы HTTP порт 80 определен как стандартный и может не указываться в URL-адресе.

Просмотр сервера

Способ доступа для пользователя Configuration Client или Operator Client, чтобы последовательно подключиться к нескольким системным точкам доступа. Системными точками доступа могут быть Management Server или Enterprise Management Server.

Рабочая станция

В среде BVMS: выделенный компьютер, на котором установлен модуль Operator Client. Этот компьютер настроен как рабочая станция в Configuration Client, чтобы включить определенные функции.

Рабочая станция Operator Client

Компьютер в окружении Bosch Video Management System для просмотра изображений в реальном времени и записанных изображений, а также для

выполнения конфигурационных действий. Приложение Operator Client установлено на этом компьютере.

Развертка изображений

Использование программного обеспечения по конвертации круглого изображения из объектива типа «рыбий глаз» с радиальной дисторсией в прямоугольное изображение для нормального просмотра (устранение искажений является коррекцией дисторсии).

Разрешение видеоканала

Количество пикселов по горизонтали и вертикали, передаваемых с видеосигналом. PAL: 1CIF = 352 x 288 2CIF = 704 x 288 4CIF = 704 x 576 QCIF = 176 x 144 NTSC 1CIF = 352 x 240 2CIF = 704 x 240 4CIF = 704 x480 QCIF = 176 x120 HD 720p = закодировано 1280 x 720 1080p = закодировано 1920 x 1080

Расписание задач

Используется для планирования событий, которые могут произойти в системе Bosch Video Management System, например, выполнение командного сценария. На странице События вы можете назначить событиям расписание задач. Для планирования событий используется также расписание записей. В стандартном расписании задач вы настраиваете временные промежутки для каждого дня недели, для выходных дней и дней исключений. В повторяющемся расписании задач вы можете настроить повторяющиеся промежутки времени. Они могут повторяться каждый день, каждую неделю, каждый месяц или каждый год.

Расписание записей

Используется для планирования записей и некоторых событий, например, запуска резервного копирования или ограничения входа в систему. В расписании записей не может быть пробелов или накладок. Это расписание определяет также качество записи видеоизображений.

Режим реального времени

Функция Operator Client. Используется для просмотра видео в режиме реального времени.

Резервный VRM

Программное обеспечение в среде BVMS. Берет на себя функцию назначенного основного диспетчера видеозаписи или вторичного диспетчера видеозаписи в случае выхода из строя.

Сервер управления

Управление устройствами сервера BVMS.

Сервер управления Enterprise

Enterprise Management Server — это сервер BVMS Management Server, на котором находится конфигурация групп Enterprise User Group. Необходима одна или несколько групп Enterprise User Group, относящихся к одному или нескольким компьютерам. Роли Enterprise Management Server и Management Server могут быть объединены в одной конфигурации.

Серия устройств

Кодеры Bosch / IP-камеры могут принадлежать к одному из следующих семейств устройств. Семейство устройств 1, семейство устройств 2, семейство устройств 3. Устройства семейства 1 могут записывать только поток 1. Устройства семейства 2 могут записывать поток 1 или поток 2. Устройства семейства 3 могут записывать поток 1, поток 2 или только I-кадр.

Сетевой видеорегистратор

Сетевой видеорегистратор Bosch; компьютер в окружении Bosch Video Management System, сохраняющий видео- и аудиоданные или выступающий в качестве резервного сетевого видеорегистратора. Этот видеорегистратор отличается от VIDOS NVR, который может быть интегрирован в Bosch Video Management System.

Система Enterprise

Enterprise System — это компонент системы Bosch Video Management System, позволяющий пользователю Operator Client одновременно получать доступ к нескольким компьютерам Management Server.

Скимминг

Взлом устройства чтения кредитных карточек. Скиммер считывает данные карточки, хранящиеся на магнитной полосе, когда владелец карточки не подозревает об этом.

Сложное событие

Комбинация нескольких событий. Комбинация использует логические выражения, т.е., AND и OR. Вы можете комбинировать только изменения состояний, например, изменение состояния подключения на отключенное или активацию расписания.

Событие

Обстоятельство или состояние, связанное с тревожным сигналом и/или действием. События могут генерироваться различными источниками, например, камерами, архивами, каталогами, цифровыми входами и т.п. Они могут включать в себя запускающие запись состояния, состояния потери сигнала, сообщения о переполнении дискового пространства, входы пользователя в систему, пусковые механизмы цифровых входов и т.п.

Список тревожных сигналов

Окно в системе Bosch Video Management System, которое используется для отображения списка активных тревожных сигналов.

Текстовые данные

Данные POS или ATM, например, дата и время или номер банковского счета, которые хранятся вместе с соответствующими видеоданными и предоставляют дополнительную информацию.

точка

Устройство обнаружения, подключенное к системе безопасности. Точки отображаются на клавиатуре по отдельности и с пользовательским текстом. Текст может описывать одну дверь, датчик движения, дымовой извещатель или защищенную область, например "Верхний этаж" или "Гараж".

Тревога

Событие, сконфигурированное для создания тревожного сигнала. Это событие представляет собой определенную ситуацию (обнаружение движения, звонок в дверь, потеря сигнала и т.п.), которая требует немедленного реагирования. Тревожный сигнал может отображать видеоизображение в реальном времени, записанное видеоизображение, план действий, веб-страницу или карту.

Устранение искажений в камере

Устранение искажений, выполняемое в самой камере.

Учетная запись Enterprise

Enterprise Account — это авторизация, позволяющая пользователю клиента Operator Client подключаться к устройствам Management Server, входящим в систему Enterprise. В Enterprise Account настраиваются все разрешения для устройств этого сервера Management Server. Клиент Operator Client может одновременно подключиться ко всем компьютерам Management Server, являющимся частью этой Enterprise System. Этот доступ управляется членством в Enterprise User Group и разрешениями на использование устройств, настроенными в Enterprise Account для этого сервера Management Server.

Файлы карт

BVMS поддерживает карты следующих форматов: PNG и JPG.

Файлы карт объектов

BVMS поддерживает следующие форматы карт объектов: PNG, JPG, PDF и DWF.

Функция внутренней связи

Используется для разговора через громкоговорители кодера. Кодер должен иметь аудиовход и аудиовыход. Функция внутренней связи предоставляется группам пользователей.

Цифровой видеорегистратор

Цифровой видеорегистратор

Шлюз видеопотока (VSG)

Виртуальное устройство, позволяющее выполнить интеграцию камер Bosch, камер ONVIF, камер JPEG, кодеров RTSP.

Эмуляция CCL

Для управления матрицей Allegiant используется командный язык консоли. Можно использовать этот набор команд для переключения IP-камеры или кодера BVMS на IP-декодер BVMS. Невозможно осуществлять прямое управление аналоговыми камерами или самой матрицей Allegiant.

Указатель

Символы

Building solutions for a better life.

202311150955