Руководство Bosch по безопасности IP-видео и данных

BOSCH

ru

Содержание

1 Введение

Несмотря на то, что в современных условиях у многих организаций введены определенные процедуры и правила в отношении кибербезопасности, стандарты в разных организациях могут отличаться по таким признакам, как размер, область действия и отрасль.
В феврале 2014 г. Национальный институт стандартов и технологии (НИСТ) ввел Общие принципы кибербезопасности. Эти принципы основаны на приказе №13636 и были разработаны с использованием существующих стандартов, рекомендаций и передовых методик. Они нацелены на снижение киберрисков в отношении важнейших инфраструктур, их сетевых устройств и данных. Эти принципы разработаны с целью помочь организациям понять как внешние, так и внутренние риски кибербезопасности и применимы к организациям любого размера, от категории уровня 1 (частичный) до уровня 4 (адаптивный).

Этот справочный документ предназначен для помощи интеграторам в усилении систем IP-видеонаблюдения от Bosch с целью достижения более полного соответствия существующим правилам и процедурам сетевой безопасности их клиентов.
В настоящем руководстве рассматриваются следующие вопросы:

- Важнейшая информация о функциях и основных характеристиках IP-видеоустройств Bosch
- Конкретные функции, которые можно изменять или отключать
- Конкретные функции, которые можно активировать и использовать
- Передовые методики, относящиеся к видеосистемам и безопасности

Основное внимание в настоящем руководстве уделено использованию Bosch Configuration Manager для выполнения указанных конфигураций. В большинстве случаев все конфигурации можно выполнить с использованием системы Bosch Video Management System, клиента Configuration Client, Bosch Configuration Manager и встроенного веб-интерфейса видеоустройства.

2 IP-видеоустройства Bosch

IP-видеоустройства становятся все более распространенными в современной сетевой среде, и, как и при наличии любых других IP-устройств в сети, при использовании этих устройств IP-администраторы и сотрудники службы безопасности имеют право знать всю полноту набора функций и возможностей устройства.

При использовании IP-видеоустройств Bosch первым уровнем вашей защиты являются сами устройства. Кодеры и камеры Bosch производятся в контролируемых и безопасных условиях и проходят постоянные проверки. Запись программы в устройства может производиться только с помощью загрузки корректной микропрограммы, разработанной специально для серии оборудования и набора микросхем.

Большинство IP-видеоустройств Bosch поставляется со встроенным чипом безопасности, обеспечивающим функции, аналогичные функциям криптомикропроцессора и так называемого Trusted Platform Module, сокращенно модуля TPM. Этот чип выступает в качестве сейфа для важнейших данных; он защищает сертификаты, пароли, лицензии и т.д. от несанкционированного доступа, даже если камера подвергается физическому вскрытию с целью получения доступа.

IP-видеоустройства Bosch прошли более чем тридцать тысяч (30000) проверок на уязвимость и возможность проникновения, проведенных независимыми поставщиками продуктов безопасности. На сегодняшний день не произошло еще ни одной успешной кибератаки на должным образом защищенное устройство.

3 Назначение IP-адресов

Все IP-видеоустройства Bosch в настоящий момент поставляются с заводскими настройками, позволяющими назначить IP-адрес DHCP.
При отсутствии доступного сервера DHCP в активной сети, в которой размещено устройство, устройство — если на нем установлена микропрограмма версии 6.32 или более поздняя — автоматически назначит адрес локального канала из диапазона 169.254.1.0 — 169.254.254.255, или 169.254.0.0/16.
В случае более ранних версий микропрограммы оно самостоятельно назначит себе IP-адрес по умолчанию 192.168.0.1.
Существует несколько инструментов назначения IP-адресов IP-видеоустройствам Bosch, в том числе:

- Программа IP Helper
- Bosch Configuration Manager
- Bosch Video Management System Configuration Client
- Bosch Video Management System Configuration Wizard

Все инструменты ПО поддерживают функцию назначения единого статического адреса IPv4, а также диапазона адресов IPv4 нескольким устройствам одновременно. Это включает маску подсети и назначение адресов шлюзам по умолчанию.
Все адреса IPv4 и значения маски подсети должны быть введены в так называемом «десятичном представлении с точками».

Замечания!
Совет о безопасности данных № 1
Одной из первостепенных мер по ограничению возможностей внешних кибератак на систему, осуществляемых несанкционированными локально подключенными сетевыми устройствами, является ограничение числа доступных неиспользуемых IP-адресов. Это можно сделать с помощью IPAM, или Управления IP-адресами (**IP A**ddress **M**anagement), совместно с разбитием на подсети диапазона IP-адресов, который будет использоваться.

Разбитие на подсети — это процесс заимствования битов из хост-части IP-адреса с целью разбития большой сети на несколько малых. Чем больше таких битов заимствуется, тем больше сетей можно создать, но тем меньше адресов узлов каждая из сетей будет поддерживать.

Суффикс	Узлы	CIDR	Заимствованные	Двоичные
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111**0**
.252	4	/30	2	.111111**00**
.248	8	/29	3	.11111**000**
.240	16	/28	4	.1111**0000**
.224	32	/27	5	.111**00000**
.192	64	/26	6	.11**000000**
.128	128	/25	7	.1**0000000**

С 1993 г. Рабочая группа проектирования Интернета (IETF) ввела новую концепцию размещения блоков адресов IPv4 способом более гибким, чем тот, что использовался ранее в архитектуре назначения адресов с использованием классов. Новый метод называется «Бесклассовой междоменной маршрутизацией» (CIDR) и используется также с адресами IPv6.

Классовые сети IPv4 делятся на классы A, B и C с числом сетевых битов 8, 16 и 24 соответственно, и класс D, используемый для групповой адресации.

Пример:
Чтобы привести простой для понимания пример, мы используем сценарий с адресом класса C. Маска подсети по умолчанию для адреса класса C — 255.255.255.0. В техническом отношении, эта маска не была разбита на подсети, так что весь последний октет доступен для действительной адресации узлов. Так как мы заимствуем биты с адреса узла, для нас доступны следующие варианты маски в последнем октете:
.128, .192, .224, .240, .248 и .252.

При использовании маски подсети 255.255.255.240 (4 бита) мы создаем 16 меньших сетей, поддерживающих 14 адресов узлов на подсеть.
- Идентификатор подсети 0:
  диапазон адресов узлов от 192.168.1.1 до 192.168.1.14. Широковещательный адрес 192.168.1.15
- Идентификатор подсети 16:
  диапазон адресов узлов от 192.168.1.17 до 192.168.1.30. Широковещательный адрес 192.168.1.31
- Идентификаторы подсети: 32, 64, 96, и т. п.

Для более крупных сетей может потребоваться следующий по размеру класс сети B или определение соответствующего блока CIDR.

Пример:
Перед развертыванием сети видеонаблюдения необходимо выполнить простой расчет необходимого количества IP-устройств в сети, чтобы обеспечить возможность для будущего расширения:
- 20 рабочих станций для видео
- 1 центральный сервер
- 1 сервер VRM
- 15 массивов хранения данных iSCSI
- 305 IP-камер

Итого = необходимо 342 IP-адреса

Учитывая рассчитанное количество IP-адресов, равное 342, для обеспечения такого количества адресов нам по минимуму требуется схема IP-адресов класса B. Использование маски подсети класса B по умолчанию 255.255.0.0 позволяет использовать в сети 65534 доступных IP-адреса.

Кроме того, сети можно планировать с помощью блока CIDR, где 23 бита используются как префикс, обеспечивая адресное пространство на 512 адресов, соответственно, 510 узлов.

Разбивая большую сеть на более мелкие составляющие, то есть на подсети, или определяя блок CIDR, вы можете снизить риск.

Пример:

	По умолчанию	**Разбито на подсети**
Диапазон IP-адресов	172.16.0.0 – 172.16.255.255	172.16.8.0 – 172.16.9.255
Маска подсети	255.255.0.0	255.255.254.0
Значение CIDR	172.16.0.0/16	172.16.8.0/23
Количество подсетей	1	128
Количество узлов	65.534	510
Избыточные адреса	65.192	168

3.1 Управление DHCP

IPAM может использовать DHCP в качестве мощного инструмента контроля и использования IP-адресов в вашей среде. DHCP можно настроить для использования конкретного набора IP-адресов. Его также можно настроить для исключения конкретного диапазона адресов.

Если вы используете DHCP, рекомендуется, при размещении видеоустройств, настроить бессрочное резервирование адреса на основе MAC-адреса каждого устройства.

Замечания!

Совет о безопасности данных №2.

Даже до использования управления IP-адресами для отслеживания использования IP-адресов, передовой методикой в управлении сетями является ограничение доступа к сети через безопасность портов на граничных коммутаторах, например, только конкретный MAC-адрес может получить доступ через конкретный порт.

4 Учетные записи и пароли пользователей

Все IP-видеоустройства Bosch поставляются с тремя встроенными учетными записями пользователя:

– **live (режим реального времени)**
: эта стандартная учетная запись пользователя обеспечивает доступ к видеоизображению в режиме реального времени.
– **user (пользователь)**
: эта расширенная учетная запись обеспечивает доступ к видео в режиме реального времени и видеозаписям, а также к такому управлению камерой, как управление PTZ. Данная учетная запись не предусматривает доступа к параметрам конфигурации.
– **service (служебная)**
: эта учетная запись администратора обеспечивает доступ ко всем меню устройства и ко всем параметрам конфигурации.

По умолчанию ни одна из учетных записей не имеет заданного пароля. Присвоение паролей является важнейшим этапом процесса защиты любого сетевого устройства. Настоятельно рекомендуется задать пароли для всех установленных сетевых видеоустройств.

Замечания!
В версии микропрограммы 6.30 управление пользователями было расширенно для большей гибкости и позволяет создавать других пользователей с именами пользователя и паролями. Бывшие уровни учетных записей теперь представляют уровни групп пользователей.
В версии микропрограммы 6.32 были введены более строгие требования к паролям (подробные сведения см. на странице *Веб-страница устройства, Страница 11*).

4.1 Применение паролей

Существует несколько способов назначения пароля в зависимости от размера системы видеонаблюдения и используемого ПО. В малых системах, состоящих из нескольких камер, пароли можно задать с использованием веб-страницы устройства или Bosch Configuration Manager, так как в нем удобно сочетаются функции одновременной конфигурации нескольких устройств и мастера конфигурации.

Замечания!
Совет о безопасности данных №3
Как уже было сказано, пароли являются важнейшим элементом защиты данных от потенциальных кибератак. Это относится ко всем устройствам во всей вашей инфраструктуре безопасности. Большинство организаций уже имеют действующие строгие правила в отношении паролей, но если вы работаете с новой системой, не имея таких правил, рекомендуем вам ознакомиться с общепринятыми требованиями к защитным паролям:
— пароли должны быть от 8 до 12 символов длиной.
— пароли должны содержать буквы как верхнего, так и нижнего регистра.
— пароли должны содержать как минимум один специальный символ.
— пароли должны содержать как минимум одну цифру.

Пример:
Использование фразы «to be or not to be» и наших основных правил для создания надежного пароля.

– 2be0rnOt!t0Be

Замечания!
Существует ряд ограничений на использование в паролях таких специальных символов, как «@», «&», «<», «>», «:», в связи с их предписанным значением в XML и других языках разметки. Несмотря на то, что веб-интерфейс пропустит такие символы, другое ПО управления и конфигурирования может отказаться их принимать.

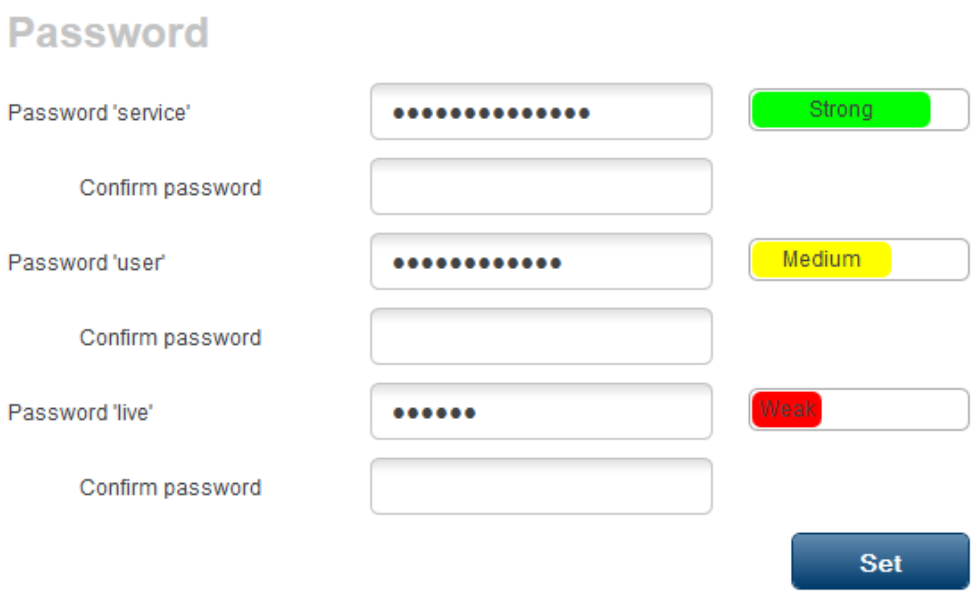
4.2 Веб-страница устройства

1. На веб-странице устройства перейдите на страницу **Конфигурация**.
2. Выберите меню общих настроек **Общие** и подменю **Управление пользователями** (Примечание: до версии микропрограммы 6.30 подменю **Управление пользователями** называлось **Пароль**).

При первом переходе на веб-страницу камеры пользователю предлагается назначить пароль для обеспечения минимальной защиты.
Это предложение будет отображаться при каждом новом переходе на веб-страницы камеры до тех пор, пока пароль не будет задан. Нажатие кнопки **OK** ведет к автоматическому открытию меню **Управление пользователями**.

В версии микропрограммы 6.30 есть возможность установки флажка **Не показывать...**. Эта возможность была исключена в версии микропрограммы 6.32 в целях избежания пробелов в безопасности.

1. Выберите меню **Управление пользователями** и введите и подтвердите пароли для каждой из трех учетных записей.
   Обратите внимание:
   – Сначала необходимо назначить пароли для наиболее высокого уровня доступа (**Пароль 'service'**).
   – В версии микропрограммы 6.20 и более поздних новый индикатор надежности пароля подскажет, насколько потенциально надежен введенный вами пароль. Это вспомогательный инструмент и он не гарантирует абсолютного соответствия введенного вами пароля требованиям безопасности конкретной установки.
2. Нажмите **Установить** для применения и сохранения изменений.



Страница **Управление пользователями** в версии микропрограммы 6.30 обеспечивает большую гибкость для создания пользователей с произвольными именами и собственными паролями. Бывшие уровни учетных записей теперь представляют уровни групп пользователей.

Стандартные пользователи продолжают существовать, используя пароли, заданные с помощью более ранней версии микропрограммы; их невозможно удалить, а также невозможно изменить уровень их группы.

Пароли можно задавать или изменять нажатием или  .
Пока все учетные записи не будут защищены паролями, будет отображаться предупреждающее сообщение.

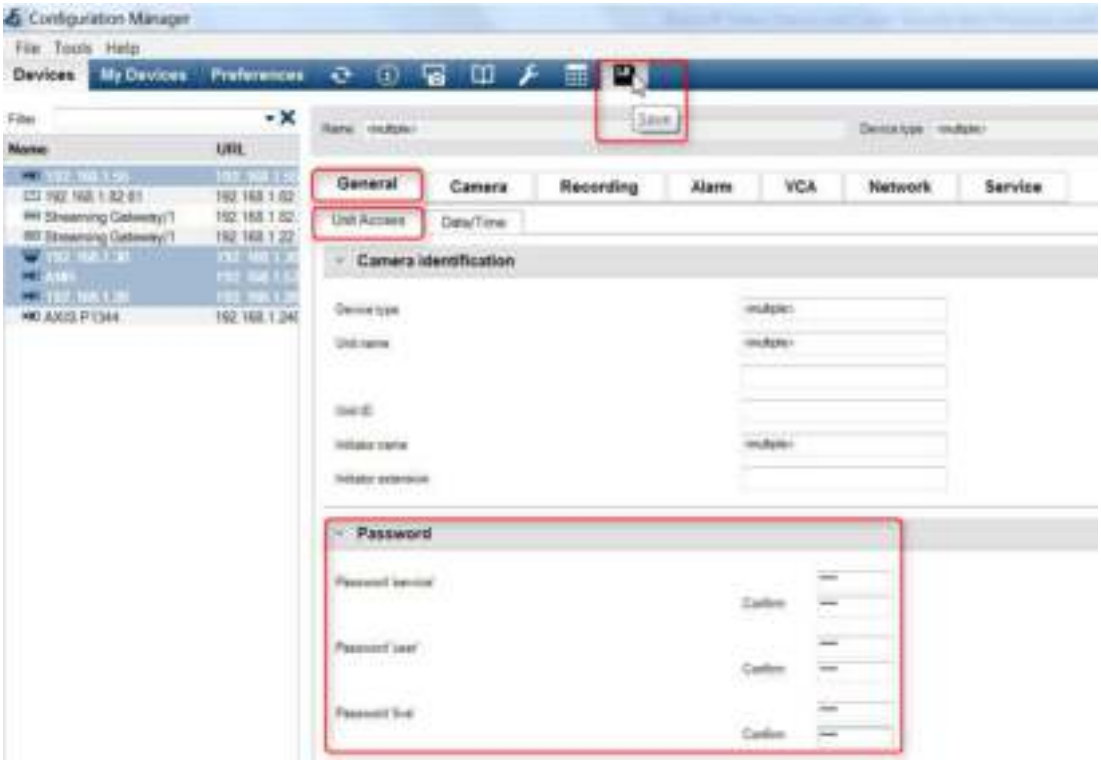
1. Чтобы добавить нового пользователя, нажмите **Добавить**.
   Отобразится всплывающее окно.
2. Введите новые данные и назначьте группу пользователя.
3. Нажмите **Установить** для сохранения изменений.

Замечания!
В версии микропрограммы 6.32 также были введены более строгие требования к паролям.
Теперь пароли должны быть как минимум 8 символов длиной.

4.3 Configuration Manager

При использовании Bosch Configuration Manager пароли можно с легкостью задавать для отдельных или нескольких устройств одновременно.

1. В Configuration Manager выберите одно или несколько устройств.
2. Выберите вкладку **Общие**, затем выберите **Доступ к устройству**.
3. В меню **Пароль** введите и подтвердите желаемый пароль для каждой из трех учетных записей (**Пароль "service"**, **Пароль "user"** и **Пароль "live"**).
4. Нажмите  для применения и сохранения изменений.



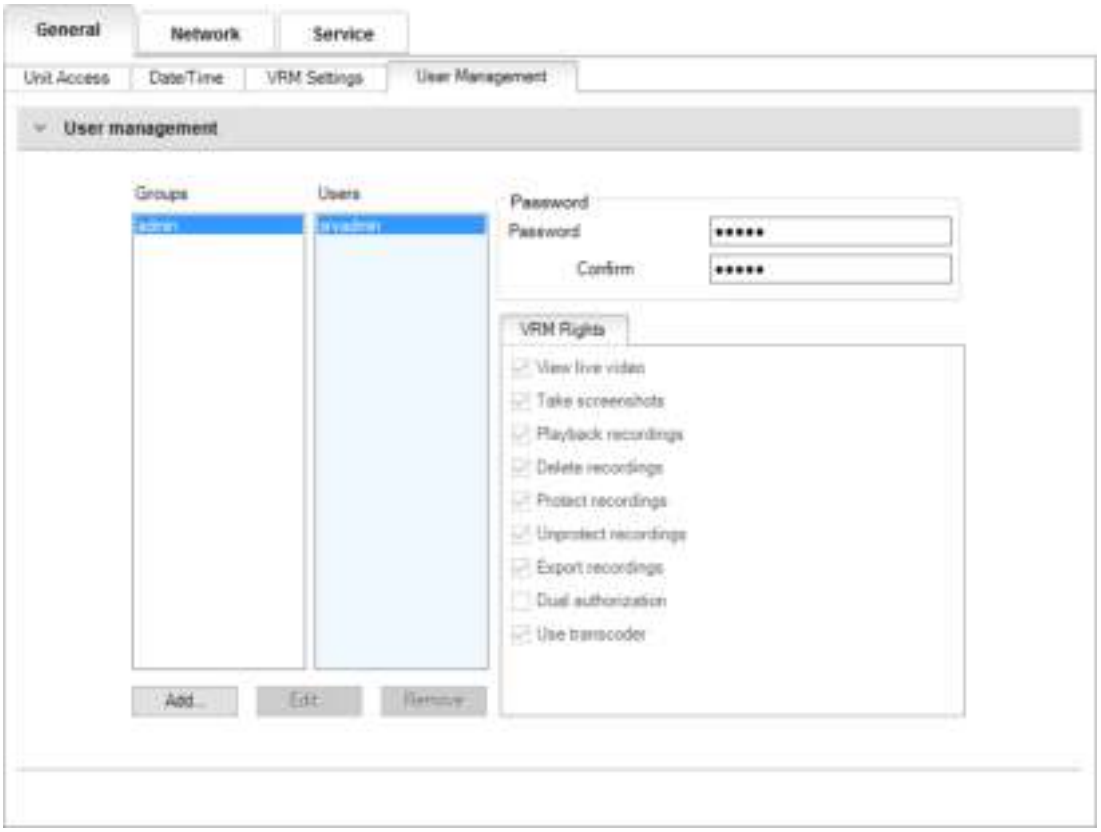
Для более крупных установок, управляемых Bosch Video Management System или Video Recording Manager, установленным на записывающей устройстве, можно задать общие пароли для всех IP-видеоустройств, добавленных к системе. Это обеспечивает простоту управления и стандартный уровень безопасности по всей сети видеосистемы.

4.4 DIVAR IP 2000 / DIVAR IP 5000

Устройства записи DIVAR IP оборудованы простым в использовании Configuration Wizard. Назначение общесистемного пароля администратора является обязательным при конфигурации системы. Пароль задается для учетной записи service всех IP-видеокамер, добавленных к системе. Возможности добавлять пароль учетной записи user также обеспечивается мастером Configuration Wizard, однако это не обязательно. Индикатор надежности пароля использует алгоритм, аналогичный алгоритму на веб-страницах камер.

4.5 Одиночная установка VRM

BoschVideo Recording Manager обеспечивает управление пользователями для еще большей гибкости и безопасности.
По умолчанию ни одной из учетных записей не присвоен пароль. Присвоение паролей является важнейшим этапом процесса защиты любого сетевого устройства. Настоятельно рекомендуется назначить пароли всем установленным в сети видеоустройствам.
То же относится к пользователям Video Recording Manager.



Кроме того, членам группы пользователей может быть предоставлен доступ к конкретным камерам и привилегиям. Таким образом обеспечивается подробное управление правами каждого пользователя.

4.6 Bosch Video Management System

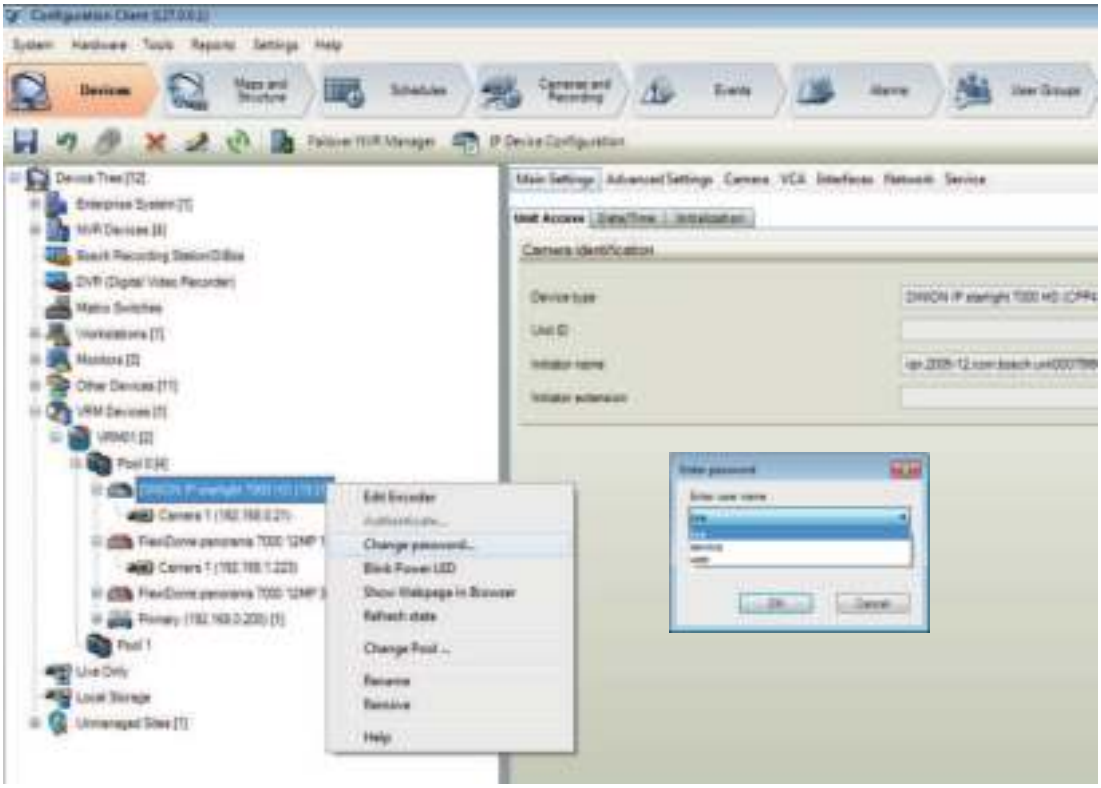
4.6.1 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: защита устройств с помощью пароля

Камеры и кодеры, управляемые Bosch Video Management System, могут быть защищены от несанкционированного доступа с помощью пароля.

Пароли для встроенных учетных записей пользователей кодеров / камер можно задать с помощью Configuration Client Bosch Video Management System.

Для того, чтобы задать пароль для встроенных учетных записей пользователей, в Configuration Client Bosch Video Management System:

1. в дереве устройств выберите желаемый кодер.
2. нажмите на кодер правой кнопкой и выберите **Изменить пароль....**
3. Введите пароль для трех встроенных учетных записей live, user и service.



4.6.2 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: защита паролем по умолчанию

Версии Bosch Video Management System 5.0 и более поздние обеспечивают возможность присвоения общих паролей на всех устройствах в видеосистемах объемом до 2000 IP-камер. Эта функция доступна в Configuration Wizard Bosch Video Management System при работе с DIVAR IP 3000 или устройствами записи DIVAR IP 7000, или через Configuration Client Bosch Video Management System в любой системе.

Для доступа к меню общих паролей в Configuration Client Bosch Video Management System:

1. в меню **Аппаратное обеспечение** выберите **Защита устройств паролем по умолчанию...**
2. В поле **Всеобщий пароль по умолч.** введите пароль и выберите **Принудительная защита паролем при активации**

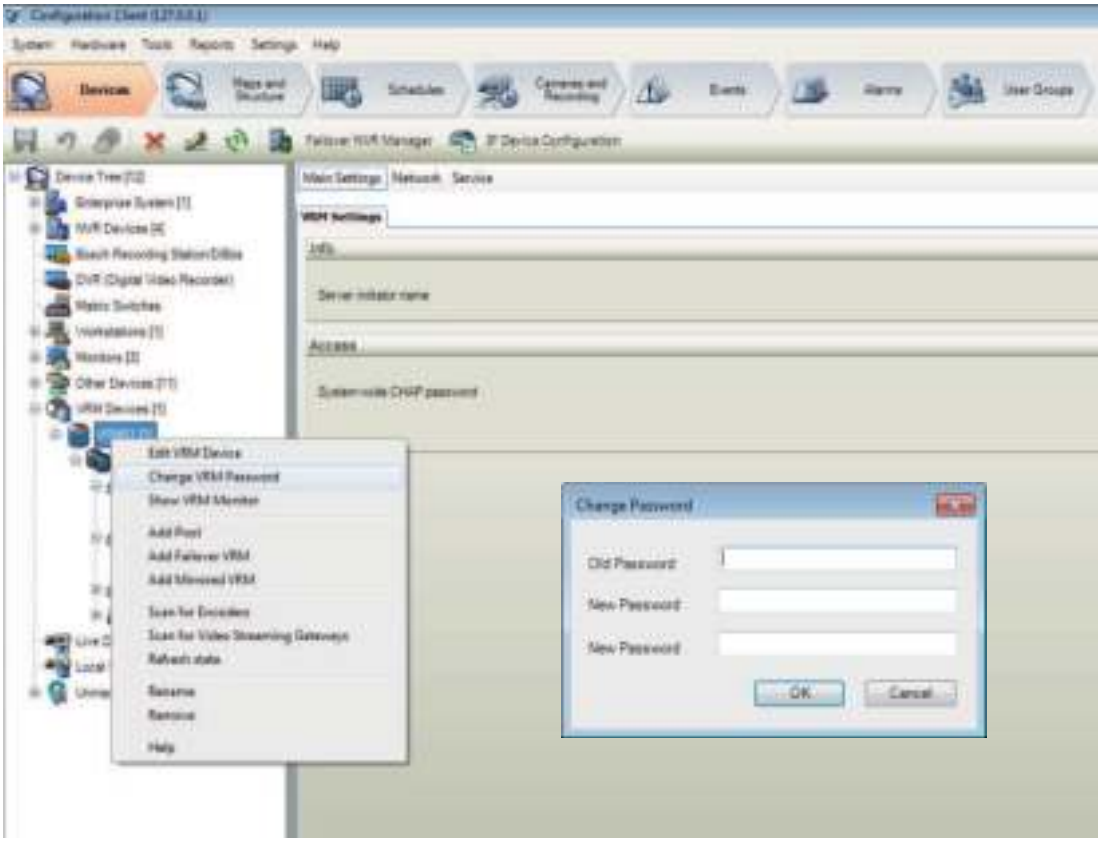
После сохранения и активации изменений в системе введенный пароль будет задан для учетных записей live, user и service на всех устройствах, включая учетную запись администратора в Video Recording Manager.

Замечания!
Если устройства уже имеют заданные пароли для каких-либо учетных записей, они не будут изменены.
Например, если пароль задан для учетной записи service, но не для live и user, общий пароль будет задан только для учетных записей live и user.

4.6.3 Конфигурация Bosch VMS и параметры VRM

По умолчанию Bosch Video Management System использует встроенную учетную запись администратора **srvadmin** для подключения к Video Recording Manager с защитой паролем. Во избежание несанкционированного доступа к Video Recording Manager учетная запись администратора **srvadmin** защищена сложным паролем.
Чтобы изменить пароль учетной записи **srvadmin** , в Configuration Client Bosch Video Management System:

1. в дереве устройств выберите устройство VRM.
2. Нажмите правой кнопкой устройство VRM и выберите **Изменить пароль VRM.** Отобразится диалоговое окно **Изменить пароль...**.
3. Введите новый пароль для учетной записи **srvadmin** и нажмите **OK**.

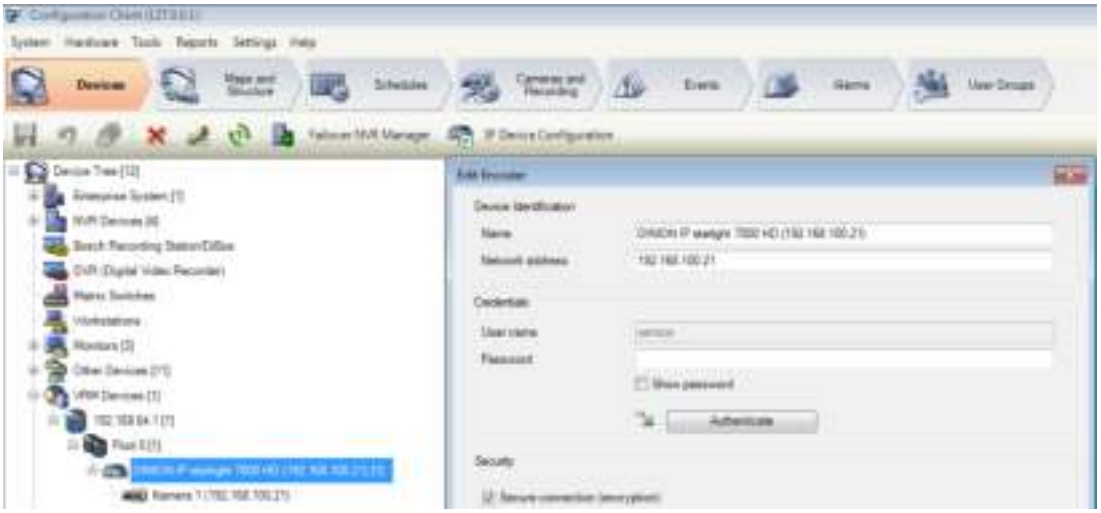


4.6.4 Bosch VMS / DIVAR IP 3000 / DIVAR IP 7000: шифрованная связь с камерами

Начиная с версии Bosch Video Management System 7.0, видеоданные в режиме реального времени и связь между камерой и Operator Client, Configuration Client, Management Server и Video Recording Manager Bosch Video Management System можно зашифровать.
После активации безопасного подключения в диалоговом окне **Изменить кодер**, сервер Bosch Video Management System, Operator Client и Video Recording Manager будут использовать безопасное подключение HTTPS для подключения камеры или кодера.
Внутренняя строка подключения Bosch Video Management System изменится с rcpp://a.b.c.d (обычное RCP + подключение к порту 1756) на https://a.b.c.d (HTTPS-подключение к порту 443).
Для устаревших устройств, не поддерживающих HTTPS, строка подключения останется неизменной (RCP +).

Если выбрана HTTPS-связь, будет использоваться связь HTTPS (TLS) для шифрования всей полезной нагрузки управления и видео через модуль шифрования устройства. При использовании TLS все управление передачей HTTPS и полезная нагрузка видео шифруется с помощью ключа шифрования AES до 256 бит длиной.
Для активации шифрованной связи в Configuration Client Bosch Video Management System:

1. в дереве устройств выберите желаемый кодер/камеру.
2. Правой кнопкой нажмите кодер/камеру и выберите **Изменить кодер**.
3. В диалоговом окне **Изменить кодер** активируйте **Безопасное соединение (шифрование).**
4. Сохраните и активируйте конфигурацию.



После активации безопасного подключения с кодером, другие протоколы можно деактивировать (см. *Общие настройки использования сетевых портов и передачи видеоданных, Страница 19*).

Замечания!
Bosch VMS поддерживает только порт HTTPS по умолчанию 443. Использование других портов не поддерживается.

5 Усиление защиты доступа к устройствам

Все IP-видеоустройства Bosch поставляются со встроенными многофункциональными веб-страницами. Веб-страницы каждого конкретного устройства поддерживают как видео в режиме реального времени, так и воспроизведение записанного видеоизображения, а также предлагают ряд определенных параметров конфигурации, которые могут быть недоступны через систему управления видео. Встроенные учетные записи выступают в качестве каналов доступа к разным разделам соответствующих веб-страниц. Несмотря на то, что доступ к веб-странице невозможно отключить с помощью самой веб-страницы (для этого можно использовать Configuration Manager), существует несколько способов скрыть присутствие устройства, ограничить доступ, а также управлять использованием видеопортов.

5.1 Общие настройки использования сетевых портов и передачи видеоданных

Все IP-видео устройства Bosch используют протокол дистанционного управления (+ RCP) для обнаружения, управления и связи. RCP + является запатентованным протоколом Bosch, использующим конкретные статические порты для обнаружения и связи с IP-видео устройствами Bosch – 1756, 1757 и 1758. При работе с Bosch Video Management System или другой сторонней системой управления видео со встроенными IP-видео устройствами Bosch через BoschVideoSDK перечисленные порты должны быть доступны в сети для корректной работы IP-видеоустройств.

Видеоизображение может транслироваться с устройств несколькими способами: UDP (динамический), HTTP (80) или HTTPS (443).
Использование портов HTTP и HTTPS может быть изменено (см. *HTTP, HTTPS и использование видеопортов, Страница 20*). Прежде чем вносить какие-либо изменения в порты, необходимо настроить требуемую форму связи с устройством. Меню Связь можно открыть с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Общие**, затем выберите **Доступ к устройству**.
3. Откройте часть страницы **Доступ к устройству**

4. В списке **Протокол** выберите желаемый протокол:

– RCP+
– HTTP (по умолчанию)
– HTTPS

При выборе связи через HTTPS, для связи между Configuration Manager и видеоустройствами будет использоваться HTTPS (TLS) для шифрования полезной нагрузки с помощью ключа шифрования AES до 256 битов длиной. Это бесплатная базовая функция. При использовании TLS все управление передачей и полезная нагрузка видео HTTPS шифруется через модуль шифрования устройства.

Замечания!
Шифрование предназначено специально для «тракта передачи». После получения видео программным или аппаратным декодером поток окончательно расшифровывается.

Замечания!
Совет о безопасности данных №4
При определении минимального уровня безопасности для доступа к устройствам с ПО клиента убедитесь, что все порты и протоколы, допускающие более низкий уровень доступа, выключены или деактивированы на устройствах.

5.1.1 HTTP, HTTPS и использование видеопортов

Использование портов HTTP и HTTPS на всех устройствах можно изменять или отключать. Шифрованная связь может быть активирована с помощью отключения порта RCP +, а также порта HTTP, что принудительно активирует шифрование для всех видов связи. При отключенном использовании портов HTTP HTTPS останется включенным и любые попытки отключить его окончатся неудачей.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Доступ к сети**.
3. Откройте часть страницы **Подробно**.

4. В части страницы **Подробно** измените порты браузера HTTP и HTTPS, а также порт RCP+, используя раскрывающийся список:
   - изменение порта браузера HTTP: 80 или порты от 10000 до 10100
   - изменение порта браузера HTTPS: 443 или порты от 10443 до 10543
   - RCP + порт 1756: **Вкл.** или **Выкл.**

Замечания!
В микропрограмме версии 6.1, если HTTP-порт деактивирован, и совершается попытка открытия веб-страницы устройства, запрос будет направлен на заданный в данный момент HTTPS-порт.
Функция перенаправления запроса отсутствует в версиях микропрограммы 6.20 и более поздних. Если HTTP-порт деактивирован, а HTTPS-порт был настроен для использования порта, отличного от 443, доступ к веб-страницам может быть получен только с помощью перехода по IP-адресу устройства и назначенному порту.

Пример:
https://192.168.1.21:10443. Любые попытки подключения к адресу по умолчанию окончатся неудачей.

5.1.2 Видео ПО и выбор порта

Изменение этих параметров также повлияет на то, какой порт используется для передачи видео при использовании ПО для управления видео в вашей сети LAN.

Если все IP-видеоустройства настроены на HTTP-порт 10000, например, и Bosch Video Management SystemOperator Client настроен для «туннелирования TCP», то все передачи видеоданных в сети будут осуществляться через HTTP-порт 10000.

Замечания!
Изменения параметров портов устройств должны соответствовать параметрам системы управления и ее компонентов, а также параметрам клиентов.

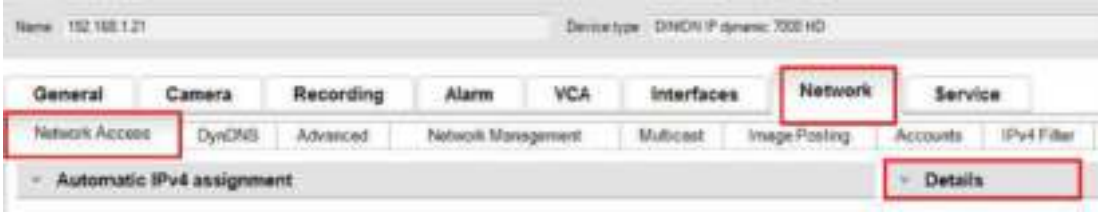
Замечания!
Совет о безопасности данных №5
В зависимости от сценария размещения и целей безопасности системы рекомендуемые методики могут отличаться. Отключение и перенаправление использования портов HTTP или HTTPSимеет свои преимущества. Изменение порта в любом протоколе исключает необходимость предоставления информации на средства сети, такие как NMAP (Network Mapper, бесплатный сканер безопасности). Приложения, такие как NMAP, обычно используются как средства диагностики для определения слабых мест какого-либо устройства в сети. Этот способ в сочетании с назначением надежного пароля повышает общий уровень безопасности системы.

5.1.3 Доступ Telnet

Telnet — протокол на уровне приложения, который обеспечивает связь с устройствами через виртуальный терминал для обслуживания и устранения неполадок. Все IP-видеоустройства Bosch поддерживают Telnet, и поддержка Telnet по умолчанию включена в версиях микропрограммы до 6,1x. Начиная с версии микропрограммы 6.20, порт Telnet отключен по умолчанию.

Замечания!
Совет о безопасности данных №6
С 2011 г. число кибератак с использованием протокола Telnet возросло. В современных условиях рекомендуется деактивация поддержки Telnet на всех устройствах до тех пор, пока протокол не потребуется для ремонта или устранения неполадок.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Доступ к сети**.
3. Откройте часть страницы **Подробно**.



4. В части страницы **Подробно** можно **включать** или **отключать Поддержка Telnet** с использованием раскрывающегося меню.

Замечания!

Совет о безопасности данных №7

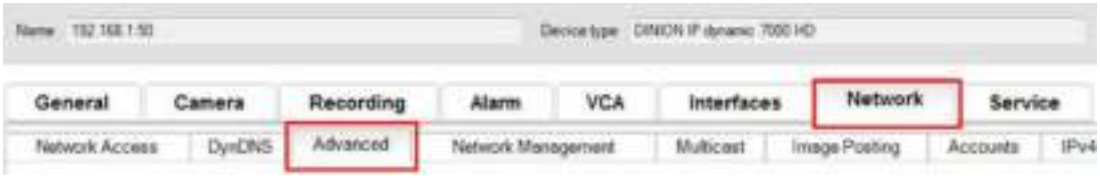
Начиная с версии микропрограмм 6.20 Telnet также поддерживается с помощью так называемых «веб-разъемов», которые используют безопасные подключения HTTPS. Веб-разъемы не используют стандартный порт Telnet и обеспечивают безопасный способ доступа к интерфейсу командной строки IP-устройства при необходимости.

5.1.4 Протокол RTSP: Real Time Streaming Protocol

Потоковая передача данных в реальном времени (RTSP) является основным видеокомпонентом, используемым протоколом ONVIFдля обеспечения потокового видео и управления устройствами для систем управления видео, соответствующих стандартам ONVIF. RTSP также используется различными сторонними видеоприложениями для базовых функций потоковой передачи, а в некоторых случаях может использоваться для устранения неполадок устройств и сети. Все IP-видеоустройства Bosch поддерживают потоковую передачу в помощью протокола RTSP.

Функциями RTSP можно легко управлять с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Дополнительно**



3. Откройте часть страницы **RTSP**.
4. В раскрывающемся меню **Порт RTSP** отключите или измените функции RTSP:
   - порт RTSP по умолчанию: 554
   - изменение порта RTSP: от 10554 до 10664

Замечания!

Совет о безопасности данных №8

В последнее время появляется все больше сообщений о кибератаках с использованием буферных атак с помощью переполнения стека RTSP. Эти атаки были нацелены на устройства конкретных поставщиков. Рекомендуемой методикой является отключение этого сервиса, если он не используется системой управления видео, соответствующей стандартам ONVIF, или для базовой потоковой передачи в режиме реального времени. Кроме того, если это позволяет принимающий клиент, связь RTSP может быть туннелирована с использованием подключения HTTPS, которое на данный момент является единственным способом передачи шифрованных данных RTSP.

Замечания!

Для получения дополнительных сведений о RTSP см. примечание о техническом обслуживании «Использование RTSP с VIP устройствами Bosch» в онлайн каталоге продуктов Bosch Security Systems по следующей ссылке:

http://resource.boschsecurity.com/documents/RTSP_VIP_Configuration_Note_enUS_9007200806939915.pdf

5.1.5 UPnP: функция Universal Plug and Play

IP-видеоустройства Bosch способны обеспечивать связь с устройствами сети с помощью функции **UPnP**. Эта функция в основном используется в малых системах с небольшим количеством камер, в которых камеры автоматически отображаются в каталоге сети ПК и могут быть с легкостью найдены. Но они также отображаются и для любого другого устройства в сети.

UPnP можно отключить с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Управление сетью**

3. Откройте часть страницы **UPnP**.
4. В раскрывающемся меню **UPnP** выберите **Отключить** для отключения **UPnP**.

Замечания!

Совет о безопасности данных №9

UPnP не следует использовать в крупных установках в связи с большим числом уведомлений о регистрации и потенциальным риском нежелательного доступа или атаки.

5.1.6 Многоадресная передача

Все IP-видео устройства Bosch способны обеспечивать как «Многоадресную передачу видео по запросу», так и «Многоадресную потоковую передачу видео». Если одноадресная передача видео основывается на адресате данных, многоадресная основывается на источнике, что может привести к возникновению проблем безопасности на уровне сети, таких как: управление групповым доступом, надежность центра группы и надежность роутера. При том, что конфигурация роутера не рассматривается в данном руководстве, существует решение в области безопасности, которое можно внедрить с самого IP-видеоустройства.

Правило TTL (time-to-live, время жизни) определяет, куда и как далеко многоадресный поток данных может перемещаться внутри сети, каждый переход при этом уменьшает его «время жизни» на одну единицу. При настройке IP-видеоустройства для многоадресного использования можно изменить TTL-пакет устройства.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Многоадресная передача**
3. Откройте часть страницы **TTL при многоадресной передаче**.
4. Измените настройки **TTL пакета** с использованием следующих значений TTL и ограничений областей:
   - значение TTL 0 = ограничено доступом к локальному узлу
   - значение TTL 1 = ограничено доступом к той же подсети
   - значение TTL 15 = ограничено доступом к тому же объекту
   - значение TTL 64 (по умолчанию) = ограничено доступом к той же области
   - значение TTL 127 = по всему миру
   - значение TTL 191 = по всему миру с ограниченной полосой пропускания
   - значение TTL 255 = неограниченные данные

Замечания!

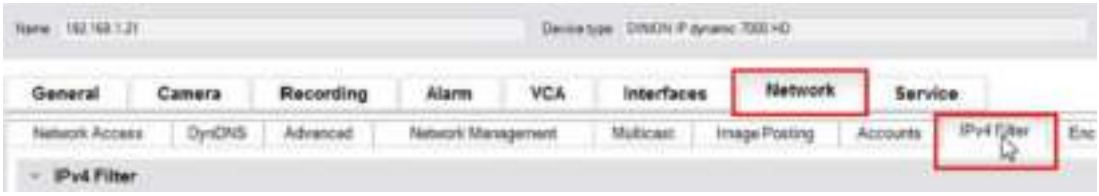
Совет о безопасности данных № 10

При работе с данными видеонаблюдения рекомендуется установить значение TLL равным 15, ограничив их перемещение тем же объектом. Если вы знаете точное максимальное число переходов, рекомендуется использовать его в качестве значения TTL.

5.1.7 Фильтр IPv4

Вы можете ограничить доступ к любому IP-видеоустройству Bosch с помощью функции фильтра IPv4. Фильтр IPv4 использует базовые функции создания подсети для задания до двух допустимых диапазонов IP-адресов. Как только диапазоны заданы, фильтр ограничивает доступ с любых IP-адресов, не входящих в данные диапазоны.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **IPv4-фильтр**.



Замечания!

Для успешной настройки данной функции необходимо иметь базовое представление о формировании подсетей или иметь доступ к калькулятору подсетей. Ввод неверных значений для данных параметров может ограничить доступ к самому устройству, и для восстановления доступа потребуется сброс до заводских настроек.

3. Для создания правила фильтра введите два значения:
   - Введите базовый IP-адрес, соответствующий правилу подсети, которое вы создаете.
     Базовый IP-адрес указывает, какую подсеть вы допускаете, и обязательно должен входить в желаемый диапазон.
   - Введите маску подсети, которая определяет IP-адреса, с которыми IP-видеоустройства будут поддерживать связь.

В следующем примере **IP-адрес 1** был введен как 192.168.1.20, а **Маска 1** как 255.255.255.240. Такие параметры ограничат доступ со всех устройств, попадающих в заданный IP-диапазон от 92.168.1.16 до 192.168.1.31.

При использовании функции**IPv4-фильтр** устройства могут сканироваться с помощью RCP +, но доступ к параметрам конфигурации и видео невозможен через клиентов, которые находятся вне диапазона разрешенных IP-адресов. Это включает доступ через веб-браузер.
Само IP-видеоустройство не обязательно должно быть расположено в допустимом диапазоне адресов.

Замечания!
Совет о безопасности данных №11
В зависимости от особенностей вашей системы использование функции **IPv4-фильтр** может снизить нежелательную видимость устройств в сети. При активации этой функции обязательно задокументируйте параметры для последующего использования.
Обратите внимание, что доступ к устройству все еще можно будет получить с помощью IPv6, поэтому использование фильтра IPv4 имеет смысл только в сетях, использующих исключительно IPv4.

5.1.8 SNMP

Протокол SNMP (Simple Network Management Protocol, протокол простого управления сетями) — это распространенный протокол для мониторинга рабочего состояния системы. Такая система наблюдения обычно имеет сервер централизованного управления, который собирает все данные совместимых компонентов и устройств системы.
SNMP обеспечивает два способа получения сведений о состоянии системы:

- Сервер управления сетью может запрашивать данные о состоянии устройства с помощью SNMP-запросов.
- Устройства могут активно сообщать серверу управления сетью о своем состоянии системы в случае ошибки или тревожных событий с помощью отправки SNMP-запросов на SNMP-сервер. Такие запросы должны быть настроены внутри устройства.

SNMP также позволяет настраивать некоторые переменные внутри устройств и компонентов.
Сведения, тип сообщений, поддерживаемый устройством, и тип запросов, которые оно может отправлять, содержатся в базе информации управления (Management Information Base), так называемом файле MIB — файле, поставляемом в комплекте с продуктом в целях простоты интеграции в систему сетевого мониторинга.

Существует три различные версии протокола SNMP:

- SNMP версии 1
  SNMP версии 1 (SNMPv1) – это первоначальное применение протокола SNMP. Он широко используется и стал фактически стандартным протоколом для контроля и

управления сетями.
Но SNMPv1 оказался под угрозой в связи с отсутствием функций безопасности. Он использует только "*строки сообщества*"в качестве паролей, которые передаются открытым текстом.
Таким образом, SNMPv1 следует использовать только тогда, когда есть гарантия, что сеть физически защищена от несанкционированного доступа.

– SNMP версии 2
SNMP версии 2 (SNMPv2), помимо прочего, включает ряд улучшений в области безопасности и конфиденциальности, а также возможность создания массового запроса для извлечения большого объема данных по одному запросу. Однако, его концепция безопасности считается слишком сложной, что и воспрепятствовало его принятию.
Таким образом, он был вскоре вытеснен версией SNMPv2c, соответствующей версии SNMPv2, но без противоречивой модели безопасности. Эта версия возвращается к методу, основанному на сообществе, используемому в SNMPv1, и имеет аналогичные пробелы в безопасности.
– SNMP версии 3
В SNMP версии 3 (SNMPv3) в основном добавлены функции безопасности и улучшения удаленной конфигурации. Они включают в себя улучшения конфиденциальности с использованием шифрования пакетов, целостности сообщений и проверки подлинности.
Эта версия также решает проблему крупномасштабного применения SNMP.

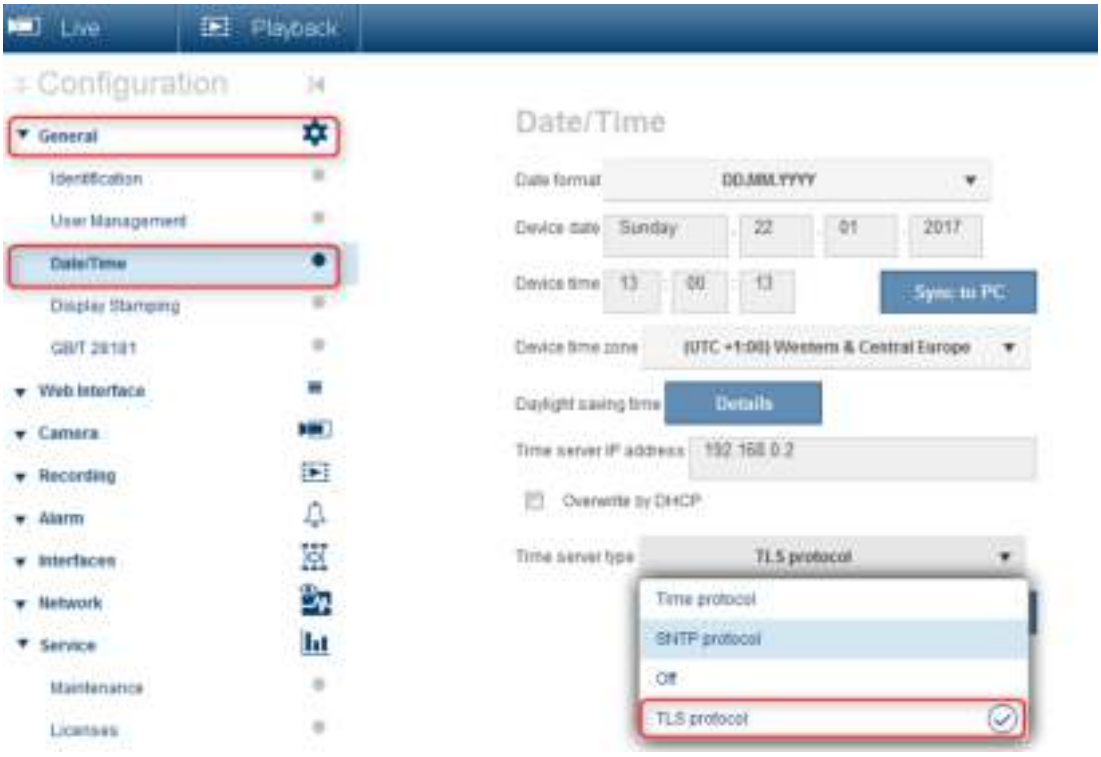
Замечания!

Совет о безопасности данных №12

Как SNMPv1, так и SNMPv2c оказались под угрозой в связи с отсутствием в них функций обеспечения безопасности. Они используют только «строки сообщества» в качестве паролей, которые передаются в виде открытого текста.
Таким образом, SNMPv1 или SNMPv2c следует использовать только тогда, когда есть гарантия, что сеть физически защищена от несанкционированного доступа.
На сегодняшний день камеры Bosch поддерживают только SNMPv1. Убедитесь, что SNMP отключен, если вы его не используете.

5.2 Защищенная временная основа

В дополнение к протоколу времени и протоколу SNTP (оба протокола являются незащищенными), в версии микропрограммы 6.20 был введен третий режим клиента сервера времени, использующий протокол TLS. Этот метод также широко известен как *TLS-Date*.
В этом режиме любой произвольный сервер HTTPS можно использовать как сервер времени. Значение времени определяется как побочный эффект процесса квитирования HTTPS. Передача данных защищена TLS. Дополнительный корневой сертификат для сервера HTTPS можно загрузить в хранилище сертификатов камеры для проверки подлинности сервера.



Замечания!

Совет о безопасности данных №13

Убедитесь, что введенный IP-адрес сервера времени имеет стабильную и надежную временную базу.

5.3 Облачные сервисы

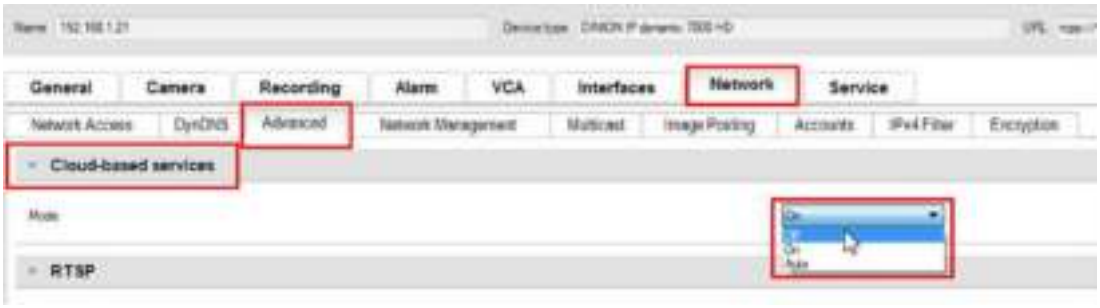
Все IP-видеоустройства Bosch могут связываться с **Облачные сервисы** Bosch. В зависимости от региона размещения это позволяет IP-видеоустройствам Bosch направлять тревожные сообщения и другие данные на центральную станцию.

Существует три режима использования **Облачные сервисы**:

- **Вкл.**:
  видеоустройство постоянно подключено к облачному серверу.
- **Авто** (по умолчанию):
  видеоустройства будут пытаться связываться с сервером несколько раз, в случае неудачи попытки связаться с облачным сервером будут прекращены.
- **Выкл.**
  отправка запросов на облачный сервер не выполняется.

Облачные сервисы можно легко отключить с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Дополнительно**.
3. Откройте часть страницы **Облачные сервисы**.
4. В раскрывающемся меню выберите **Выкл.**



Замечания!

Совет о безопасности данных №14

Если вы используете **Облачные сервисы** Bosch, сохраните конфигурацию по умолчанию. Во всех других случаях установите режим **Облачные сервисы** в положение **Выкл.**

6 Повышение уровня безопасности хранилищ

Хранилища iSCSI следует установить с защищенном месте. Доступ к защищенной области должен обеспечиваться через систему управления доступом и контролироваться. Группа пользователей, которая имеет доступ к центральному серверному помещению, должна быть ограничена небольшим количеством лиц.

Так как IP-камеры и кодеры Bosch способны устанавливать сеанс iSCSI напрямую с диском iSCSI и записывать видеоданные на диск iSCSI, устройства iSCSI должны быть подключены к той же сети LAN или WAN, что и периферийные устройства Bosch.

Для предотвращения несанкционированного доступа к записанным видеоданным устройства iSCSI должны быть защищены от несанкционированного доступа:

- По умолчанию устройства iSCSI предоставляют всем инициаторам iSCSI доступ к устройствам LUN iSCSI. Чтобы обеспечить исключительный доступ компонентов системы управления видео Bosch (камеры, кодеры, рабочие станции и серверы) к устройствам LUN iSCSI, можно отключить сопоставление LUN по умолчанию. Чтобы разрешить доступ устройств к целевым устройствам iSCSI Bosch Video Management System, классифицированные имена iSCSI (IQN) всех компонентов в Bosch Video Management System должны быть настроены на всех целевых устройствах iSCSI. Это требует усилий во время установки, но сводит к минимуму риск утраты, утечки или подделки видеоданных.
- Используйте проверку подлинности с помощью пароля через CHAP для обеспечения доступа к целевому устройству iSCSI только для известных устройств. Задайте пароль CHAP на целевом устройстве iSCSI и введите настроенный пароль в конфигурацию VRM. Пароль CHAP действителен для VRM и автоматически отправляется на все устройства. Если пароль CHAP используется в среде VRMBosch Video Management System, все системы хранения должны использовать тот же пароль.
- Удалите все имена пользователей и пароли по умолчанию с целевого устройства iSCSI.
- Используйте надежный пароль для учетной записи администратора целевого устройства iSCSI.
- Отключите доступ администратора через telnet для целевых устройств iSCSI; используйте вместо этого доступ через SSH.
- Защитите консольный доступ к целевому устройству iSCSI с помощью надежного пароля.
- Отключите неиспользуемые карты сетевого интерфейса.
- Контролируйте состояние системы хранилищ iSCSI с помощью сторонних инструментов для выявления ошибок.

7 Усиление безопасности серверов

7.1 Серверы Windows

Все компоненты сервера, такие как Bosch VMSManagement Server и Video Recording Manager должны быть размещены в защищенном месте. Доступ к защищенной области должен обеспечиваться через систему управления доступом и контролироваться. Группа пользователей, которая имеет доступ к центральному серверному помещению, должна быть ограничена небольшим количеством лиц.
Даже если оборудование сервера установлено в защищенном месте, необходимо обеспечить его защиту от несанкционированного доступа.

7.1.1 Рекомендуемые настройки оборудования для серверов

– BIOS сервера позволяет устанавливать пароли более низкого уровня.
  Эти пароли запрещают определенным лицам запускать компьютер, запускать подключаемые устройства, а также изменять параметры BIOS или интерфейса UEFI (единый расширяемый микропрограммный интерфейс) без разрешения.
– Во избежание передачи данных серверу, порты USB и CD / DVD-привод должны быть отключены.
  Также необходимо отключить неиспользуемые порты NIC и такие порты управления, как интерфейс HP ILO (HP Integrated Lights-Out); консольные порты должны быть отключены или защищены паролями.

7.1.2 Рекомендуемые настройки безопасности для операционной системы Windows

Серверы должен быть частью домена Windows.
При интеграции серверов в домен Windows пользователи сети получают разрешение на доступ через центральный сервер. Так как эти учетные записи часто имеют требования к надежности и сроку действия пароля, такая интеграция может повысить уровень безопасности по сравнению с местными учетными записями, которые не имеют таких ограничений.

7.1.3 Обновления для Windows

Обновления программного обеспечения Windows следует регулярно устанавливать и отслеживать. Обновления Windows часто включают в себя исправления для недавно обнаруженных пробелов в безопасности, таких как уязвимость Heartbleed SSL, затронувшая миллионы компьютеров по всему миру. Исправления для таких значительных проблем следует устанавливать.

7.1.4 Установка антивирусного ПО

Установите антивирусное и антишпионское ПО и обеспечьте его регулярное обновление.

7.1.5 Рекомендуемые настройки для операционной системы Windows

Для сервера с операционной системой Windows рекомендуется использовать следующие параметры локальной групповой политики. Для изменения локальной групповой политики по умолчанию используйте редактор локальной групповой политики (LGP).
Вы можете открыть редактор LGP с помощью командной строки или используя консоль управления Microsoft (MMC).

Чтобы открыть редактор LGP из командной строки:

- нажмите **Пуск**, в поле поиска **Пуск** введите **gpedit.msc** и нажмите Enter.

Чтобы открыть редактор LGP как встраиваемый модуль MMC:

1. нажмите **Пуск**, в поле поиска **Пуск** введите **mmc** и нажмите клавишу Enter.
2. В диалоговом окне **добавления и удаления встраиваемых модулей** нажмите **редактор объектов групповой политики** и нажмите кнопку **добавить**.
3. В диалоговом окне **выберите объект групповой политики** нажмите **обзор**.
4. Нажмите **компьютер** для изменения объекта локальной групповой политики и нажмите кнопку **пользователи** для изменения объектов групповой политики администратора, не администратора и пользователя.
5. Нажмите **Готово**

7.1.6 Активировать контроль учетных записей на сервере

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> локальная политика -> настройки безопасности

Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора	Активирован
Контроль учетных записей: позволить приложениям UIAccess запрашивать расширение прав доступа без использования безопасного рабочего стола	Отключен
Контроль учетных записей: запрос на расширение прав администратором в режиме одобрения администратором	Запрос разрешения
Контроль учетных записей: запрос на расширение прав для обычных пользователей	Запрос учетных данных в системе безопасного рабочего стола
Контроль учетных записей: обнаружение установки приложений и запрос расширения прав	Активирован
Контроль учетных записей: расширять права только для подписанных и проверенных исполняемых файлов	Отключен
Контроль учетных записей: все администраторы работают в режиме одобрения администратором	Активирован
Контроль учетных записей: переключение в режим безопасного рабочего стола при выполнении запроса на расширение прав	Активирован
Контроль учетных записей: виртуализация ошибок записи в файл и реестр в пользовательское расположение	Активирован

LCP -> конфигурация компьютера -> шаблоны администратора -> компоненты Windows -> интерфейс учетных данных пользователя

Нумеровать учетные записи администратора при расширении прав	Отключен

7.1.7 Отключение автозапуска

LCP -> конфигурация компьютера -> шаблоны администратора -> компоненты Windows -> политика автозапуска

Отключить автозапуск	Включить все диски

По умолчанию для автозапуска	Флажок установлен, не выполнять команды автозапуска
Отключить автозапуск для недисковых устройств	Активирован

7.1.8 Внешние устройства

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> локальная политика -> настройки безопасности

Устройства: разрешить отстыковку без выполнения входа	Отключен
Устройства: разрешено форматирование и извлечение подключаемых устройств	Администраторы
Устройства: не позволять пользователям устанавливать драйверы принтера	Активирован
Устройства: предоставлять доступ к CD-ROM только пользователям, выполнившим вход на местном уровне	Активирован
Устройства: предоставлять доступ к дискетному приводу только пользователям, выполнившим вход на местном уровне	Активирован

7.1.9 Конфигурация назначения прав пользователя

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> назначение прав пользователя

Доступ к диспетчеру учетных данных в качестве надежного оператора	Никто
Доступ к компьютеру через сеть	Проверенные пользователи
Действовать как часть операционной системы	Никто
Добавить рабочие станции к домену	Никто
Разрешить вход через службы удаленного рабочего стола	Администраторы, пользователи удаленного рабочего стола
Архивировать файлы и каталоги	Администраторы
Изменить время системы	Администраторы
Изменить часовой пояс	Администраторы, локальная служба
Создать файл страницы	Администраторы
Создание символическое обозначение объекта	Никто
Создать постоянные совместно используемые объекты	Никто
Отладить программы	Никто
Ограничить доступ к данному компьютеру из сети	Анонимный вход, гость
Запретить вход в качестве пакетного задания	Анонимный вход, гость

Запретить вход в качестве службы	Никто
Запретить локальный вход	Анонимный вход, гость
Запретить вход через службы удаленного рабочего стола	Анонимный вход, гость
Разрешить использование компьютера и учетных записей пользователей для делегирования	Никто
Принудительно завершать работу с удаленного компьютера	Администраторы
Создавать журналы безопасности	Локальная служба, сетевая служба
Увеличить приоритет планирования	Администраторы
Загружать и удалять драйверы устройств	Администраторы
Управлять журналом проверок и безопасности	Администраторы
Изменить метку объекта	Никто
Изменить значения среды микропрограммы	Администраторы
Выполнять задачи техобслуживания устройства	Администраторы
Задать параметры единого процесса	Администраторы
Задать параметры производительности системы	Администраторы
Отключить компьютер от установочной станции	Администраторы
Восстановить файлы и каталоги	Администраторы
Выключить систему	Администраторы
Синхронизировать служебные данные каталогов	Никто
Получить контроль файлов и других объектов	Администраторы

7.1.10 Экранная заставка

– Активировать защищенную паролем заставку и определить время ожидания:
LCP -> конфигурация пользователя -> шаблоны администратора -> панель управления -> персонализация

Активировать заставку	Активирован
Защитить заставку паролем	Активирован
Время ожидания заставки	1800 секунд

7.1.11 Активировать настройки требований к паролям

– Включение требований к паролям обеспечит соответствие паролей пользователей минимальным требованиям

LCP -> параметры Windows -> Параметры безопасности -> политика учетных записей -> политика паролей

Вести журнал паролей	Хранить 10 последних паролей
Максимальный срок действия пароля	90 дней
Минимальный срок действия пароля	1 день

Минимальная длина пароля	10 символов
Пароль должен соответствовать требованиям сложности	Активирован
Хранить пароль с использованием обратимого шифрования для всех пользователей в домене	Отключен

7.1.12 Отключить службы Windows, не обязательные для функционирования

– Отключение служб Windows, не обязательных для функционирования, обеспечивает более высокий уровень безопасности и сводит к минимуму количество точек воздействия.

Служба шлюза на уровне приложения	Отключен
Диспетчер приложений	Отключен
Браузер компьютера	Отключен
Клиент отслеживания изменившихся связей	Отключен
Функция обнаружения поставщика узла	Отключен
Функция обнаружения ресурсов публикации	Отключен
Доступ к устройствам интерфейса пользователя	Отключен
Общий доступ к подключению к Интернету (ICS)	Отключен
Диспетчер обнаружения топологии канального уровня	Отключен
Планировщик классов мультимедиа	Отключен
Автономные файлы	Отключен
Диспетчер автоматических подключений удаленного доступа	Отключен
Диспетчер подключения удаленного доступа	Отключен
Маршрутизация и удаленный доступ	Отключен
Обнаружение оборудования оболочки	Отключен
Консольный помощник специального управления	Отключен
Обнаружение SSDP	Отключен
Аудио Windows	Отключен
Компоновщик предельных значений аудио Windows	Отключен

7.1.13 Учетные записи пользователей операционной системы Windows

Учетные записи пользователей операционной системы Windows должны быть защищены сложными паролями.
Серверы обычно управляются и обслуживаются с помощью учетных записей администратора Windows, убедитесь что учетные записи администратора защищены надежными паролями.

Пароли должны содержать символы из трех следующих категорий:

- Символы верхнего регистра европейских языков (От A до Z, с диакритическими знаками, греческие и кириллические символы)
- Символы нижнего регистра европейских языков (от a до z, эсцет, с диакритическими знаками, греческие и кириллические символы)
- Базовые 10 цифр (от 0 до 9)
- Не буквенно-цифровые символы: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Любой символ Unicode, попадающий в категорию буквенного, но не являющийся символом верхнего или нижнего регистра. Это включает символы Unicode из азиатских языков.

Использование блокировки учетной записи Windows для предотвращения успешных попыток взлома пароля.
Windows8.1 Базовые рекомендации безопасности 10/15/15:
- 10 неудачных попыток входа
- Блокировка 15 минут
- Сброс счетчиков в течение 15 минут

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> политика учетной записи -> политика блокировки учетной записи

Продолжительность блокировки учетной записи	Продолжительность блокировки учетной записи
Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа	Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа
Сброс счетчика блокировки через	Сброс счетчика блокировки через

- Убедитесь, что пароль сервера по умолчанию и пароль операционной системы Windows заменены новыми надежными паролями.

7.1.14 Включить брандмауэр на сервере

▸ Включить связь стандартного порта Bosch VMS в соответствии с портами Bosch VMS.

Замечания!

Совет о безопасности данных №15

См. документацию Bosch VMSпо установке и использованию для получения подробных сведений о параметрах соответствующих портов и их использовании. Не забудьте еще раз проверить параметры обновления микропрограммы или ПО.

8 Усиление безопасности клиентов

8.1 Рабочие станции Windows

Настольные операционные системы Windows, используемые для клиентских приложений Bosch VMS, таких как Bosch VMS, Operator Client или Configuration Client, устанавливаются за пределами защищенного места. Рабочие станции должны быть усилены для защиты видеоданных, документов и других приложений от несанкционированного доступа. Необходимо применить или проверить следующие настройки.

8.1.1 Рекомендуемые параметры оборудования рабочей станции Windows

- Установите пароль BIOS/ UEFI, чтобы запретить запуск альтернативных операционных систем.
- С целью предотвращения передачи данных клиенту USB-порты, а также CD и DVD-приводы должны быть отключены. Кроме того, неиспользуемые порты NIC также следует отключить.

8.1.2 Рекомендуемые настройки безопасности для операционной системы Windows

- Рабочая станция должна быть частью домена Windows.
  Интеграция рабочей станции в домен Windows позволит централизованно управлять параметрами безопасности.
- Обновления Windows
  . Следите за последними исправлениями и обновлениями ПО Windows.
- Установка антивирусного ПО
  Установите антивирусное и антишпионское ПО и регулярно обновляйте его.

8.1.3 Рекомендуемые настройки для операционной системы Windows

Для сервера с операционной системой Windows рекомендуется использовать следующие параметры локальной групповой политики. Для изменения локальной групповой политики по умолчанию используйте редактор локальной групповой политики (LGP).
Вы можете открыть редактор LGP с помощью командной строки или используя консоль управления Microsoft (MMC).

Чтобы открыть редактор LGP из командной строки:

- нажмите **Пуск**, в поле поиска **Пуск** введите **gpedit.msc** и нажмите Enter.

Чтобы открыть редактор LGP как встраиваемый модуль MMC:

1. нажмите **Пуск**, в поле поиска **Пуск** введите **mmc** и нажмите клавишу Enter.
2. В диалоговом окне **добавления и удаления встраиваемых модулей** нажмите **редактор объектов групповой политики** и нажмите кнопку **добавить**.
3. В диалоговом окне **выберите объект групповой политики** нажмите **обзор**.
4. Нажмите **компьютер** для изменения объекта локальной групповой политики и нажмите кнопку **пользователи** для изменения объектов групповой политики администратора, не администратора и пользователя.
5. Нажмите **Готово**

8.1.4 Активировать контроль учетных записей на сервере

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> локальная политика -> настройки безопасности

Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора	Активирован
Контроль учетных записей: позволить приложениям UIAccess запрашивать расширение прав доступа без использования безопасного рабочего стола	Отключен
Контроль учетных записей: запрос на расширение прав администратором в режиме одобрения администратором	Запрос разрешения
Контроль учетных записей: запрос на расширение прав для обычных пользователей	Запрос учетных данных в системе безопасного рабочего стола
Контроль учетных записей: обнаружение установки приложений и запрос расширения прав	Активирован
Контроль учетных записей: расширять права только для подписанных и проверенных исполняемых файлов	Отключен
Контроль учетных записей: все администраторы работают в режиме одобрения администратором	Активирован
Контроль учетных записей: переключение в режим безопасного рабочего стола при выполнении запроса на расширение прав	Активирован
Контроль учетных записей: виртуализация ошибок записи в файл и реестр в пользовательское расположение	Активирован

LCP -> конфигурация компьютера -> шаблоны администратора -> компоненты Windows -> интерфейс учетных данных пользователя

Нумеровать учетные записи администратора при расширении прав	Отключен

8.1.5 Отключение автозапуска

LCP -> конфигурация компьютера -> шаблоны администратора -> компоненты Windows -> политика автозапуска

Отключить автозапуск	Включить все диски
По умолчанию для автозапуска	Флажок установлен, не выполнять команды автозапуска
Отключить автозапуск для недисковых устройств	Активирован

8.1.6 Внешние устройства

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> локальная политика -> настройки безопасности

Устройства: разрешить отстыковку без выполнения входа	Отключен
Устройства: разрешено форматирование и извлечение подключаемых устройств	Администраторы

Устройства: не позволять пользователям устанавливать драйверы принтера	Активирован
Устройства: предоставлять доступ к CD-ROM только пользователям, выполнившим вход на местном уровне	Активирован
Устройства: предоставлять доступ к дискетному приводу только пользователям, выполнившим вход на местном уровне	Активирован

8.1.7 Конфигурация назначения прав пользователя

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> назначение прав пользователя

Доступ к диспетчеру учетных данных в качестве надежного оператора	Никто
Доступ к компьютеру через сеть	Проверенные пользователи
Действовать как часть операционной системы	Никто
Добавить рабочие станции к домену	Никто
Разрешить вход через службы удаленного рабочего стола	Администраторы, пользователи удаленного рабочего стола
Архивировать файлы и каталоги	Администраторы
Изменить время системы	Администраторы
Изменить часовой пояс	Администраторы, локальная служба
Создать файл страницы	Администраторы
Создание символическое обозначение объекта	Никто
Создать постоянные совместно используемые объекты	Никто
Отладить программы	Никто
Ограничить доступ к данному компьютеру из сети	Анонимный вход, гость
Запретить вход в качестве пакетного задания	Анонимный вход, гость
Запретить вход в качестве службы	Никто
Запретить локальный вход	Анонимный вход, гость
Запретить вход через службы удаленного рабочего стола	Анонимный вход, гость
Разрешить использование компьютера и учетных записей пользователей для делегирования	Никто
Принудительно завершать работу с удаленного компьютера	Администраторы
Создавать журналы безопасности	Локальная служба, сетевая служба
Увеличить приоритет планирования	Администраторы
Загружать и удалять драйверы устройств	Администраторы

Управлять журналом проверок и безопасности	Администраторы
Изменить метку объекта	Никто
Изменить значения среды микропрограммы	Администраторы
Выполнять задачи техобслуживания устройства	Администраторы
Задать параметры единого процесса	Администраторы
Задать параметры производительности системы	Администраторы
Отключить компьютер от установочной станции	Администраторы
Восстановить файлы и каталоги	Администраторы
Выключить систему	Администраторы
Синхронизировать служебные данные каталогов	Никто
Получить контроль файлов и других объектов	Администраторы

8.1.8 Экранная заставка

– Активировать защищенную паролем заставку и определить время ожидания:
LCP -> конфигурация пользователя -> шаблоны администратора -> панель управления -> персонализация

Активировать заставку	Активирован
Защитить заставку паролем	Активирован
Время ожидания заставки	1800 секунд

8.1.9 Активировать настройки требований к паролям

– Включение требований к паролям обеспечит соответствие паролей пользователей минимальным требованиям

LCP -> параметры Windows -> Параметры безопасности -> политика учетных записей -> политика паролей

Вести журнал паролей	Хранить 10 последних паролей
Максимальный срок действия пароля	90 дней
Минимальный срок действия пароля	1 день
Минимальная длина пароля	10 символов
Пароль должен соответствовать требованиям сложности	Активирован
Хранить пароль с использованием обратимого шифрования для всех пользователей в домене	Отключен

8.1.10 Отключить службы Windows, не обязательные для функционирования

– Отключение служб Windows, не обязательных для функционирования, обеспечивает более высокий уровень безопасности и сводит к минимуму количество точек воздействия.

Служба шлюза на уровне приложения	Отключен

Диспетчер приложений	Отключен
Браузер компьютера	Отключен
Клиент отслеживания изменившихся связей	Отключен
Функция обнаружения поставщика узла	Отключен
Функция обнаружения ресурсов публикации	Отключен
Доступ к устройствам интерфейса пользователя	Отключен
Общий доступ к подключению к Интернету (ICS)	Отключен
Диспетчер обнаружения топологии канального уровня	Отключен
Планировщик классов мультимедиа	Отключен
Автономные файлы	Отключен
Диспетчер автоматических подключений удаленного доступа	Отключен
Диспетчер подключения удаленного доступа	Отключен
Маршрутизация и удаленный доступ	Отключен
Обнаружение оборудования оболочки	Отключен
Консольный помощник специального управления	Отключен
Обнаружение SSDP	Отключен
Аудио Windows	Отключен
Компоновщик предельных значений аудио Windows	Отключен

8.1.11 Учетные записи пользователей операционной системы Windows

Учетные записи пользователей операционной системы Windows должны быть защищены сложными паролями.
Серверы обычно управляются и обслуживаются с помощью учетных записей администратора Windows, убедитесь что учетные записи администратора защищены надежными паролями.

Пароли должны содержать символы из трех следующих категорий:

- Символы верхнего регистра европейских языков (От A до Z, с диакритическими знаками, греческие и кириллические символы)
- Символы нижнего регистра европейских языков (от a до z, эсцет, с диакритическими знаками, греческие и кириллические символы)
- Базовые 10 цифр (от 0 до 9)
- Не буквенно-цифровые символы: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Любой символ Unicode, попадающий в категорию буквенного, но не являющийся символом верхнего или нижнего регистра. Это включает символы Unicode из азиатских языков.

Использование блокировки учетной записи Windows для предотвращения успешных попыток взлома пароля.
Windows8.1 Базовые рекомендации безопасности 10/15/15:

– 10 неудачных попыток входа
– Блокировка 15 минут
– Сброс счетчиков в течение 15 минут

LCP -> конфигурация компьютера -> параметры Windows -> параметры безопасности -> политика учетной записи -> политика блокировки учетной записи

Продолжительность блокировки учетной записи	Продолжительность блокировки учетной записи
Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа	Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа
Сброс счетчика блокировки через	Сброс счетчика блокировки через

– Убедитесь, что пароль сервера по умолчанию и пароль операционной системы Windows заменены новыми надежными паролями.
– Отключите неиспользуемые учетные записи операционной системы Windows.
– Отключите удаленный доступ к рабочему столу клиентской рабочей станции.
– Запускайте рабочую станцию без прав администратора в целях избежания изменения параметров системы стандартным пользователем.

8.1.12 Активируйте брандмауэр на рабочей станции

▸ Включить связь стандартного порта Bosch VMS в соответствии с портами Bosch VMS.

Замечания!

Совет о безопасности данных №16

См. документацию Bosch VMSпо установке и использованию для получения подробных сведений о параметрах соответствующих портов и их использовании. Не забудьте еще раз проверить параметры обновления микропрограммы или ПО.

9 Защита доступа к сети

В настоящий момент многие малые и средние системы IP-видеонаблюдения размещены в существующей сетевой инфраструктуре клиентов как «очередное ИТ-приложение». Несмотря на преимущества в отношении цены и обслуживания, такой тип размещения также подвергает систему нежелательным угрозам, в том числе внутренним. Необходимо принять соответствующие меры и избегать ситуаций, когда видеозапись события попадает в Интернет или социальные сети. Такие ситуации могут не только нарушить конфиденциальность, но и в потенциале нанести вред компании.

Существует две основные технологии создания сети-в-сети. Какая именно будет выбрана создателями ИТ-инфраструктуры во многом зависит от существующей сетевой инфраструктуры, имеющегося сетевого оборудования и требуемых возможностей и топологии сети.

9.1 VLAN: виртуальная сеть LAN

Виртуальная сеть LAN создается путем разделения LAN на несколько сегментов. Сегментация сети осуществляется с помощью конфигурации сетевого коммутатора или роутера. VLAN имеет следующее преимущество : потребности в ресурсах могут быть удовлетворены без изменений в сетевых подключениях устройства.
Качество схем обслуживания, применяемых к конкретных сегментам, например, для видеонаблюдения, может повысить не только уровень безопасности, но и производительности.

Сети VLAN внедряются на канальном уровне сети (уровень OSI 2) и обеспечивают аналогию созданию IP-подсетей (см. *Назначение IP-адресов, Страница 7*) на уровне сети (уровень OSI 3).

9.2 VPN: виртуальная частная сеть

Виртуальная частная сеть — это отдельная (частная) сеть, которая часто основывается на нескольких общественных сетях или Интернете. Существует множество протоколов для создания VPN, которая обычно представляет собой тоннель, по которому перемещаются защищенные данные. Виртуальные частные сети можно создать в виде двухточечных туннелей, всеобщих подключений или многопортовых подключений. Сеть VPN может быть развернута с шифрованной связью или просто использовать безопасное соединение в рамках самой VPN.

VPN может использоваться для подключения к удаленным сайтам через подключения глобальной сети (WAN), но при этом также обеспечивать конфиденциальность и повышать уровень безопасности локальной сети (LAN). Поскольку виртуальная частная сеть действует как отдельная сеть, все устройства, добавленные к VPN, будут работать гладко, как если бы они были частью обычной сети. VPN не только обеспечивает дополнительный уровень защиты для системы наблюдения, но и предлагает дополнительное преимущество сегментации бизнес-данных производственной сети и видеоданных.

Замечания!

Совет о безопасности данных №17

Если это применимо, VPN или VLAN повышают уровень безопасности системы видеонаблюдения в существующей ИТ-инфраструктуре.

Помимо зашиты системы от несанкционированного доступа в совместно используемой ИТ-инфраструктуре, необходимо уделить внимание тому, кто имеет право подключаться к этой сети вообще.

9.3 Отключение неиспользуемых портов коммутаторов

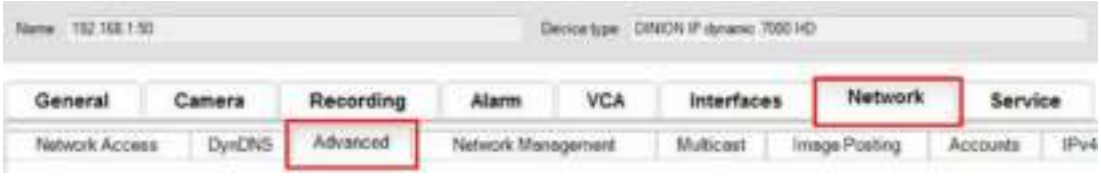
Отключение неиспользуемых сетевых портов обеспечивает невозможность доступа к сети несанкционированных устройств. Это снижает риск чьих-либо попыток получить доступ к подсети безопасности с помощью подключения своего устройства к коммутатору или неиспользуемому сетевому разъему. Возможность отключения конкретных портов является стандартным решением для управляемых коммутаторов, низкозатратным и подходящим для корпоративного применения.

9.4 802. 1 x защищенные сети

Все IP-видеоустройства Bosch можно настроить как клиенты 802.1x Эта возможность позволяет им проходить проверку подлинности для подключения к серверу RADIUS и участия в защищенной сети. Прежде чем размещать видеоустройства в безопасной сети, вам потребуется прямое подключение к видеоустройству с ноутбука специалиста технической поддержки для ввода учетных данных, как указано ниже.

Сервисы 802.1x можно легко настроить с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Дополнительно**



3. Откройте часть страницы **802.1x**.
4. В раскрывающемся списке **802.1x выберите Вкл.**
5. Введите действительный **Удостоверение** и **Пароль.**
6. Сохраните изменения.
7. Отключите и разместите устройства в защищенной сети.

Замечания!
Сам по себе 802.1x не обеспечивает безопасное соединение между запрашивающим устройством и сервером проверки подлинности.
В результате имя пользователя и пароль могут быть «украдены» из сети. 802.1x может использовать EAP-TLS для обеспечения безопасной связи.

9.4.1 Расширяемый протокол проверки подлинности — безопасность транспортного уровня

Расширяемый протокол проверки подлинности (EAP) обеспечивает поддержку нескольких методов проверки подлинности. Безопасность транспортного уровня (TLS) обеспечивает взаимную проверку подлинности, согласование с целостно-защищенным набором шифров и обмен ключами между двумя конечными точками. EAP-TLS поддерживает взаимную проверку подлинности сертификатов и формирование ключей. Другими словами, EAP-TLS включает процесс, в котором и сервер, и клиент отправляют друг другу сертификат.

Замечания!

Совет о безопасности данных №18

Обратитесь к специальной технической белой книге «Проверка подлинности сети — 802.1x — обеспечение безопасности сетевой периферии», доступной в каталоге продукции Bosch Security Systems по ссылке:
http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

10 Установление доверия с помощью сертификатов

Все IP-камеры Bosch с версией микропрограммы 6.10 или более поздней используют хранилище сертификатов, которое можно найти в меню **Обслуживание** конфигурации камеры.

Конкретные сертификаты серверов, сертификаты клиентов и доверенные сертификаты могут быть добавлены в хранилище.

Чтобы добавить сертификат в хранилище:

1. На веб-странице устройства перейдите на страницу **Конфигурация**.
2. Выберите меню **Обслуживание** и подменю **Сертификаты**.
3. В разделе **Список файлов** выберите **Добавить**.
4. Загрузите желаемые сертификаты.
   После завершения загрузки сертификаты отображаются в разделе **Список использования**.
5. В разделе **Список использования** выберите желаемый сертификат.
6. Для активации использования сертификатов камеру необходимо перезагрузить. Для перезагрузки камеры нажмите **Установить**.

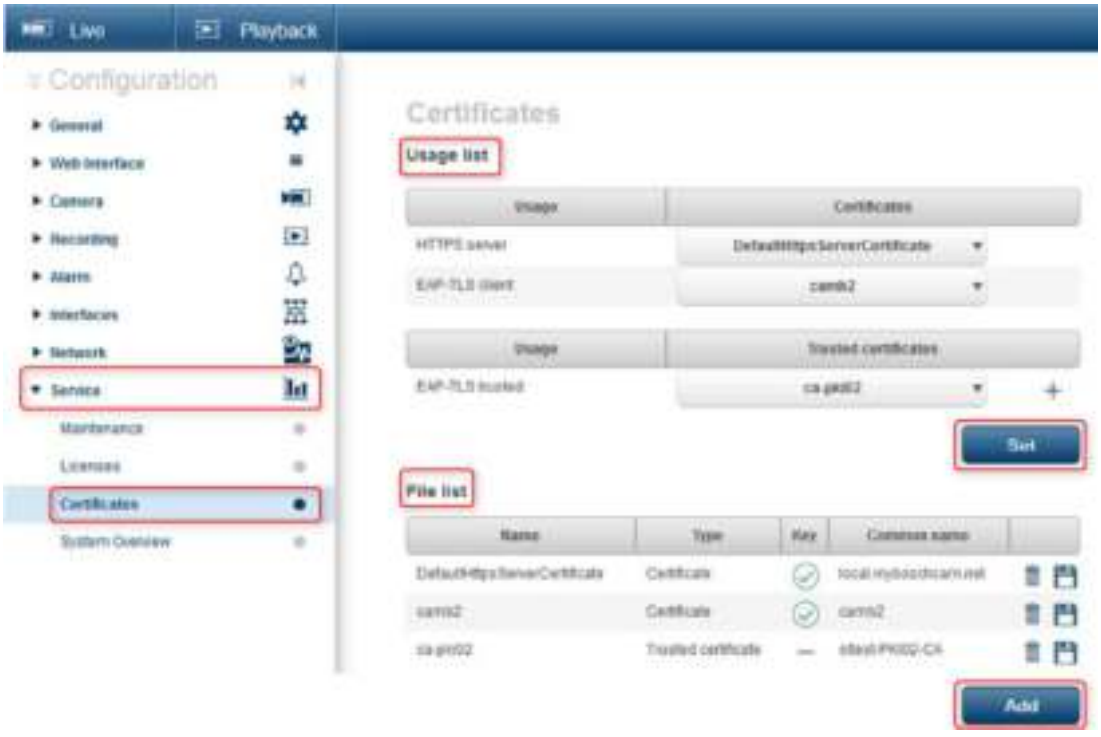


Рисунок 10.1: Пример: сертификаты EAP/TLS хранятся в камере Bosch с версией микропрограммы 6.11.

10.1 Хранится в безопасном месте (модуль TPM)

Ключи хранятся в чипе, аналогичном используемому в криптомикропроцессорах, также называемом «Доверенный платформенный модуль» или кратко модуль TPM. Этот чип выступает в качестве сейфа для важнейших данных; он защищает сертификаты, пароли, лицензии и т.д. от несанкционированного доступа, даже если камера подвергается физическому вскрытию с целью получения доступа.

Сертификаты принимаются в формате *.pem, *.cer или *.crt и должны быть закодированы в Base64. Их можно загрузить единым файлом или разделить на файлы сертификатов и ключей и загрузить в этом порядке как отдельные файлы для последующего автоматического объединения.

Начиная с версии микропрограммы 6.20, поддерживаются частные защищенные паролем ключи PKCS#8 (шифрованные с помощью AES), которые должны быть загружены в формате *.pem и закодированы в Base64.

10.2 Сертификаты TLS

Все видеоустройства Bosch с версией микропрограммы до 6.1 поставляются с предустановленным сертификатом TLS и частным ключом, который используется для связи HTTPSавтоматически. Сертификат по умолчанию и ключ предназначены исключительно для целей тестирования, так как все устройства поставляются с одним и тем же сертификатом по умолчанию.

Начиная с версии микропрограммы 6.20, при необходимости для подключений HTTPS автоматически создается уникальный для устройства самозаверяющий сертификат, обеспечивающий уникальную проверку подлинности. Данный самозаверяющий сертификат можно вручную обновить, просто удалив его. Устройство самостоятельно создаст новый сертификат, как только это потребуется.

Если устройства размещены в среде, где для проверки подлинности каждого отдельного IP-видеоустройства требуются дополнительные этапы, новые сертификаты и частные ключи могут быть созданы и загружены на эти видеоустройства. Новые сертификаты можно получить у органа сертификации или их можно создать, например, с помощью комплекта инструментов для работы с OpenSSL.

10.2.1 Веб-страница устройства

Сертификаты можно загрузить с использованием веб-страницы видеоустройства.
На странице **Сертификаты** можно удалять и добавлять новые сертификаты, а также задавать параметры их использования.

См. также

– *Установление доверия с помощью сертификатов, Страница 45*

10.2.2 Configuration Manager

В Configuration Manager сертификаты можно легко загружать на отдельные устройства или на несколько устройств одновременно.
Чтобы загрузить сертификаты:

1. в Configuration Manager выберите одно или несколько устройств.
2. Нажмите правой кнопкой и выберите **Отправка файла**, затем нажмите **Сертификат SSL...**.
   Откроется окно WindowsExplorer для выбора сертификата для загрузки.

Замечания!
Сертификаты можно загружать с помощью Configuration Manager, но определение использования необходимо осуществлять с помощью веб-страницы **Сертификаты**.

Замечания!
Совет о безопасности данных №19
Сертификаты следует использовать для авторизации одного устройства. Рекомендуется создать конкретный сертификат для каждого устройства на основе главного сертификата. Если устройства используются в общественных сетях, рекомендуется получить сертификаты от общественного управления по сертификатам, или получить подпись такого органа на сертификатах; такой орган также может подтвердить происхождение и действительность — другими словами подлинность — сертификата устройства.

11 Функция установления подлинности видеоизображения

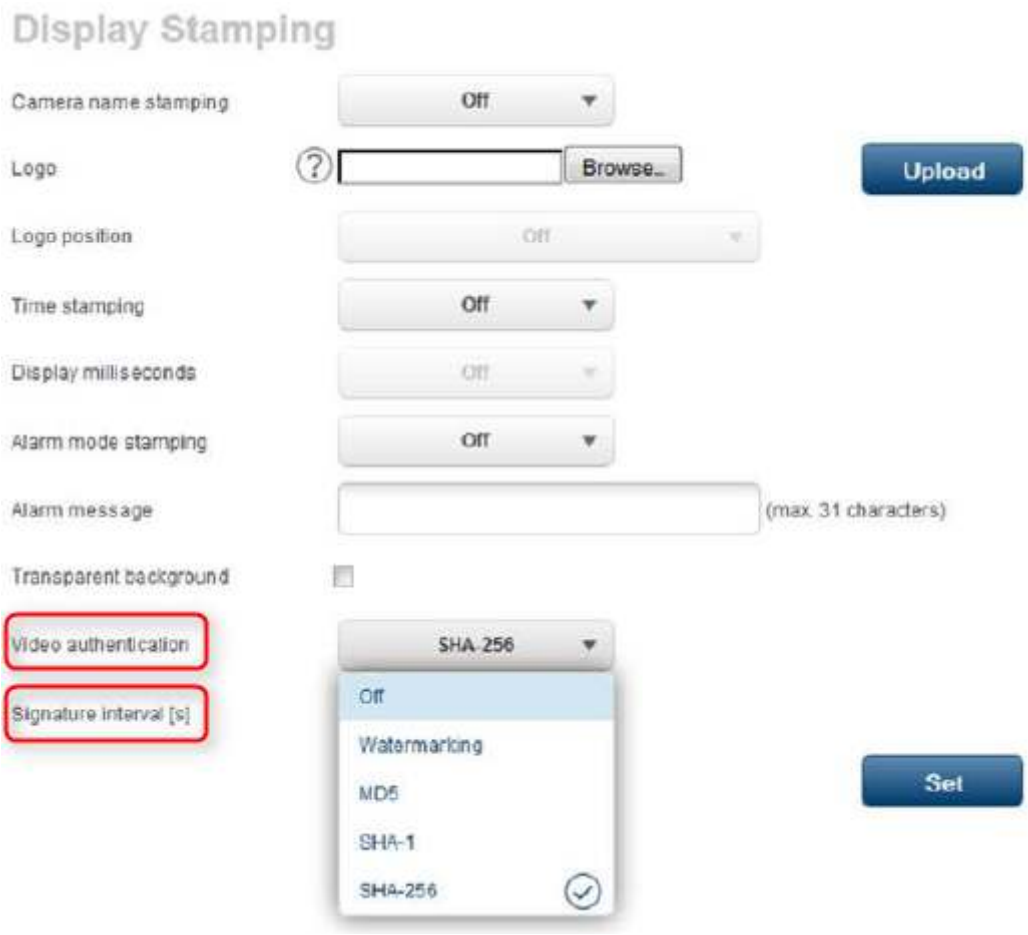
Как только устройства в системе будут должным образом защищены и пройдут проверку подлинности, стоит также следить за видеоданными, получаемыми с них. Этот метод называется проверкой подлинности видео.

Проверка подлинности видео связана только с методами проверки подлинности видео. Проверка подлинности видео никаким образом не связана с передачей видео или данных.

До выхода микропрограммы 5.9 водяные знаки наносились на видеопоток с помощью простого алгоритма контрольной суммы. При работе с базовым нанесением водяных знаков нет смысла использовать сертификаты или шифрование. Контрольная сумма — это базовое измерение «постоянности данных» файла, которое подтверждает целостность файла.

Чтобы настроить проверку подлинности видео, например, в веб-браузере:

1. Перейдите в меню **Общие** и выберите **Надписи на экране**.
2. В раскрывающееся меню **Проверка подлинности видео** выберите нужный вариант:
   Микропрограмма версии 5.9 и более поздние версии обеспечивают три параметра установления подлинности видеоизображений помимо классических водяных знаков:
   - MD5: краткое сообщение, производящее 128-битовое хеш-значение.
   - SHA-1: разработанный управлением национальной безопасности США федеральный стандарт обработки информации, опубликованный Национальным институтом стандартов и технологии США. SHA-1 производит 160-битовое хеш-значение.
   - SHA-256: SHA-256 формирует практически уникальное 256-битовое (32-байтовое) хеш-значение фиксированного размера.



Замечания!
Хеш является необратимой функцией, ее невозможно расшифровать.

При использовании установления подлинности видеоизображений каждый пакет видеопотока хэшируется. Эти хэши встроены в поток видео и хэшируются сами вместе с видеоданными. Это гарантирует целостность содержания потока.

Хэши регулярно подписываются с определенным интервалом с использованием частного ключа хранящегося в модуле TPM устройства сертификата. Запись по тревоге и изменения блоков в записях iSCSI закрываются подписью в целях обеспечения непрерывной подлинности видео.

Замечания!
Расчет цифровой подписи требует вычислительной мощности, которая может повлиять на общую производительность камеры, если его проводить слишком часто. Поэтому следует выбрать приемлемый интервал.

Так как хэши и цифровые подписи внедряются в поток видео, они также сохраняются в записи, позволяя устанавливать подлинность видеоизображений также для воспроизведения и экспорта.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com