MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2024 R1

Руководство администратора

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

Содержание

Copyright, товарные знаки и ограничение ответственности

Товарные знаки

XProtect является зарегистрированным товарным знаком компании Milestone Systems A/S.

Microsoft и Windows — зарегистрированные товарные знаки Microsoft Corporation. App Store — знак обслуживания Apple Inc. Android — зарегистрированный товарный знак Google Inc.

Все другие товарные знаки, упоминаемые в данном документе, являются товарными знаками соответствующих владельцев.

Ограничение ответственности

Этот документ, составленный с должным вниманием, предназначен исключительно для предоставления общей информации.

За любые риски, которые возникают в связи с использованием данной информации, несет ответственность получатель, и никакие заявления в этом документе не должны толковаться как предоставление каких-либо гарантий.

Компания Milestone Systems A/S сохраняет за собой право вносить изменения без предварительного уведомления.

Все имена людей и организаций, использованные в примерах данного документа, являются вымышленными. Любое сходство с действительными организациями или людьми, живыми или умершими, является случайным и ненамеренным.

Этот продукт может использовать стороннее программное обеспечение, на которое могут распространяться особые условия и положения. В таких случаях дополнительные сведения см. в файле `3rd_party_software_terms_and_conditions.txt`, который находится в папке установки системы Milestone.

Обзор

Что нового?

В Management Client 2024 R1

XProtect Management Client

Документация Management Client на русском языке

Теперь справка для Management Client доступна и на русском языке.

Установка сервера записи обработки отказа / сервера записи

Теперь при установке сервера записи или сервера записи обработки отказа файлы каждого соответствующего сервера размещаются в отдельных папках в папке Milestone: **XProtect Сервер отказоустойчивости** и **XProtectсервер записи**.

Если вы выполняете обновление XProtect, эти папки также создаются в процессе обновления, и в них располагаются файлы для каждого типа серверов.

Раньше файлы сервера записи обработки отказа и сервера записи устанавливались в одну и ту же папку, что могло вызвать проблемы при масштабировании продуктов или работе на разных версиях Microsoft .NET.

В Management Client 2023 R3

XProtect Management Client

для аутентификации можно использовать Azure Active Directory. В процессе установки можно выбрать **Аутентификацию с аккаунтом Windows** либо вариант **Интеграция с Azure Active Directory**, обеспечивающий комплексную безопасность.

Дополнительные сведения об установке XProtect с функциями комплексной безопасности Azure см. в разделе Установка системы — вариант «Пользовательская» на стр. 176.

XProtect Management Client

Теперь доступен параметр (не доверять сертификату сервера) для аутентификации по учетной записи Windows и для интеграции с Azure Active Directory. Для интеграции с Azure Active Directory этот параметр обязателен. Параметр (не доверять сертификату сервера) обеспечивает проверку правильности сертификатов сервера до начала установки.

XProtect Management Client:

Добавлено новое пользовательское разрешение для сигналов тревоги **Изменять настройки сигналов тревоги**, которое позволяет администраторам изменять определения, состояния, категории и звуки сигналов тревоги, а также условия сохранения сигналов тревоги и событий. Соответствующие разрешения для изменения определений сигналов тревоги были удалены из существующего пользовательского разрешения **Управлять**, и для управления настройками сигналов тревоги администраторам потребуются оба пользовательских разрешения: **Изменять настройки сигналов тревоги** и **Управлять**.

Новое пользовательское разрешение **Изменять настройки сигналов тревоги** не применяется к существующим пользователям и должно быть вручную назначено пользователям, которым требуется уровень доступа администратора для настройки сигналов тревоги после установки или обновления.

Сведения о пользовательской установке см. в разделе Роли (узел «Безопасность») на стр. 561

В Management Client 2023 R2

XProtect Management Client:

Теперь адаптивное потоковое воспроизведение можно настраивать для использования в режиме воспроизведения. Этот способ называется «адаптивное воспроизведение». Дополнительные сведения приведены в разделе Адаптивное воспроизведение (объяснение) на стр. 253.

XProtect Management Client:

Теперь при установке компонентов XProtect в рамках пользовательской установки можно использовать предварительно созданную базу данных. Сведения о пользовательской установке см. в разделе Установка системы — вариант «Пользовательская» на стр. 176

XProtect Management Client:

Были добавлены новые пользовательские разрешения для ограничений в отношении видео, которые позволяют администраторам настраивать права для создания, просмотра, изменения и удаления видео, а также назначать их пользователям. Дополнительные сведения приведены в разделе Роли (узел «Безопасность») на стр. 561

В Management Client 2023 R1

XProtect Incident Manager:

- Для исполнения GDPR или других применимых законов в отношении личных данных, администраторы XProtect Management Client теперь могут определять время хранения для проектов с инцидентами.

В Management Client 2022 R3

XProtect Incident Manager:

- Расширение XProtect Incident Manager теперь совместимо с XProtect Expert, XProtect Professional+ и XProtect Express+ (версии 2022 R3 или более поздней).
- XProtect Incident Manager может показывать более 10 000 проектов с инцидентом.

В Management Client 2022 R2

XProtect Incident Manager:

- Первый выпуск этого расширения.
- Это расширение XProtect Incident Manager совместимо с XProtect Corporate версии 2022 R2 и более поздними, а также с XProtect Smart Client версии 2022 R2 и более поздними.

XProtect LPR:

- Стили регистрационного знака, которые входят в состав модулей стран, теперь перечислены на одной странице.
- Для упрощения работы со стилями регистрационных знаков можно объединять их в псевдонимы стилей в соответствии с вашими потребностями в распознавании номерных знаков.
- Теперь списки соответствия поддерживают псевдонимы стилей регистрационных знаков.

В Management Client 2022 R1

Шифрование сервера событий:

- Можно настроить шифрование двусторонних подключений между сервером событий и компонентами, обменивающимися данными с сервером событий, включая LPR Server.

  Дополнительные сведения приведены в разделе Включить шифрование сервера событий на стр. 333.

Вход в систему через внешнего IDP:

- Теперь в Milestone XProtect VMS можно входить в систему при помощи внешнего IDP. Вход в систему через внешнего IDP — это альтернатива входу в систему в качестве пользователя Active Directory или базового пользователя. Благодаря входу в систему через внешнего IDP можно выполнить требования, настроенные для базового пользователя, и при этом получить разрешение на доступ к компонентам и устройствам в XProtect.

  Дополнительные сведения приведены в разделе Внешний IDP (объяснение).

Обновление данных об оборудовании

- Теперь можно просмотреть текущую версию прошивки аппаратного устройства, обнаруженного системой в Management Client.

  Дополнительные сведения приведены в разделе Обновление данных об оборудовании на стр. 380.

XProtect Management Server Failover

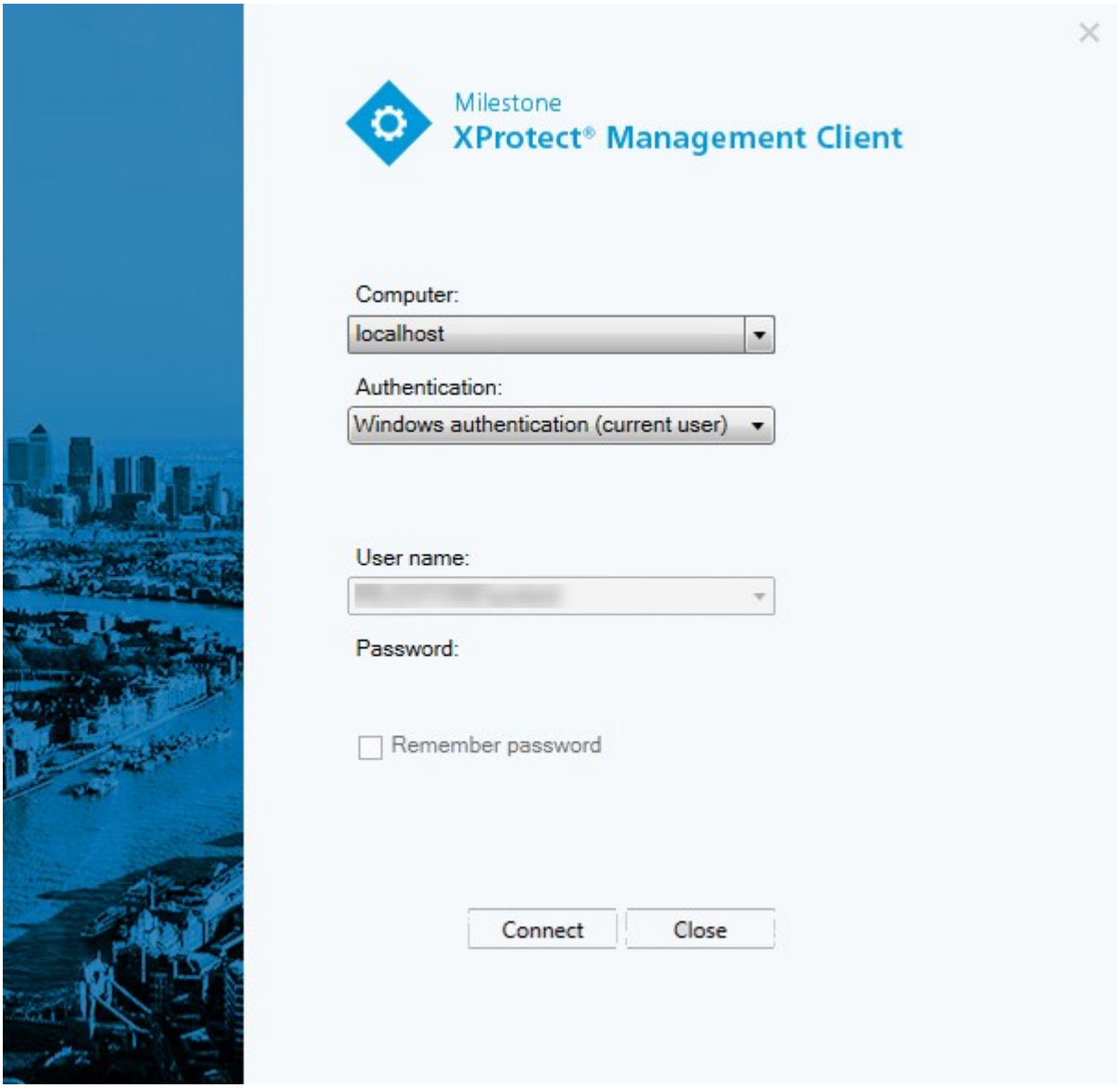
- Теперь можно обеспечить высокий уровень доступности системы путем настройки сервера управления для обработки отказа между двумя дублирующими друг друга компьютерами. В случае отказа компьютера, на котором работает сервер управления, его функции берет на себя второй компьютер. Репликация данных в режиме реального времени обеспечивает идентичность баз данных сервера управления, сервера регистрации и сервера событий на обоих компьютерах.

  Дополнительные сведения приведены в разделе XProtect Management Server Failover на стр. 57.

Вход в систему (объяснение)

При запуске Management Client необходимо ввести учетные данные для подключения к системе.

Если установлены XProtect Corporate 2016 или XProtect Expert 2016 либо их более новые версии, после установки исправления можно входить в системы, на которых работают более старые версии продукта. Поддерживаются версии XProtect Corporate 2013 и XProtect Expert 2013 либо более новые.



Авторизация имени пользователя (объяснение)

Система позволяет администраторам настраивать пользователей таким образом, что они могут входить в систему, только если это авторизует второй пользователь с достаточным уровнем разрешений. В этом случае XProtect Smart Client или Management Client потребует наличия второй авторизации при входе в систему.

У пользователя, связанного со встроенной ролью **Администраторы**, всегда есть разрешение на авторизацию, и он не обязан вводить данные второй учетной записи, кроме случаев, когда он связан с другой ролью, которой требуются такие данные.

Пользователей, которые входят в систему через внешнего IDP, нельзя настроить так, чтобы применялось требование авторизации вторым пользователем.

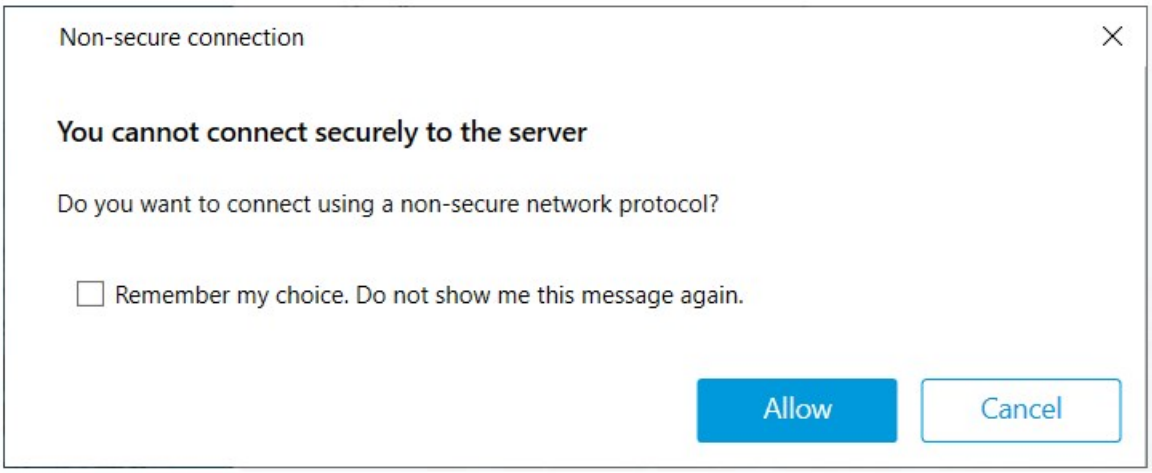
Для связывания авторизации входа в систему с ролью:

- Установите параметр **Требуется авторизация входа в систему** для выбранной роли на вкладке **Сведения** (см. раздел Настройки ролей) в разделе **Роли**, чтобы при входе в систему пользователю требовалась дополнительная авторизация.
- Установите параметр **Авторизовать пользователей** для выбранной роли на вкладке **Общая безопасность** (см. раздел Настройки ролей) в разделе **Роли**, чтобы пользователь мог авторизовать вход в систему других пользователей

Для одного и того же пользователя можно выбрать оба параметра. Это означает, что пользователю потребуется дополнительная авторизация при входе в систему, но при этом он сможет авторизовать вход в систему других пользователей, за исключением своего собственного.

Вход в систему с помощью незащищенного подключения

При входе в Management Client может отобразиться запрос на выполнение входа с использованием незащищенного сетевого протокола.



- Чтобы войти в систему и проигнорировать уведомление, нажмите кнопку **Разрешить**. Чтобы предотвратить повторное отображение уведомления в будущем, выберите пункт **Запомнить выбор. Больше не показывать это сообщение** или выберите раздел **Инструменты** > **Параметры**, а затем — **Разрешить незащищенное подключение к серверу (требуется перезапуск Management Client)**.

Дополнительные сведения о защищенной связи см. в разделе Защищенное соединение (объяснение) на стр. 162.

Изменение пароля базового пользователя

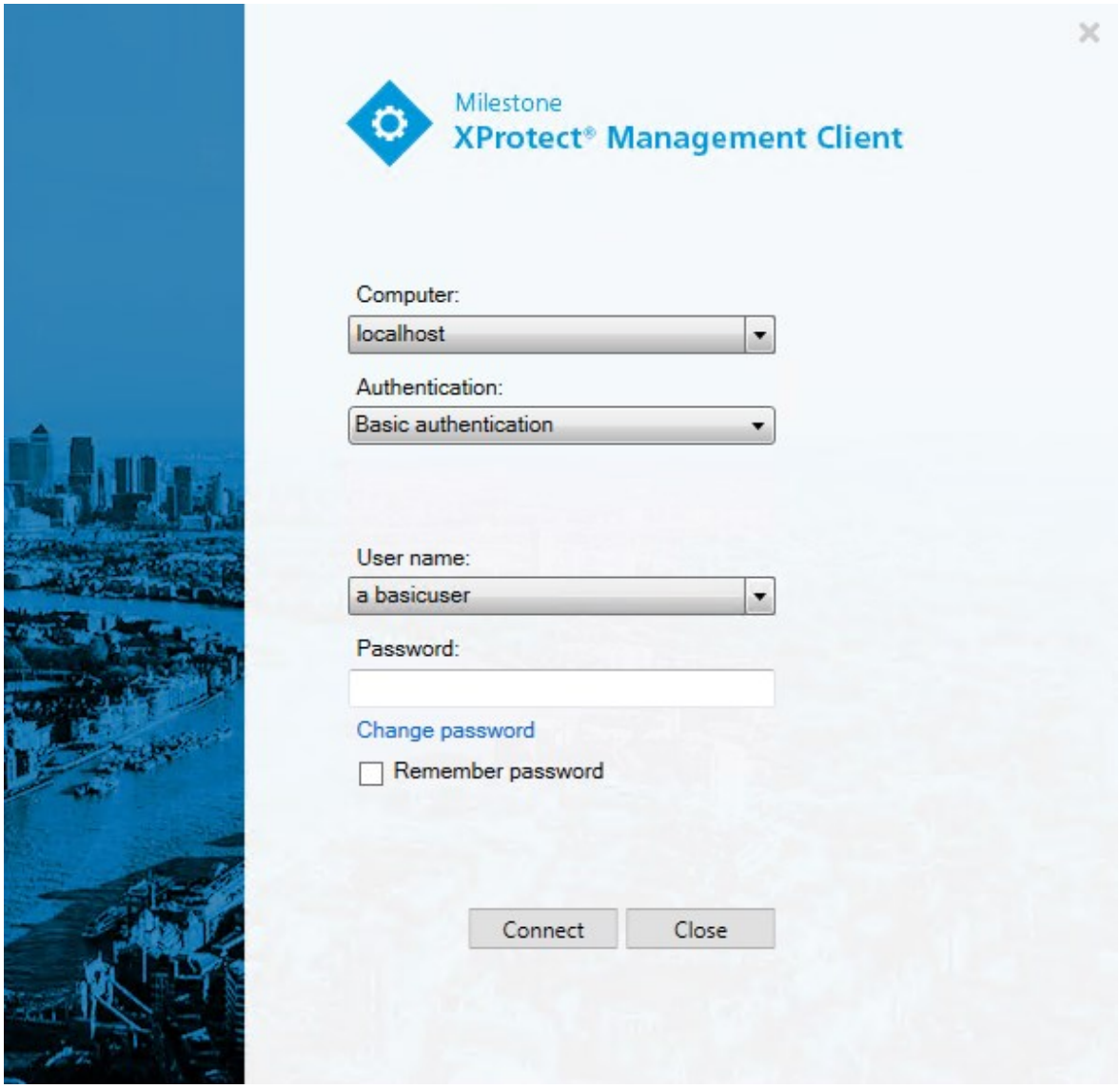
Если вы вошли в систему как **Базовый пользователь**, вы можете изменить свой пароль. С другими методами аутентификации пароль может изменить только администратор. Регулярное изменение пароля повышает степень защиты ПО для управления видео XProtect .

Требования

Требуемая версия ПО для управления видео XProtect — 2021 R1 или более новая.

Действия:

1. Запустите Management Client. Откроется окно входа в систему.
2. Укажите данные для входа в систему. В списке **Аутентификация** выберите **Базовая аутентификация**. Появится ссылка **Изменить пароль**.



3. Нажмите эту ссылку. Откроется окно браузера.
4. Выполните инструкции и сохраните изменения.
5. Теперь входить в Management Client можно по новому паролю.

Обзор продуктов

Продукты VMS XProtect — это программное обеспечение для управления видео, предназначенное для систем всех конфигураций и размеров. XProtect позволяет решать самые разнообразные задачи — от защиты магазинов от вандализма до управления системой с большим количеством объектов и высокими требованиями к безопасности. Эти решения применяются для централизованного управления всеми устройствами, серверами и пользователями и дают возможность использовать чрезвычайно гибкую систему правил, основанную на расписаниях и событиях.

Ваша система состоит из следующих основных компонентов:

- **Сервер управления** — центр системы, состоящий из нескольких серверов
- Один или несколько **серверов записи**
- Одна или несколько систем **XProtect Management Client**
- **XProtect Download Manager**
- Одна или несколько систем **XProtect® Smart Client**
- При необходимости один или несколько экземпляров **XProtect Web Client** и (или) систем клиента **XProtect Mobile**.

Также в вашей системе имеется полностью интегрированная функция Matrix для распределенного просмотра видео с любой камеры системы наблюдения на любом компьютере с установленной XProtect Smart Client.

Систему можно установить на виртуализированных серверах или на нескольких физических серверах в рамках распределенной схемы. Также см. Распределенная система на стр. 100.

При экспорте видеодоказательств из XProtect Smart Client система также позволяет включить в ее состав автономный XProtect® Smart Client – Player. XProtect Smart Client – Player позволяет получателям видеодоказательств (например, офицерам полиции, внутренним или внешним следователям и другим лицам) выбирать и воспроизводить экспортированные записи без необходимости устанавливать ПО на своих компьютерах.

Благодаря установке самых многофункциональных продуктов (см. раздел Сравнение продуктов на стр. 127) ваша система способна работать с неограниченным количеством камер, серверов и пользователей, которые при необходимости могут быть расположены на нескольких объектах. Ваша система может работать с IPv4 и IPv6.

Компоненты системы

Сервер управления (объяснение)

Сервер управления — это центральный компонент VMS. На нем хранится конфигурация системы наблюдения — в базе данных SQL Server, которая может находиться на SQL Server на сервере управления либо на отдельном SQL Server в сети. Также он отвечает за аутентификацию и разрешения пользователей, систему правил и ряд других задач.

Для повышения производительности системы можно развернуть несколько серверов управления как Milestone Federated Architecture™. Сервер управления работает в качестве службы и обычно устанавливается на выделенном сервере.

Пользователи подключаются к серверу управления при первоначальной аутентификации, а затем прозрачно подключаются к серверам записи для получения доступа к видеозаписям и т. д.

Системы и базы данных SQL Server (объяснение)

Сервер управления, сервер событий, сервер регистрации, XProtect Incident Manager, и Identity Provider сохраняют, среди прочего, конфигурацию системы, сигналы тревоги, события и сообщения регистрации в следующих базах данных SQL Server:

- **Наблюдение: Сервер управления и событий**
- **Surveillance_IDP: IDP**
- **Surveillance_IM: Incident Manager**
- **LogserverV2: LogServer**

Сервер управления и сервер событий используют одну и ту же базу данных SQL Server, тогда как сервер регистрации XProtect Incident Manager, и Identity Provider используют собственные базы данных SQL Server. Местоположение баз данных по умолчанию — `C:\Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA`, где {nn} — версия SQL Server.

Установщик системы включает Microsoft SQL Server Express, представляющий собой бесплатную версию SQL Server.

Для очень крупных систем или систем, выполняющих много входящих и исходящих транзакций с базами данных SQL Server, Milestone рекомендует использовать выпуски SQL Server Microsoft® SQL Server® Standard или Microsoft® SQL Server® Enterprise на выделенном компьютере в сети и на выделенном жестком диске, не используемом для других целей. Установка SQL Server на отдельном диске повышает общую производительность системы.

Чтобы просмотреть список поддерживаемых версий SQL Server, перейдите на страницу https://www.milestonesys.com/systemrequirements/.

Дополнительные сведения о Identity Provider см. в разделе Identity Provider (объяснение) на стр. 73.

Дополнительные сведения о базе данных и ведении журналов XProtect Incident Manager приведены в отдельном руководстве администратора по XProtect Incident Manager.

Сервер записи (объяснение)

Сервер записи отвечает за взаимодействие с сетевыми камерами и видеокодерами, записывая и получая звуковую информацию и видео, а также предоставляя клиентам доступ к звуковой информации и видео как в режиме трансляции, так и в виде записи. Сервер записи также отвечает за взаимодействие с другими продуктами Milestone, подключенными с помощью технологии Milestone Interconnect.

Драйверы устройств

- Сетевые камеры и видеокодеры взаимодействуют при помощи драйвера устройства, специально разработанного для отдельных камер или серии аналогичных устройств от одного производителя.
- Начиная с выпуска 2018 R1 драйверы устройств разделяются на два комплекта драйверов: стандартный комплект драйверов с драйверами более новых версий и комплект драйверов для старых устройств с драйверами старых версий
- Обычный комплект драйверов устанавливается автоматически при установке сервера записи. Впоследствии обновить драйверы можно путем загрузки и установки более новой версии комплекта драйверов
- Установить комплект драйверов для старых устройств можно только в том случае, если в системе установлен обычный комплект драйверов. Драйверы из комплекта драйверов для старых устройств устанавливаются автоматически, если предыдущая версия уже установлена в системе. Этот комплект можно загрузить и установить вручную со страницы загрузки программного обеспечения (https://www.milestonesys.com/downloads/)

Мультимедийная база данных

- Сервер записи хранит полученные звуковые данные и видеоданные в специализированной высокопроизводительной базе медиаданных, оптимизированной для записи и хранения таких данных
- База медиаданных поддерживает различные уникальные функции, например многоэтапное архивирование, снижение качества видео, шифрование, а также добавление цифровой подписи к записям

Система использует серверы записи для записи потоков видеоданных и обмена данными с камерами и другими устройствами. Система наблюдения, как правило, состоит из нескольких серверов записи.

Серверы записи — это компьютеры, на которых установлено ПО Recording Server, настроенные для взаимодействия с сервером управления. Серверы записи отображаются на панели **Обзор**: откройте папку **Серверы** и выберите **Серверы записи**.

Обратная совместимость с версиями сервера записи, предшествующими этой версии сервера управления, ограничена. Вы можете получать доступ к записям на серверах записи со старыми версиями, однако для изменения их конфигурации их версия должна соответствовать этой версии сервера управления. Milestone рекомендует обновить все серверы записи в системе до версии сервера управления.

Сервер записи поддерживает шифрование потоков данных, отправляемых клиентам и службам:

- Включить шифрование для клиентов и серверов на стр. 335
- Просмотр состояния шифрования при подключении к клиентам на стр. 317

Также сервер данных поддерживает шифрование подключения к серверу управления.

- Включить шифрование при передаче на сервер управления и из него на стр. 329

Существует несколько вариантов управления серверами записи:

- Добавление оборудования на стр. 232
- Move hardware на стр. 373
- Удаление всего оборудования с сервера записи на стр. 393
- Удаление сервера записи на стр. 393

При работе службы Recording Server очень важно, чтобы Проводник Windows и другие программы не использовали файлы или папки базы медиаданных, связанные с вашей системой. В противном случае возможен сценарий, в котором сервер записи не сможет переименовать или переместить соответствующие файлы медиаданных. В результате сервер записи может остановиться. Для перезапуска остановленного сервера записи остановите службу Recording Server, закройте программу, использующую соответствующие файлы или папки медиаданных, и перезапустите службу Recording Server.

Мобильный сервер (объяснение)

Мобильный сервер обеспечивает пользователям клиента XProtect Mobile и пользователям XProtect Web Client возможность подключения к системе.

Помимо выполнения функций системного шлюза для этих двух клиентов, мобильный сервер может перекодировать видео, так как исходный видеопоток с камеры во многих случаях слишком «тяжел» для пропускной способности, доступной пользователям клиентов.

Если выполняется установка типа **Распределенная** или **Пользовательская**, Milestone рекомендует устанавливать мобильный сервер на выделенном сервере.

Сервер событий (объяснение)

Сервер событий обрабатывает различные задачи, связанные с событиями, сигналами тревоги и картами, а также, возможно, с интеграцией модулей сторонних производителей при помощи MIP SDK.

События

- Все системные события объединяются на сервере событий, поэтому существует единое место и интерфейс, которые партнеры могут использовать для интеграции на основе системных событий

- Кроме того, сервер событий позволяет третьим сторонам получать доступ к отправке событий в систему при помощи интерфейса типичных событий или событий аналитики.

Сигналы тревоги

- Сервер событий используется для размещения функции отправки сигналов тревоги, логики и состояния сигналов тревоги, а также для управления базой данных сигналов тревоги. База данных сигналов тревоги хранится в той же базе данных SQL Server, которую использует сервер управления.

Messages

- Обработка обмена сообщениями осуществляется сервером событий. Благодаря этому встраиваемые расширения могут отправлять сообщения между такими средами, как XProtect Smart Client, Management Client, сервер событий и автономные службы, в режиме реального времени.

Карты

- Сервер событий используется для размещения карт, которые настраиваются и используются в XProtect Smart Client

MIP SDK

- Наконец, на сервер можно установить разработанные сторонними производителями встраиваемые расширения и использовать возможности доступа к системным событиям

Сервер регистрации (объяснение)

Сервер регистрации хранит все записи журналов системы в базе данных SQL Server. База данных записей журналов может работать на том же SQL Server, что и база данных системных настроек сервера управления, либо на отдельном SQL Server. Как правило, сервер регистрации устанавливается на том же сервере, что и сервер управления. При этом он может быть установлен на отдельном сервере с целью повышения производительности и сервера управления, и сервера регистрации.

API Gateway (объяснение)

MIP VMS API представляет собой унифицированный RESTful API на базе стандартных отраслевых протоколов, таких как OpenAPI, и предназначен для обеспечения доступа к функциям VMS XProtect, упрощения процесса интеграции проектов и использования в качестве основы для облачных коммуникаций.

XProtect VMS API Gateway обеспечивает возможности интеграции через Milestone Integration Platform VMS API (MIP VMS API).

API Gateway устанавливается локально и выполняет функции внешнего интерфейса и общей точки входа для служб RESTful API и WebSocket Messaging API для всех текущих компонентов сервера VMS (сервер управления, сервер событий, серверы записи, сервер регистрации и т.д.). Службу API Gateway можно установить на тот же хост, где находится сервер управления, или отдельно. Кроме того, можно установить несколько экземпляров (каждый на отдельном хосте).

RESTful API частично реализуется каждым отдельным компонентом сервера VMS, и API Gateway может просто передавать эти запросы и ответы. Что касается других запросов, API Gateway будет преобразовывать запросы и ответы соответствующим образом.

На данный момент API конфигурации, размещаемый на сервере управления, доступен как RESTful API. Также доступны RESTful API событий, API сообщений WebSockets и RESTful API сигналов тревоги, размещенные на сервере событий.

Дополнительные сведения приведены в API Gatewayруководстве администратора и в справочной документации Milestone Integration Platform VMS API.

Резерв

Сервер управления для обработки отказа

Сервер управления — это центральный компонент VMS. На нем хранится конфигурация системы наблюдения — в базе данных SQL Server, которая может находиться на SQL Server на сервере управления либо на отдельном SQL Server в сети. Также он отвечает за аутентификацию и разрешения пользователей, систему правил и ряд других задач.

Чтобы свести к минимуму время простоя системы, можно настроить сервер управления для отработки отказа, установив сервер управления в кластер. Таким образом, кластер гарантирует, что в случае отказа одного сервера управления его функции возьмет на себя другой компьютер.

Вы можете установить сервер управления в кластер, используя:

XProtect Management Server Failover

XProtect Management Server Failover — это расширение VMS XProtect, которое может помочь вам в следующих случаях:

- Сбой сервера — вы можете запустить компоненты системы с другого компьютера и заняться решением проблемы.
- Вам необходимо установить системные обновления и исправления безопасности — установка исправлений безопасности на автономном сервере управления может занять много времени и привести к длительным простоям в работе. Отказоустойчивый кластер позволяет применять обновления системы и исправления безопасности с минимальным временем простоя.
- Вам необходимо стабильное соединение — пользователи имеют постоянный доступ к видео в режимах наблюдения и воспроизведения, а также к настройкам системы.

Для настройки XProtect Management Server Failover необходимо установить сервер управления, сервер регистрации и сервер событий, работающие на двух компьютерах. Если первый компьютер перестанет работать, компоненты VMS начнут работать на втором компьютере. Кроме того, вы можете воспользоваться преимуществами безопасной репликации баз данных VMS в режиме реального времени, когда SQL Server работает в отказоустойчивом кластере.

Дополнительные сведения см. в руководстве администратора XProtect Management Server Failover.

Отказоустойчивый кластер Windows Server (WSFC)

Отказоустойчивый кластер Windows Server (WSFC) — это группа независимых серверов, которые работают вместе, чтобы повысить доступность приложений и сервисов. В случае сбоя узла или службы кластера службы, размещенные на этом узле, можно автоматически или вручную перенести на другой доступный узел.

Сервер управления можно установить на несколько серверов в кластере серверов. Благодаря этому можно максимально сократить время простоя системы. Если один из серверов кластера выходит из строя, другой сервер кластера автоматически берет на себя функции сервера управления.

В системе наблюдения может быть только один активный сервер управления, при этом другие серверы управления могут быть настроены как резервные.

По умолчанию служба Management Server ограничивает количество отказов до двух раз в течение шести часов. Если это значение превышено, службы Management Server не будут автоматически запускаться с помощью службы кластеризации. Это значение можно изменить в соответствии со вашими потребностями.

Дополнительные сведения см. в руководстве по отказоустойчивости кластеров.

Сервер записи обработки отказа (объяснение)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Сервер записи обработки отказа — это дополнительный сервер записи, который берет на себя функции стандартного сервера записи, если тот становится недоступным. Для сервера записи обработки отказа можно настроить два режима: **сервер холодного резерва** или **сервер горячей замены**.

Серверы записи обработки отказа устанавливаются так же, как и стандартные серверы записи (см. Установка сервера записи обработки отказа с помощью Download Manager на стр. 189). После установки серверов записи обработки отказа они отображаются в Management Client. Milestone рекомендует устанавливать серверы записи обработки отказа на отдельных компьютерах. Убедитесь, что для серверов записи обработки отказа настроен правильный IP-адрес/имя хоста сервера управления. Разрешения пользователя для учетной записи пользователя, от имени которой выполняется служба сервера отказоустойчивости, предоставляются в процессе установки. Они включают:

- разрешения на запуск/останов для сервера записи обработки отказа;
- разрешения доступа на чтение и запись для файла RecorderConfig.xml.

Если для шифрование выбран сертификат, администратор должен предоставить пользователю резервного сервера разрешение на доступ для чтения для выбранного закрытого ключа сертификата.

Если сервер записи обработки отказа берет на себя функции сервера записи, в котором применяется шифрование, Milestone рекомендует также подготовить сервер записи обработки отказа для использования шифрования. Дополнительные сведения приведены в разделах Защищенное соединение (объяснение) на стр. 162 и Установка сервера записи обработки отказа с помощью Download Manager на стр. 189.

Вы можете указать, какой тип обработки отказа требуется на уровне устройства. Для каждого устройства на сервере записи выберите тип поддержки: «полная», «только при прямой передаче» или «без обработки отказа». Это поможет определить приоритетность ресурсов обработки отказа и, например, настроить обработку отказа только для видео, но не для звуковой информации, или обработку отказа только для самых важных, а не для всех, камер.

Когда система работает в режиме обработки отказа, нельзя заменять или перемещать оборудование, обновлять сервер записи или вносить изменения в конфигурации устройств, включая параметры хранения или видеопотоков.

Сервер записи обработки отказа в режиме холодной замены

В конфигурации холодной замены сервера записи обработки отказа можно объединять несколько серверов записи обработки отказа в группу отказоустойчивых серверов. Вся группа отказоустойчивых серверов будет принимать на себя функции любого из нескольких предварительно выбранных серверов записи, если один их них станет недоступен. Количество создаваемых групп не ограничено (см. Объединение серверов записи обработки отказа в группу холодной замены на стр. 230).

Группирование имеет четкое преимущество: когда вам впоследствии потребуется указать, какие серверы записи обработки отказа должны принимать на себя функции сервера записи, можно выбрать группу таких серверов. Если в выбранной группе несколько серверов записи обработки отказа, у вас будет несколько таких серверов, готовых принять на себя функции сервера записи, если он станет недоступным. Можно указать дополнительную группу серверов обработки отказа, которая будет принимать на себя функции основной группы, если все серверы записи в основной группе заняты. Сервер записи обработки отказа может одновременно принадлежать только одной группе.

Серверы записи обработки отказа в группе отказоустойчивых серверов упорядочиваются в последовательность. Последовательность определяет порядок, в котором серверы записи обработки отказа будут принимать на себя функции сервера записи. По умолчанию последовательность отражает порядок добавления серверов записи обработки отказа в группу отказоустойчивых серверов: первый добавленный сервер является первым в последовательности. Если необходимо, эти сведения можно изменить.

Серверы записи обработки отказа в режиме горячей замены

В конфигурации сервера записи обработки отказа горячей замены вы назначаете один сервер записи обработки отказа для резервирования только **одного** сервера записи. По этой причине система может поддерживать режим «ожидания» для этого сервера записи обработки отказа, то есть он синхронизируется с правильной/текущей конфигурацией сервера записи, для которого он выделен, и резервирование выполняется гораздо быстрее, чем в конфигурации сервера записи обработки отказа холодной замены. Как упоминалось выше, серверы горячей замены назначаются только одному серверу записи и их нельзя группировать. Серверы обработки отказа, уже входящие в группу отказоустойчивых серверов, нельзя назначить в качестве серверов записи горячей замены.

Проверка сервера записи обработки отказа

Чтобы проверить объединение видеоданных с сервера отказоустойчивости с сервером записи, необходимо сделать сервер записи недоступным, остановив службу сервера записи или завершив работу компьютера этого сервера.

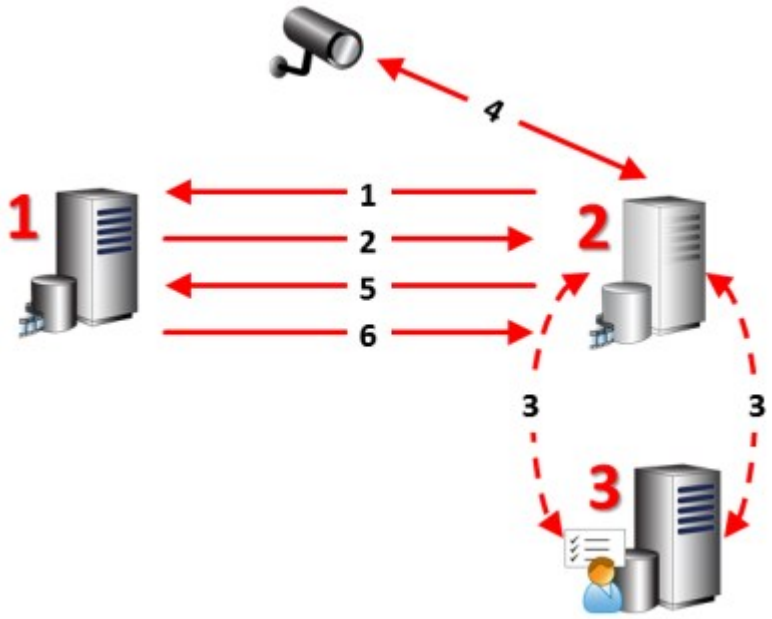
Ручное вмешательство в сеть, такое как отсоединение сетевого кабеля или блокировка сети с помощью инструмента тестирования, недопустимо.

Функции сервера записи обработки отказа (объяснение)

- Серверы записи обработки отказа проверяет состояние соответствующих серверов записи каждые 0,5 с. Если сервер записи не отвечает в течение 2 секунд, он считается недоступным. В этом случае его заменяет сервер записи обработки отказа.
- Сервер записи обработки отказа в режиме холодной замены заменяет недоступный сервер записи в течение пяти секунд плюс время, необходимое для запуска службы Recording Server сервера записи и подключения к камерам. Сервер записи обработки отказа в режиме горячей замены срабатывает быстрее, поскольку служба Recording Server уже запущена с правильной конфигурацией и ей достаточно запустить камеры для передачи данных. Во время запуска нельзя сохранять записи и просматривать видео в реальном времени с задействованных камер.
- При возобновлении доступа к серверу записи он автоматически заменяет сервер записи обработки отказа. Записи, хранящиеся на сервере записи обработки отказа, автоматически объединяются с базами данных сервера записи. Время, необходимое для объединения, зависит от количества записей, пропускной способности сети и других факторов. Во время объединения данных нельзя просматривать записи за период, в течение которого функционировал сервер записи обработка отказа.

- Если сервер записи обработки отказа должен взять на себя функции другого сервер записи во время объединения данных в режиме холодной замены, объединение данных с сервером записи А откладывается и происходит переход на сервер записи Б. При возобновлении доступа к серверу записи Б сервер записи обработки отказа возобновляет процесс объединения. При этом объединение записей происходит одновременно на сервере записи А и сервере записи Б.
- Сервер горячей замены не может заменить дополнительный сервер записи, поскольку он может работать в режиме горячей замены только для одного сервера записи. Однако если сервер записи снова станет недоступным, его снова заменит сервер горячей замены, при этом сохранятся записи за предыдущий период. Сервер записи хранит данные до тех пор, пока они не будут объединены с основным устройством записи или пока на сервере записи обработки отказа не закончится свободное место.
- Решение по обработке отказа не обеспечивает полного резервирования. Его можно использовать только как надежный способ минимизировать время простоя. Если сервер записи снова становится доступным, служба Failover Server проверяет его готовность к хранению записей. Только после этого сервер записи может снова отвечать за хранение записей. Таким образом потеря записей на этом этапе весьма маловероятна.
- Для пользователей клиента процесс перехода на сервер записи обработки отказа практически незаметен. Возможно непродолжительное прерывание соединения. Обычно оно длится всего несколько секунд, когда происходит переход на сервер записи обработки отказа. Во время прерывания соединения пользователи не смогут получить доступ к видео с отключенного сервера записи. Пользователи клиента могут возобновить просмотр видео в реальном времени, как только сервер записи обработки отказа приступит к работе. Поскольку последние записи хранятся на сервере записи обработки отказа, пользователи могут воспроизводить записи после того, как запустится сервер записи обработки отказа. Клиенты не могут воспроизводить старые записи, хранящиеся только на недоступном сервере записи, пока этот сервер записи не возобновит работу и не заменит сервер записи обработки отказа. Доступ к архивным записям недоступен. Когда сервер записи возобновляет работу, запускается процесс объединения, в ходе которого записи, сделанные во время отработки отказа, объединяются с базой данных сервера записи. Во время объединения данных нельзя воспроизводить записи за период, в течение которого функционировал сервер записи обработки отказов.
- В режиме холодной замены не требуется настраивать сервер записи обработки отказа в качестве резервного для другого сервера записи обработки отказа. Это связано с тем, что вы назначаете группы отказоустойчивых серверов, а не конкретные серверы записи обработки отказа для замены конкретных серверов записи. Группа отказоустойчивых серверов должна содержать как минимум один сервер записи обработки отказа, при этом можно добавить необходимое количество серверов записи обработки отказа. Если группа отказоустойчивых серверов содержит более одного сервера записи обработки отказа, несколько серверов записи обработки отказа могут заменить недоступный сервер.
- В режиме горячей замены нельзя настроить серверы записи обработки отказа или серверы горячей замены в качестве резерва для сервера горячей замены.

Этапы обработки отказа (объяснение)



Описание
Задействованные серверы (номера выделены красным): 1. Recording Server 2. Failover Recording Server 3. Management Server
Порядок обработки отказа в режиме **холодной замены**: 1. Сервер записи обработки отказа устанавливает непрерывное TCP-соединение с сервером записи, что позволяет контролировать функционирование сервера записи. 2. Соединение прервано. 3. Сервер записи обработки отказа запрашивает текущую конфигурацию сервера записи у сервера управления. Сервер управления передает запрошенную конфигурацию, сервер записи обработки отказа принимает информацию, активируется и берет на себя функции сервера записи.

Описание
4. Сервер записи обработки отказа и соответствующие камеры обмениваются видеоданными. 5. Сервер записи обработки отказа продолжает попытки восстановить соединение с сервером записи. 6. Сервер записи обработки отказа отключается после восстановления соединения с сервером записи. Сервер записи получает видеоданные (если таковые имеются), записанные во время простоя. Эти видеоданные добавляются в базу данных сервера записи.
Порядок обработки отказа в режиме **горячей замены**: 1. Сервер горячей замены устанавливает непрерывное TCP-соединение с сервером записи, что позволяет контролировать функционирование назначенного ему сервера записи. 2. Соединение прервано. 3. Сервер горячей замены получает информацию о текущей конфигурации назначенного сервера записи от сервера управления и начинает запись вместо него. 4. Сервер горячей замены и соответствующие камеры обмениваются видеоданными. 5. Сервер горячей замены продолжает попытки восстановить соединение с сервером записи. 6. Сервер горячей замены возвращается в режим горячей замены после восстановления соединения с сервером записи. Сервер записи получает видеоданные (если таковые имеются), записанные во время простоя. Эти видеоданные добавляются в базу данных сервера записи.

Службы Failover Recording Server (объяснение)

На сервере записи обработки отказа устанавливаются две службы:

- Служба Failover Server, которая управляет процессами передачи функций сервера записи. Эта служба постоянно работает и контролирует состояние соответствующих серверов записи.
- Служба Failover Recording Server, которая обеспечивает работу сервера записи обработки отказа в качестве сервера записи.

  В режиме холодной замены служба запускается лишь при необходимости, то есть когда сервер записи обработки отказа, работающий в режиме холодной замены, выполняет функции сервера записи. Запуск этой службы обычно занимает пару секунд. В зависимости от локальных настроек безопасности и других факторов запуск может занять больше времени.
  В режиме горячей замены служба работает постоянно, благодаря чему сервер горячей замены срабатывает быстрее, чем сервер записи обработки отказа в режиме холодной замены.

Клиенты

Management Client (объяснение)

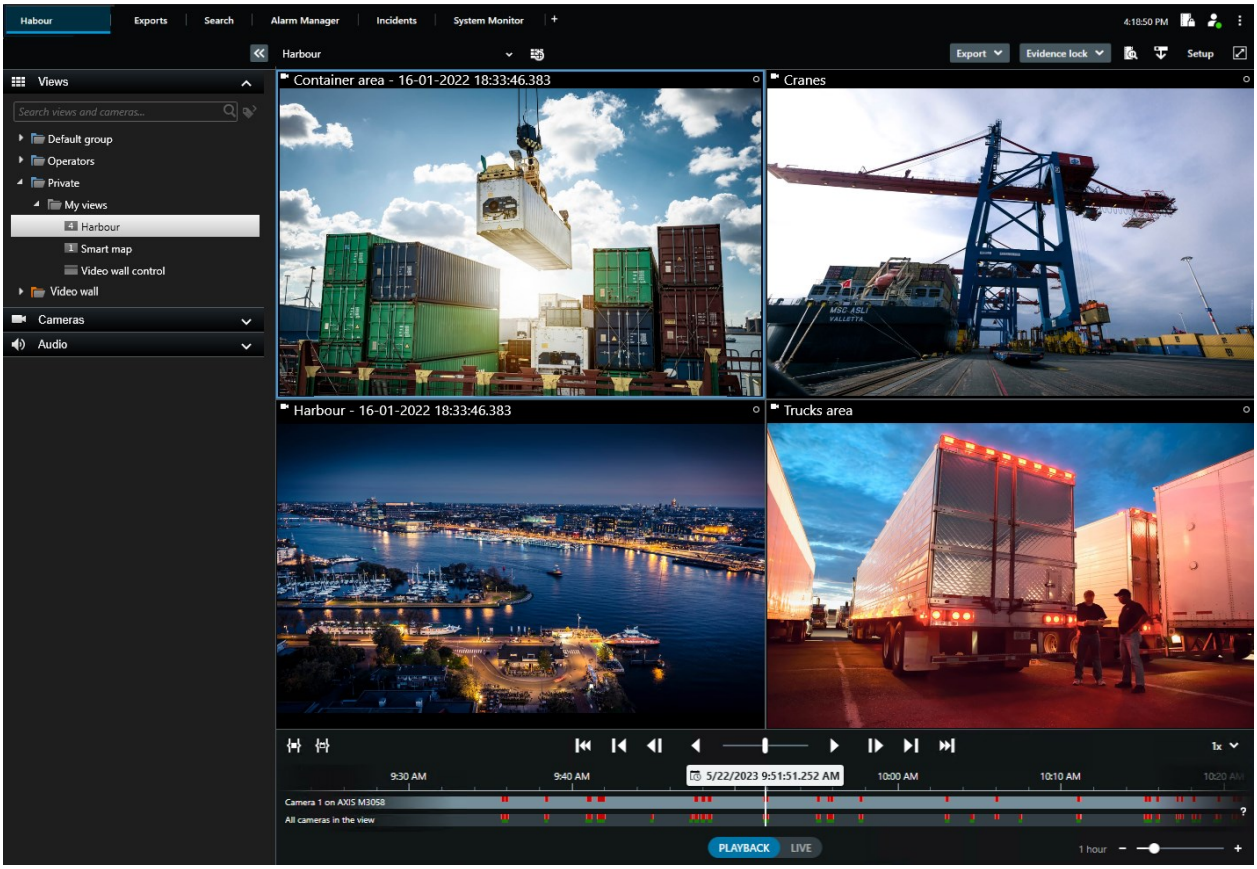
Management Client — это многофункциональный клиент администрирования для повседневного управления системой и ее настройки. Он доступен на нескольких языках.

Его обычно устанавливают на рабочей станции администратора системы наблюдения или на аналогичной рабочей станции.

XProtect Smart Client (объяснение)

XProtect Smart Client — это традиционное приложение для ПК, помогающее в управлении IP-камерами видеонаблюдения. Оно обеспечивает интуитивное управление установками системы безопасности, предоставляя пользователям доступ к видео в реальном времени и записи, мгновенное управление камерами и подключенными устройствами безопасности, а также возможность осуществлять расширенный поиск записей и метаданных.

XProtect Smart Client предлагает настраиваемый пользовательский интерфейс, который можно оптимизировать для задач отдельных операторов и адаптировать к пользователям с разным уровнем подготовки и полномочий.



Интерфейс можно приспособить к условиям работы, выбрав светлую или темную тему оформления. В нем предусмотрены вкладки, оптимизированные для работы, и основная шкала времени для максимального удобства наблюдения.

С помощью MIP SDK можно интегрировать разные типы систем безопасности, бизнес-систем и приложений для видеоаналитики, для управления которыми используется XProtect Smart Client.

XProtect Smart Client должен быть установлен на компьютерах операторов. Администраторы системы наблюдения управляют доступом к системе с помощью Management Client. Записи, которые просматривают клиенты, предоставляются системой XProtect через службу Image Server. Эта служба работает в фоновом режиме на сервере системы управления. Дополнительное аппаратное обеспечение не требуется.

Клиент XProtect Mobile (объяснение)

Клиент XProtect Mobile — это мобильное решение для наблюдения, тесно связанное с остальными компонентами системы XProtect. Он работает на планшете или смартфоне под управлением Android либо на планшете, смартфоне или портативном аудиоплееере производства Apple® и предоставляет доступ к камерам, представлениям и другим функциям, настроенным в клиентах управления.

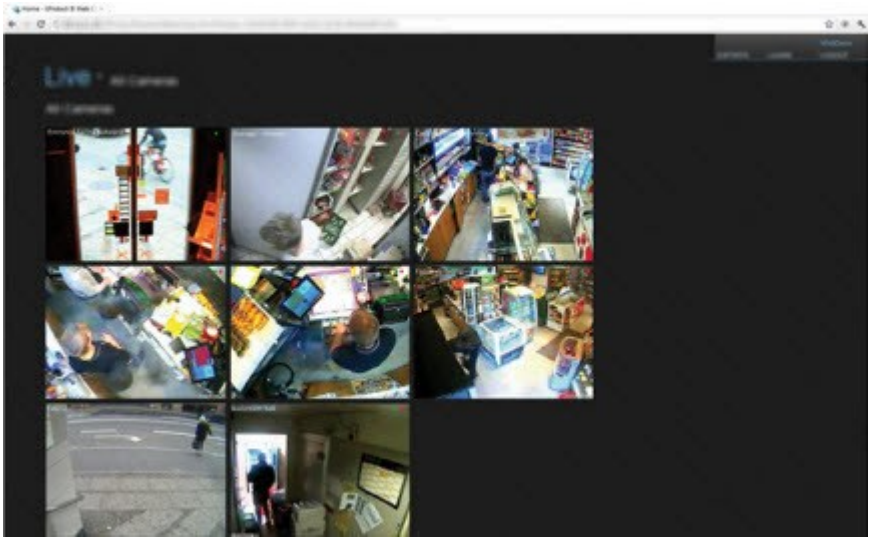
Клиент XProtect Mobile можно использовать для просмотра и воспроизведения видео в режиме трансляции и записанного видео с одной или нескольких камер, управления PTZ-камерами (поворотными камерами с трансфокатором), активации устройств вывода и событий, а также использования функции Video Push для отправки видео с устройства в систему XProtect.

Если вы хотите использовать клиент XProtect Mobile с системой, необходимо иметь сервер XProtect Mobile для установки соединения между клиентом XProtect Mobile и системой. После настройки сервера XProtect Mobile загрузите бесплатный клиент XProtect Mobile из Google Play или App Store и начните использовать XProtect Mobile.

Для того, чтобы передавать видео в систему XProtect, необходимо иметь одну лицензию на устройство.

XProtect Web Client (объяснение)

XProtect Web Client — это веб-клиент для просмотра и воспроизведения видео, а также обмена видео. Он обеспечивает мгновенный доступ к наиболее часто используемым функциям наблюдения, например просмотру видео в режиме реального времени, воспроизведению записанного видео, печати и экспорта доказательств. Доступ к функциям зависит от конкретных пользовательских разрешений, которые задаются в Management Client.



Для предоставления доступа к XProtect Web Client необходимо иметь сервер XProtect Mobile, обеспечивающий подключение XProtect Web Client к вашей системе. Сам по себе XProtect Web Client не требует установки и работает в большинстве веб-браузеров. После настройки сервера XProtect Mobile можно осуществлять мониторинг системы XProtect из любого места с помощью компьютера или планшета с доступом в Интернет (при условии, что вы знаете правильный внешний адрес/Интернет-адрес, имя пользователя и пароль).

Расширения XProtect

Про расширения XProtect

Milestone разработала различные расширения. Расширения — это продукты, которые расширяют функциональность ПО для управления видео XProtect дополнительными специализированными возможностями.

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

XProtect Access

Для использования XProtect Access необходимо приобрести базовую лицензию, разрешающую доступ к этой функции в системе XProtect. Также необходимо получить лицензию управления доступом для каждой двери, которую вы хотите контролировать.

Возможно использование XProtect Access в системах управления доступом со специализированным модулем XProtect Access.

Функция интеграции управления доступом включает новые возможности, упрощающие интеграцию систем контроля доступа клиентов с XProtect. Преимущества для вас:

- Общий интерфейс оператора для нескольких систем управления доступом в XProtect Smart Client
- Более быстрая и эффективная интеграция систем управления доступом
- Более широкий набор функций для оператора (см. ниже)

Преимущества XProtect Smart Client для оператора:

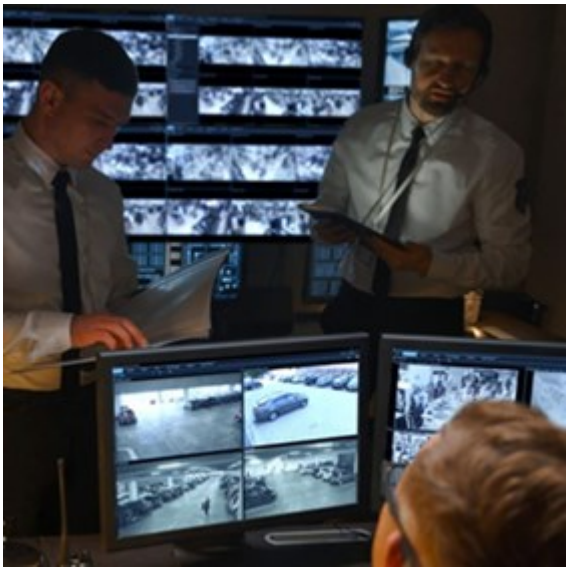
- Мониторинг событий и точек доступа в режиме реального времени
- Передача запросов доступа с помощью оператора
- Интеграция карт
- Определение тревог для событий управления доступом
- Анализ событий в точка доступа
- Централизованный обзор и управление состояниями дверей
- Информация о владельцах карт и управление ими

В **контрольном журнале** регистрируются команды, выполняемые каждым пользователем в системе управления доступом из XProtect Smart Client.

Прежде чем вы сможете запустить интеграцию, помимо базовой лицензии XProtect Access необходимо установить встраиваемое расширение интеграции конкретного поставщика на сервере событий.

XProtect Incident Manager

XProtect Incident Manager является расширением, которое позволяет организациям документировать инциденты в сочетании с доказательствами эпизодов (видео и, возможно, аудио) из VMS XProtect.



Пользователи XProtect Incident Manager могут сохранять всю информацию инцидентов в проектах с инцидентами. Из проектов с инцидентами они могут отслеживать статус и действия в каждом инциденте. Таким образом, пользователи могут эффективно управлять инцидентами и передавать убедительные доказательства инцидентов, как коллегам внутри компании, так и органам власти за пределами компании.

XProtect Incident Manager помогает организациям получить общее представление инцидентам в исследуемой области. Это знание позволяет организациям принимать меры по предотвращению аналогичных инцидентов в будущем.

В XProtect Management Client администраторы VMS XProtect организации могут определять доступные свойства инцидентов в XProtect Incident Manager согласно потребностям организации. Операторы XProtect Smart Client инициируют, сохраняют и управляют проектами с инцидентами и добавляют различную информацию в них. Она включает в себя произвольный текст, свойства инцидента, определенные администраторами, и эпизоды из VMS XProtect. Для полной отслеживаемости VMS XProtect записывает в журналы, когда администраторы определяют и редактируют свойства инцидентов, а также когда операторы создают и обновляют проекты с инцидентами.

XProtect LPR

XProtect LPR включает функции анализа контента на основе видео (VCA) и распознавания номерных знаков автомобилей, которые взаимодействуют с системой наблюдения и XProtect Smart Client.

Для считывания символов на номерном знаке XProtect LPR использует систему оптического распознавания символов на изображениях, для настройки которой используются специальные параметры камеры.

Функцию распознавания номерного знака (LPR) можно дополнить собственными функциями наблюдения, такими как запись и активация вывода на основе событий.

Примеры событий в XProtect LPR:

- Активация записей системы наблюдения определенного качества
- Активация сигналов тревоги
- Сопоставление с положительными и отрицательными списками соответствия
- Открытие ворот
- Включение фар
- Передача видео инцидентов на экраны компьютеров конкретных сотрудников отдела безопасности
- Отправка текстовых сообщений на мобильные телефоны

Используя событие, можно активировать сигналы тревоги в XProtect Smart Client.

XProtect Smart Wall

XProtect Smart Wall — это дополнительное расширение, позволяющее создавать видеостены, соответствующие особым требованиям к безопасности. XProtect Smart Wall обеспечивает обзор всех видеоданных в системе XProtect VMS[1] и поддерживает любые сочетания мониторов.

[1]Система управления видео (Video Management Software).

XProtect Smart Wall позволяет операторам просматривать статические видеостены в соответствии с настройками системного администратора; используются фиксированный набор камер и макет мониторов. Однако видеостена также управляется операторами в том смысле, что операторы могут контролировать то, что отображается на видеостене. Сюда входят:

- Перемещение на видеостену камер и содержимого других типов, например изображений, текста, сигналов тревоги и интеллектуальных карт
- Отправка полных представлений на мониторы.
- В случае определенных событий применяются альтернативные препозиции[1]

Наконец, с помощью правил можно осуществлять автоматическое изменение препозиций на основе определенных событий или расписаний.

XProtect Transact

XProtect Transact — это расширение к решениям IP–видеонаблюдения Milestone, позволяющее наблюдать за текущими транзакциями и изучать завершенные транзакции. Транзакции связаны с цифровой системой видеонаблюдения, отслеживающей транзакции, например, чтобы помочь доказать факт мошенничества или предъявить доказательства, изобличающие преступника. Между строками транзакций и видеоизображениями предусмотрена связь один к одному.

[1]Предварительно заданный макет для одного или нескольких мониторов Smart Wall в XProtect Smart Client. Препозиции определяют, какие камеры будут показаны и какой будет структура содержимого на каждом мониторе видеостены.

Данные транзакций могут поступать из различных источников, например, из пунктов продажи (POS) или банкоматов (ATM). При выборе линии транзакций в области просмотра будут показаны стоп-кадры со всех камер, что даст вам возможность просмотреть записи. Под областью просмотра будет показана транзакция, связанная с выбранной линией.

XProtect Management Server Failover

Если на автономном компьютере, на котором запущен сервер управления или SQL Server, произошел сбой оборудования, это не повлияет на записи или сервер записи. Тем не менее, сбои оборудования могут привести к простою в работе операторов и администраторов, не вошедших в клиенты.

XProtect Management Server Failover — это расширение VMS XProtect, которое может помочь вам в следующих случаях:

- Сбой сервера — вы можете запустить компоненты системы с другого компьютера и заняться решением проблемы.
- Вам необходимо установить системные обновления и исправления безопасности — установка исправлений безопасности на автономном сервере управления может занять много времени и привести к длительным простоям в работе. Отказоустойчивый кластер позволяет применять обновления системы и исправления безопасности с минимальным временем простоя.
- Вам необходимо стабильное соединение — пользователи имеют постоянный доступ к видео в режимах наблюдения и воспроизведения, а также к настройкам системы.

Для настройки XProtect Management Server Failover необходимо установить сервер управления, сервер регистрации и сервер событий, работающие на двух компьютерах. Если первый компьютер перестанет работать, компоненты VMS начнут работать на втором компьютере. Кроме того, вы можете воспользоваться преимуществами безопасной репликации баз данных VMS в режиме реального времени, когда SQL Server работает в отказоустойчивом кластере.

XProtect Hospital Assist

XProtect Hospital Assist создано специально для отделений больниц, занимающихся лечением пациентов, которые нуждаются в круглосуточном или ситуативном наблюдении.

Расширение VMS XProtect — это специальное решение для удаленного наблюдения за пациентами, которое позволяет больнице:

- Повысить эффективность работы персонала.
- Оперативно реагировать на инциденты.
- Обеспечивать высококачественный уход за пациентами.

С помощью этого расширения XProtect пользователи XProtect Smart Client могут:

- Добавить записку к изображениям с камеры с помощью функции «Записка».
- Размыть видеопоток в режиме реального времени с помощью функции «Размытие для маскировки».
- Получить сигнал тревоги при падении пациента с помощью функции «Обнаружение падений».
- Прослушивать несколько помещений и общаться с пациентом удаленно с помощью функции «Аудио мультирум».

Husky IVO System Health

Husky IVO System Health помогает получить быстрый обзор общего состояния всех устройств Husky IVO, которые вы специально подключили к серверу управления XProtect, чтобы сообщить данные о состоянии системы.

Данные о состоянии системы для устройств Husky IVO, которые не были подключены к серверу управления XProtect специально для отправки данных о состоянии системы, отображаться не будут.

Статус подключенных устройств Husky IVO отображается в узле Husky IVO System Health в XProtect Management Client. Husky IVO System Health отображает только данные о состоянии системы от устройств Husky IVO.

Требуется установка встраиваемого расширения

Узел Husky IVO System Health доступен только после установки встраиваемого расширения Husky IVO System Health на сервер управления XProtect.

Бета-версия

Husky IVO System Health в настоящее время доступно как бета-версия. Внешний вид и функции окончательной версии могут отличаться от бета-версии.

Индикаторы состояния системы

Общие индикаторы состояния, отображаемые в узле обзора Husky IVO System Health:

- **Все в порядке**: Нет никаких обнаруженных проблем, о которых нужно сообщить.
- **Требует проверки**: Обнаружена одна или несколько проблем, требующих проверки.
- **Отсутствуют данные**: Невозможно сообщить о статусе из-за недостаточности данных.

Проверьте состояние системы конкретного устройства

Также могут быть отображены данные о состоянии системы конкретных устройств Husky IVO. Выберите имя устройства в узле обзора состояния системы, чтобы открыть новую страницу, на которой отображается ключевая статистика состояния системы для этого устройства.

Данные о состоянии системы для отдельных устройств обычно отображают следующие ключевые показания состояния:

- **Состояние хранилища данных**: Состояние хранилища машины, а также выбранный вариант управления хранилищем.
- **Использование ОП**: Общий объем оперативной памяти в ГБ, а также текущий объем свободной оперативной памяти в ГБ.
- **Нагрузка на ЦП**: Текущая нагрузка на ЦП, измеряемая в процентах от максимальной теоретической нагрузки.
- **Температура ЦП**: Температура процессора в градусах Цельсия и Фаренгейта.
- **Сеть**: Статус онлайн/офлайн всех зарегистрированных слотов сетевых карт в устройстве.

Некоторые данные о состоянии системы зависят от аппаратного обеспечения устройства, например, данные источника питания отображаются для устройств, которые имеют варианты двойного (резервного) питания, а данные о нагрузке на графический процессор и его температуре отображаются для устройств, которые имеют дискретные карты графического процессора.

Подключение к состоянию системы Husky

Каждое устройство Husky IVO необходимо вручную подключить к клиенту управления с помощью локального программного обеспечения Husky Assistant.

К узлу Husky IVO System Health можно подключать следующие версии Husky IVO:

• Milestone Husky IVO 150D, версия 2 или более поздняя

• Milestone Husky IVO 350T, версия 3 или более поздняя

• Milestone Husky IVO 350R или более поздняя

• Milestone Husky IVO 700R, версия 2 или более поздняя

• Milestone Husky IVO 1000R, версия 2 или более поздняя

• Milestone Husky IVO 1800R или более поздняя

Поскольку процесс подключения к состоянию системы запускается на странице **Состояние системы** в Husky Assistant, возможно, вам придется обновить Husky Assistant на отдельных устройствах Husky IVO до последней версии, чтобы получить доступ к странице **Состояние системы**.

Невозможно выполнить массовое или автоматическое подключение нескольких машин Husky IVO для отправки данных о состоянии системы на сервер управления XProtect.

Чтобы подключить устройство Husky IVO, необходимо нажать кнопку **Подключить** на странице **Состояние системы** в Husky Assistant на устройстве Husky IVO и указать адрес машины клиента управления, а также учетные данные администратора.

Устранение неполадок Husky IVO

Вы не можете устранять неполадки или исправлять проблемы с устройством Husky IVO, о которых сообщается, с сервера управления XProtect. Вместо этого вам необходимо напрямую получить доступ к рассматриваемым устройствам для устранения каких-либо последствий или неполадок.

Устройства

Оборудование (объяснение)

Оборудование — это:

- Физический модуль, напрямую подключенный к серверу записи системы наблюдения по протоколу IP (например, камера, видеокодер, модуль ввода/вывода)
- Сервер записи на удаленном объекте в схеме Milestone Interconnect

В системе предусмотрено несколько способов добавления оборудования на серверы записи.

> Если оборудование находится за маршрутизатором с поддержкой NAT или брандмауэром, может потребоваться указать другой номер порта и настроить на маршрутизаторе/брандамауэре сопоставление порта и IP-адреса, используемого оборудованием.

Мастер **добавления оборудования** обнаруживает оборудование, такое как камеры и видеокодеры, в сети и добавляет его на серверы записи в системе. Этот мастер также помогает добавлять серверы дистанционной записи для конфигураций Milestone Interconnect. Добавлять оборудование можно только на **один сервер записи** за раз.

Предварительная настройка оборудования (объяснение)

Определенные производители требуют, чтобы до первого добавления готового к работе оборудования в программную систему для управления видео в этом оборудовании были заданы учетные данные. Данный процесс называется предварительной настройкой оборудования и выполняется при помощи мастера **Предварительная настройка аппаратных устройств**, который запускается при обнаружении такого оборудования мастером Добавление оборудования на стр. 232.

Важная информация о мастере **Предварительная настройка аппаратных устройств**:

- Оборудование, требующее наличия первоначальных учетных данных до его добавления в программную систему для управления видео, нельзя добавить при помощи стандартных учетных данных, и оно должно быть настроено через мастер или путем прямого подключения к оборудованию
- Применять учетные данные (имя пользователя и пароль) можно только к тем полям, которые помечены как **не задано**
- Изменить учетные данные (имя пользователя и пароль) После того, как **состояние** оборудования изменится на **настроено**, изменить учетные данные (имя пользователя или пароль) будет невозможно
- Предварительная настройка относится к готовому к использованию оборудованию и выполняется только один раз. После предварительной настройки управление оборудованием осуществляется так же, как управление любым другим оборудованием в Management Client
- После закрытия мастера **Предварительная настройка аппаратных устройств** предварительно настроенное оборудования появится в мастере Добавление оборудования на стр. 232 и может быть добавлено в систему

Настоятельно рекомендуется добавить предварительно настроенное оборудование в систему путем запуска мастера Добавление оборудования на стр. 232 после того, как вы закроете мастер **Предварительная настройка аппаратных устройств**. Management Client не сохранит предварительно настроенные учетные записи, если вы не добавите оборудование в систему.

Устройства (объяснение)

В оборудовании имеется ряд устройств, управлять которыми можно по отдельности, например:

- В физической камере имеются устройства, представляющие визуальную часть (объективы), а также микрофоны, динамики, метаданные, ввод и вывод (внешние или встроенные)
- В видеокодере имеется несколько аналоговых камер, отображаемых в одном списке устройств, представляющих визуальную часть (объективы), а также микрофоны, динамики, метаданные, ввод и вывод (внешние или встроенные)
- В модуле ввода/вывода имеются устройства, представляющие вводные и выводные каналы (например, для осветительных приборов)
- В выделенном аудиомодуле имеются устройства, отражающие микрофоны и вводы и выводы динамиков
- В схеме Milestone Interconnect удаленная система отображается как оборудование со всеми устройствами удаленной системы, включенными в один список

При добавлении оборудования система автоматически добавляет его устройства.

Сведения о поддерживаемом оборудовании см. на странице «Поддерживаемое оборудование» на веб-сайте Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/)

В следующих разделах описан каждый из типов добавляемых устройств.

Камеры

Камеры передают в систему видеопотоки, которые можно просматривать в реальном времени и которые система может записывать для воспроизведения в будущем. Разрешения пользователей для просмотра видео определяются ролями.

Микрофоны

На многие устройства можно установить внешние микрофоны. В некоторых устройствах имеются встроенные микрофоны.

Микрофоны передают в систему аудиопотоки, которые можно прослушивать в реальном времени и которые система может записывать для воспроизведения в будущем. Систему можно настроить так, чтобы она получала события микрофона, которые запускают соответствующие действия.

Разрешения пользователей для прослушивания микрофонов определяются ролями. Прослушивать микрофоны из Management Client нельзя.

Динамики

На многие устройства можно установить внешние динамики. В некоторых устройствах имеются встроенные динамики.

Система отправляет аудиопоток на динамики, только когда пользователь нажимает клавишу связи в XProtect Smart Client. Также эту функцию можно использовать из XProtect Web Client и XProtect® Mobile. Аудиосигнал динамика записывается только во время разговора Разрешения пользователей для разговора через динамики определяются ролями. Разговаривать через динамики из Management Client нельзя.

Для одновременного разговора двух пользователей их разрешения для разговора через динамики определяются ролями. При назначении ролей можно установить приоритет динамика в диапазоне от очень высокого до очень низкого. Если одновременно хотят разговаривать два пользователя, это сможет сделать только пользователь, роль которого имеет самый высокий приоритет. Если одновременно хотят разговаривать два пользователя с одной и той же ролью, применяется принцип очереди.

Метаданные

Устройства хранения метаданных передают в систему потоки данных, которые можно использовать для просмотра данных о данных, например данных, описывающих видеоизображение, содержимое объектов на изображении или место, где было записано изображение. Метаданные могут быть связаны с камерами, микрофонами или динамиками.

Метаданные могут формироваться:

- самим устройством, передающим данным, например камерой, передающей видео;
- системой или интеграцией сторонних производителей через универсальный драйвер метаданных.

Создаваемые устройствами метаданные автоматически связываются с одним или несколькими устройствами на одном и том же оборудовании.

Разрешения пользователей для просмотра метаданных определяются ролями.

Вводы

На многих устройствах на входные порты можно установить внешние модули. Модули ввода — это, как правило, внешние датчики. Внешние датчики можно использовать, например, чтобы определить, открыты ли двери, окна или ворота. Входной сигнал из таких внешних модулей ввода обрабатывается системой как события.

Такие события можно использовать в правилах. Например, можно создать правило, согласно которому камера должна начинать запись при активации ввода и останавливать запись через 30 секунд после его деактивации.

Выводы

На многих устройствах на выходные порты можно установить внешние модули. Благодаря этому включать или отключать осветительные приборы, сирены и т. п можно с помощью системы.

Выходы можно использовать при создании правил. Так, можно создавать правила автоматической активации и деактивации выводом, а также правила выполнения действий при изменении состояния вывода.

Группы устройств (объяснение)

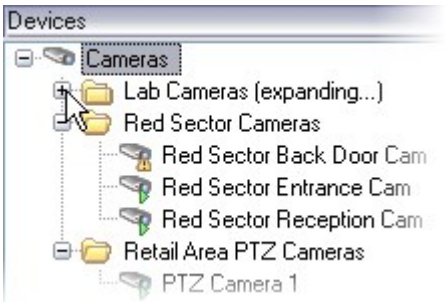
Объединение устройств в группы выполняется во время работы с мастером **Добавить оборудование**, однако группы можно менять и добавлять по мере необходимости.

Вы можете облегчить себе работу путем объединения в группы устройств различных типов (камеры, микрофоны, динамики, метаданные, вводы и выводы), работающие в системе:

- Группы устройств помогают создать четкое представление об устройствах в системе
- Устройство можно включить в несколько групп
- Можно создавать подгруппы, а также подгруппы в подгруппах

- Задать общие свойства для всех устройств в группе можно одним действием
- Свойства устройств, заданные при помощи группы, хранятся не в группе, а на отдельных устройствах
- При работе с ролями можно одним действием задать общие настройки безопасности для всех устройств в группе
- При работе с правилами можно одним действием применить правило ко всем устройствам в группе

Можно добавлять необходимое количество групп устройств, но нельзя смешивать устройства разных типов (например, камеры и динамики) в одной группе.



Для просмотра и изменения всех свойств создавайте группы устройств, состоящие **менее** чем из 400 устройств.

При удалении группы устройств удаляется только сама группа. Для удаления устройства (например, камеры) из систем используйте уровень сервера записи.

В следующих примерах рассмотрено создание групп устройств из камер, но те же принципы применимы ко всем типам устройств

Добавление группы устройств

Указание устройств, которые необходимо включить в группу устройств

Указание общих свойств для всех устройств в группе

Хранилище носителей

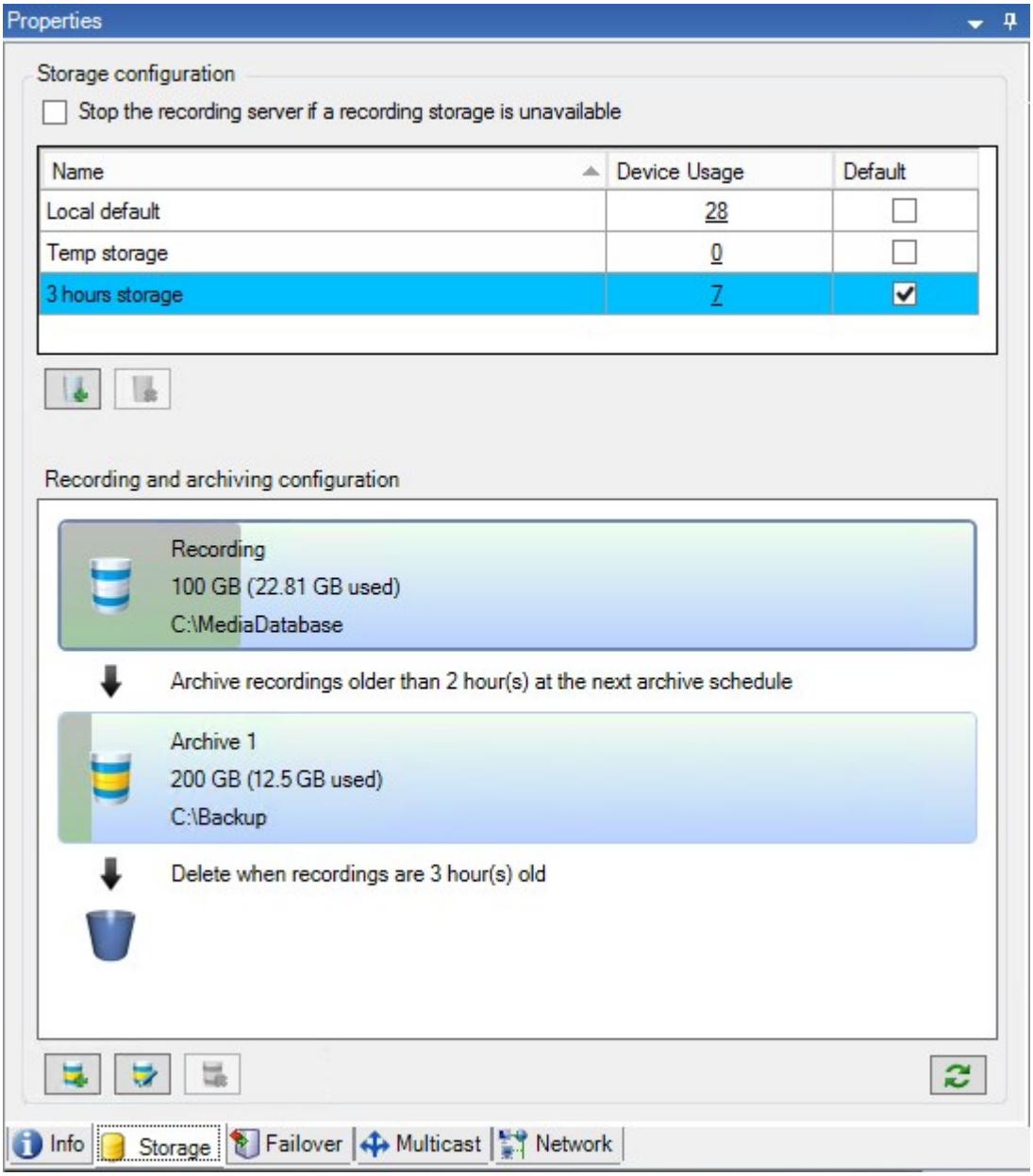
Хранение и архивирование (объяснение)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

На вкладке **Хранение** можно просматривать и настраивать хранилища для выбранного сервера записи и управлять ими.

Текущий объем свободного места в архивах и хранилищах записей отмечается горизонтальной чертой. Вы можете задать поведение сервера записи в ситуациях, когда хранилища записей становятся недоступными. Это особенно актуально, если система включает серверы отказоустойчивости.

Если вы используете функцию **Защита доказательств**, место, занятое материалами защиты доказательств, обозначается вертикальной красной чертой.



Когда камера записывает видео или звуковую информацию, все соответствующие записи по умолчанию помещаются в заданное хранилище. Каждое хранилище состоит из хранилища записей, в котором записи находятся в базе данных записей **Запись**. По умолчанию в хранилище нет архивов, но их можно создать.

Чтобы база данных записей не переполнялась, можно создать дополнительные хранилища (см. раздел Добавление нового хранилища на стр. 216). Также в каждом хранилище можно создать архивы (см. раздел Создание архива в хранилище на стр. 217) и архивировать данные для обеспечения их сохранности.

Архивирование — это автоматический перенос записей (например, из базы данных камеры в другое местоположение). Таким образом, можно хранить любое количество записей, независимо от размера базы данных записей. При архивировании также можно выполнять резервное копирование записей на другой носитель данных.

Настройка хранения и архивирования данных осуществляется на каждом сервере записи.

Если архивированные записи хранятся локально или на доступных сетевых дисках, для их просмотра можно использовать XProtect Smart Client.

Если диск выходит из строя, а хранилище записей становится недоступным, горизонтальная полоска окрашивается в красный цвет. В XProtect Smart Client можно по-прежнему просматривать видео в режиме реального времени, однако запись и архивирование останавливаются до восстановления диска. Если система настроена на использование серверов записи обработки отказа, можно указать, что сервер записи должен прекратить работу, чтобы серверы отказоустойчивости взяли на себя его функции (см. раздел Указание действий, выполняемых при недоступности хранилища записей на стр. 215).

В приведенной ниже информации преимущественно рассмотрены камеры и видеоданные, но при этом она относится и к микрофонам и звуковой информации.

В целях повышения производительности дисков Milestone рекомендует использовать выделенный жесткий диск для хранилищ и архивов записей. При форматировании жесткого диска важно изменить **Размер кластера** с 4 килобайт на 64 килобайта. Это значительно повысит производительность диска при операциях записи. На веб-сайте Microsoft (https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95) можно получить дополнительные сведения о размерах кластера диска, а также найти справочную информацию.

Самые старые данные в базе данных всегда автоматически архивируются (или удаляются, если не задан следующий архив), когда остается менее 5 ГБ свободного пространства. Если остается менее 1 ГБ свободного места, данные удаляются. Базе данных всегда требуется 250 МБ свободного пространства. Если вы достигли этого лимита, потому что данные не удаляются достаточно быстро, попытки записи в базу данных могут закончиться сбоем, а новые данные не удастся записать до тех пор, пока не освободится достаточно места на диске. Фактический максимальный размер базы данных — это указанное вами количество гигабайт минус 5 ГБ.

Для систем, соответствующих требованиям FIPS 140-2, с операциями экспорта и базами данных архивирования мультимедиа из версий VMS XProtect, предшествующих 2017 R1, шифрование которых выполнятся с помощью шифров, не соответствующих FIPS, данные необходимо архивировать там, где к ним можно будет получить доступ после включения FIPS. Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

Присоединение устройств к хранилищу

После настройки параметров хранилища и архивирования для сервера записи можно включить хранилище и архивирование отдельных камер или группы камер. Это можно сделать как для отдельных устройств, так и для группы устройств. См. раздел Подключение устройства или группы устройств к хранилищу на стр. 217.

Эффективное архивирование

При включении архивирования для камеры или группы камер содержимое хранилища записей автоматически переносится в первый архив с заданной вами периодичностью.

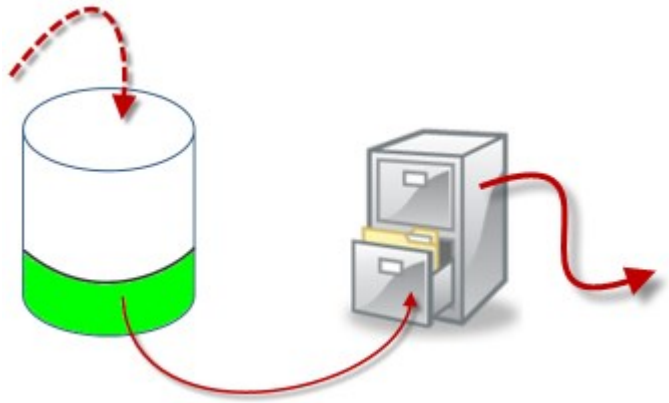
В зависимости от ваших требований можно настроить один или несколько архивов для каждого из хранилищ. Архивы могут располагаться непосредственно на компьютере сервера записи или в другом местонахождении, к которому у системы имеется доступ (например, на сетевом диске).

Правильная настройка архивирования позволяет оптимизировать потребности в хранилище данных. Зачастую требуется, чтобы архивированные записи (особенно предназначенные для длительного хранения) занимали как можно меньше места. В таких случаях можно немного снизить качество изображения. Повысить эффективность архивирования можно на вкладке **Хранилище** сервера записи. Там необходимо настроить несколько взаимосвязанных параметров:

- Хранение в хранилище записей
- Размер хранилища записей
- Хранение архивов
- Размер архивов

- Расписание архивирования
- Шифрование
- FPS — Frames per Second (к/с, кадров в секунду)

Поля, определяющие размер, задают размер хранилища записей, представленного в виде цилиндра, и его архивов соответственно:



При настройке времени хранения и размера для хранилища записей, представленного в виде белой области цилиндра, задается срок, по истечении которого будет выполнено архивирование старых записей. В нашем иллюстрированном примере вы архивируете записи, когда прошел срок, заданный для архивирования.

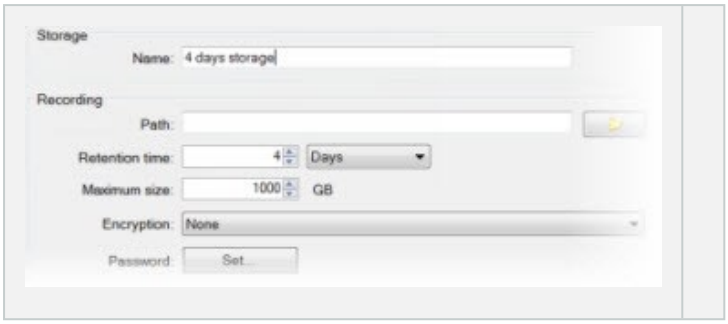
Настройка времени хранения и размера архивов определяет время, в течение которого записи хранятся в архиве. Записи остаются в архиве в течение указанного времени или до тех пор, пока архив не достигнет заданного лимита размера. При выполнении условий этих настроек система начинает перезаписывать старые записи в архиве.

Расписание архивирования определяет, как часто и в какое время выполняется архивирование.

Количество кадров в секунду (FPS) определяет размер данных в базах данных.

Для архивирования записей все эти параметры должны быть настроены в соответствии друг с другом. Это означает, что период хранения следующего архива всегда должен быть более продолжительным, чем период хранения текущего архива или базы данных записей. Это связано с тем, что количество дней хранения, заданное для архива, включает все периоды хранения, ранее указанные в процессе. Также архивирование всегда должно выполняться с меньшими интервалами, чем период хранения. В противном случае данные могут быть утеряны. Если время хранения составляет 24 часа, любые данные старше 24 часов удаляются. Таким образом, для того, чтобы безопасно перенести данные в очередной архив, важно запускать архивирование чаще, чем каждые 24 часа.

Пример: Для этих хранилищ (изображение слева) задано время хранения 4 дня, а для следующего архива (изображение справа) — 10 дней. Предусмотрено, что архивирование будет выполняться ежедневно в 10:30. Этот интервал архивирования значительно меньше времени хранения.



Также архивированием можно управлять с помощью правил и событий.

Структура архива (объяснение)

При архивировании записей они хранятся в архиве в виде определенной структуры подкаталогов.

> При обычном использовании системы структура подкаталогов полностью прозрачна для всех пользователей системы: обзор всех записей при помощи XProtect Smart Client доступен пользователям независимо от того, архивированы записи или нет. Знание структуры подкаталогов особенно полезно, если требуется выполнить резервное копирование архивированных записей.

Система автоматически создает отдельные подкаталоги в каждом из архивных каталогов сервера записи. Эти подкаталоги получают имя соответствующего устройства и архивной базы данных.

Так как записи из различных камер можно хранить в одном и том же архиве, и поскольку архивирование для каждой камеры выполняется, вероятнее всего, через равные интервалы времени, также автоматически создаются дополнительные подкаталоги.

Каждый из этих подкаталогов обозначает приблизительно один час записи. Почасовая разбивка позволяет удалять только относительно небольшие части данных архива, если он достиг максимально допустимого размера.

Подкаталоги получают имя устройства, после которого следует указание на источник записей (из накопителя для хранения данных или по протоколу SMTP), **плюс** дата и время последней записи базы данных из подкаталога.
Схема присвоения имен

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most recent recording]\
```

Из накопителя для хранения данных:

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of most
recent recording]\
```

По протоколу SMTP:

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of most
recent recording]\
```

Пример из реальной жизни

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

Подкаталоги

Автоматически добавляются даже дополнительные подкаталоги. Количество и характер этих подкаталогов зависит от характера самих записей. Например, если записи технически разделены на эпизоды, добавляется несколько различных подкаталогов. Зачастую так бывает, если для активации записей использована функция обнаружения движений.

- **Медиаданные**: В этой папке содержатся медиаданные: видео или звуковая информация (но не оба типа сразу)
- **Уровень подвижности**: В этой папке содержатся сетки уровня подвижности, созданные на основе видеоданных с использованием нашего алгоритма обнаружения движений. На основе этих данных можно выполнять очень быстрый поиск с помощью функции интеллектуального поиска в XProtect Smart Client.
- **Движение**: В этой папке хранятся эпизоды движения. Эпизод движения — это фрагмент, для которого в видеоданных обнаружено движение. Эта информация используется, например, в шкале времени в XProtect Smart Client
- **Запись**: В этой папке хранятся эпизоды записи. Эпизод записи — это фрагмент, для которого имеются согласованные записи медиаданных. Эта информация используется, например, для формирования шкалы времени в XProtect Smart Client
- **Подпись**: В этой папке хранятся подписи, сгенерированные для медиаданных (из папки «Медиаданные»). С помощью этой информации можно удостовериться в том, что в медиаданные не вносились несанкционированные изменения с момента их записи

Если требуется выполнить резервное копирование архивов, архивы можно размещать адресно (если известны основы структуры подкаталогов).

Примеры резервного копирования

При резервном копировании содержимого целого архива необходимо выполнять резервное копирование требуемого архивного каталога и всего его содержимого. Например, все следующее:

```
...F:\OurArchive\
```

При резервном копировании записей с определенной камеры за определенный период времени необходимо выполнять резервное копирование только содержимого соответствующих подкаталогов. Например, все следующее:

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

Буферизация перед событием и хранение записей (объяснение)

Буферизация перед событием — это возможность записывать звуковую информацию и видео до наступления активирующего события. Эта функция полезна в случаях, когда требуется записать звуковую информацию или видео, которые предшествуют событию активации записи (например, открытию двери).

Буферизация перед событием возможна благодаря тому, что система непрерывно получает аудио- и видеопотоки из подключенных устройств и временно сохраняет их в течение заданного периода буферизации перед событием.

- При активации правила записи временные записи становятся постоянными на то время записи перед событием, которое задано в правиле.
- Если правила записи не активируются, временные записи в предварительном буфере автоматически удаляются по прошествии заданного времени буферизации перед событием.

Хранение временных записей при буферизации перед событием

Вы можете задать местонахождение хранилища для временных записей при буферизации перед событием:

- В памяти; период буферизации перед событием ограничен 15 секундами.
- На диске (в базе медиаданных); можно выбрать любую продолжительность.

Сохранение данных в память вместо диска позволяет повысить производительность системы, но предусматривает только непродолжительные периоды буферизации перед событием.

Когда записи сохраняются в память, и вы делаете некоторые из временных записей постоянными, оставшиеся временные записи безвозвратно удаляются. Если требуется сохранить оставшиеся записи, включите сохранение записей на диск.

Аутентификация

Active Directory (объяснение)

Active Directory — это распределенная служба каталогов, разработанная Microsoft для доменных сетей Windows. Она входит в состав большинства операционных систем семейства Windows Server. Она осуществляет идентификацию ресурсов сети, чтобы к ним могли получать доступ пользователи или приложения.

Если установлена Active Directory, пользователей Windows можно добавлять из Active Directory. Также базовых пользователей можно добавлять без Active Directory. Существуют некоторые системные ограничения, связанные с базовыми пользователями.

Пользователи (объяснение)

Термин **пользователи** относится преимущественно к пользователям, подключающимся к системе наблюдения при помощи клиентов. Настройка таких пользователей может осуществляться двумя способами:

- В качестве **базовых пользователей** с аутентификацией по сочетанию пользовательского имени и пароля.
- В качестве **пользователей Windows** с аутентификацией на основе их регистрационного имени в Windows

Пользователи Windows

Для добавления пользователей Windows применяется Active Directory. Active Directory (AD) — это служба каталогов, разработанная Microsoft для доменных сетей Windows. Она входит в состав большинства операционных систем семейства Windows Server. Она осуществляет идентификацию ресурсов сети, чтобы к ним могли получать доступ пользователи или приложения. В Active Directory используются понятия пользователей и групп.

Пользователи — это объекты Active Directory, представляющие физических лиц с учетной записью пользователя. Пример:

Группы — это объекты Active Directory с несколькими пользователями. В этом примере в группу управления входят три пользователя:

В группы может входить любое количество пользователей. При добавлении в систему группы все ее пользователи добавляются одним действием. После добавления группы в систему любые изменения, вносимые в группу в Active Directory, например последующее добавление новых членов или удаление старых членов, немедленно отражаются в системе. Пользователь может быть членом сразу нескольких групп.

Active Directory можно использовать для добавления в систему сведений о существующих пользователях и группах. Это дает вам некоторые преимущества:

- Пользователи и группы задаются в Active Directory централизованно, поэтому не требуется создавать учетные записи пользователей заново
- Не требуется настраивать аутентификацию пользователей в системе, так как аутентификация выполняется Active Directory

Перед тем, как вы сможете добавлять пользователей и группы с помощью службы Active Directory, необходимо установить в сети сервер с Active Directory.

Базовые пользователи

Если у системы отсутствует доступ к Active Directory, создайте базового пользователя. Сведения о настройке базовых пользователей см. в разделе Создание базовых пользователей на стр. 315.

Identity Provider (объяснение)

Identity Provider app pool (IDP) — это системный объект, который применяется для создания и поддержания идентификационной информацией базовых пользователей, а также управления ей.

Также Identity Provider предоставляет службы аутентификации и регистрации связанным приложениям или службам, в данном случае: серверу записи, серверу управления, сборщику данных и серверу отчетов.

При входе в клиенты и службы XProtect как базовый пользователь запрос передается в Identity Provider. После завершения аутентификации пользователь может вызвать сервер управления.

Identity Provider работает в IIS в качестве составной части сервера управления с использованием того же SQL Server с отдельной базой данных и отвечает за создание и обработку коммуникационных маркеров OAuth, используемых службами при обмене информацией (Surveillance_IDP).

Журналы Identity Provider хранятся по адресу: `\\ProgramData\Milestone\IDP\Logs`.

Внешний IDP (объяснение)

IDP — это сокращение для Identity Provider. Внешний IDP — это внешнее приложение и служба, в которых можно хранить данные удостоверений пользователей и управлять ими, а также предоставлять функции аутентификации пользователей для других систем. Внешний IDP можно связать с ПО для управления видео XProtect.

XProtect поддерживает внешние IDP, совместимые с механизмом OpenID Connect (OIDC).

Аутентификация пользователя

Если настроен внешний IDP, клиенты XProtect поддерживают использование внешних IDP в качестве дополнительной опции аутентификации.

Когда адрес компьютера на экране входа клиента указывает на VMS XProtect с настроенным внешним IDP, будет инициирован вызов API, и опция аутентификации для внешнего IDP будет доступна на экране входа. Вызов API активируется при запуске клиента и при каждом изменении адреса.

Конкретный API, который запрашивает клиент, является общедоступным API, который не требует аутентификации пользователя, поэтому клиент всегда может прочитать эту информацию.

Заявки

Заявка — это заявление о себе, которое делает такой объект как пользователь или приложение.

Заявка состоит из названия заявки и значения заявки. Например, название заявки может быть стандартным названием, описывающим содержимое значения заявки, а значение заявки может быть именем группы. Другие примеры заявок от внешнего IDP: Пример заявок от внешнего IDP.

Заявки не являются обязательными. Однако они необходимы для автоматического связывания пользователей внешних IDP с ролями в VMS XProtect для определения разрешений пользователей. Заявки включаются в токен идентификатора пользователя из внешнего IDP и посредством связи с ролями определяют разрешения пользователя в XProtect.

Если заявки, связанные с ролями VMS XProtect, не предоставлены пользователям внешнего IDP, пользователи внешнего IDP могут быть созданы в VMS XProtect при первом входе в систему. В этом случае пользователи внешнего IDP не привязаны ни к каким ролям. Затем администратор VMS XProtect должен вручную добавить пользователей к ролям.

Предварительные условия для внешних IDP

Следующие шаги необходимо выполнить во внешнем IDP, прежде чем он будет настроен в VMS.

- Идентификатор и секретный ключ клиента для использования с VMS XProtect должны быть созданы во внешнем IDP. Дополнительные сведения приведены в разделе Уникальные пользовательские имена для пользователей внешнего IDP на стр. 76.

- Должен быть известен центр аутентификации внешнего IDP. Для получения дополнительной информации см. информацию о центре аутентификации для внешнего IDP в диалоговом окне **Параметры**.
- URI перенаправления на VMS XProtect должны быть настроены в IDP. Дополнительные сведения приведены в разделе Добавление URI перенаправления для веб-клиентов на стр. 429.
- При необходимости для пользователей или групп в IDP необходимо настроить заявки, связанные с VMS.
- VMS XProtect должна быть полностью настроена с использованием сертификатов, чтобы гарантировать, что весь обмен данными осуществляется через зашифрованный протокол https., в противном случае большинство внешних IDP не будут принимать запросы от VMS XProtect и ее клиентов, или часть потока обмена данными и обмен токенами безопасности не будут выполнены.
- Для VMS XProtect и всех клиентских компьютеров или смартфонов, которые должны использовать внешний IDP, должна быть возможность связаться с адресом входа внешнего IDP.

Предоставление пользователям возможности входить в ПО для управления видео XProtect через внешнего IDP

- Из внешнего IDP создайте пользователей и заявки для идентификации пользователей как пользователей внешнего IDP в VMS XProtect. Создание заявок не является обязательным шагом, но именно так вы включаете автоматическое связывание пользователей с ролями. Дополнительные сведения приведены в разделе Заявки на стр. 74.
- Из VMS XProtect создайте конфигурацию, которая позволяет Identity Provider, встроенному в VMS, обращаться к внешнему IDP. Дополнительные сведения о том, как создать конфигурацию для внешнего IDP, приведены в разделе Добавление и настройка внешнего IDP.
- Из ПО для управления видео XProtect настройте аутентификацию пользователей, привязав заявки пользователей от внешнего IDP к ролям XProtect. Дополнительные сведения о том, как привязывать заявки к ролям, приведены в разделе Привязка заявок от внешнего IDP к ролям вXProtect.
- Войдите в клиент XProtect, используя внешний IDP для аутентификации пользователя, см. Войдите систему через внешнего IDP на стр. 310.

Идентификаторы URI перенаправления

Идентификатор URI перенаправления задает страницу, на которую пользователя перенаправляется после успешной аутентификации. Во внешнем IDP необходимо добавить адрес сервера управления, за которым следует **Путь обратного вызова**, заданный в XProtect Management Client. Например, https://management-server-computer.company.com/idp/signin-oidc

В зависимости от того, как осуществляется доступ к VMS XProtect, как настроена сеть, серверы и Microsoft Active Directory, может потребоваться несколько URI перенаправления, см. некоторые примеры ниже:

Примеры

Сервер управления с доменом в URL-адресе или без него:

- “https://[server_name]/idp/signin-oidc”
- “https://[server_name].[domain_name]/idp/signin-oidc”

Мобильный сервер с доменом в URL-адресе или без него:

- “https://[server_name]:[mobile_port]/idp/signin-oidc”
- “https://[server_name].[domain_name]:[mobile_port]/idp/signin-oidc”

Если мобильный сервер настроен для доступа через Интернет, также необходимо добавить общедоступный адрес и порты.

Уникальные пользовательские имена для пользователей внешнего IDP

Для пользователей, которые входят в Milestone XProtect через внешнего IDP, автоматически создаются пользовательские имена.

Внешний IDP предоставляет набор заявок для автоматического создания имени для пользователя в XProtect, а в XProtect используется алгоритм для получения от внешнего IDP имени, являющегося уникальным в базе данных ПО для управления видео.

Пример заявок от внешнего IDP

Заявки состоят из названия заявки и значения заявки. Пример:

Название заявки	Стоимость заявки
name	Раз Ван
по эл. почте	123@domain.com
amr	pwd
idp	00o2ghkgazGgi9BIE5d7
preferred_username	321@domain.com
vmsRole	Оператор
locale	ru-RU

Название заявки	Стоимость заявки
given_name	Раз
family_name	Линдберг
zoneinfo	Америка/Лос-Анджелес
email_verified	Истина

Использование номера эпизода заявки для создания пользовательских имен в XProtect

В XProtect приоритет поиска при создании пользователя в ПО для управления видео XProtect определяется номером эпизода заявки, указанным в приведенной ниже таблице. В ПО для управления видео XProtect используется первое доступное имя заявки:

Название заявки	Номер эпизода	Описание
UserNameClaimType	1	Настроенная привязка с одной заявкой, задающая имя пользователя. Заявка задается в поле **Заявка для использования при создании пользовательского имени** на вкладке **Внешний IDP** в разделе **Инструменты** > **Параметры**.
preferred_username	2	Заявка, которая может поступить от внешнего IDP. Стандартная заявка, обычно используемая в OIDC (OpenID Connect).
name	3	
given_name family_ name	4	Имя и фамилия вместе, например «Боб Джонсон».
по эл. почте	5	
Первая доступная заявка + #(первый доступный номер)	6	Например, «Боб#1»

Указание конкретных заявок для создания пользовательских имен в XProtect

Администраторы XProtect могут задать конкретную заявку от внешнего IDP, которая должна использоваться для создания пользовательского имени в ПО для управления видео XProtect. Когда администратор задает заявку, которую необходимо использовать при создании пользовательского имени в ПО для управления видео XProtect, название заявки необходимо писать именно так, как выглядит название заявки от внешнего IDP.

- Заявку, которую необходимо использовать для пользовательского имени, можно задать в поле **Заявка для использования при создании пользовательского имени**, на вкладке **Внешний IDP** в разделе **Инструменты** > **Параметры** .

Удаление пользователей внешнего IDP

Удаление пользователей, созданных в XProtect регистрационным именем внешнего IDP, осуществляется по тому же принципу, что и удаление базового пользователя, причем пользователя можно удалить в любой момент времени после его создания.

Если пользователь удален в XProtect, и этот пользователь повторно входит в систему через внешнего IDP, в XProtect будет создан новый пользователь. Тем не менее данные, связанные с пользователем в XProtect (например, данные закрытого просмотра и роли), будут утрачены, и эту информацию потребуется вновь создавать для пользователя в XProtect.

При удалении внешнего IDP в Management Client удаляются и любые пользователи, подключенные к ПО для управления видео через внешнего IDP.

Безопасность

Роли и разрешения роли (объяснение)

Все пользователи в VMS Milestone XProtect относятся к какой-либо роли.

Роли определяют разрешения пользователей, включая устройства, к которым пользователи могут получить доступ. Кроме того, с помощью ролей задаются разрешения безопасности и доступа в системе управления видео.

Система поставляется с ролью по умолчанию **Администраторы** с полным доступом ко всем функциям системы, однако, как правило, в системе требуется настроить несколько ролей, назначая разным пользователям разные права доступа. Вы можете добавить столько ролей, сколько потребуется. См. раздел Назначение ролям пользователей и групп и их удаление из ролей на стр. 313.

Например, вам может потребоваться настроить разные типы ролей для пользователей XProtect Smart Client в зависимости от устройств, к которым они получают доступ, или аналогичных ограничений, которые требуют разграничения пользователей.

Для разграничения пользователей вам потребуется:

- создать и настроить роли, которые необходимы для решения бизнес-задач вашей организации;
- добавить пользователей и группы пользователей, которым вы назначите ту или иную роль;
- создать профили Smart Client и профили Management Client, чтобы задать, что могут видеть пользователи в интерфейсе XProtect Smart Client и Management Client.

  С помощью ролей можно управлять только разрешениями пользователей на доступ, а те тем, какие компоненты они будут видеть в интерфейсе XProtect Smart Client или Management Client. Создавать отдельный профиль Management Client для пользователей, которые не будут работать с Management Client, не требуется.

Для удобства пользователей XProtect Smart Client и пользователей Management Client с ограниченным доступом к функциям Management Client необходимо обеспечить согласованность разрешений, предоставляемых ролью, и элементами пользовательского интерфейса в рамках профиля Smart Client или Management Client.

> Для получения доступа к Management Server важно, чтобы для всех ролей было включено разрешение системы безопасности **Подключение**. Это разрешение находится в разделе **Настройки ролей** > **Management Server** > Вкладка «Общая безопасность» (роли) на стр. 563.

Для настройки ролей откройте раздел **Безопасность** > **Роли**

Разрешения роли

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

При создании роли в системе можно назначить эту роль ряду разрешений для системных компонентов или функций, которые доступны соответствующей роли, и которые она может использовать.

Например, можно создать роли, наделенные только разрешениями для доступа к функциям в XProtect Smart Client или других клиентах просмотра Milestone, и будет разрешен только просмотр определенных камер. Если вы создаете такие роли, у них не должно быть разрешений для доступа и использования Management Client, а только права доступа к некоторым или всем функциям, имеющимся в XProtect Smart Client или других клиентах.

Для такого разграничения необходимо настроить роль, наделенную некоторыми или самыми типовыми административными разрешениями, например разрешениями на добавление и удаление камер, серверов и аналогичных функций. Также можно создавать роли, у которых есть некоторые разрешения системного администратора либо большинство из них. Это может быть полезным, например, если организации требуется отделить работников с правом администрирования ряда параметров системы от работников, которым разрешено управлять системой в целом.

Роли дают возможность предоставлять различные административные разрешения на доступ или изменение огромного количества функций системы. Возьмем, к примеру, разрешение на изменение настроек серверов или камер в системе. Это разрешение задается на вкладке **Общая безопасность** (см. раздел Вкладка «Общая безопасность» (роли) на стр. 563). Для предоставления отдельному системному администратору права на запуск Management Client необходимо присвоить роли разрешения на чтение для сервера управления.

Для получения доступа к Management Server важно, чтобы для всех ролей было включено разрешение системы безопасности **Подключение**. Это разрешение находится в разделе **Настройки ролей** > **Management Server** > Вкладка «Общая безопасность» (роли) на стр. 563.

Кроме того, для каждой роли можно отразить те же самые ограничения в пользовательском интерфейсе Management Client, связав каждую роль с профилем Management Client, в пользовательском интерфейсе которого удалены соответствующие функции системы. Дополнительные сведения приведены в разделе Профили Management Client (объяснение) на стр. 83.

Для предоставления роли таких дифференцированных административных разрешений работник с полной административной ролью по умолчанию должен настроить соответствующую роль в разделе **Безопасность** > **«Роли» > вкладка «Сведения» > «Добавить новую»**. При настройке новой роли ее можно связать с вашими собственными профилями аналогично этим же операциям при настройке любой другой роли в системе или использовать системные профили по умолчанию. Дополнительные сведения приведены в разделе Добавление правила и его настройка на стр. 312.

После того, как вы задали профили, связанные с ролью, перейдите на вкладку **Общая безопасность** и задайте разрешения для этой роли.

Разрешения, которые можно задать для роли, зависят от конкретных продуктов. Предоставить роли все доступные разрешения можно только в XProtect Corporate.

Маски конфиденциальности (объяснение)

Маски конфиденциальности (объяснение)

При помощи конфиденциальной маскировки можно указать, какие области видео с камеры требуется закрыть масками конфиденциальности при демонстрации клиентам. Например, если камера наблюдения направлена на улицу, можно закрыть некоторые участки здания (окна или двери) масками конфиденциальности, чтобы защитить конфиденциальность жильцов. В некоторых странах этого требует законодательство.

Маски конфиденциальности можно сделать сплошными или размытыми. Маски можно наложить как на видео в режиме реального времени, так и на записанное и экспортированное видео.

Маски конфиденциальности применяются и фиксируются в конкретной области изображения, передаваемого камерой. В связи с этим закрытая область не перемещается вслед за движениями при панорамировании/наклоне/зуммировании, а постоянно закрывает одну и ту же область изображения. На некоторых PTZ-камерах можно включить конфиденциальную маскировку на основе положений на самой камере.

Существует два типа масок конфиденциальности:

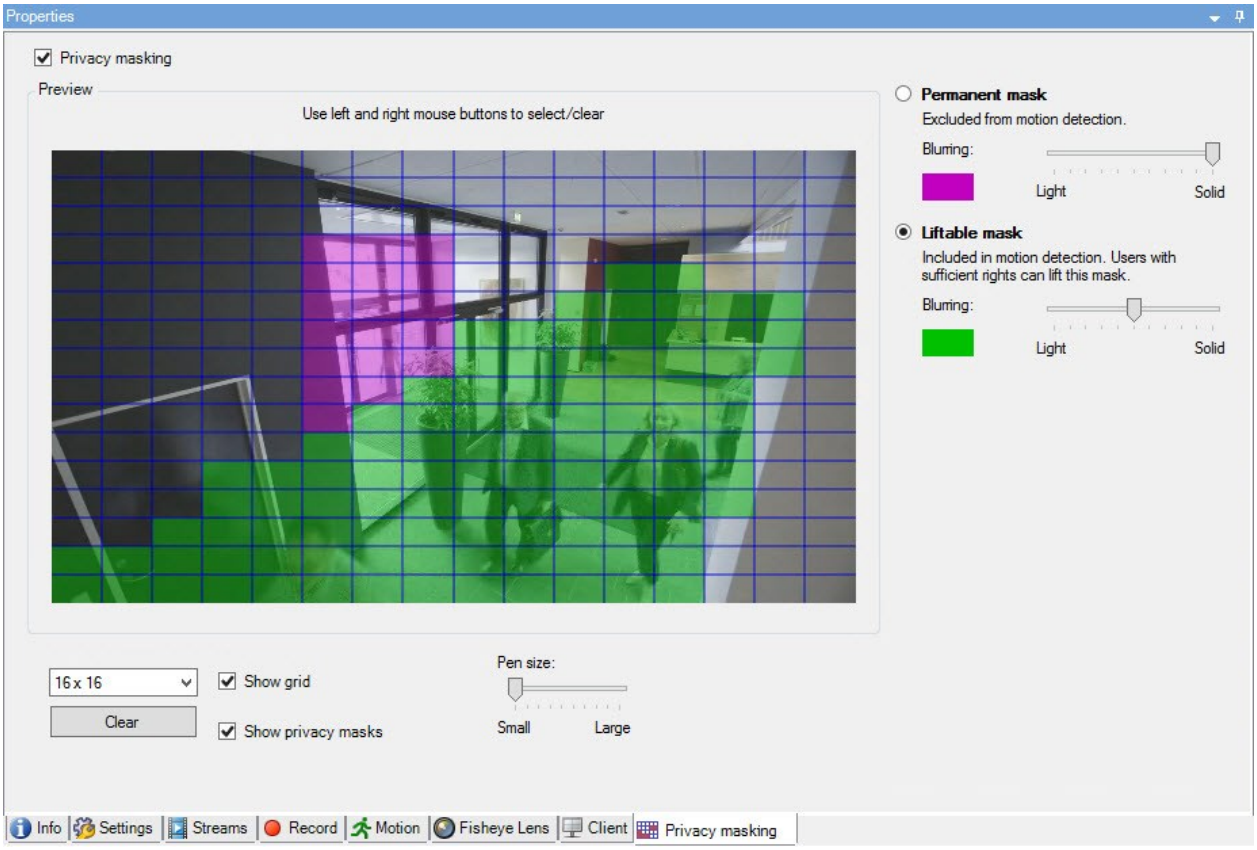
- **Постоянная маска конфиденциальности**: В этой маске области в клиентах всегда закрыты. Ее можно использовать для охвата областей видеоданных, которые никогда не требуют наблюдения, например, мест общего пользования или зон, где наблюдение запрещено. Из постоянных масок конфиденциальности исключаются области обнаружения движений.
- **Съемная маска конфиденциальности**: Области с масками этого типа могут быть временно открыты в XProtect Smart Client пользователями, у которых есть разрешение снимать маски конфиденциальности. Если у вошедшего в систему пользователя XProtect Smart Client нет разрешения на снятие масок конфиденциальности, система отобразит запрос на одобрение операции пользователем с достаточными правами.
  Маски конфиденциальности снимаются до истечения времени ожидания или до повторной активации масок пользователем. Помните о том, что маски конфиденциальности снимаются на видео со всех камер, к которым у пользователя есть доступ

При обновлении системы 2017 R3 или более старой системы с включенными масками конфиденциальности маски будут преобразованы в съемные маски.

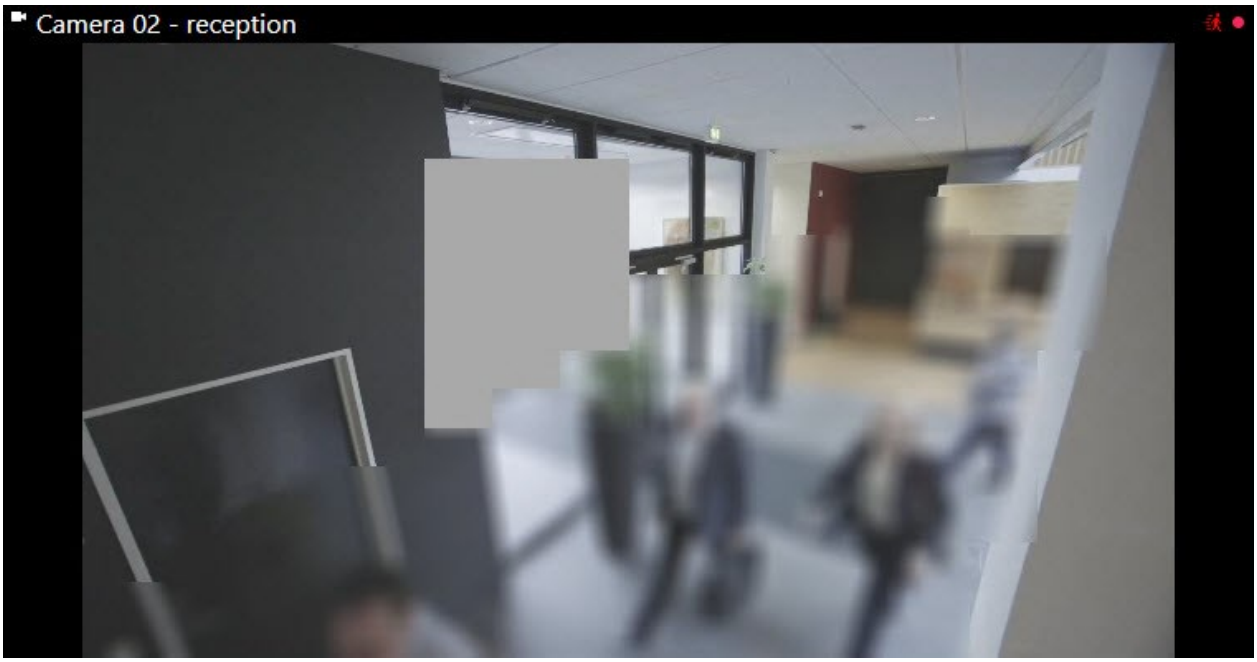
При экспорте или воспроизведении пользователем записанного видео с клиента оно включает маски конфиденциальности, заданные в момент записи, даже если впоследствии они были удалены или изменены. Если при экспорте отключается защита конфиденциальности, экспортированное видео **не** содержит съемных масок конфиденциальности.

Слишком частое изменение настроек конфиденциальной маскировки (например, еженедельное) может привести к перегрузке системы.

Пример вкладки **Конфиденциальная маскировка** с настроенными масками конфиденциальности:



А вот так они отображаются в клиентах:



Вы можете ознакомить пользователей клиентов с настройками постоянных и съемных масок конфиденциальности.

Профили Management Client (объяснение)

С помощью профилей Management Client системные администраторы могут изменять пользовательский интерфейс Management Client для других пользователей. Привяжите профили Management Client к ролям, чтобы в интерфейсе были доступны только функции, необходимые соответствующим ролям администраторов.

Профили Management Client обеспечивают только визуальное представление функциональности системы, не предоставляя доступа к ней. Общий доступ к функциям системы определяется ролью, присвоенной отдельным пользователям. Дополнительные сведения о том, как управлять общим доступом к функциям системы с учетом роли, приведены в разделе Управление отображением функций в профиле Management Client.

Вы можете изменить настройки видимости всех элементов Management Client. По умолчанию профиль Management Client имеет доступ к просмотру всех функций в Management Client.

Профили Smart Client (объяснение)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Все пользователи в Milestone XProtect VMS принадлежат к роли, к которой подключен профиль Smart Client.

Роли определяют разрешения пользователей, а профили Smart Client — компоненты пользовательского интерфейса XProtect Smart Client, видимые пользователям.

Все установки Milestone XProtect VMS включают профиль Smart Client по умолчанию, для которого настроена конфигурация по умолчанию, предусматривающая отображение большей части конфигурации, доступной в системе вашей организации. Некоторые параметры по умолчанию отключены.

Если в организации несколько разных ролей, можно отключить функции XProtect Smart Client, к которым у конкретной роли нет (или не должно быть) доступа.

Например, в системе может быть роль, для ежедневной работы которой не требуется воспроизведение видео. С этой целью для роли можно создать новый профиль Smart Client, в котором отключен профиль **Воспроизведение**. При отключении этого параметра в профиле Smart Client для пользователей XProtect Smart Client с ролью, использующей этот профиль Smart Client, в интерфейсе XProtect Smart Client больше не будет отображаться режим **Воспроизведение**.

Важно отметить, что профили Smart Client в основном контролируют то, что пользователи могут видеть в интерфейсе XProtect Smart Client, а не фактические разрешения на доступ для этой роли. Разрешения на доступ, такие как доступ для чтение, изменение или удаление, контролируются параметрами ролей. Так, у пользователей XProtect Smart Client могут быть разрешения на функции в их роли, которые они не могут видеть в пользовательском интерфейсе, так как они отключены в профиле Smart Client.

Для удобства пользователей XProtect Smart Client необходимо обеспечить согласованность разрешений, предоставляемых ролью, и элементами пользовательского интерфейса в рамках профиля Smart Client.

Чтобы создать или изменить профили Smart Client, разверните узел **Клиент** и выберите **Профили Smart Client**.

Ознакомьтесь с информацией о связях между профилями Smart Client, ролями и профилями времени и об их совместном использовании (см. Создание и настройка профилей Smart Client, ролей и профилей времени на стр. 286).

Защита доказательств (объяснение)

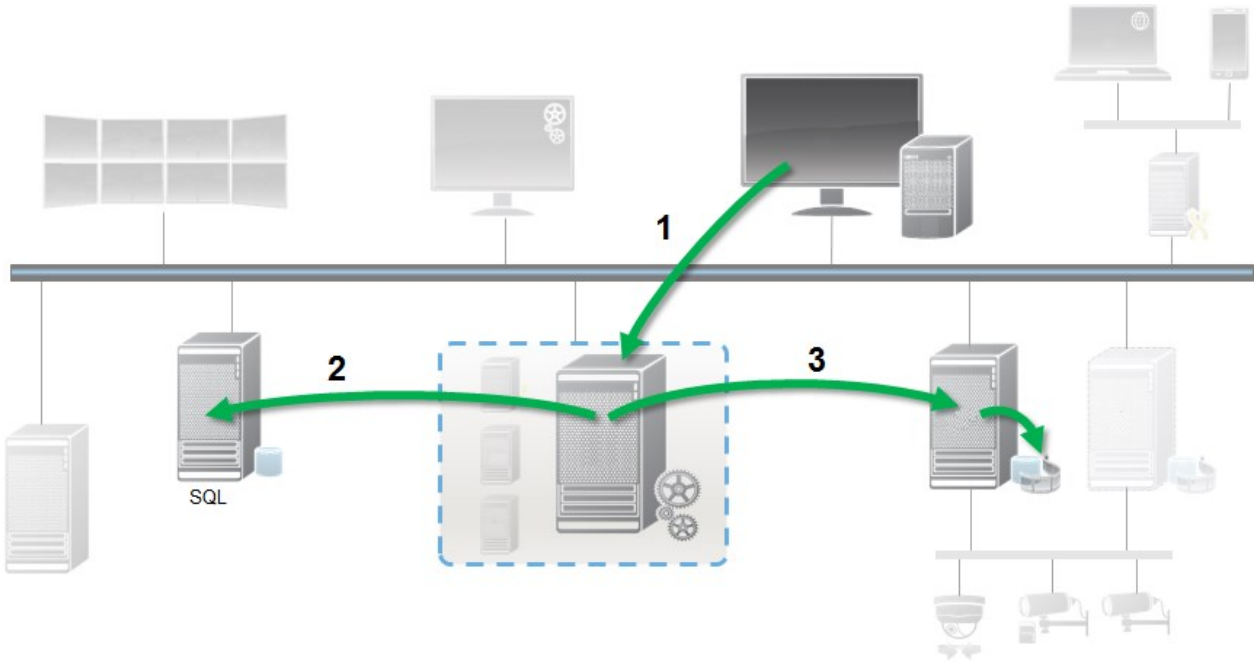
Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Начиная с VMS XProtect версии 2020 R2, если вы обновляете сервер управления с одной из предыдущих версий, создание или изменение защиты доказательств на серверах записи версии 2020 R1 или более ранних будет невозможным до тех пор, пока эти серверы записи не будут обновлены.
Это также означает, что, если оборудование перенесено с одного сервера записи (версии 2020 R1 или более ранней) на другой сервер записи, и на нем по-прежнему есть записи, защиту доказательств не удастся создать или изменить.

При помощи функции защиты доказательств операторы клиентов могут обеспечить защиту видеоэпизодов (включая звуковую информацию) и других данных от удаления (например, на период следствия или суда). Дополнительные сведения см. в руководстве пользователя XProtect Smart Client.

Защищенные данные не могут быть удалены ни автоматически — системными средствами по истечении заданного времени хранения, так и в других ситуациях — ни вручную — пользователями клиентов. Система или пользователь не сможет удалить доказательство до тех пор, пока его не разблокирует пользователь с достаточным уровнем разрешений.

Структурная диаграмма защиты доказательств:



1. Пользователь XProtect Smart Client создает защиту доказательств. Информация отправляется на сервер управления.
2. Сервер управления хранит информацию о защите доказательств в базе данных SQL Server.
3. Сервер управления сообщает серверу записи о необходимости хранения и защиты защищенных записей в базе данных.

Когда оператор создает защиту доказательств, защищенные данные остаются в исходном хранилище записей и переносятся на архивные диски вместе с незащищенными данными. При этом защищенные данные:

- Сохраняются в течение времени хранения, настроенного для защиты доказательств. В теории — до бесконечности
- Сохраняют исходное качество записи, даже если для незащищенных данных настроено снижение качества видео

Когда оператор создает защиту, минимальный размер эпизода равен продолжительности периода, на которые база данных разбивает записанные файлы, то есть, по умолчанию — одному часу. Это можно изменить: для этого требуется изменить файл RecorderConfig.xml на сервере записи. Если небольшой эпизод захватывает два периода продолжительностью один час, система блокирует записи в обоих периодах.

В контрольном журнале Management Client фиксируются события создания, изменения или удаления защиты доказательств пользователем.

Отсутствие достаточного пространства на диске не влияет на защищенные данные. Вместо этого удаляются самые старые незащищенные данные. Если незащищенных данных, которые можно удалить, не осталось, система останавливает запись. Можно создавать правила и сигналы тревоги, активируемые событиями заполнения диска, и получать уведомления в автоматическом режиме.

За исключением того, что больший объем данных хранится в течение более длительного времени, что теоретически отражается на объеме свободного пространства дисковых накопителей, фактически функция защиты доказательств не влияет на производительность системы.

При переносе оборудования (см. раздел Move hardware на стр. 373) на другой сервер записи:

- Записи, защищенные при помощи функции защиты доказательств, остаются на старом сервере в течение времени хранения, заданного при создании защиты.
- Пользователь XProtect Smart Client по-прежнему может защитить данные при помощи защиты доказательств, если записи были сделаны на камере до ее переноса на другой сервер записи. Даже если камера переносится несколько раз, а записи хранятся на нескольких серверах записи.

По умолчанию всем операторам назначен профиль защиты доказательств по умолчанию, но у них отсутствуют пользовательские разрешения на доступ к этой функции. Сведения о задании разрешений роли для доступа к защите доказательств см. на вкладке Устройство (роли), в пункте «Настройки ролей». Сведения о задании профиля защиты доказательств роли см. на вкладке Сведения (роли), в пункте «Настройки ролей».

В Management Client можно изменить свойства профиля защиты доказательств по умолчанию и создать дополнительные профили защиты доказательств, а также назначить их ролям вместо профиля по умолчанию.

Правила и события

Правила (объяснение)

Правила задают действия, которые должны выполняться в определенных условиях. Пример: При обнаружении движений (условие) камера должна начинать запись (действие).

Ниже приведены **примеры** вариантов применения правил:

- Запуск и остановка записи
- Установка при просмотре в режиме реального времени частоты кадров, отличной от значения по умолчанию
- Установка при записи частоты кадров, отличной от значения по умолчанию
- Запуск и остановка PTZ-патрулирования
- Приостановка и возобновление PTZ-патрулирования
- Перемещение PTZ-камер в определенные положения
- Активация или деактивация вывода
- Отправка уведомлений по электронной почте
- Создание записей журналов
- Создание событий

- Применение новых настроек устройства (например, другого разрешения в камере)
- Включение отображения видео в получателях Matrix
- Запуск и остановка встраиваемых расширений
- Запуск и остановка потоков с устройств

Остановка устройства означает, что видео больше не передается с устройства в систему. В этом случае просмотр видео в режиме реального времени или его запись невозможны. Для сравнения, устройство, на котором остановлен поток, по-прежнему может взаимодействовать с сервером записи, и вы можете автоматически запустить поток из устройства при помощи правила, в отличие от ситуации, когда устройство отключено в Management Client вручную.

> Некоторые правила требуют, чтобы для соответствующих устройств были включены определенные функции. Например, правило, согласно которому камера должна вести запись, не будет действовать как задумано, если для соответствующей камеры не включена запись. Перед тем, как создавать правило, Milestone рекомендует убедиться, что задействованные устройства функционируют надлежащим образом.

Уровень сложности правил

Точное количество параметров зависит от создаваемого типа правила, а также от количества устройств в системе. Правила обеспечивают высокий уровень гибкости: вы можете сочетать события и временные условия, задавать несколько действий в рамках одного правила, а зачастую создавать правила, охватывающие несколько устройств в системе или все эти устройства.

Правила можно сделать настолько простыми или сложными, насколько это необходимо. Например, можно создать очень простое правило, зависящее от времени:

Пример	Объяснение
Очень простое правило, зависящее от времени	По понедельникам с 08:30 до 11:30 (условие времени) камера 1 и камера 2 должны начинать запись (действие) в начале этого периода времени и останавливать запись (завершающее действие) по окончании этого периода времени.
Очень простое правило, зависящее от событий	При обнаружении движения (условие события) на камере 1 камера 1 должна немедленно начинать запись (действие), а затем останавливать запись (завершающее действие) по прошествии 10 секунд.

Пример	Объяснение
	Даже если правило, зависящее от событий, активируется событием на одном устройстве, можно указать, что действия должны выполняться на одном или нескольких других устройствах.
Правило, задействующее несколько устройств	При обнаружении движений (условие события) на камере 1 камера 2 должна немедленно начинать запись (действие), а сирена, подключенная к выводу 3, должна немедленно включаться (событие). Затем, по прошествии 60 секунд, камера 2 должна останавливать запись (завершающее действие), а сирена, подключенная к выводу 3, должна отключаться (завершающее действие).
Правила, в которых сочетаются время, события и устройства	При обнаружении движений (условие события) на камере 1, если день недели — суббота или воскресенье (условие времени), камера 1 и камера 2 должны немедленно начинать запись (действие), а руководителю службы безопасности должно быть отправлено уведомление. Затем, по прошествии 5 секунд после того, как на камере 1 или камере 2 движение перестает обнаруживаться, 2 камеры должны остановить запись (завершающее действие).

В зависимости от потребностей организации бывает полезным создать множество простых правил, а не несколько сложных правил. Так, даже при наличии большого количества небольших правил в системе по ним проще понять, для чего именно они применяются. Кроме того, чем проще будут правила, тем проще активировать и деактивировать их отдельные элементы. При наличии простых правил можно деактивировать и активировать правила целиком.

Правила и события (объяснение)

Правила — это один из ключевых элементов системы. Правила определяют чрезвычайно важные настройки, например когда камеры должны вести запись, когда PTZ-камеры должны вести патрулирование, когда необходимо отправлять уведомления и т. п.

Пример: правило, согласно которому конкретная камера должна начинать запись при обнаружении движений:

События — ключевые элементы при использовании мастера **Управление правилом**. В мастере события используются преимущественно для активации действий. Например, можно создать правило, согласно которому при наступлении **события** обнаружения движений система наблюдения должна выполнить **действие** запуска записи видео с определенной камеры.

Правила могут активироваться условиями следующих типов:

Имя	Описание
События	Когда в системе наблюдения происходят события (например, обнаруживается движение или система получает входной сигнал от внешних датчиков).
Интервал времени	Когда вы указываете конкретные периоды времени, например: `Thursday 16th August 2007 from 07.00 to 07.59` или `every Saturday and Sunday`
Интервал времени отработки отказа	Периоды времени, когда отработка отказа выполняется или не выполняется.
Повторяющееся время	При задании выполнения действия на основе подробного, повторяющегося расписания. Пример: • Еженедельно по вторникам каждый 1 час между 15:00 и 15:30 • В 15 день каждые 3 месяца в 11:45 • Ежедневно каждый 1 час между 15:00 и 19:00 Время основано на параметрах локального времени сервера, на котором установлен Management Client.

В разделе **Правила и события** можно работать со следующими элементами:

- **Правила**: Правила — это один из ключевых элементов системы. Поведение системы наблюдения в очень значительной степени определяется правилами. При создании правила можно использовать все типы событий.

- **Профили времени**: Профили времени — это периоды времени, заданные в Management Client. Они используются при создании правил в Management Client, например для создания правила, в котором указано, что определенное действие должно выполняться в рамках определенного профиля времени
- **Профили уведомлений**: Профили уведомления можно использовать для настройки заранее подготовленных уведомлений по электронной почте, которые могут автоматически активироваться правилом (например, при наступлении определенного события)
- **Пользовательские события**: Пользовательские события — это персонализированные события, с помощью которых пользователи могут вручную активировать события в системе или реагировать на входные сигналы из системы
- **События аналитики**: События аналитики — это данные, полученные от сторонних поставщиков анализа видео (VCA). События аналитики можно использовать для установки сигналов тревоги
- **Типичные события**: Типичные события позволяют активировать действия в сервере событий XProtect путем отправки простых строк в систему по IP-сети

Профили времени (объяснение)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Профили времени — это периоды времени, заданные администратором. Профили времени можно использовать при создании правил: например, правила, согласно которому определенное действие должно выполняться в течение определенного периода времени.

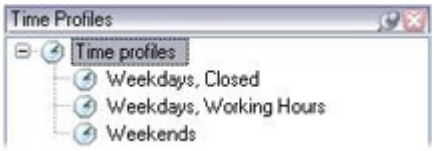
Профили времени назначаются ролям наряду с профилями Smart Client. По умолчанию всем ролям назначен стандартный профиль времени **Всегда**. Это означает, что у участников ролей, которым назначен этот стандартный профиль времени, отсутствуют зависящие от времени лимиты на их пользовательские разрешения в системе. Также ролям можно назначать альтернативный профиль времени.

Профили времени — чрезвычайно гибкая функция: они могут быть основаны на одном или нескольких разовых периодах времени, на одном или нескольких повторяющихся периодах времени или на сочетании разовых и повторяющихся моментов времени. Многие пользователи могут быть знакомы с концепциями разовых и повторяющихся периодов времени по календарным приложениям (например, приложениям из пакета Microsoft® Outlook).

Профили времени всегда работают по местному времени. Так, если в системе имеются серверы записи, находящиеся в разных часовых поясах, любые действия (например, запись через камеры), связанные с профилями времени, выполняются по местному времени каждого сервера записи. Пример: Если профиль времени охватывает период с 08:30 до 09:30, любые связанные действия на

сервере записи, находящемся в Нью-Йорке, выполняются, когда местное время Нью-Йорке — с 08:30 до 09:30, тогда как те же самые действия на сервере записи, находящемся в Лос-Анджелесе, выполняются на несколько часов позднее, когда местное время в Лос-Анджелесе — с 08:30 до 09:30.

Для создания профилей времени и управления ими откройте раздел **Правила и события** > **Профили времени**. Откроется список **Профили времени**. Только в качестве примера:



Сведения об альтернативе профилям времени приведены в разделе Профили продолжительности светового дня (объяснение).

Профили продолжительности светового дня (объяснение)

Зачастую при размещении камеры на улице требуется уменьшить разрешение камеры, включить черно-белый режим или изменить другие настройки, когда становится темно или светло. Чем севернее или южнее относительно экватора расположены камеры, тем сильнее время восхода и захода Солнца отличается в течение года. В связи с этим нельзя использовать обычные фиксированные профили времени для корректировки настроек камеры в соответствии со световыми условиями.

В таких ситуациях вместо них можно создать профили продолжительности светового дня, чтобы задать время восхода и захода Солнца в конкретной географической зоне. При помощи географических координат система рассчитывает время восхода и захода Солнца, ежедневно учитывая даже скорректированное летнее время. В результате этого профиль времени автоматически учитывает ежегодные изменения во времени восхода/захода Солнца в выбранной зоне, благодаря чему профиль используется только по мере необходимости. Все моменты времени и даты основаны на настройках времени и даты сервера управления. Также можно задать положительное или отрицательное смещение (в минутах) времени начала (восход Солнца) и времени окончания (заход Солнца). Смещение времени начала и времени окончания может быть одинаковым или разным.

Профили продолжительности светового дня можно использовать при создании как правил, так и ролей.

Профили уведомлений (объяснение)

С помощью профилей уведомлений можно настраивать заранее подготовленные уведомления по электронной почте. Уведомления могут автоматически активироваться правилом (например, когда происходит определенное событие).

При создании профиля уведомлений вы указываете текст сообщения и определяете, хотите ли вы включать в отправляемые по электронной почте кадры видео и видеоклипы в формате AVI.

Возможно, потребуется отключить сканеры электронной почты, которые могут помешать приложению отправлять уведомления.

Требования для создания профилей уведомлений

Перед созданием профилей уведомлений необходимо задать настройки почтового сервера для уведомлений по электронной почте.

Для обеспечения безопасности обмена данными с почтовым сервером можно установить на него необходимые сертификаты безопасности.

Если вместе с уведомлениями по электронной почте необходимо отправлять видеоклипы в формате AVI, сначала необходимо задать параметры сжатия:

1. Перейдите в раздел **Инструменты** > **Параметры**. Откроется окно **Параметры**.
2. Настройте почтовый сервер на вкладке **Почтовый сервер** (Вкладка «Почтовый сервер» (параметры) на стр. 422) и параметры сжатия на вкладке **Создание AVI** Вкладка «Генерирование AVI» (параметры) на стр. 423.

Пользовательские события (объяснение)

Если требуемое событие отсутствует в списке **Обзор событий**, можно создать собственные (пользовательские) события. Используйте такие пользовательские события для интеграции других систем с вашей системой наблюдения.

При помощи пользовательских событий данные, полученные из сторонних систем управления доступом, можно использовать в качестве событий в системе. События могут впоследствии активировать действия. Например, таким образом можно начать запись видео с соответствующих камер, когда кто-нибудь входит в здание.

Также пользовательские события можно использовать для ручной активации событий при просмотре видео в режиме реального времени в XProtect Smart Client или автоматической активации, если они применяются в правилах. Например, когда происходит пользовательское событие 37, PTZ-камера 224 должна остановить патрулирование и перейти на исходную предустановку 18.

При помощи ролей можно задать, какие из ваших пользователей могут активировать пользовательские события. При необходимости пользовательские события можно использовать двумя способами одновременно:

События	Описание
Для предоставления	В этом случае пользовательские события позволяют конечным

События	Описание
возможности активации событий вручную в XProtect Smart Client	пользователям активировать события вручную при просмотре видео в режиме реального времени в XProtect Smart Client. Когда пользовательское событие возникает потому, что пользователь XProtect Smart Client активировал его вручную, правило может активировать одно или несколько событий в системе.
Для предоставления возможности активации событий при помощи API	В этом случае пользовательские события можно активировать за пределами системы наблюдения. Использование пользовательских событий в таком сценарии требует, чтобы при их активации применялся отдельный API (прикладной программный интерфейс, то есть комплекс стандартных блоков для создания или персонализации приложений). Для такого использования пользовательских событий требуется аутентификация при помощи Active Directory. Так, активация пользовательских событий (даже за пределами системы) может выполняться только авторизованными пользователями. Кроме того, через API пользовательские события можно связать с метаданными, определяющими устройства или группы устройств. Это чрезвычайно удобно, если пользовательские события используются для активации правил, так как избавляет от необходимости иметь для каждого устройства правило, делающее, в сущности, одно и то же. Пример: Компания использует систему управления доступом на 35 входах, каждый из которых оборудован устройством для управления доступом. При активации устройства управления доступом в системе активируется пользовательское событие. Пользовательское событие применяется в правиле для начала записи на камере, связанной с активированным устройством управления доступом. В метаданных указано, какая из камер связана с этим правилом. Таким образом, компании не требуется иметь 35 пользовательских событий и 35 правил, активируемых пользовательскими событиями. Достаточно одного пользовательского события и одного правила. Когда пользовательские события применяются таким образом, не всегда нужно, чтобы они были доступны для ручной активации в XProtect Smart Client. Чтобы определить, какие из пользовательских событий должны быть видны в XProtect Smart Client, можно использовать роли.

События аналитики (объяснение)

События аналитики — как правило, это данные, полученные от сторонних поставщиков анализа видео (VCA).

Использование событий аналитики в качестве основы для сигналов тревоги — это процесс, состоящий из трех этапов:

- Этап первый. Включение функции событий аналитики и настройка ее безопасности. Воспользуйтесь списком допустимых адресов, чтобы задать, кто именно может отправлять данные о событиях в систему и по какому порту будут передаваться данные
- Этап второй. Создание события аналитики (возможно, с описанием события) и его тестирование
- Этап третий. Использование события аналитики в качестве источника для определения тревоги

Настройка событий аналитики осуществляется в списке **Правила и события** на вкладке **Навигация по сайту**.

Для использования событий, основанных на анализе видео, необходим сторонний инструмент анализа видео для передачи данных системе. Какой инструмент анализа видео использовать — зависит только от вас. Главное — чтобы он соответствовал формату. Сведения об этом формате приведены в документации MIP SDK по событиям аналитики.

За дополнительными сведениями обратитесь к поставщику своей системы. Сторонние инструменты анализа видео разрабатываются независимыми партнерами, которые разрабатывают решения на базе открытой платформы Milestone. Эти решения могут повлиять на производительность системы.

Типичные события (объяснение)

Типичные события позволяют активировать действия в сервере событий XProtect путем отправки простых строк в систему по IP-сети.

Для активации типичных событий можно использовать любое оборудование или программное обеспечение, которое способно отправлять строки по протоколу TCP или UDP. Система может анализировать полученные по протоколу TCP или UDP пакеты данных и автоматически активировать типичные события, когда соблюдены определенные критерии. Таким способом можно выполнить интеграцию системы с внешними источниками данных, например с системами управления доступом и системами сигнализации. Это позволит максимально возможному количеству внешних источников данных взаимодействовать с системой.

Благодаря концепции источников данных можно не заботиться об адаптации сторонних инструментов к стандартам вашей системы. При помощи источников данных можно взаимодействовать с конкретным оборудованием или программным обеспечением через конкретный IP-порт и точно устанавливать, как будут обрабатываться байты, поступающие на этот порт. Каждое типичное событие действует в паре с источником данных и формирует язык, используемый для взаимодействия с конкретным оборудованием или программным обеспечением.

Работа с источниками данных требует общего знания IP-сетей и специальных знаний в области определенного оборудования и ПО, с которыми вы хотите обмениваться данными. Можно использовать множество различных параметров. Готовых решений при этом не существует. По сути, система предоставляет в ваше распоряжение инструменты, но не решение. В отличие от пользовательских событий, типичные события не предусматривают аутентификацию. В результате

этого их проще активировать, но для того, чтобы не подвергать риску систему безопасности, допускаются только события из локального хоста. Можно предоставить разрешение другим IP-адресам клиента из вкладки **Типичные события** в меню **Параметры**.

Веб-перехватчики (объяснение)

Веб-перехватчики представляют собой HTTP-запросы, которые позволяют веб-приложениям взаимодействовать друг с другом и упрощают передачу данных в реальном времени из одного приложения в другое при возникновении предварительно заданного события, такого как отправка данных события на заданную конечную точку веб-перехватчика при входе пользователя в систему или передача камерой ошибки.

Конечная точка веб-перехватчика (URL-адрес веб-перехватчика) — это предварительно заданный адрес, на который передаются данные событий, который можно сравнить с номером телефона для односторонней связи.

Веб-перехватчики можно использовать для создания интерграций, подписанных на выбранные события в XProtect. При активации события на конечную точку, заданную для этого события, передается запрос HTTP POST. В теле запроса HTTP POST содержатся данные события в формате JSON.

Веб-перехватчики не опрашивают систему для получения данных или активированных событий, при возникновении событий система сама передает данные событий на конечную точку веб-перехватчика, что снижает ресурсоемкость веб-перехватчиков и ускоряет настройку, по сравнению с опрашивающими решениями.

Веб-перехватчики можно настроить для интеграции с помощью сценариев кода или без них.

> Необходимо убедиться, что данные событий, передаваемые из XProtect, соответствуют текущим требованиям законодательства вашей страны в отношении данных и защиты конфиденциальности.

Функция веб-перехватчиков по умолчанию установлена и готова к использованию в XProtect 2023R1 и более поздних версий. Она представлена действием **Веб-перехватчики** на вкладке **Правила** в Management Client.

Сигналы тревоги

Сигналы тревоги (объяснение)

> Этот компонент доступен только в случае, если установлен XProtect Event Server.

В этом разделе описано, как настроить срабатывание сигналов тревоги при наступлении событий в системе.

На базе функций сервера событий система управления тревогами обеспечивает возможность централизованного обзора, контроля и масштабирования тревог для произвольного количества систем (включая другие системы XProtect) в вашей организации. Сигналы тревоги могут срабатывать на основе следующих факторов:

- **Внутренние системные события**

  Например, движение, ответ или отсутствие ответа от сервера, неисправность архивации, отсутствие места на диске и т. д.

- **Внешние интегрированные события**

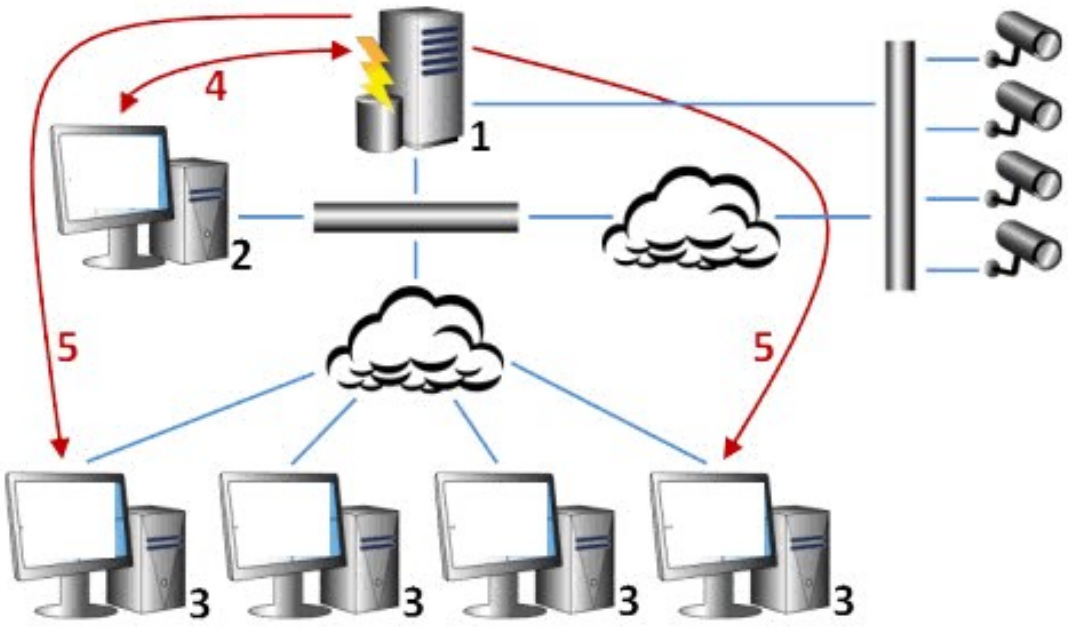
  К этой группе относится несколько типов внешних событий:

  - **События аналитики**

    Как правило, это данные, полученные от сторонних поставщиков анализа видео (VCA).

  - **MIPСобытия модулей**

    С помощью MIP SDK сторонние разработчики могут подключать к вашей системе собственные модули, например, для интеграции внешних систем управления доступом и т. п.



Расшифровка

1. Система наблюдения
2. Management Client

3. XProtect Smart Client
4. Конфигурация тревог
5. Поток данных тревог

Управление сигналами тревог осуществляется через список тревог в XProtect Smart Client. Сигналы тревоги также можно интегрировать с интеллектуальной картой XProtect Smart Client и функциями карты.

Конфигурация тревог

Настройка сигналов тревоги включает следующее:

- динамическую настройку обработки сигналов тревоги на основе ролей;
- единый технический обзор компонентов: серверов, камер и внешних устройств;
- настройку единой системы регистрации всех входящих сигналов тревоги и системной информации;
- работу с встраиваемыми расширениями, которые обеспечивают настраиваемую интеграцию других систем, например внешних систем управления доступом или систем, основанных на анализе видео.

Как правило, сигналы тревоги определяются видимостью объекта, вызвавшего тревогу. Это значит, что существует четыре возможных аспекта, которые связаны с сигналами тревоги и определяют, кто и в какой степени может управлять сигналами тревоги:

Имя	Описание
Видимость источника/устройства	Если пользователь не видит устройство, запускающее сигнал тревоги, то он не сможет увидеть и сам сигнал в списке сигналов тревоги в XProtect Smart Client.
Право активировать пользовательские события	С помощью этого разрешения пользователь может запускать пользовательские события в XProtect Smart Client.
Внешние встраиваемые расширения	Использование внешних встраиваемых расширений в системе обеспечивает управление правами пользователей, связанными с обработкой сигналов тревоги.
Общие права роли	Укажите разрешения, доступные пользователю: только просмотр или также управление сигналами тревоги. Действия пользователя при работе с сигналами в разделе **Сигналы тревоги** зависят от его роли и настроек, установленных для данной роли.

На вкладке **Сигналы тревоги и события** в разделе **Опции** можно указать настройки сигналов тревоги, событий и журналов.

Интеллектуальная карта

Интеллектуальная карта (объяснение)

Интеллектуальная карта в XProtect® Smart Client и XProtect Mobile дает возможность просматривать устройства и взаимодействовать с ними в разных точках мира с правильной географической привязкой. В отличие от функции обычных карт, где для каждого местоположения представлена отдельная карта, интеллектуальная карта дает общую картину в одном представлении.

Настройка функции интеллектуальной карты в Management Client выполняется следующим образом:

- Настройте картографические фоны, которые могут использоваться для интеллектуальной карты. Для этого необходимо обеспечить интеграцию интеллектуальной карты с одной из следующих служб:
  - Bing Maps
  - Google Maps
  - Milestone Map Service
  - OpenStreetMap
- Включите Bing Maps или Google Maps в XProtect Management Client или XProtect Smart Client.
- Включите функцию редактирования интеллектуальных карт, включая устройства, в XProtect Smart Client.
- Задайте географическое положение ваших устройств в XProtect Management Client.
- Настройте интеллектуальную карту с помощью Milestone Federated Architecture.

Интеграция интеллектуальных карт с Google Maps (объяснение)

Если вы хотите встроить Google Maps в интеллектуальную карту, вам потребуется базовый ключ Maps Static API, предоставляемый компанией Google. Для получения ключа Maps Static API необходим платежный аккаунт в Google Cloud. Счет выставляется в соответствии с объемом загрузки карт в течение месяца.

После получения ключа API необходимо ввести его в XProtect Management Client. Также см. Включение Bing Maps или Google Maps в Management Client на стр. 352.

Если вы используете брандмауэр с ограниченным доступом, разрешите доступ к соответствующим доменам. Google Maps может потребоваться разрешение на использование исходящего трафика с помощью maps.googleapis.com на каждом устройстве, на котором работает Smart Client.

Дополнительная информация:

- Платформа Google Maps — начало работы:https://cloud.google.com/maps-platform/
- Руководство по расчетам на платформе Google Maps: https://developers.google.com/maps/billing/gmp-billing
- Руководство разработчика по Maps Static API: https://developers.google.com/maps/documentation/maps-static/dev-guide

Добавление цифровой подписи в ключ Maps Static API

Если предполагается, что операторы XProtect Smart Client будут делать более 25 000 запросов к картам в день, для ключа Maps Static API потребуется цифровая подпись. С помощью цифровой подписи серверы Google проверяют, авторизован ли сайт, генерирующий запросы с использованием вашего API-ключа. Кроме того, Google рекомендует использовать цифровую подпись в качестве дополнительного уровня безопасности, независимо от требований к использованию. Для получения цифровой подписи требуется получить секрет подписи URL. Дополнительные сведения приведены в разделе https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual.

Интеграция интеллектуальных карт с Bing Maps (объяснение)

Если вы хотите встроить Bing Maps в интеллектуальную карту, вам потребуется базовый ключ или корпоративный ключ. Разница между ними заключается в том, что базовые ключи бесплатны, при этом они допускают ограниченное количество транзакций. После использования бесплатного количества операций, транзакции становятся платными или доступ к сервису карт приостанавливается. Корпоративный ключ обеспечивает неограниченное количество транзакций, но его нужно приобретать отдельно.

Дополнительные сведения о Bing Maps приведены в разделе https://www.microsoft.com/en-us/maps/licensing/.

После получения ключа API необходимо ввести его в XProtect Management Client. См. раздел Включение Bing Maps или Google Maps в Management Client на стр. 352.

Если вы используете брандмауэр с ограниченным доступом, разрешите доступ к соответствующим доменам. Bing Maps может потребоваться разрешение на использование исходящего трафика с помощью *.virtualearth.net на каждом устройстве, на котором работает Smart Client.

Кэшированные файлы интеллектуальных карт (объяснение)

Если в качестве картографического фона используется Google Maps, файлы не кэшируются.

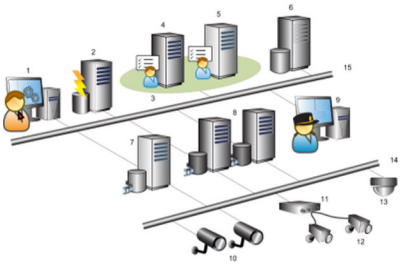
Файлы, которые используются для картографического фона, получены с сервера фрагментов карты. Время хранения файлов в папке кэша зависит от значения, выбранного в списке **Удаление кэшированных файлов интеллектуальных карт** в диалоговом окне **Настройки** в XProtect Smart Client. Хранение файлов осуществляется одним из следующих способов:

- в течение неограниченного срока (**Никогда**);
- в течение 30 дней, если файл не используется (**При неиспользовании в течение 30 дней**);
- до тех пор, пока оператор не выйдет из XProtect Smart Client (**При выходе**).

При изменении адреса сервера фрагментов автоматически создается новая папка кэша. Предыдущие файлы карт сохраняются в соответствующей папке кэша на локальном компьютере.

Архитектура

Распределенная система



Пример распределенной системы. Можно использовать столько камер, серверов записи и подключенных клиентов, сколько потребуется.

Все компьютеры распределенной системы должны входить в домен или рабочую группу.

Расшифровка

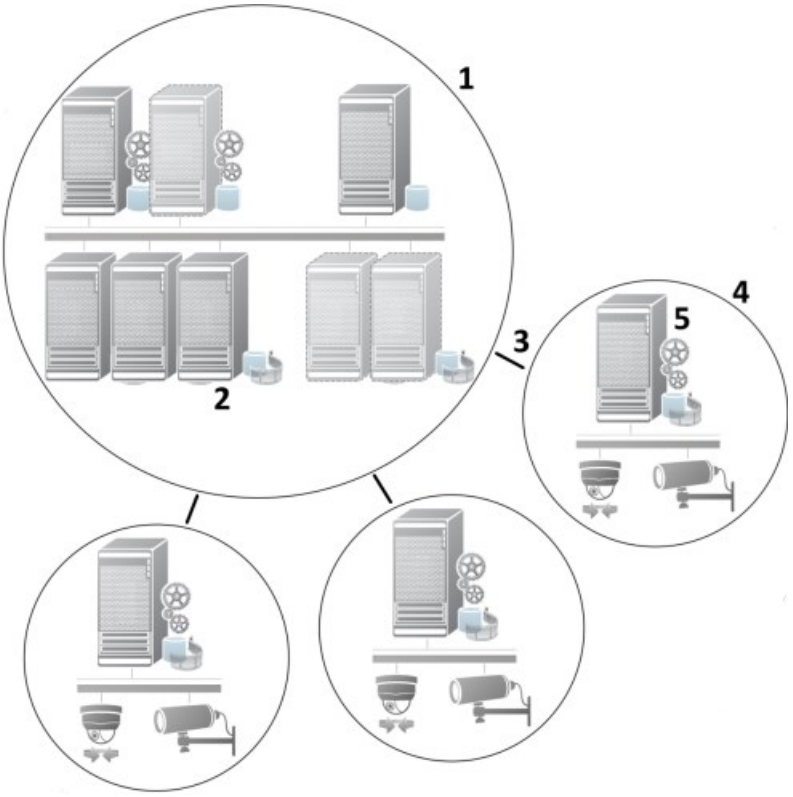
1. Management Client(-ы)
2. Сервер событий
3. Кластер Microsoft
4. Сервер управления
5. Сервер управления для обработки отказа
6. Сервер с SQL Server
7. Сервер записи обработки отказа
8. Серверы записи
9. XProtect Smart Client(-ы)
10. IP-видеокамеры
11. Видеокодер
12. Аналоговые камеры
13. PTZ IP-камера
14. Сеть камер
15. Сеть серверов

Milestone Interconnect (объяснение)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Milestone Interconnect™ дает возможность подключить несколько небольших, физически разнесенных систем XProtect к центральному объекту XProtect Corporate. Такие небольшие объекты (так называемые удаленные объекты) можно создавать для мобильных систем (например, катеров, автобусов и поездов). Такие объекты не требуют постоянного сетевого подключения.

На иллюстрации ниже показан вариант настройки Milestone Interconnect в вашей системе:



1. Центральный объект XProtect Corporate Milestone Interconnect
2. Драйверы Milestone Interconnect (обеспечивают связь между серверами записи центрального и удаленного объектов, выбираются в списке драйверов при добавлении удаленных систем через мастер **добавления оборудования**)
3. Подключение Milestone Interconnect
4. Удаленный объект Milestone Interconnect (удаленный объект вместе с установленной системой, пользователями, камерами и т.д.)
5. Удаленная система Milestone Interconnect (текущая техническая система на удаленном объекте)

Чтобы добавить удаленные объекты в центральный объект, используйте мастер **добавления оборудования** на центральном объекте (см. Добавление удаленного объекта в центральный объект Milestone Interconnect на стр. 344).

Каждый удаленный объект работает автономно и обеспечивает выполнение любых стандартных задач, связанных с наблюдением. В зависимости от сетевых подключений и соответствующих разрешений пользователей (см. Назначение разрешений на стр. 345), Milestone Interconnect обеспечивает прямую передачу изображения с камер удаленных объектов и воспроизведение записей с удаленных объектов на центральном объекте.

Центральный объект имеет доступ только к тем устройствам, которые доступны для указанной учетной записи пользователя (при добавлении удаленного объекта). Таким образом, локальные системные администраторы могут контролировать, какие устройства доступны центральному объекту и его пользователям.

На центральном объекте можно просмотреть системный статус подключенных камер, при этом нельзя напрямую узнать состояние удаленного объекта. Вместо этого для мониторинга удаленного объекта можно использовать события удаленного объекта для активации тревог или прочих уведомлений на центральном объекте (см. Настройка реагирования центрального объекта на события, связанные с удаленными объектами на стр. 347).

Кроме того, система обеспечивает возможность передачи записей с удаленных объектов на центральный на основе событий, правил/расписаний или запросов пользователей XProtect Smart Client, выполняемых вручную.

Центральными объектами могут быть только системы XProtect Corporate. Все остальные продукты, в том числе XProtect Corporate, могут выполнять функции удаленных объектов. В зависимости от конкретной установки различаются версии, количество камер, а также то, как устройства и события, полученные с удаленного объекта, обрабатываются (или не обрабатываются) центральным объектом. Более подробная информация о взаимодействии конкретных продуктов XProtect при настройке Milestone Interconnect приведена на сайте Milestone Interconnect (https://www.milestonesys.com/products/expand-your-solution/milestone-extensions/interconnect/).

Выбор между Milestone Interconnect и Milestone Federated Architecture (объяснение)

В физически распределенной системе, в которой пользователям центрального объекта требуется доступ к видео на удаленном объекте, можно выбрать один из двух вариантов: Milestone Interconnect™ или Milestone Federated Architecture™.

Milestone рекомендует Milestone Federated Architecture в следующих случаях:

- сетевое подключение между центральным и федеративным сайтами стабильно;
- в сети используется один и тот же домен;
- небольшое количество крупных объектов;
- пропускная способность соответствует целям использования.

Milestone рекомендует Milestone Interconnect в следующих случаях:

- сетевое подключение между центральным и удаленным объектами нестабильно;
- вы или ваша организация хотите использовать другой продукт XProtect для удаленных объектов;
- в сети используются разные домены или рабочие группы;
- большое количество небольших объектов.

Milestone Interconnect и лицензирование

Для работы Milestone Interconnect нужны лицензии на камеры Milestone Interconnect центрального объекта, позволяющие просматривать видео с устройств на удаленных объектах. Необходимое количество лицензий на камеры Milestone Interconnect зависит от количества устройств на удаленных объектах, с которых нужно получать данные. В качестве центрального сайта может использоваться только XProtect Corporate.

Статус лицензий на камеры Milestone Interconnect отображается на странице **Информация о лицензиях** на центральном объекте.

Настройки Milestone Interconnect (объяснение)

Существует три способа запустить Milestone Interconnect. Способ настройки зависит от конкретного сетевого подключения, порядка воспроизведения записей, а также от способа получения дистанционных записей и степени их обработки.

Три наиболее распространенных варианта настройки описаны ниже:

Прямое воспроизведение с удаленных объектов (при наличии стабильного подключения к сети)

Наиболее простой вариант настройки. Центральный объект подключен к удаленным объектам в постоянном режиме, а пользователи центрального объекта дистанционно воспроизводят записи непосредственно с удаленных объектов. Для этого необходимо использовать параметр **Воспроизведение записей удаленной системы** (см. Воспроизведение напрямую с камеры удаленного объекта на стр. 346).

Получение выбранных эпизодов дистанционной записи с удаленных объектов (периодически ограниченное соединение) на основе правил или при использовании XProtect Smart Client

Используется, когда выбранные эпизоды записей (с удаленных объектов) должны храниться централизованно, чтобы обеспечить независимость от удаленных объектов. Возможность независимого доступа важна в случае отказа сети или ограниченного соединения. Параметры получения дистанционных записей настраиваются на вкладке **Дистанционное получение** (см. Вкладка «Дистанционное получение» на стр. 470).

Дистанционное получение записей может быть запущено с XProtect Smart Client при необходимости или в соответствии с заданным правилом. В некоторых сценариях удаленные объекты подключены к сети, а в других — большую часть времени отключены от сети. Как правило, это зависит от отрасли. Для некоторых отраслей характерно, когда центральный объект постоянно подключен к удаленным объектам (например, штаб-квартира предприятия розничной торговли (центральный объект) и несколько магазинов (удаленные объекты)). В других отраслях, в частности, в транспортной отрасли, удаленные объекты являются мобильными (например, автобусы, поезда, суда и так далее) и могут устанавливать сетевое соединение нерегулярно. Если сетевое подключение прерывается во время получения дистанционной записи, операция возобновится при первой же возможности.

Если система обнаружит автоматическое получение или запрос на получение от XProtect Smart Client за пределами интервала времени, указанного на вкладке **Дистанционное получение**, такой запрос будет принят, однако задача не будет запущена до наступления установленного интервала времени. Новые задачи на получение дистанционной записи будут поставлены в очередь и начнут выполняться при наступлении установленного интервала времени. Вы можете посмотреть отложенные задачи на получение дистанционной записи в разделе **Информационная панель системы** -> **Текущие задачи**.

После сбоя подключения по умолчанию запускается получение недостающих дистанционных записей с удаленных объектов.

Использование удаленных объектов подобно тому, как сервер записи использует накопитель для хранения данных на камере. Как правило, удаленные объекты подключены к центральному объекту, обеспечивая прямую передачу данных, которые записываются центральным объектом. В случае сбоя сетевого подключения центральный объект не сможет записывать эпизоды. Однако после восстановления подключения центральный объект автоматически получит дистанционные записи, относящиеся к периоду отключения. Для этого необходимо установить флажок **Автоматически получить дистанционные записи при восстановлении подключения** (см. Получение дистанционных записей с камер удаленного объекта на стр. 346) на вкладке камеры **Запись**.

В зависимости от специфики вашей организации вы можете комбинировать любые из перечисленных решений.

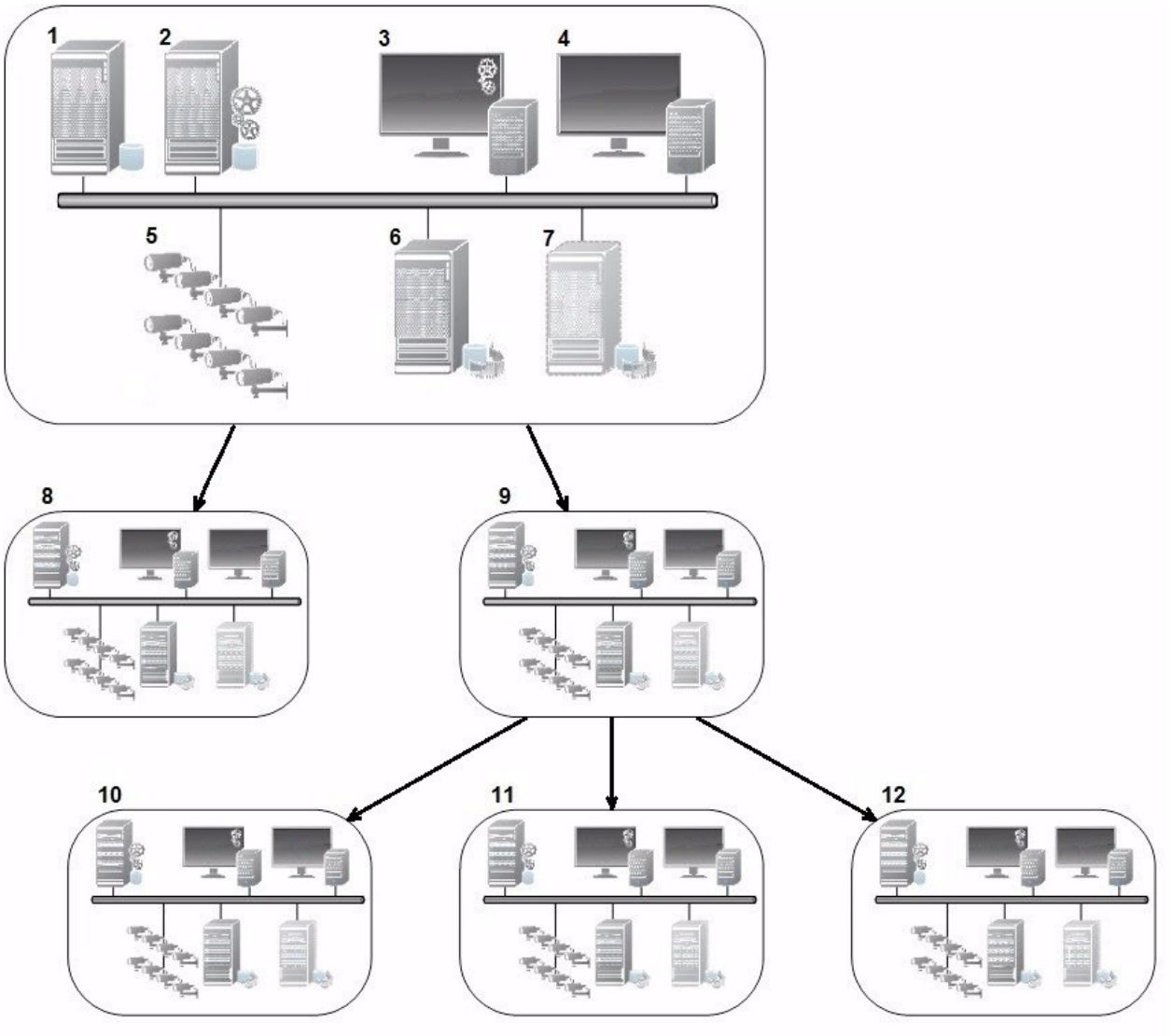
Настройка Milestone Federated Architecture

XProtect Expert поддерживает федерацию только в качестве дочернего сайта.

Milestone Federated Architecture объединяет несколько отдельных стандартных систем в иерархию федеративных сайтов, включающую родительские и дочерние сайты. Пользователи клиента с соответствующими разрешениями получают свободный доступ к видео, звуковой информации и другим ресурсам на отдельных сайтах. Администраторы могут централизованно управлять всеми сайтами версии 2018 R1 и более поздних версий в рамках федеративной иерархии с учетом разрешений для отдельных сайтов.

В системах Milestone Federated Architecture не поддерживаются базовые пользователи, поэтому необходимо добавлять пользователей с помощью службы Active Directory как пользователей Windows.

Milestone Federated Architecture имеет один центральный объект (сайт верхнего уровня) и неограниченное количество федеративных сайтов (см. Настройка системы для работы с федеративными сайтами на стр. 338). Выполнив вход на сайт, вы получаете доступ к информации обо всех дочерних сайтах, включая информацию о дочерних сайтах этих сайтов. Связь устанавливается между двумя сайтами после отправки соответствующего запроса с родительского сайта (см. Добавление сайтов в иерархию на стр. 340). Дочерний сайт может быть связан лишь с одним родительским сайтом. При добавлении дочернего сайта, администратором которого вы не являетесь, в иерархию федеративных сайтов запрос должен быть принят администратором дочернего сайта.



Компоненты настройки Milestone Federated Architecture:

1. Сервер с SQL Server
2. Сервер управления
3. Management Client
4. XProtect Smart Client
5. Камеры
6. Сервер записи
7. Сервер записи обработки отказа
8. до 12. Федеративные сайты

Синхронизация иерархии

Родительский сайт содержит обновляемый список всех своих дочерних сайтов, их дочерних сайтов и т.д. Иерархия федеративных сайтов поддерживает регулярную синхронизацию между сайтами, а также синхронизацию при добавлении или удалении сайта системным администратором. Синхронизация иерархии выполняется последовательно, уровень за уровнем. Каждый уровень передает и принимает сигнал до тех пор, пока он не достигнет сервера, который запрашивает информацию. Каждый раз система отправляет не более 1 МБ данных. В зависимости от количества уровней может потребоваться некоторое время, чтобы изменения, внесенные в иерархию, отобразились в Management Client. Вы не можете самостоятельно запланировать синхронизацию.

Поток данных

Система отправляет данные связи или конфигурации, когда пользователь или администратор просматривает трансляцию или запись видео либо выполняет настройку сайта. Объем данных зависит от того, что именно просматривается или настраивается и в каком объеме.

Взаимодействие Milestone Federated Architecture с другими продуктами и системные требования

- Возможность открытия Management Client в Milestone Federated Architecture поддерживается в трех основных выпусках, включая текущий. В случае нестандартных настроек Milestone Federated Architecture потребуется отдельная версия Management Client, соответствующая версии сервера.
- Если центральный объект использует XProtect Smart Wall, функции XProtect Smart Wall можно также использовать в иерархии федеративных сайтов.
- Если центральный объект использует XProtect Access, а пользователь XProtect Smart Client входит на сайт в иерархии федеративных сайтов, уведомления о запросах доступа с федеративных сайтов также появляются в XProtect Smart Client.
- Системы XProtect Expert 2013 или более поздних версий можно добавлять в иерархию федеративных сайтов только как дочерние сайты.
- Milestone Federated Architecture не требует дополнительных лицензий.
- Дополнительные сведения о вариантах применения и преимуществах см. в техническом описании, посвященном Milestone Federated Architecture.

Создание иерархии федеративных сайтов

Перед началом построения иерархии в Management Client Milestone рекомендует составить карту с указанием желаемых связей между сайтами.

Установите и настройте каждый сайт в федеративной иерархии как обычную автономную систему со стандартными системными компонентами, параметрами, правилами, расписаниями,

администраторами, пользователями и их разрешениями. Если у вас уже установлены и настроены сайты, и вам нужно только объединить их в иерархию федеративных сайтов, ваши системы готовы к настройке.

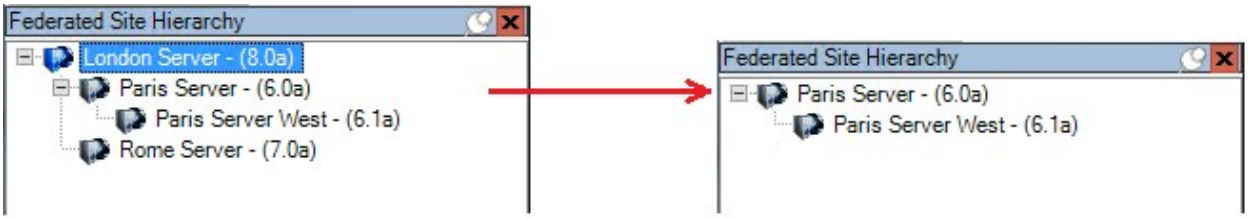
После установки отдельных сайтов настройте их для работы в качестве федеративных сайтов (см. Настройка системы для работы с федеративными сайтами на стр. 338).

Чтобы создать иерархию, войдите на сайт, который вы хотите использовать в качестве центрального, и добавьте (см. Добавление сайтов в иерархию на стр. 340) первый федеративный сайт. После установления связи два сайта автоматически формируют иерархию федеративных сайтов на панели **Иерархия федеративных сайтов** в Management Client. Вы можете добавлять туда новые сайты для расширения федеративной иерархии.

После создания иерархии федеративных сайтов пользователи и администраторы могут войти на сайт, чтобы получить доступ к этому сайту и другим доступным федеративным сайтам. Доступ к федеративным сайтам определяется разрешениями пользователей.

Количество сайтов, которые можно добавить в федеративную иерархию, не ограничено. Кроме того, вы можете привязать сайт старой версии продукта к новой версии и наоборот. Номера версий отображаются автоматически, их нельзя удалить. Сайт, на который вы вошли, отображается в верхней части панели **Иерархия федеративных сайтов** и считается главным сайтом.

Ниже приведен пример федеративного сайта в Management Client. Слева показано, что пользователь вошел на сайт верхнего уровня. Справа показано, что пользователь вошел на один из дочерних сайтов, Paris Server, который теперь является главным сайтом.



Значки статуса в Milestone Federated Architecture

Значки обозначают возможные состояния сайта:

Описание	Значок
Сайт верхнего уровня всей иерархии работает.	
Сайт верхнего уровня всей иерархии работает, но существует проблема, требующая вмешательства. Отображается над значком сайта верхнего уровня.	

Описание	Значок
Сайт работает.	
Сайт ожидает принятия в иерархию.	
Сайт подключен, но пока не работает.	

Порты, используемые системой

Ниже перечислены все компоненты XProtect и необходимые для них порты. Например, чтобы брандмауэр блокировал только нежелательный трафик, требуется указать используемые системой порты. Следует включать только эти порты. Списки также включают порты, используемые для локальных процессов.

Они объединены в две группы:

- **Серверные компоненты** (службы) работают на определенных портах. Поэтому им требуется ожидать получения запросов от клиентов на этих портах. Таким образом, для входящих и исходящих подключений эти порты должны быть открыты в Брандмауэре Windows.
- **Клиентские компоненты** (клиенты) инициируют подключения к определенным портам в серверных компонентах. Таким образом, эти порты должны быть открыты для исходящих подключений. Как правило, в Брандмауэре Windows исходящие подключения открыты по умолчанию.

Если не указано иное, порты для серверных компонентов должны быть открыты для входящих подключений, а порты для клиентских компонентов должны быть открыты для исходящих подключений.

Имейте в виду, что серверные компоненты могут действовать в качестве клиентов других серверных компонентов. Они не описаны в настоящем документе.

Номера портов представляют собой номера по умолчанию, но их можно изменить. Обратитесь в службу поддержки Milestone, если вам требуется изменить порты, которые нельзя настроить при помощи Management Client.

Серверные компоненты (входящие подключения)

В каждом из следующих разделов перечислены порты, которые должны быть открыты для конкретной службы. Чтобы понять, какие из портов требуется открыть на определенном компьютере, необходимо принять во внимание все работающие на компьютере службы.

Служба Management Server и связанные процессы

Номер порта	Протокол	Процесс	Подключения из...	Цель
80	HTTP	IIS	Все серверы и XProtect Smart Client и Management Client	Назначение портов 80 и 443 одинаково. Однако использование VMS конкретного порта зависит от применения вами сертификатов для защиты обмена данными. • Если обмен данными не защищен сертификатами, VMS использует порт 80. • Если обмен данными защищен сертификатами, VMS использует порт 443, кроме передачи данных из сервера событий в сервер управления. При передаче данных из сервера событий в сервер управления используется Windows Secured Framework (WCF) и аутентификация Windows по порту 80.
443	HTTPS	IIS		
6473	TCP	Служба Management Server	Значок Management Server Manager на панели задач, только локальное подключение.	Отображение состояния и управление службой.
8080	TCP	Сервер управления	Только локальное подключение.	Обмен данными между внутренними процессами на сервере.
9000	HTTP	Сервер управления	Службы Recording Server	Веб-служба для внутреннего обмена данными между серверами.
12345	TCP	Служба	XProtect Smart	Обмен данными между системой и

Номер порта	Протокол	Процесс	Подключения из...	Цель
		Management Server	Client	получателями Matrix. Номер порта можно изменить в Management Client.
12974	TCP	Служба Management Server	Служба SNMP Windows	Обмен данными с агентом расширения SNMP. Не используйте этот порт для других целей, даже если в системе не используется SNMP. В системах XProtect 2014 и предшествующих версий использовался номер порта 6475. В системах XProtect 2019 R2 и предшествующих версий использовался номер порта 7475.

SQL ServerСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
1433	TCP	SQL Server	Служба Management Server	Хранение и получение конфигураций через Identity Provider.
1433	TCP	SQL Server	Служба Event Server	Хранение и получение событий через Identity Provider.
1433	TCP	SQL Server	Служба Log Server	Хранение и получение записей журнала через Identity Provider.

Data CollectorСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
7609	HTTP	IIS	На компьютере сервера управления: Службы Data Collector на всех остальных серверах. На другом компьютере: Служба Data Collector на сервере управления.	Системный монитор.

Event ServerСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
1234	TCP/UDP	Служба Event Server	Любой сервер, передающий типичные события в вашу систему XProtect.	Прослушивание типичных событий из внешних систем или устройств. Только если включен соответствующий источник данных.
1235	TCP	Служба Event Server	Любой сервер, передающий типичные события в вашу систему XProtect.	Прослушивание типичных событий из внешних систем или устройств. Только если включен соответствующий источник данных.
9090	TCP	Служба Event Server	Любая система или устройства, передающие события аналитики в вашу систему XProtect.	Прослушивание событий аналитики из внешних систем или устройств. Актуально, только если включена функция «События аналитики».

Номер порта	Протокол	Процесс	Подключения из...	Цель
22331	TCP	Служба Event Server	XProtect Smart Client и Management Client	Конфигурация, события, сигналы тревоги и данные карт.
22332	WS/WSS HTTP/HTTPS*	Служба Event Server	API Gateway и Management Client	REST API событий, событий/подписок на состояние, API сообщений WebSockets и REST API сигналов тревоги.
22333	TCP	Служба Event Server	Приложения и встраиваемые расширения MIP.	Обмен сообщениями MIP.

* Ошибка 403 будет возвращена при получении доступа к HTTP для доступа к конечной точке, поддерживающей только HTTPS.

Recording ServerСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
25	SMTP	Служба Recording Server	Камеры, кодеры и устройства ввода/вывода.	Прослушивание сообщений о событиях с устройств. Порт отключен по умолчанию. (Не рекомендуется) при включении этой функции открывается порт для незашифрованных подключений, и это не рекомендуется.
5210	TCP	Служба Recording Server	Серверы записи обработки отказа.	Объединение баз данных после запуска сервера записи обработки отказа.

Номер порта	Протокол	Процесс	Подключения из...	Цель
5432	TCP	Служба Recording Server	Камеры, кодеры и устройства ввода/вывода.	Прослушивание сообщений о событиях с устройств. Порт отключен по умолчанию.
7563	TCP	Служба Recording Server	XProtect Smart Client, Management Client	Получение видео- и аудиопотоков, команд PTZ.
8966	TCP	Служба Recording Server	Значок Recording Server Manager на панели задач, только локальное подключение.	Отображение состояния и управление службой.
9001	HTTP	Служба Recording Server	Сервер управления	Веб-служба для внутреннего обмена данными между серверами. Если используется несколько экземпляров сервера записи, каждому экземпляру необходимо назначить собственный порт. Номерами дополнительных портов будут 9002, 9003 и т.д.
11000	TCP	Служба Recording Server	Серверы записи обработки отказа	Опрос состояния серверов записи.
12975	TCP	Служба Recording Server	Служба SNMP Windows	Обмен данными с агентом расширения SNMP. Не используйте этот порт для других целей, даже если в системе не используется SNMP. В системах XProtect 2014 и предшествующих версий использовался номер порта 6474. В системах XProtect 2019 R2 и

Номер порта	Протокол	Процесс	Подключения из...	Цель
				предшествующих версий использовался номер порта 7474.
65101	UDP	Служба Recording Server	Только локальное подключение	Прослушивание уведомлений о событиях от драйверов.

Помимо входящих подключений к службе Recording Server, перечисленных выше, служба Recording Server устанавливает исходящие подключения к:

- Камеры
- Сетевые видеорегистраторы
- Удаленные взаимосвязанные сайты (Milestone Interconnect ICP)

Службы Failover Server и Failover Recording Server

Номер порта	Протокол	Процесс	Подключения из...	Цель
25	SMTP	Служба Failover Recording Server	Камеры, кодеры и устройства ввода/вывода.	Прослушивание сообщений о событиях с устройств. Порт отключен по умолчанию. (Не рекомендуется) при включении этой функции открывается порт для незашифрованных подключений, и это не рекомендуется.
5210	TCP	Служба Failover Recording	Серверы записи обработки отказа	Объединение баз данных после запуска сервера записи обработки отказа.

Номер порта	Протокол	Процесс	Подключения из...	Цель
		Server		
5432	TCP	Служба Failover Recording Server	Камеры, кодеры и устройства ввода/вывода.	Прослушивание сообщений о событиях с устройств. Порт отключен по умолчанию.
7474	TCP	Служба Failover Recording Server	Служба SNMP Windows	Обмен данными с агентом расширения SNMP. Не используйте этот порт для других целей, даже если в системе не используется SNMP.
7563	TCP	Служба Failover Recording Server	XProtect Smart Client	Получение видео- и аудиопотоков, команд PTZ.
8844	UDP	Служба Failover Recording Server	Обмен данными между службами Failover Recording Server.	Обмен данными между серверами.
8966	TCP	Служба Failover Recording Server	Значок Failover Recording Server Manager на панели задач, только локальное подключение.	Отображение состояния и управление службой.
8967	TCP	Служба Failover Server	Значок Failover Server Manager на панели задач, только локальное подключение.	Отображение состояния и управление службой.
8990	HTTP	Служба Failover Server	Служба Management Server	Мониторинг состояния службы Failover Server.

Номер порта	Протокол	Процесс	Подключения из...	Цель
9001	HTTP	Служба Failover Server	Сервер управления	Веб-служба для внутреннего обмена данными между серверами.

Помимо исходящих подключений к службе Failover Server/Failover Recording Server, указанным выше, служба Failover Server/Failover Recording Server устанавливает исходящие подключения к обычным записывающим устройствам, камерам, а также для передачи видео (Video Push).

Log ServerСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
22337	HTTP	Служба Log Server	Все компоненты XProtect, кроме сервера записи.	Запись в, чтение из и настройка сервера регистрации.

Этот порт использует HTTP, но связь шифруется с помощью системы безопасности сообщений, которая использует WS-Security для защиты сообщений. Дополнительные сведения см. в разделе Безопасность сообщений в WCF.

Mobile ServerСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
8000	TCP	Служба	Значок Mobile Server Manager на	Приложение SysTray.

Номер порта	Протокол	Процесс	Подключения из...	Цель
		Mobile Server	панели задач, только локальное подключение.	
8081	HTTP	Служба Mobile Server	Мобильные клиенты, веб-клиенты и Management Client.	Отправка потоков данных; видео и аудио.
8082	HTTPS	Служба Mobile Server	Мобильные клиенты и веб-клиенты.	Отправка потоков данных; видео и аудио.
40001 - 40099	HTTP	Служба Mobile Server	Сервис Recording Server	Video Push Mobile Server. Это диапазон портов отключен по умолчанию.

LPR ServerСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
22334	TCP	Служба LPR Server	Сервер событий	Получение распознанных номерных знаков и статуса сервера. Для подключения на сервере событий должно быть установлено встраиваемое расширение распознавания номерного знака (LPR).
22334	TCP	Служба LPR Server	Значок LPR Server Manager на панели задач, только локальное подключение.	Приложение SysTray

Milestone Open Network BridgeСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
580	TCP	Служба Milestone Open Network Bridge	Клиенты ONVIF	Аутентификация и запросы конфигурации видеопотоков.
554	RTSP	Служба RTSP	Клиенты ONVIF	Потоковая передача запрошенного видео на клиенты ONVIF.

XProtect DLNA ServerСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
9100	HTTP	Служба DLNA Server	Устройство DLNA	Обнаружение устройств и предоставление конфигурации каналов DLNA. Запрос видеопотоков.
9200	HTTP	Служба DLNA Server	Устройство DLNA	Потоковая передача запрошенного видео на устройства DLNA.

XProtect Screen RecorderСлужба

Номер порта	Протокол	Процесс	Подключения из...	Цель
52111	TCP	XProtect	Служба	Предоставляет видео с монитора. Выглядит

Номер порта	Протокол	Процесс	Подключения из...	Цель
		Screen Recorder	Recording Server	и действует так же, как камера на сервере записи. Номер порта можно изменить в Management Client.

Служба XProtect Incident Manager

Номер порта	Протокол	Процесс	Подключения из...	Цель
80	HTTP	IIS	XProtect Smart Client и Management Client	Назначение портов 80 и 443 одинаково. Однако использование VMS конкретного порта зависит от применения вами сертификатов для защиты обмена данными. • Если обмен данными не защищен сертификатами, VMS использует порт 80. • Если обмен данными защищен сертификатами, VMS использует порт 443.
443	HTTPS	IIS		

Серверные компоненты (исходящие подключения)

Management ServerСлужба

Номер порта	Протокол	Подключения к...	Цель
443	HTTPS	Сервер лицензий, на котором размещена служба управления лицензиями. Обмен данными по https://www.milestonesys.com/OnlineActivation/ LicenseManagementService.asmx	Активация лицензий.

Recording ServerСлужба

Номер порта	Протокол	Подключения к...	Цель
80	HTTP	Камеры, сетевые видеорегистраторы, кодеры Взаимосвязанные сайты	Аутентификация, конфигурация, потоки данных, видео и аудио. Вход в систему
443	HTTPS	Камеры, сетевые видеорегистраторы, кодеры	Аутентификация, конфигурация, потоки данных, видео и аудио.
554	RTSP	Камеры, сетевые видеорегистраторы, кодеры	Потоки данных, видео и аудио.
7563	TCP	Взаимосвязанные сайты	Потоки данных и события.
11000	TCP	Серверы записи обработки отказа	Опрос состояния серверов записи.
40001–40099	HTTP	Служба Mobile Server	Функция Video Push мобильного сервера. Это диапазон портов отключен по умолчанию.

Службы Failover Server и Failover Recording Server

Номер порта	Протокол	Подключения к...	Цель
11000	TCP	Серверы записи обработки отказа	Опрос состояния серверов записи.

Event ServerСлужба

Номер порта	Протокол	Подключения к...	Цель
80	HTTP	API Gateway и Management Server	Доступ к API конфигурации из API Gateway
443	HTTPS	API Gateway и Management Server	Доступ к API конфигурации из API Gateway
443	HTTPS	Milestone Customer Dashboard через https://service.milestonesys.com/	Отправка статуса, событий и сообщений об ошибках из системы XProtect в Milestone Customer Dashboard.

Log ServerСлужба

Номер порта	Протокол	Подключения к...	Цель
443	HTTP	Сервер журналов	Пересылка сообщений на сервер регистрации.

API Gateway

Номер порта	Протокол	Подключения к...	Цель
443	HTTPS	Management Server	RESTful API
22332	WS/WSS HTTP/HTTPS*	Management Client	REST API событий, событий/подписок на состояние, API сообщений WebSockets и REST API сигналов тревоги.

Камеры, кодеры и устройства ввода/вывода (входящие подключения)

Номер порта	Протокол	Подключения из...	Цель
80	TCP	Основные и резервные серверы записи	Аутентификация, конфигурация и потоки данных; видео и аудио.
443	HTTPS	Основные и резервные серверы записи	Аутентификация, конфигурация и потоки данных; видео и аудио.
554	RTSP	Основные и резервные серверы записи	Потоки данных; видео и аудио.

Камеры, кодеры и устройства ввода/вывода (исходящие подключения)

Номер порта	Протокол	Подключения к...	Цель
25	SMTP	Основные и резервные серверы записи	Отправка уведомлений о событиях (не рекомендуется).
5432	TCP	Основные и резервные серверы записи	Отправка уведомлений о событиях. Порт отключен по умолчанию.
22337	HTTP	Сервер журналов	Пересылка сообщений на сервер регистрации.

Только несколько моделей камер могут устанавливать исходящие подключения.

Клиентские компоненты (исходящие подключения)

XProtect Smart Client, XProtect Management Client, сервер XProtect Mobile

Номер порта	Протокол	Подключения к...	Цель
80	HTTP	API Gateway и служба Management Server	Аутентификация и другие API в API Gateway.
443	HTTPS	API Gateway и служба Management Server	Аутентификация базовых пользователей, если включено шифрование и другие API в API Gateway.
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com по адресу 52.178.114.226)	Management Client и Smart Client иногда проверяют, доступна ли онлайн-справка, получая доступ к URL-адресу справки.
7563	TCP	Служба Recording Server	Получение видео- и аудиопотоков, команд PTZ.
22331	TCP	Служба Event Server	сигналы тревоги.

XProtect Web Client, клиент XProtect Mobile

Номер порта	Протокол	Подключения к...	Цель
8081	HTTP	Сервер XProtect Mobile	Получение видео- и аудиопотоков.
8082	HTTPS	Сервер XProtect Mobile	Получение видео- и аудиопотоков.

API Gateway

Номер порта	Протокол	Подключения к...	Цель
80	HTTP	Management Server	RESTful API
443	HTTPS	Management Server	RESTful API

Пулы приложений

VMS содержит стандартные пулы приложений, такие как .NET v4.5, .NET v4.5 Classic и DefaultAppPool. Пулы приложений, доступные в вашей системе, отображаются в диспетчере служб Internet Information Services (IIS). В дополнение к упомянутым выше стандартным пулам приложений вместе с Milestone XProtect VMS поставляется набор пулов приложений VideoOS.

Пулы приложений в Milestone XProtect

В таблице ниже приведены пулы приложений VideoOS, поставляемые с Milestone XProtect.

Имя	Идентификатор	Цель
.NET v4.5	ApplicationPoolId	Стандартная функция IIS
.NET v4.5 Classic	ApplicationPoolId	Стандартная функция IIS
DefaultAppPool	ApplicationPoolId	Стандартная функция IIS
VideoOS ApiGateway	NetworkService	Размещает шлюз API XProtect, который затем становится общедоступным API и шлюзом для VMS.
VideoOS Classic	NetworkService	Размещает унаследованные компоненты, такие как локальная справка, в основном для обеспечения обратной совместимости.
VideoOS IDP	NetworkService	Размещает API Identity Provider. Identity Provider

Имя	Идентификатор	Цель
		создает, поддерживает идентификационную информацию базовых пользователей и управляет ей, а также предоставляет службы аутентификации и регистрации нуждающимся приложениям или службам.
VideoOS IM	NetworkService	Размещает API XProtect Incident Manager. XProtect Incident Manager документирует инциденты и комбинирует их с доказательствами эпизода (видео и, если применимо, аудио) из XProtect VMS.
VideoOS Management Server	NetworkService	Размещает API конфигурации, API компонентов сервера и другие службы Management Server, а также управляет авторизацией пользователей.

Имя	Идентификатор	Цель
VideoOS ReportServer	NetworkService	Размещает веб-приложение, отвечающее за сбор и создание отчетов о сигналах тревоги и событиях.
VideoOS ShareService	NetworkService	Размещает службу, которая упрощает общий доступ к отметкам и видео в режиме реального времени между пользователями клиента XProtect Mobile.

Работа с пулами приложений

На странице **Пулы приложений** в окне **Службы IIS** вы можете добавить пулы приложений или задать значения по умолчанию для пула приложений, а также просматривать приложения, размещенные в каждом пуле.

Откройте страницу «Пулы приложений»

1. В меню **Пуск** Windows откройте **Диспетчер информационных служб Интернета (IIS)**.
2. На панели **Подключения** нажмите имя среды и выберите **Пулы приложений**.
3. В области **Действия** нажмите **Добавить пул приложений** или **Задать значения по умолчанию для пула приложений**, чтобы выполнить соответствующую задачу.
4. Выберите пул приложений на странице **Пулы приложений**, чтобы отобразить дополнительные параметры в области **Действия** для каждого пула приложений.

Сравнение продуктов

VMS XProtect включает следующие продукты:

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+
- XProtect Essential+

Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Лицензирование

Лицензии (объяснение)

Бесплатная версия XProtect Essential+

После установки системы XProtect Essential+ в ней можно работать с восемью бесплатными лицензиями на устройство. Активация лицензий происходит автоматически, а активация оборудования осуществляется при его добавлении в систему.

Остальная часть данного раздела и содержимое других разделов этой документации, связанных с лицензированием, будет актуальна только при переходе на продукт XProtect с расширенными функциями и при необходимости изменить код лицензии на программное обеспечение (SLC) (см. Изменение кода лицензии на программное обеспечение на стр. 140).

Лицензии на продукты VMS XProtect (за исключением XProtect Essential+)

Файл лицензии программного обеспечения и код лицензии на программное обеспечение

При покупке программного обеспечения и лицензий вы получите:

- Подтверждение заказа и файл лицензии на программное обеспечение (SLC) с расширением .lic по электронной почте
- Договор обслуживания Milestone Care

Ваш код лицензии на программное обеспечение также указан в подтверждении заказа. Код содержит несколько цифр и букв, разделенных дефисами. Например:

- Версия продукта 2014 или более ранняя: xxx-xxxx-xxxx
- Версия продукта 2016 или более поздняя: xxx-xxx-xxx-xx-xxxxxx

Файл лицензии программного обеспечения содержит всю информацию о приобретенных вами продуктах VMS, расширениях XProtect и лицензиях. Milestone рекомендует хранить информацию о коде лицензии на программное обеспечение и копию файла лицензии программного обеспечения в надежном месте для последующего использования. Код лицензии на программное обеспечение также можно найти в окне **Сведения о лицензии** в Management Client. Чтобы открыть окно **Сведения о лицензии**, на панели **Навигация по сайту** перейдите к узлу **Основы** -> **Сведения о лицензии**. Файл лицензии программного обеспечения или код лицензии на программное обеспечение может потребоваться, например для создания учетной записи пользователя My Milestone, обращения к реселлеру за поддержкой или при необходимости внести изменения в систему.

Общее описание процедуры установки и лицензирования

Сначала необходимо загрузить программное обеспечение с нашего сайта (https://www.milestonesys.com/downloads/). Во время установки (см. Установка новой системы XProtect на стр. 164) программы потребуется файл лицензии программного обеспечения. Вы не сможете завершить установку без файла лицензии программного обеспечения.

После завершения установки и добавления нескольких камер необходимо активировать лицензии (см. Активация лицензии (объяснение) на стр. 131). Активация лицензий выполняется в окне **Сведения о лицензии** в Management Client. Здесь также приводится обзор лицензий для всех установок с одним кодом лицензии на программное обеспечение. Чтобы открыть окно **Сведения о лицензии**, на панели **Навигация по сайту** перейдите к узлу **Основы** -> **Сведения о лицензии**.

Типы лицензий

В системе лицензирования XProtect несколько типов лицензий.

Базовые лицензии

У вас есть как минимум базовая лицензия на один из продуктов XProtect. У вас также могут быть базовые лицензии на расширения XProtect.

Лицензии на устройства

У вас как минимум несколько лицензий на устройства. Вообще говоря, для каждого аппаратного устройства с камерой, подключаемого к системе, нужна одна лицензия на устройство. Однако это может зависеть от типа устройства и от того, поддерживается ли аппаратное обеспечение устройства системой Milestone. Дополнительные сведения приведены в разделах Поддерживаемые аппаратные устройства на стр. 130 и Неподдерживаемые аппаратные устройства на стр. 131.

Для применения функции Video Push XProtect Mobile нужна одна лицензия на каждое мобильное устройство или планшет, которые должны передавать видео в вашу систему.

Лицензии на устройства не нужны для динамиков, микрофонов и устройств ввода-вывода, подключенных к камерам.

Поддерживаемые аппаратные устройства

Вообще говоря, для каждого аппаратного устройства с камерой, подключаемого к системе, нужна одна лицензия на устройство. Однако для некоторых поддерживаемых аппаратных устройств нужно несколько лицензий. Информацию о количестве лицензий, необходимых для аппаратного устройства, приведена на сайте Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Для видеокодеров до 16 каналов требуется только одна лицензия на каждый IP-адрес кодера. У видеокодера могут быть один или несколько IP-адресов.

Если у видеокодера более 16 каналов, требуется одна лицензия на каждую активированную камеру видеокодера, причем это требование распространяется и на первые 16 активированных камер.

Неподдерживаемые аппаратные устройства

Неподдерживаемые аппаратные устройства нуждаются в одной лицензии на каждую активированную камеру, использующую видеоканал.

Неподдерживаемые аппаратные устройства не показаны в списке поддерживаемого аппаратного обеспечения на сайте Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Лицензии на камеры Milestone Interconnect™

Для работы Milestone Interconnect нужны лицензии на камеры Milestone Interconnect центрального объекта, позволяющие просматривать видео с устройств на удаленных объектах. Необходимое количество лицензий на камеры Milestone Interconnect зависит от количества устройств на удаленных объектах, с которых нужно получать данные. В качестве центрального сайта может использоваться только XProtect Corporate.

Лицензии на расширения XProtect

Для большинства расширений XProtect требуются дополнительные лицензии. Файл лицензии программного обеспечения также содержит информацию о ваших лицензиях на расширения. У некоторых расширений предусмотрены собственные файлы лицензий.

Активация лицензии (объяснение)

Код лицензии на программное обеспечение нужно зарегистрировать до начала установки (см. Зарегистрируйте код лицензии на программное обеспечение на стр. 160). Также необходимо активировать лицензии, связанные с кодом лицензии на программное обеспечение, чтобы обеспечить работу установленной системы VMS XProtect и расширений XProtect, а также передачу данных в систему с отдельных аппаратных устройств. Дополнительные сведения о всех типах лицензий XProtect приведены в разделе Типы лицензий на стр. 130.

Есть несколько способов активации лицензий. Все они доступны в окне **Сведения о лицензии**. Оптимальный способ активации зависит от политик вашей организации и наличия у сервера управления доступа к Интернету. Информация об активации лицензий приведена в разделе Активируйте лицензии на стр. 137.

После первоначальной активации лицензий VMS XProtect не требуется каждый раз активировать лицензии на устройства, когда вы добавляете аппаратное устройство с камерой. Это возможно благодаря встроенным возможностям системы лицензирования XProtect. Дополнительные сведения об этих функциях системы приведены в разделе Льготный период активации лицензии (объяснение) на стр. 132 и Изменения устройств без активации (объяснение) на стр. 133.

Автоматическая активация лицензии (объяснение)

Для упрощения обслуживания и дополнительной гибкости Milestone рекомендует включить автоматическую активацию лицензии, если это разрешено политиками вашей организации. Для автоматической активации лицензии необходимо, чтобы сервер управления был подключен к сети. Дополнительные сведения о порядке включения автоматической активации лицензии приведены в разделе Включить автоматическую активацию лицензии на стр. 137.

Преимущества включения автоматической активации лицензий

- Система активирует аппаратные устройства через несколько минут после их добавления, удаления, замены или внесения других изменений, которые влияют на использование лицензий. Таким образом запускать активацию лицензии вручную требуется лишь в редких случаях. Исключения приведены в разделе Случаи, при которых требуется активация лицензии вручную на стр. 132.
- Установленное количество изменений устройств без активации равно нулю.
- Нет аппаратных устройств с действующим льготным периодом или с истекающим сроком действия.
- Если срок действия одной из базовых лицензий истекает в течение 14 дней, то в целях дополнительной предосторожности система XProtectкаждую ночь будет пытаться активировать лицензии в автоматическом режиме.

Случаи, при которых требуется активация лицензии вручную

Если вы вносите в систему следующие изменения, требуется активация лицензии вручную.

- Приобретениедополнительныхлицензий(см.Приобретениедополнительныхлицензийнастр. 139)
- Переходнановуюилирасширенную версиюсистемыVMS(см.Требованиякобновлениюнастр.407)
- Покупка или продление подписки Milestone Care
- Получение разрешения на дополнительные изменения устройств без активации (см. Изменения устройств без активации (объяснение) на стр. 133)

Льготный период активации лицензии (объяснение)

После установки VMS и добавления устройств (аппаратных устройств, камер Milestone Interconnect или лицензий на двери) для них действует 30-дневный льготный период, если не включена автоматическая активация лицензий. Вы должны активировать лицензии до окончания 30-дневного льготного периода, если у вас не осталось доступных изменений устройств без активации, иначе ваши устройства перестанут отправлять видео в систему наблюдения.

Изменения устройств без активации (объяснение)

Функция изменения устройств без активации обеспечивает гибкие встроенные возможности системы лицензирования XProtect. Даже если вы решите активировать лицензии вручную, вы можете избежать необходимости активировать лицензии при каждом добавлении или удалении аппаратных устройств.

Количество изменений устройств без активации различно для разных систем и вычисляется на базе нескольких переменных. Подробное описание см. в разделе Расчет доступного количества изменений устройств без активации (объяснение) на стр. 133.

Через год после последней активации лицензии использованное число изменений устройств без активации автоматически сбрасывается до нуля. После этого можно продолжать добавлять и заменять аппаратные устройства, не активируя лицензии.

Если система наблюдения долгое время работает в автономном режиме, например на судне, уходящем в дальнее плавание, или в очень отдаленных местах без доступа к Интернету, вы можете обратиться к реселлеру Milestone и запросить увеличение числа изменений устройств без активации.

Потребность в увеличении количества изменений без активации потребуется обосновать. Milestone рассматривает каждый запрос в индивидуальном порядке. Если вы получите дополнительное количество изменений устройств без активации, вам потребуется активировать лицензии, чтобы зарегистрировать такое дополнительное количество в системе XProtect.

Расчет доступного количества изменений устройств без активации (объяснение)

Доступное количество изменений устройств без активации рассчитывается с учетом трех переменных. Если у вас несколько установок программы Milestone, переменные применяются к каждой из них по отдельности. Переменные:

- **C%** — фиксированный процент от общего количества активированных лицензий
- **Cmin** — фиксированное минимальное количество изменений устройств без активации
- **Cmax** — фиксированное максимальное количество изменений устройств без активации

Количество изменений устройств без активации не должно быть меньше значения **Cmin** или больше значения **Cmax**. Значение, рассчитываемое на основе переменной **C%**, меняется в зависимости от количества активированных устройств в каждой установке в вашей системе. Устройства, добавленные в результате изменения без активации, не считаются активированными с помощью переменной **C%**.

Milestone задает значения всех трех переменных. Эти значения могут быть изменены без предварительного уведомления. Значения переменных определяются с учетом характеристик конкретного продукта.

Примеры, рассчитанные с учетом следующих параметров: C% = 15%, Cmin = 10 и Cmax = 100

Вы приобрели 100 лицензий на устройства. Затем добавили в систему 100 камер. Если вы не включили автоматическую активацию лицензии, количество изменений устройства без активации будет равно нулю. После активации лицензий у вас в распоряжении будет 15 изменений устройств без активации.

Вы приобрели 100 лицензий на устройства. Затем добавили в систему 100 камер и активировали лицензии. Количество изменений устройств без активации равно 15. После этого вы решили удалить одно аппаратное устройство из системы. Теперь у вас 99 активированных устройств, а количество изменений устройств без активации сократилось до 14.

Вы приобрели 1000 лицензий на устройства. Затем добавили в систему 1000 камер и активировали лицензии. Количество изменений устройств без активации равно 100. В соответствии с переменной **C%** вам должно было быть доступно 150 изменений устройств без активации. Однако с учетом переменной **Cmax** вам доступно только 100 изменений устройств без активации.

Вы приобрели 10 лицензий на устройства. Затем добавили в систему 10 камер и активировали лицензии. Количество изменений устройств без активации равно 10 с учетом переменной **Cmin**. Если бы это значение рассчитывалось только на основе переменной **C%**, то в результате расчета получалось бы значение 1 (15 % от 10 = 1,5 с округлением до 1).

Вы приобрели 115 лицензий на устройства. Затем добавили в систему 100 камер и активировали лицензии. Количество изменений устройств без активации равно 15. Вы добавили еще 15 камер без их активации, воспользовавшись 15 из 15 доступных изменений устройств без активации. После этого вы удалили из системы 50 камер, а количество изменений устройств без активации уменьшилось до 7. Это значит, что 8 камер, ранее добавленных в рамках 15 изменений устройств без активации, перешли под действие льготного периода. Вы добавили 50 новых камер. Так как в последний раз вы активировали 100 камер в системе, количество изменений устройств без активации снова стало равно 15. Соответственно 8 камер, которые попали под действие льготного периода, перешли в категорию изменений устройств без активации. 50 новых камер попадают под действие льготного периода.

Milestone Care™ (объяснение)

Milestone Care — это название комплексной программы обслуживания и поддержки продуктов XProtect на протяжении всего срока их службы.

Milestone Care обеспечивает доступ к различным типам материалов для самостоятельного изучения, включая статьи в Knowledge Base, руководства и учебные пособия на нашем веб-сайте поддержки (https://www.milestonesys.com/support/).

Для получения дополнительных преимуществ вы можете приобрести расширенные подписки Milestone Care.

Milestone Care Plus

Если у вас есть подписка Milestone Care Plus, то вам также доступны бесплатные обновления текущего продукта VMS XProtect. Более того, вы можете перейти на расширенные версии продуктов VMS XProtect по выгодной цене. Milestone Care Plus также обеспечивает дополнительные функциональные возможности:

- сервис «Панель мониторинга клиента»,
- функция интеллектуального соединения,
- полный набор функций Push-уведомлений.

Milestone Care Premium

Если у вас есть подписка Milestone Care Premium, вы также можете напрямую связаться со службой поддержки Milestone. При обращении в службу поддержки Milestone не забудьте указать сведения об идентификаторе Milestone Care.

Истечение срока действия, продление и приобретение расширенных подписок Milestone Care

Срок действия расширенных типов подписки Milestone Care Plus и Milestone Care Premium отображается в окне **Сведения о лицензии** в таблице **Установленные продукты**. См. раздел Установленные продукты на стр. 142.

Если вы хотите приобрести или продлить подписку Milestone Care после установки системы, активируйте лицензии вручную, чтобы отобразилась корректная информация о Milestone Care. См. раздел Интерактивная активация лицензии на стр. 138 или Автономная активация лицензий на стр. 138.

Лицензии и замена оборудования (объяснение)

Если вы хотите заменить камеру на новую из-за ее неисправности или по иным причинам, есть несколько оптимальных способов, как это сделать.

Если вы удаляете камеру с сервера записи, у вас освобождается лицензия на устройство, однако вы лишитесь полного доступа ко всем базам данных (камеры, микрофоны, устройства ввода и вывода) и настройкам этой камеры. Чтобы сохранить доступ к базам данных старой камеры и повторно использовать ее настройки при установке новой, выполните указанные ниже действия.

Замена камеры на аналогичную

Если при замене камеры на аналогичную (тот же производитель, марка и модель) вы присвоите новой камере тот же IP-адрес, что был у старой камеры, вы сохраните полный доступ ко всем ее базам данных. Новая камера будет использовать те же базы данных и настройки. В этом случае вы подключаете сетевой кабель к новой камере, ничего не меняя в настройках Management Client.

Замена камеры на камеру с другими характеристиками

При замене существующей камеры на камеру с другими характеристиками (отличается производитель, марка или модель) используйте мастер **Замена оборудования** (см. Замена оборудования на стр. 377) для сопоставления всех соответствующих баз данных старой камеры с новой и повторного использования ее настроек.

Активация лицензии после замены оборудования

Если вы включили автоматическую активацию лицензии (см. Включить автоматическую активацию лицензии на стр. 137), новая камера активируется автоматически.

Если автоматическая активация лицензий отключена, а все доступные изменения устройств без активации были использованы (см. Изменения устройств без активации (объяснение) на стр. 133), активируйте лицензии вручную. Дополнительные сведения об активации лицензий вручную приведены в разделе Интерактивная активация лицензии на стр. 138 и Автономная активация лицензий на стр. 138.

Обзор лицензий

Необходимость получения информации о коде лицензии на программное обеспечение, количестве приобретенных лицензий и их статусе может быть обусловлена рядом причин. Вот некоторые из них:

- Вам необходимо добавить новое аппаратное устройство или даже несколько. Возникает ряд вопросов. Есть ли у вас неиспользованные лицензии на устройства или нужно приобретать новые?
- Скоро закончится льготный период некоторых аппаратных устройств? Тогда вам необходимо активировать их до того, как они перестанут отправлять данные в VMS.
- Вам известно, что службе поддержки нужен код лицензии на программное обеспечение и идентификатор Milestone Care, чтобы помочь вам. Но как их узнать?
- У вас много установок XProtect и для всех них используется одинаковый код лицензии на программное обеспечение. А вы знаете, где используются лицензии и каков их статус?

Вы можете найти эту информацию в окне **Сведения о лицензии**.

Чтобы открыть окно **Сведения о лицензии**, на панели **Навигация по сайту** перейдите к узлу **Основы** -> **Сведения о лицензии**.

Дополнительную информацию о различных сведениях и функциях, доступных в окне **Сведения о лицензии**, см. в разделе Окно «Сведения о лицензии» на стр. 141.

Активируйте лицензии

Есть несколько способов активации лицензий. Все они доступны в окне **Сведения о лицензии**. Оптимальный способ активации зависит от политик вашей организации и наличия у сервера управления доступа к Интернету.

Чтобы открыть окно **Сведения о лицензии**, на панели **Навигация по сайту** перейдите к узлу **Основы** -> **Сведения о лицензии**.

Дополнительную информацию о различных сведениях и функциях, доступных в окне **Сведения о лицензии**, см. в разделе Окно «Сведения о лицензии» на стр. 141.

Включить автоматическую активацию лицензии

Для упрощения обслуживания и дополнительной гибкости Milestone рекомендует включить автоматическую активацию лицензии, если это разрешено политиками вашей организации. Для автоматической активации лицензии необходимо, чтобы сервер управления был подключен к сети.

Дополнительные сведения о преимуществах автоматической активации лицензий приведены в разделе Автоматическая активация лицензии (объяснение) на стр. 132.

1. На панели **Навигация по сайту** в узле **Основы** -> **Сведения о лицензии** выберите **Включить автоматическую активацию лицензии**.
2. Введите имя пользователя и пароль, которые вы хотите использовать для автоматической активации лицензии:
   - Введите имя существующего пользователя и пароль для входа в систему регистрации ПО.
   - Чтобы создать учетную запись для нового пользователя, перейдите по ссылке **Создать нового пользователя** и пройдите процедуру регистрации. Если вы еще не зарегистрировали код лицензии на программное обеспечение, это необходимо сделать.

   Учетные данные хранятся в файле на сервере управления.
3. Нажмите кнопку **OK**.

Если впоследствии вы захотите изменить имя пользователя и (или) пароль автоматической активации, перейдите по ссылке **Редактировать учетные данные активации**.

Отключение автоматической активации лицензии

Если в вашей организации запрещено использовать автоматическую активацию лицензий, или же вы передумали ее использовать, отключите автоматическую активацию лицензий.

Способ отключения зависит от дальнейших планов по использованию автоматической активации лицензий.

Отключить, но сохранить пароль для последующего использования:

1. На панели **Навигация по сайту** в узле **Основы** -> **Сведения о лицензии** снимите флажок **Включить автоматическую активацию лицензии**. Имя пользователя и пароль будут храниться на сервере управления и в дальнейшем.

Отключить и удалить пароль:

1. На панели **Навигация по сайту** в узле **Основы** -> **Сведения о лицензии** нажмите **Редактировать учетные данные активации**.
2. Нажмите **Удалить пароль**.
3. Подтвердите удаление имени пользователя и пароля с сервера управления.

Интерактивная активация лицензии

Если на сервере управления есть выход в Интернет, при этом вы предпочитаете запустить процесс активации вручную, то для вас это самый оптимальный вариант активации лицензии.

1. На панели **Навигация по сайту** в узле **Основы** -> **Сведения о лицензии** выберите **Активировать лицензию вручную**, затем выберите **Онлайн**.
2. Откроется диалоговое окно **Интерактивная активация**:
   - Если вы уже зарегистрированы в системе, введите имя пользователя и пароль.
   - Чтобы создать учетную запись для нового пользователя, нажмите ссылку **Создать нового пользователя**. Если вы еще не зарегистрировали код лицензии на программное обеспечение, это необходимо сделать.
3. Нажмите кнопку **OK**.

Если во время интерактивной активации появится сообщение об ошибке, следуйте инструкциям на экране, чтобы устранить проблему, или обратитесь в службу поддержки Milestone.

Автономная активация лицензий

Если на сервере управления вашей организации нет доступа к Интернету, активируйте лицензии вручную в автономном режиме.

1. На панели **Навигация по сайту** в узле **Основы** -> **Сведения о лицензии** выберите **Активировать лицензию вручную** > **Автономно** > **Экспорт активированной лицензии**, чтобы экспортировать файл запроса лицензии (LRQ) с информацией о добавленных вами аппаратных устройствах и других компонентах, требующих лицензии.
2. Файлу запроса лицензии (LRQ) автоматически присваивается то же имя, что и коду лицензии на программное обеспечение. Если у вас несколько объектов, не забудьте переименовать файлы, чтобы можно было легко идентифицировать, какой файл принадлежит тому или иному объекту.

3. Скопируйте файл запроса лицензии на компьютер с доступом в Интернет и авторизуйтесь на нашем веб-сайте (https://online.milestonesys.com/), чтобы получить активированный файл лицензии программного обеспечения (LIC).
4. Скопируйте полученный файл в формате LIC на свой компьютер с помощью Management Client. Имя файла совпадает с именем файла запроса лицензии.
5. На панели **Навигация по сайту** в узле **Основы** -> **Сведения о лицензии** выберите **Активировать лицензию в автономном режиме** > **Импорт активированной лицензии**, а затем выберите файл лицензии программного обеспечения, чтобы импортировать его и активировать лицензии.
6. Нажмите кнопку **Готово** для завершения процесса активации.

Активация лицензий после льготного периода

Если вы предпочитаете активировать лицензию вручную, но не успели сделать это в течение льготного периода (лицензии на аппаратные устройства, камеры Milestone Interconnect, двери и т.д.), то устройство, использующее эту лицензию, станет недоступным и перестанет передавать данные в систему наблюдения.

Однако даже если льготный период действия лицензии истек, конфигурация устройства и заданные настройки сохраняются и используются при активации лицензии.

Чтобы возобновить доступ к устройствам, активируйте лицензии вручную любым удобным способом. Дополнительные сведения приведены в Автономная активация лицензий на стр. 138 или Интерактивная активация лицензии на стр. 138.

Приобретение дополнительных лицензий

Если вы хотите добавить дополнительные аппаратные устройства, системы Milestone Interconnect, двери или прочие элементы, которыми вы пользуетесь, вам необходимо приобрести дополнительные лицензии, чтобы эти устройства могли отправлять данные в вашу систему:

- Для приобретения дополнительных лицензий обратитесь к реселлеру XProtect.

Если вы приобрели новые лицензии на существующую версию системы наблюдения:

- достаточно активировать новые лицензии вручную, чтобы получить к ним доступ. Дополнительные сведения приведены в Интерактивная активация лицензии на стр. 138 или Автономная активация лицензий на стр. 138.

Если вы приобрели новые лицензии и обновленную версию системы наблюдения:

- вместе с обновленным файлом лицензии программного обеспечения (LIC) вы также получите новые лицензии и новую версию. Используйте новый файл лицензии программного обеспечения в процессе установки новой версии. Дополнительные сведения приведены в разделе Требования к обновлению на стр. 407

Изменение кода лицензии на программное обеспечение

При запуске установки с временным кодом лицензии на программное обеспечение или при обновлении до продукта XProtect с расширенными функциями вы можете сменить код лицензии на программное обеспечение на постоянный или более сложный. Как только вы получите новый файл лицензии на программное обеспечение, вы сможете изменить код лицензии, не прибегая к удалению или переустановке.

Это можно сделать локально на сервере управления или удаленно с помощью Management Client.

С помощью значка на панели задач сервера управления

1. На сервере управления перейдите в область уведомлений на панели задач.

2. Нажмите правой кнопкой мыши значок **Сервер управления** и выберите **Изменить лицензию**.
3. Нажмите **Импорт лицензии**.
4. Затем выберите соответствующий файл лицензии программного обеспечения. После этого под кнопкой **Импорт лицензии** появится выбранное местонахождение файла лицензии программного обеспечения.
5. Нажмите **OK**. Все готово к регистрации кода лицензии на программное обеспечение. См. раздел Зарегистрируйте код лицензии на программное обеспечение на стр. 160.

От Management Client

1. Скопируйте полученный файл в формате LIC на свой компьютер с помощью Management Client.
2. На панели **Навигация по сайту** в узле **Основы** -> **Сведения о лицензии** выберите **Активировать лицензию в автономном режиме** > **Импорт активированной лицензии**, а затем выберите файл лицензии программного обеспечения, который необходимо импортировать.
3. Откройте файл лицензии на программное обеспечение и убедитесь, что он отличается от используемого в данный момент.
4. Все готово к регистрации кода лицензии на программное обеспечение. См. раздел Зарегистрируйте код лицензии на программное обеспечение на стр. 160.

В ходе этой процедуры файл лицензии программного обеспечения только импортируется и изменяется, но активируется. Не забудьте активировать лицензию. Дополнительные сведения приведены в разделе Активируйте лицензии на стр. 137.

Во время работы XProtect Essential+ вы можете изменить лицензию только с помощью значка на панели задач сервера управления. Нельзя изменить лицензию с помощью Management Client.

Окно «Сведения о лицензии»

В окне **Сведения о лицензии** можно отслеживать все лицензии с одним файлом лицензии программного обеспечения на этом и на всех других объектах, ваши подписки Milestone Care, а также выбрать способ активации лицензий.

Чтобы открыть окно **Сведения о лицензии**, на панели **Навигация по сайту** перейдите к узлу **Основы** -> **Сведения о лицензии**.

Дополнительные сведения о принципах работы системы лицензирования XProtect приведены в разделе Лицензии (объяснение) на стр. 129.

Зарегистрирован на

В этой области окна **Сведения о лицензии** перечислены контактные данные владельца лицензии, указанные во время регистрации программного обеспечения.

Если область **Зарегистрирован на** не отображается, нажмите кнопку **Обновить** в нижнем правом углу окна.

Нажмите **Редактировать сведения**, чтобы изменить информацию о владельце лицензии. Нажмите **Лицензионное соглашение с конечным пользователем**, чтобы просмотреть соглашение, принятое перед установкой.

Milestone Care

В этом разделе можно получить информацию о текущей подписке Milestone Care™. Даты истечения срока действия подписок указаны в таблице **Установленные продукты**.

Дополнительные сведения о Milestone Care доступны по соответствующим ссылкам или в разделе Milestone Care™ (объяснение) на стр. 134.

Установленные продукты

Информация обо всех установленных базовых лицензиях на VMS XProtect и расширениях XProtect, которые используют одинаковый файл лицензии программного обеспечения:

- Продукты и их версии
- Код лицензии на программное обеспечение продуктов
- Дата истечения срока действия кода лицензии на программное обеспечение. Как правило, действует без ограничений.
- Дата истечения срока действия подписки Milestone Care Plus.
- Дата истечения срока действия подписки Milestone Care Premium.

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 20 R	M01-C01-211-01-	Unlimited	16-11-20	16-11-20
Milestone XProtect Smart Wall	M01-P03-100-01-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08-100-01-	Unlimited	Unlimited	

Обзор лицензий - все сайты

Информация о количестве активированных лицензий на устройства и других лицензий в файле лицензий программного обеспечения, а также сведения об общем количестве доступных лицензий в системе. Благодаря этой информации легко определить, сможете ли вы расширить свою систему без приобретения дополнительных лицензий.

Чтобы получить подробный обзор статуса лицензий, активированных на других сайтах, перейдите по ссылке **Сведения о лицензии — все сайты**. Информация о разделе **Сведения о лицензии — текущий сайт** указана ниже.

License Overview - All sites License Details - All Sites...

License Type	Activated
Device Licenses	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

Если у вас есть лицензии на расширения XProtect, то дополнительные сведения доступны в узлах, относящихся к конкретным расширениям XProtect, на панели **Навигация по сайту**.

Сведения о лицензиях — текущий сайт

В столбце **Активировано** указано количество активированных лицензий на устройства или других лицензий на этом сайте.

В столбце **Изменения без активации** отображается количество используемых изменений устройств без активации (см. Изменения устройств без активации (объяснение) на стр. 133) и количество доступных изменений в год.

Если у вас есть неактивированные лицензии, для которых действует льготный период, они указаны в столбце **Идет льготный период**. Дата окончания срока действия первой лицензии, срок действия которой истекает, отображается под таблицей и выделена красным цветом.

Если вы забудете активировать лицензии до завершения льготного периода. Эти лицензии показаны в столбце **Льготный период завершился**. Дополнительные сведения приведены в разделе Активация лицензий после льготного периода на стр. 139.

Если количество используемых лицензий превышает количество доступных, информация о них указывается в столбце **Без лицензии**. Такие лицензии нельзя использовать в вашей системе. Дополнительные сведения приведены в разделе Приобретение дополнительных лицензий на стр. 139.

Если у вас есть лицензии, у которых действует льготный период, и лицензии с истекшим льготным периодом, или отсутствует необходимое количество лицензий, при каждом входе в систему будет появляться соответствующее напоминание Management Client.

License Details - Current Site: [redacted]

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Device Licenses	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

Если у вас есть аппаратные устройства, использующие более одной лицензии, под таблицей **Сведения о лицензиях — текущий сайт** появится ссылка **Нажмите здесь, чтобы открыть полный отчет о лицензии на устройство**. Пройдя по ссылке, вы узнаете, сколько лицензий требуется для каждого аппаратного устройства.

Аппаратные устройства без лицензий обозначаются в Management Client восклицательным знаком. Восклицательный знак используется в разных ситуациях. Наведите курсор на восклицательный знак, чтобы увидеть причину.

Функции системы активации лицензий

Ниже приведены три таблицы:

- Флажок для включения автоматической активации лицензии и ссылка на редактирование учетных данных пользователя для автоматической активации лицензии. Дополнительные сведения приведены в разделах Автоматическая активация лицензии (объяснение) на стр. 132 и Включить автоматическую активацию лицензии на стр. 137.
  Если автоматическая активация не удалась, сообщение о сбое будет выделено красным цветом. Дополнительные сведения доступны по ссылке **Подробная информация**.
  При установке некоторых лицензий, в том числе XProtect Essential+, автоматическая активация лицензий включена, и отключить ее невозможно.

- Раскрывающийся список для активации лицензий вручную в интерактивном или автономном режиме. Дополнительные сведения приведены в разделах Интерактивная активация лицензии на стр. 138 и Автономная активация лицензий на стр. 138.
- В правом нижнем углу окна отображается время последней активации лицензий (в автоматическом режиме или вручную) и время последнего обновления информации в окне. Метки времени соответствуют сведениям с сервера, а не с локального компьютера.

Требования и рекомендации

Декретное время (объяснение)

Декретное время — это практика перевода часов таким образом, чтобы увеличить количество дневного света вечером и уменьшить его утром. В зависимости от страны/региона декретное время используется по-разному.

При работе с системой наблюдения, которая напрямую зависит от времени, важно знать, как система обрабатывает декретное время.

> Не изменяйте параметры декретного времени, если в данный момент действует декретное время или если у вас есть записи, сделанные в декретное время.

Весна: Переход со стандартного времени на декретное

Переход со стандартного времени на декретное не вызывает затруднений, поскольку время сдвигается на один час вперед.

Пример:

Часы переходят с 02:00 стандартного времени на 03:00 декретного времени, а сутки состоят из 23 часов. В этом случае отсутствуют данные между 02:00 и 03:00 утра, поскольку для этого дня этот час не существует.

Осень: Переход с декретного времени на стандартное

Осенью при переходе с декретного времени на стандартное происходит возврат на один час назад.

Пример:

Часы переходят назад с 02:00 декретного времени на 01:00 стандартного времени. Таким образом, этот час повторяется, а в сутках насчитывается 25 часов. Дойдя до 01:59:59, время сразу же возвращается к 01:00:00. Если бы система не отреагировала, она перезаписала бы этот час, так что первый экземпляр 01:30 был бы переписан вторым экземпляром 01:30.

Чтобы исключить такую возможность, система архивирует текущее видео в случае изменения системного времени более чем на пять минут. Вы не сможете просмотреть первый экземпляр времени 01:00 в каком-либо клиенте, при этом данные будут записаны и сохранены. Вы можете просмотреть это видео в XProtect Smart Client, если напрямую откроете архивную базу данных.

Серверы времени (объяснение)

При получении изображений на них сразу же добавляется метка времени. Так как камеры являются отдельными устройствами, которые могут быть оснащены отдельными модулями синхронизации,

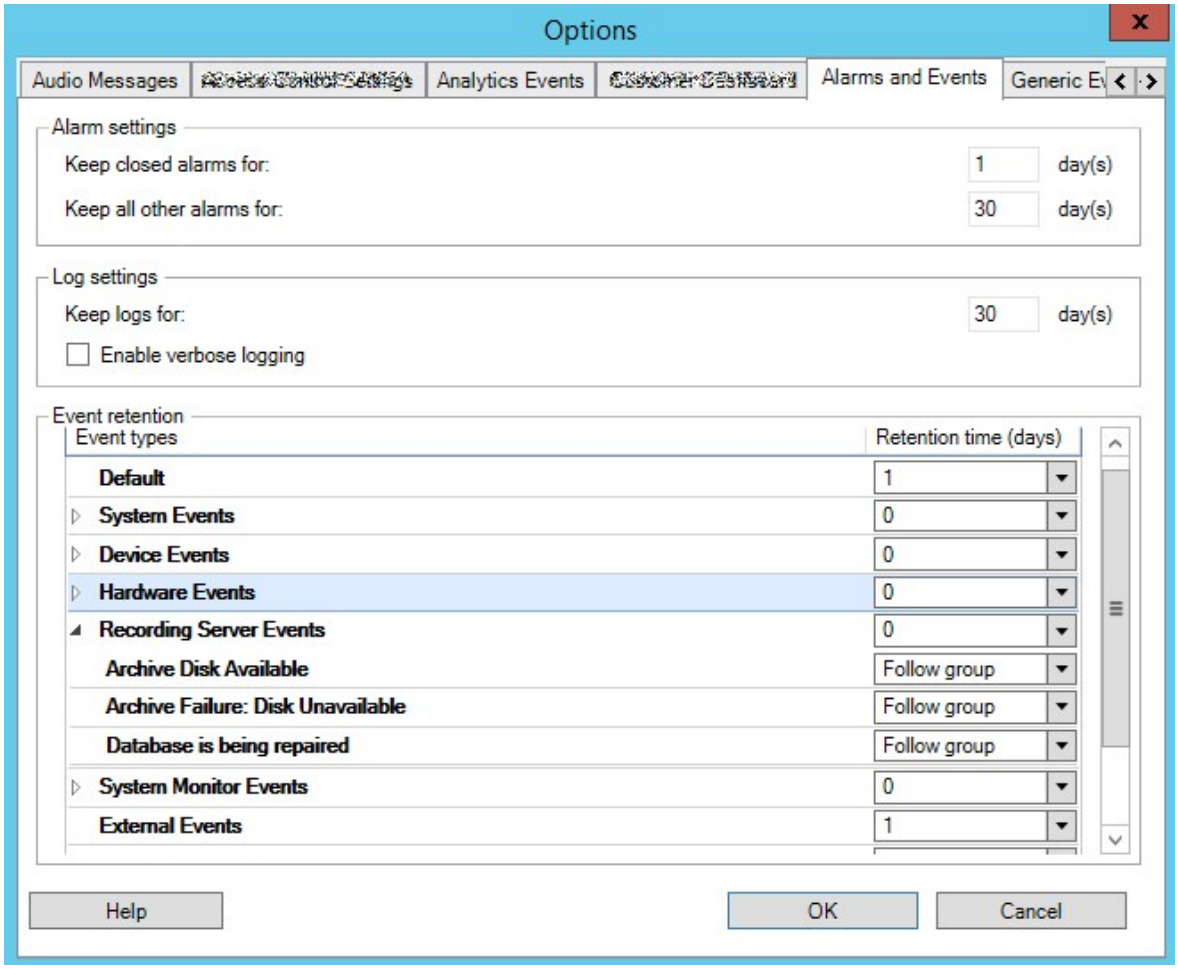
время камеры и системное время могут отличаться. В некоторых случаях это может привести к путанице. Если ваши камеры поддерживают метки времени, Milestone рекомендует автоматически синхронизировать время камеры и системное время с помощью сервера времени.

Информация о настройке сервера времени приведена на сайте Microsoft (https://www.microsoft.com/). Наберите в строке поиска «**сервер времени**», «**служба времени**» или аналогичные ключевые слова.

Ограничение размера базы данных

Для того чтобы база данных SQL Server (см. раздел Системы и базы данных SQL Server (объяснение) на стр. 38) не разрослась до размера, который отражается на производительности системы, можно задать срок хранения (в днях) различных типов событий и сигналов тревоги в базе данных.

1. Откройте меню **Инструменты**.
2. Откройтераздел**Параметры**>перейдитенавкладку**Сигналытревогиисобытия**.



3. Задайте необходимые настройки. Дополнительные сведения приведены в разделе Вкладка «Сигналы тревоги и события» (параметры) на стр. 434.

IPv4 и IPv6 (объяснение)

Ваша система поддерживает протоколы IPv6 и IPv4. Также как и XProtect Smart Client.

IPv6 является последней версией интернет-протокола (IP). Интернет-протокол определяет формат IP-адресов и их использование. IPv6 одновременно используется с более распространенной версией IPv4. Протокол IPv6 был разработан для того, чтобы решить проблему нехватки адресов в протоколе IPv4. Адреса IPv6 имеют длину 128 разрядов, в то время как адреса IPv4 — только 32 разряда.

Это значит, что адресная книга Интернета увеличилась с 4,3 миллиарда уникальных адресов до 340 ундециллионов (340 триллионов триллионов триллионов) адресов. Фактор роста — 79 октиллионов (миллиардов миллиардов миллиардов).

Все больше организаций внедряют IPv6 в своих сетях. Например, все инфраструктуры федеральных агентств США должны быть совместимы с IPv6. Примеры и иллюстрации настоящего руководства ориентированы на IPv4, поскольку эта версия интернет-протокола по-прежнему является наиболее распространенной. IPv6 также поддерживается системой.

Использование системы с протоколом IPv6 (объяснение)

При использовании системы с IPv6 действуют следующие условия:

Серверы

Как правило, серверы могут использовать как IPv4, так и IPv6. Однако если хотя бы один сервер в вашей системе (например, сервер управления или сервер записи) требует определенной версии интернет-протокола, все остальные серверы в системе должны использовать ту же версию интернет-протокола.

Пример: В системе все серверы, кроме одного, могут использовать как IPv4, так и IPv6. Исключением является сервер, который поддерживает только IPv6. Это означает, что все серверы должны использовать протокол IPv6 для связи друг с другом.

Устройства

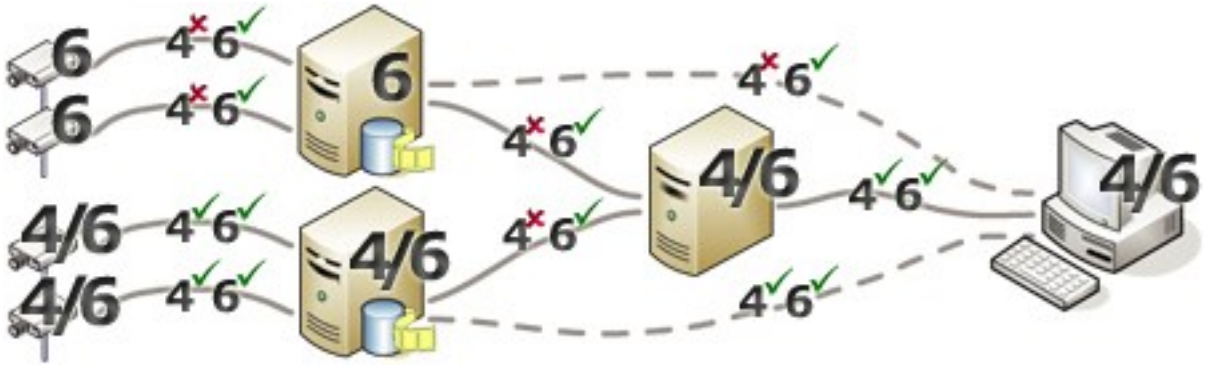
Вы можете использовать устройства (камеры, устройства ввода, устройства вывода, микрофоны, динамики) с версией интернет-протокола, отличной от той, которая используется для связи с сервером, при условии что ваше сетевое оборудование и серверы записи также поддерживают данную версию интернет-протокола устройства. Также см. иллюстрацию ниже.

Клиенты

Если ваша система использует протокол IPv6, пользователи должны подключаться с помощью XProtect Smart Client. XProtect Smart Client поддерживает IPv6 и IPv4.

Если один или несколько серверов в системе могут использовать **исключительно** протокол IPv6, пользователи XProtect Smart Client **должны** использовать IPv6 для связи с этими серверами. Важно помнить, что установленные системы XProtect Smart Client подключаются к серверу управления для первоначальной аутентификации, а затем к соответствующим серверам записи для получения доступа к записям.

Однако пользователям XProtect Smart Client не обязательно самим находиться в сети IPv6, если сетевое оборудование поддерживает обмен данными между различными версиями интернет-протокола, и они установили протокол IPv6 на свои компьютеры. Также см. иллюстрацию. Для установки IPv6 на компьютере клиента откройте командную строку, введите ***Ipv6 install***, и нажмите **ВВОД**.
Иллюстрация к примеру



Пример: Поскольку один сервер в системе может использовать только IPv6, взаимодействие с ним должно осуществляться по протоколу IPv6. Кроме того, этот сервер определяет версию интернет-протокола для связи между всеми остальными серверами в системе.

Запись адресов IPv6 (объяснение)

Адрес IPv6 обычно задается в виде восьми групп из четырех шестнадцатеричных цифр, отделенных друг от друга двоеточием.

Пример: *2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

Вы можете сократить адреса, удалив начальные нули в каждой группе. Также обратите внимание, что некоторые четырехзначные группы могут состоять исключительно из нулей. Если несколько таких групп 0000 расположено подряд, вы можете сократить адреса, заменив группы 0000 двумя двоеточиями, при условии, что в адресе будет только одно такое двойное двоеточие.

Пример:
2001:0B80:0000:0000:0000:0F80:3FA8:18AB можно сократить до

2001:B80:0000:0000:0000:F80:3FA8:18AB, если убрать начальные нули, или до

2001:0B80::0F80:3FA8:18AB, если удалить группы 0000, или даже до

2001:B80::F80:3FA8:18AB, если удалить начальные нули, а также группы 0000.

Использование IPv6-адресов в URL-адресах

IPv6-адреса содержат двоеточия. Однако двоеточия используются и в других типах синтаксиса сетевой адресации. Например, в протоколе IPv4 двоеточие используется для разделения IP-адреса и номера порта, если они одновременно используются в URL. В протоколе IPv6 этот принцип сохранен. Во избежание путаницы IPv6-адреса заключаются в квадратные скобки, когда они используются в URL.

Пример URL с IPv6-адресом:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB], который, как правило, можно сократить. Например, так: *http://[2001:B80::F80:3FA8:18AB]*

Пример URL с IPv6-адресом и номером порта:
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]:1234, который, как правило, можно сократить. Например, так: *http://[2001:B80::F80:3FA8:18AB]:1234*

Дополнительные сведения о протоколе IPv6 приведены на сайте IANA (https://www.iana.org/numbers/). IANA (Администрация адресного пространства Интернет) — это организация, отвечающая за глобальную координацию IP-адресов.

Виртуальные серверы

Все компоненты системы можно запускать на виртуализированных серверах Windows®, например VMware® и Microsoft® Hyper-V®.

Зачастую к виртуализации прибегают для более эффективного использования аппаратных ресурсов. Обычно виртуальные серверы, работающие на аппаратном хост-сервере, незначительно нагружают виртуальный сервер, к тому же они часто работают не одновременно. Однако серверы записи записывают данные со всех камер и все видеопотоки. Это создает повышенную нагрузку на центральный процессор, память, сеть и систему хранения данных. Как следствие, при запуске на виртуальном сервере преимущества виртуализации в значительной степени снижаются, поскольку в большинстве случаев задействуются все доступные ресурсы.

При работе в виртуальной среде важно, чтобы на аппаратном хосте оставалось столько же физической памяти, сколько выделено для виртуальных серверов. Кроме того, виртуальному серверу, на котором работает сервер записи, должно быть выделено достаточно ресурсов центрального процессора и памяти, что не предусмотрено по умолчанию. Обычно серверу записи требуется 2–4 ГБ в зависимости от конфигурации. К другим узким местам относятся распределение сетевых адаптеров и производительность жестких дисков. Рассмотрите возможность выделения физического сетевого адаптера на хосте виртуального сервера, на котором выполняется сервер записи. Таким образом упрощается контроль за тем, чтобы сетевой адаптер не перегружался трафиком других виртуальных серверов. Если один сетевой адаптер используется для нескольких виртуальных серверов, то в результате большого сетевого трафика сервер записи не сможет получить и записать заданное количество изображений.

Защита баз данных записей от повреждений

В базах данных камер могут возникать повреждения. Для решения этой проблемы существует несколько вариантов восстановления базы данных. Milestone рекомендует принять соответствующие меры для предотвращения повреждения баз данных камеры.

Отказ жесткого диска: защита дисков

Жесткие диски являются механическими устройствами, подверженными воздействию внешних факторов. Ниже приведены примеры внешних факторов, которые могут привести к повреждению жесткого диска и баз данных камеры:

- вибрация (убедитесь, что сервер системы наблюдения и окружающее его пространство устойчивы);
- сильный нагрев (убедитесь, что обеспечена достаточная вентиляция сервера);
- сильные магнитные поля (необходимо избегать);
- перебои в подаче электроэнергии (обязательно используйте источник бесперебойного питания (ИБП));
- статическое электричество (при использовании жесткого диска необходимо обеспечить заземление);
- воздействие огня, воды и т.д. (необходимо избегать).

Диспетчер задач Windows: будьте внимательны при завершении процессов

При работе в диспетчере задач Windows будьте внимательны и не завершайте процессы, которые затрагивают систему наблюдения. Если вы завершите работу приложения или системной службы с помощью кнопки **Снять задачу** в диспетчере задач Windows, у этого процесса не будет возможности сохранить состояние или данные перед прекращением работы. Это может привести к повреждению баз данных камер.

Как правило, диспетчер задач Windows выводит предупреждение при попытке завершить процесс. Если вы не знаете, как завершение процесса отразится на системе наблюдения, при появлении предупреждающего сообщения о необходимости завершения процесса нажмите **Нет**.

Перебои в подаче электроэнергии: использование ИБП

Самой распространенной причиной повреждения баз данных является внезапное отключение сервера записи, в результате которого файлы не сохраняются, а операционная система завершает работу некорректно. Причиной этого могут быть перебои в подаче электроэнергии, случайное выдергивание кабеля питания сервера или другие подобные ситуации.

Лучший способ защитить серверы записи от внезапного отключения — установить ИБП (источник бесперебойного питания) на каждый сервер.

ИБП работает как дополнительный источник электропитания от аккумулятора, который обеспечивает необходимую мощность для сохранения открытых файлов и безопасного отключения системы в случае перебоев в подаче электроэнергии. Существуют различные варианты ИБП, но в большинстве из них предусмотрено программное обеспечение для автоматического сохранения открытых файлов, оповещения системных администраторов и т.д.

Выбор подходящего типа ИБП в соответствии с условиями вашей организации — сугубо индивидуальный процесс. При оценке своих потребностей учитывайте время работы, которое ИБП должен обеспечивать при перебоях в подаче электроэнергии. Сохранение открытых файлов и правильное завершение работы операционной системы может занять несколько минут.

Журнал транзакций базы данных SQL Server (объяснение)

Каждый раз, когда в базу данных SQL Server вносятся изменения, база данных SQL Server фиксирует их в журнале транзакций.

С помощью журнала транзакций можно восстановить предыдущую версию и отменить изменения в базе данных SQL Server с помощью Microsoft® SQL Server Management Studio. По умолчанию база данных SQL Server хранит журнал транзакций в течение неограниченного времени. Соответственно, количество записей в журнале транзакций постоянно увеличивается. Журнал транзакций по умолчанию располагается на системном диске. Постоянное увеличение размера журнала транзакций может препятствовать нормальной работе Windows.

Чтобы избежать подобной ситуации, рекомендуется регулярно сбрасывать данные журнала транзакций. Сброс данных не уменьшает размер файла журнала транзакций, а очищает его содержимое и тем самым препятствует переполнению журнала. Система VMS не сбрасывает данные журнала транзакций. В SQL Server предусмотрено несколько способов сброса данных журнала транзакций. Для получения дополнительной информации посетите страницу поддержки Microsoft https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017 и наберите в строке поиска *Усечение журнала транзакций*.

Минимальные системные требования

Информация о системных требованиях к разным приложениям VMS и компонентам системы приведена на сайте Milestone (https://www.milestonesys.com/systemrequirements/).

Перед началом установки

Milestone рекомендует ознакомиться с требованиями, изложенными в следующих разделах, перед тем как приступать к установке.

Подготовка серверов и сети

Операционная система

Убедитесь, что на всех серверах проведена чистая установка операционной системы Microsoft Windows, а также ее обновление всеми актуальными обновлениями Windows.

Информация о системных требованиях к разным приложениям VMS и компонентам системы приведена на сайте Milestone (https://www.milestonesys.com/systemrequirements/).

Microsoft® .NET Framework

Убедитесь в том, что на всех серверах установлен продукт Microsoft .NET Framework 4.8 или более поздней версии.

Сеть

Назначьте статические IP-адреса или зарезервируйте DHCP для всех компонентов системы и камер. Чтобы гарантировать необходимую полосу пропускания в сети, необходимо понимать, как и когда работа системы влияет на использование полосы пропускания. Основная нагрузка на сеть обусловлена работой трех элементов:

- Видеопотоков камер
- Отображения видеоданных на клиентах
- Архивирования записанных видеоданных

Сервер записи получает видеопотоки от камер, что обусловливает постоянную нагрузку на сеть. Клиенты, отображающие видеоданные, используют полосу пропускания сети. Если не происходит изменения видов клиентов, то эта нагрузка остается неизменной. Изменение содержания вида, поиск по видеоданным или воспроизведение приводят к динамическому изменению нагрузки.

Архивирование записанного видео — необязательная функция, позволяющая системе переносить записи в сетевое хранилище, если на компьютере будет недостаточно места. Это плановая задача, для которой необходимо установить график. Обычно архивирование происходит на сетевой диск, что делает такую нагрузку на сеть плановой и динамической.

Необходимо предусмотреть запас по полосе пропускания, чтобы сеть могла справляться с такими скачками трафика. Это позволит улучшить отклик системы и общее качество взаимодействия с пользователями.

Подготовка к работе с Active Directory

Для добавления пользователей в систему через службу Active Directory необходим сервер Active Directory, который выступает в роли контроллера домена.

Для удобства управления пользователями и группами Milestone рекомендует установить и настроить Microsoft Active Directory® перед установкой системы XProtect. Если вы добавили сервер управления в Active Directory после установки системы, потребуется переустановить сервер управления и заменить пользователей на новых пользователей Windows, заданных в Active Directory.

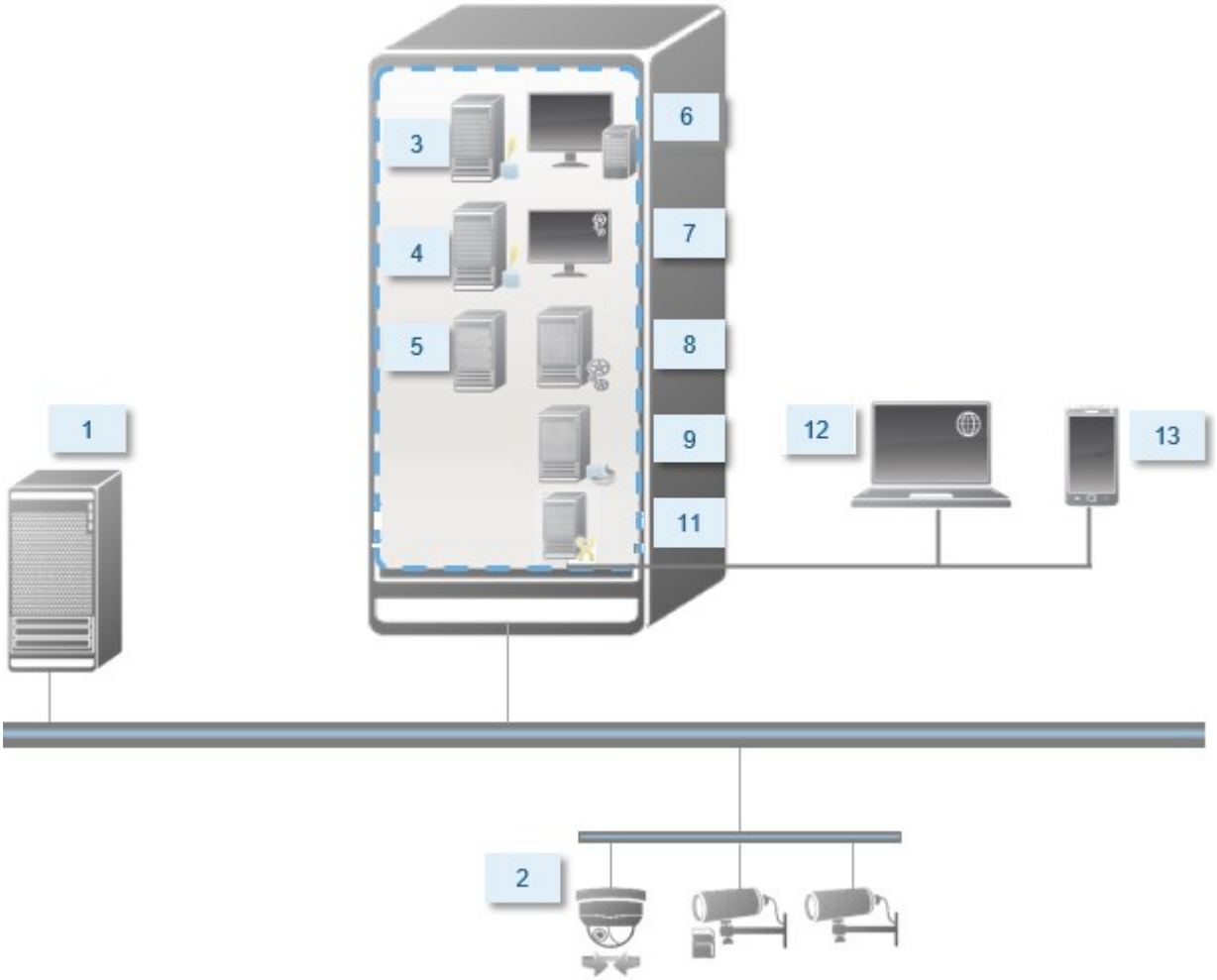
В системах Milestone Federated Architecture не поддерживаются базовые пользователи, поэтому если вы планируете использовать Milestone Federated Architecture, добавьте пользователей с помощью службы Active Directory как пользователей Windows. Если у вас не установлен компонент Active Directory, следуйте инструкциям в разделе Установка в рабочих группах на стр. 201 во время установки.

Способ установки

Выберите способ установки в мастере установки. При выборе следует исходить из требований вашей организации. Но, скорее всего, вы уже определились со способом установки при покупке системы.

Опции	Описание
Один компьютер	Установка всех компонентов сервера и клиента и SQL Server на текущий компьютер. После завершения установки вы сможете настроить систему, используя мастер настройки. Если вы выберете «Продолжить», сервер записи выполнит поиск оборудования в вашей сети. После этого вы сможете выбрать аппаратные устройства, которые нужно добавить в систему. Максимальное количество аппаратных устройств, которые можно добавить, используя мастер настройки, зависит от базовой лицензии. Кроме того, в представлениях предварительно настраиваются камеры и создается роль «Оператор» по умолчанию. После установки откроется XProtect Smart Client, и система будет готова к работе.
Пользовательская	Сервер управления выбран в списке компонентов системы и устанавливается по умолчанию. Однако вы можете самостоятельно выбрать различные компоненты сервера и клиента, которые следует установить на текущий компьютер. Сервер записи по умолчанию не выбран в списке компонентов, но вы можете поменять настройки. В дальнейшем можно установить компоненты, которые не были выделены, на другие компьютеры.

Установка на один компьютер

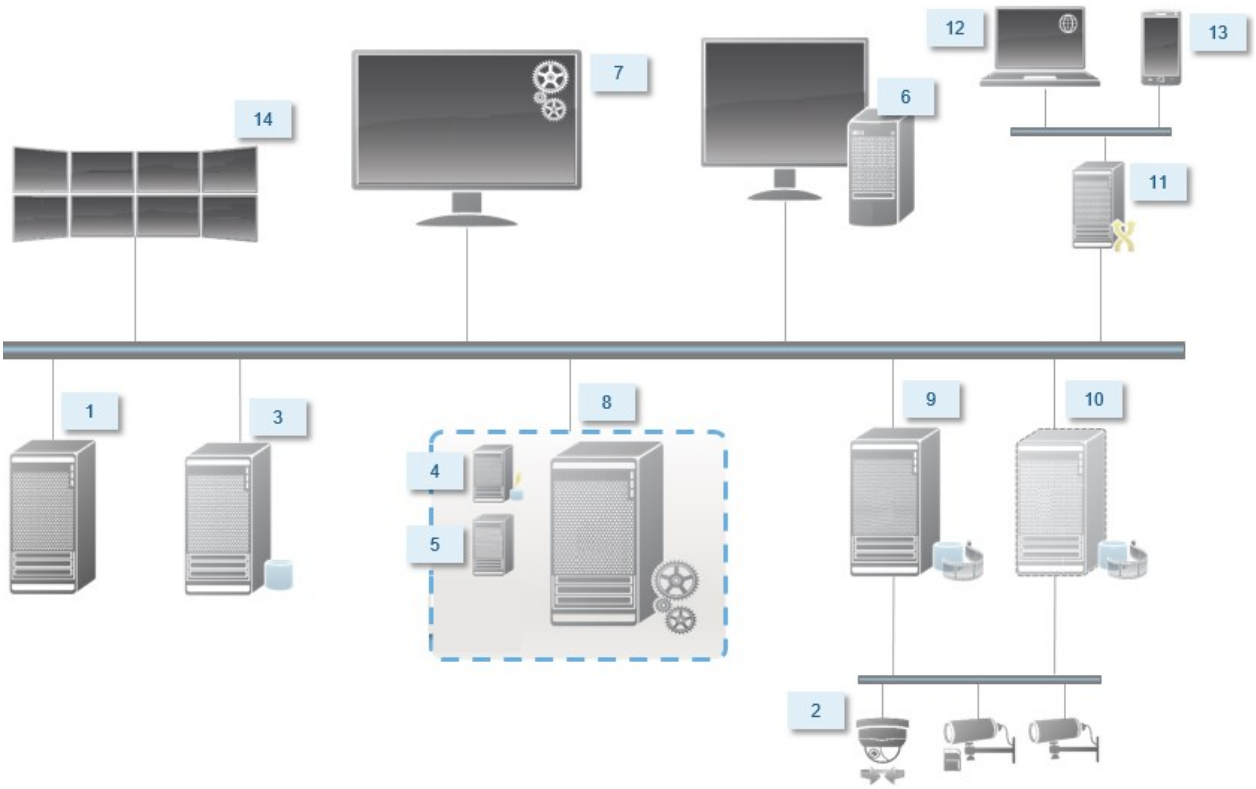


Стандартные компоненты системы:

1. **Active Directory**
2. **Устройства**
3. **Сервер с SQL Server**
4. **Сервер событий**
5. **Сервер журналов**
6. **XProtect Smart Client**
7. **Management Client**
8. **Сервер управления**
9. **Сервер записи**

10. **Сервер записи обработки отказа**
11. **XProtect MobileСервер**
12. **XProtect Web Client**
13. **XProtect MobileКлиент**
14. **XProtect Smart Client с XProtect Smart Wall**

Пользовательская установка на примере компонентов распределенной системы



Выбор версии SQL Server

Microsoft® SQL Server® Express — это бесплатная версия SQL Server, которую легко установить и подготовить к работе в отличие от других версий SQL Server.

Мастер установки устанавливает Microsoft SQL Server Express 2022, если SQL Server еще не установлено компьютере. Когда вы устанавливаете VMS XProtect в качестве обновления, мастер сохраняет предыдущую установку SQL Server.

Чтобы проверить, соответствует ли ваша система требованиям к версиям SQL Server, см. https://www.milestonesys.com/systemrequirements/.

Для очень крупных систем или систем, выполняющих много входящих и исходящих транзакций с базами данных SQL Server, Milestone рекомендует использовать выпуски SQL Server Microsoft® SQL Server® Standard или Microsoft® SQL Server® Enterprise на выделенном компьютере в сети и на выделенном жестком диске, не используемом для других целей. Установка SQL Server на отдельном диске повышает общую производительность системы.

Выберите учетную запись службы

В процессе установки вам будет предложено указать учетную запись для запуска служб Milestone на этом компьютере. Службы будут работать под этой учетной записью независимо от того, какой пользователь вошел в систему. Убедитесь, что у учетной записи есть все необходимые разрешения пользователя. Например, разрешения на выполнение задач, доступ к сети и файлам, а также доступ к общим сетевым папкам.

Можно выбрать предварительно заданную учетную запись или пользовательскую учетную запись. При выборе ориентируйтесь на параметры среды, в которой будет установлена система:

Среда домена

В среде домена:

- Milestone рекомендует использовать встроенную учетную запись сетевой службы

  Это упрощает использование, даже если вам нужно развернуть систему на нескольких компьютерах.

- Можно также использовать учетные записи пользователей домена, однако их настройка может оказаться более сложной.

Рабочие группы

В рабочих группах Milestone рекомендует использовать учетную запись локального пользователя со всеми необходимыми правами. Как правило, это учетная запись администратора.

> При установке компонентов системы на нескольких компьютерах выбранная учетная запись пользователя должна быть настроена на всех компьютерах с идентичным именем пользователя, паролем и правами доступа.

Аутентификация Kerberos (объяснение)

Kerberos — протокол сетевой аутентификации на базе билетов. Протокол предназначен для аутентификации клиент/сервер или сервер/сервер.

Kerberos можно использовать как альтернативу более раннему протоколу аутентификации Microsoft NT LAN (NTLM).

Kerberos требует взаимной аутентификации, когда клиент аутентифицируется в службе, а служба аутентифицируется в клиенте. Таким образом, обеспечивается более безопасная аутентификация клиентов XProtect на серверах XProtect без раскрытия пароля.

Для активации взаимной аутентификации в системе VMS XProtect необходимо зарегистрировать имена участников-служб (Service Principal Names, SPN) в Active Directory. SPN — это псевдоним, который обеспечивает уникальную идентификацию объекта, например службы сервера XProtect. Каждая служба, использующая взаимную аутентификацию, должна иметь зарегистрированное SPN-имя, чтобы клиенты могли идентифицировать службу в сети. Взаимная аутентификация без корректно зарегистрированных SPN недоступна.

В таблице ниже перечислены различные службы Milestone с соответствующими номерами портов, которые необходимо зарегистрировать:

Служба	Номер порта
Management Server — IIS	80 — настраивается
Management Server — внутренний	8080
Recording Server — служба сбора данных Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334

Количество служб, которые необходимо зарегистрировать в Active Directory, зависит от текущей установки. Data Collector устанавливается автоматически при установке службы Management Server, Recording Server, Event Server или Failover Server.

Для пользователя, запускающего службу, необходимо зарегистрировать два SPN: одно с именем хоста и одно с полным доменным именем.

Если вы запускаете службу под учетной записью пользователя сетевой службы, зарегистрируйте два SPN для каждого компьютера, на котором запущена эта служба.

Схема определения имен SPN для Milestone:

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

Ниже приведен пример SPN для службы Recording Server, запущенной на компьютере со следующими параметрами:

```
Hostname: Record-Server1
Domain: Surveillance.com
```

Регистрируемые SPN:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

Исключения при проверке на вирусы (объяснение)

Как и в случае с любым другим программным обеспечением баз данных, если на компьютере с программным обеспечением XProtect установлена антивирусная программа, вам потребуется добавить в исключения конкретные типы файлов и папки, а также конкретный сетевой трафик. Если не предусмотреть такие исключения, то процесс сканирования на вирусы будет потреблять значительное количество ресурсов системы. Более того, процесс сканирования может временно блокировать файлы, что приведет к сбою процесса записи или даже к повреждению баз данных.

Когда требуется провести сканирование на вирусы, не следует сканировать папки сервера записи, в которых находятся базы данных записи (по умолчанию `C:\mediadatabase\` и все подпапки). Также следует избегать сканирования на вирусы каталогов архивных хранилищ.

Дополнительно необходимо создать следующие исключения:

- Типы файлов: .blk, .idx, .pic
- Папки и подпапки:
  - `C:\Program Files\Milestone` или `C:\Program Files (x86)\Milestone`
  - `C:\ProgramData\Milestone\IDP\Logs`
  - `C:\ProgramData\Milestone\KeyManagement\Logs`
  - `C:\ProgramData\Milestone\MIPSDK`
  - `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Event Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Log Server`
  - `C:\ProgramData\Milestone\XProtect Management Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb`
- Исключите сканирование сети по следующим портам TCP:

Продукт	Порты TCP
XProtectСистема управления видео	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

или

- Исключите сканирование сети для следующих процессов:

Продукт	Процессы
XProtectСистема управления видео	VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS. Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

В вашей организации могут действовать строгие правила в отношении сканирования вирусов, необходимо обязательно добавить в исключения вышеупомянутые папки и файлы.

Как можно настроить работу VMS XProtect в режиме, соответствующем стандарту FIPS 140-2?

Чтобы настроить выполнение VMS XProtect в режиме FIPS 140-2, необходимо обеспечить следующие условия:

- Операционная система Windows должна выполняться в режиме, одобренном FIPS 140-2. Информацию о включении FIPS можно найти на сайте Microsoft.
- Автономные интеграции модулей сторонних производителей должны выполняться в ОС Windows с поддержкой FIPS.
- Подключение к устройствам должно обеспечивать режим работы, соответствующий требованиям FIPS 140-2.
- Данные в базе данных мультимедиа должны шифроваться с помощью шифров, соответствующих требованиям FIPS 140-2.

  Это требование можно обеспечить, запустив инструмент обновления базы данных мультимедиа. Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

Подготовка к установке VMS XProtect в систему с поддержкой FIPS

Несмотря на то, что новые версии VMS XProtect можно устанавливать на компьютеры с поддержкой FIPS, обновление VMS XProtect невозможно, если FIPS включен в операционной системе Windows.

Если вы обновляете систему, перед установкой отключите политику безопасности FIPS для Windows на всех компьютерах, входящих в состав VMS, включая компьютер с SQL Server.

Программа установки VMS XProtect проверяет политику безопасности FIPS и блокирует запуск установки, если FIPS включен.

Однако при обновлении с версии VMS XProtect 2020 R3 и более поздних отключать FIPS не нужно.

После установки компонентов VMS XProtect на все компьютеры и подготовки системы к использованию FIPS включите политику безопасности FIPS в Windows на всех компьютерах в вашей системе VMS.

Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

Зарегистрируйте код лицензии на программное обеспечение

Перед установкой обязательно убедитесь, что знаете название и местоположение файла лицензии на программное обеспечение, полученного от Milestone.

Можно установить бесплатную версию XProtect Essential+. Эта версия поддерживает ограниченный набор функций XProtect и ограниченное количество камер. Для установки XProtect Essential+ требуется соединение с Интернетом.

Код лицензии на программное обеспечение (SLC) указан в подтверждении заказа; имя файла лицензии соответствует SLC.

Milestone рекомендует зарегистрировать SLC на нашем сайте (https://online.milestonesys.com/) перед установкой. Ваш реселлер мог сделать это за вас.

Драйверы устройств (объяснение)

Драйверы видеоустройств используются в системе для управления и обмена данными с камерами, подключенными к серверу записи. Драйвер устройств необходимо установить на каждом сервере записи в системе.

Начиная с выпуска 2018 R1 драйверы устройств разделяются на два комплекта драйверов: стандартный комплект драйверов с драйверами более новых версий и комплект драйверов для старых устройств с драйверами старых версий.

Обычный комплект драйверов устанавливается автоматически при установке сервера записи. Впоследствии вы можете обновить драйверы, загрузив и установив более новую версию комплекта драйверов. Milestone регулярно выпускает новые версии драйверов устройств, которые доступны на странице загрузки (https://www.milestonesys.com/downloads/) нашего веб-сайта в виде комплектов драйверов (Device Pack). При обновлении комплекта драйверов новую версию можно установить поверх любой установленной версии.

Установить комплект драйверов для старых устройств можно только в том случае, если в системе установлен обычный комплект драйверов. Драйверы из комплекта драйверов для старых устройств устанавливаются автоматически, если предыдущая версия уже установлена в системе. Это комплект можно загрузить и установить вручную со страницы загрузки программного обеспечения (https://www.milestonesys.com/downloads/).

Перед установкой остановите службу Recording Server, в противном случае потребуется перезагрузить компьютер.

Всегда используйте драйверы устройств последней версии, чтобы обеспечить оптимальную производительность.

Требования к установке в автономном режиме

При установке системы на сервер, работающий в автономном режиме, вам потребуется следующее:

- файл `Milestone XProtect VMS Products 2024 R1 System Installer.exe`;
- файл лицензии программного обеспечения (код лицензии на программное обеспечение) для вашей системы XProtect;

- установочный носитель ОС, включая необходимую версию .NET (https://www.milestonesys.com/systemrequirements/).

Защищенное соединение (объяснение)

Протокол HTTPS является расширением протокола HTTP и обеспечивает безопасный обмен данными по сетям. В HTTPS шифрование протокола связи выполняется с помощью протокола TLS или его предшественника, SSL.

В VMS XProtect безопасный обмен данными реализуется за счет использования TLS/SSL с асимметричным шифрованием (RSA).

В протоколах TLS и SSL используется пара ключей (открытый и закрытый) для аутентификации, защиты и управления безопасными подключениями.

Центр сертификации (ЦС) — это любое лицо, выдающее корневые сертификаты. Это может быть интернет-служба, выдающая корневые сертификаты, или любое лицо, вручную создающее и распространяющее сертификат. ЦС может выдавать сертификаты веб-службам, то есть любому ПО, использующему обмен данными по протоколу HTTPS. Этот сертификат содержит два ключа: открытый и закрытый. Открытый ключ устанавливается на клиентах веб-службы (клиенты службы) путем установки открытого сертификата. Закрытый ключ используется для подписывания сертификатов серверов, которые устанавливаются на сервере. Когда клиент службы вызывает веб-службу, веб-служба передает клиенту сертификат сервера, включая открытый ключ. Клиент службы может проверить сертификат сервера, используя уже установленный открытый сертификат ЦС. На этом этапе клиент и сервер могут использовать открытый и закрытый сертификаты сервера для обмена секретным ключом и создания защищенного TLS/SSL-подключения.

Что касается сертификатов, распространяемых вручную, их необходимо установить до того, как клиент сможет проводить такую проверку.

Дополнительные сведения о протоколе TLS см. в разделе Transport Layer Security.

У сертификатов есть ограниченный срок действия. VMS XProtect не предупреждает о приближении истечения срока действия сертификата. Если срок действия сертификата истекает:
• клиенты больше не доверяют серверу записи с просроченным сертификатом и не могут обмениваться с ним данными;
• сервер записи больше не доверяет серверу управления с просроченным сертификатом и не может обмениваться с ним данными;
• мобильные устройства больше не доверяют мобильному серверу с просроченным сертификатом и не могут обмениваться с ним данными.

Для продления сертификатов выполните инструкции в этом руководстве, как и при создании сертификатов.

Дополнительные сведения см. в руководстве по сертификатам, посвященном защите систем XProtect VMS.

Установка

Установка новой системы XProtect

Установите XProtect Essential+

Можно установить бесплатную версию XProtect Essential+. Эта версия поддерживает ограниченный набор функций XProtect и ограниченное количество камер. Для установки XProtect Essential+ требуется соединение с Интернетом.

Эта версия устанавливается на один компьютер в рамках типа установки **Один компьютер**. В варианте **Один компьютер** все серверные и клиентские компоненты устанавливаются на текущем компьютере.

Milestone рекомендует перед установкой внимательно ознакомиться со следующим разделом: Перед началом установки на стр. 151.

Для установок с поддержкой FIPS нельзя обновить VMS XProtect, если поддержка FIPS включена в операционной системе Windows. Перед установкой отключите политику безопасности FIPS для Windows на всех компьютерах, входящих в состав VMS, включая компьютер с SQL Server. Однако при обновлении с версии VMS XProtect 2020 R3 и более поздних отключать FIPS не нужно. Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

После первоначальной установки можно продолжить работу с мастером настройки. В зависимости от аппаратного обеспечения и конфигурации сервер записи выполняет сканирование сети для поиска аппаратного обеспечения. Затем можно выбрать аппаратные устройства для добавления в систему. Камеры предварительно настроены в представлениях, кроме того, вы можете включить другие устройства, такие как микрофон и динамики. Пользователей можно добавлять в систему с ролью оператора или администратора. После установки откроется XProtect Smart Client, и система будет готова к работе.

Кроме того, если закрыть мастер установки, откроется XProtect Management Client, где можно внести настройки вручную, например добавить в систему аппаратные устройства и пользователей.

Если вы переходите с предыдущей версии продукта, система не выполняет поиск оборудования и не создает новые представления и профили пользователей.

1. Загрузите программное обеспечение из Интернета (https://www.milestonesys.com/downloads/) и запустите файл `Milestone XProtect VMS Products 2024 R1 System Installer.exe`.
2. Установщик будет распакован. В зависимости от параметров безопасности, появятся одно или несколько предупреждений Windows®. Для продолжения распаковки файлов установки необходимо положительно ответить на каждое предупреждение.
3. По завершении появится мастер установки **Milestone XProtect VMS**.
    1. Выберите **Язык** для установки (это не то же самое, что язык системы после установки; его можно будет выбрать позже). Нажмите **Продолжить**.
    2. Прочитайте *Лицензионное соглашение с конечным пользователем Milestone*. Установите отметку **Я принимаю условия лицензионного соглашения** и нажмите **Продолжить**.
    3. На странице **Параметры конфиденциальности** укажите, хотите ли вы делиться данными об использовании, и нажмите **Продолжить**.

        Если система должна соответствовать требованиям GDPR Евросоюза, не включайте сбор данных. Дополнительные сведения о защите данных и сборе данных по использованию см. в руководстве по конфиденциальности GDPR.

        Режим конфиденциальности всегда можно изменить. Также см. Системные настройки (диалоговое окно опций).

    4. Перейдите по ссылке **XProtect Essential+** для загрузки бесплатного файла лицензии.

        Файл бесплатной лицензии будет загружен и показан в поле **Укажите или выберите расположение файла лицензии**. Нажмите **Продолжить**.
4. Выберите **Один компьютер**.

    Отобразится перечень компонентов для установки (данный перечень нельзя редактировать). Нажмите **Продолжить**.

5. На странице **Назначить пароль для конфигурации системы** введите пароль для защиты конфигурации системы. Этот пароль потребуется вам при восстановлении или расширении системы (например, при добавлении кластеров).

   Очень важно сохранить этот пароль и держать его в надежном месте. Если вы забудете этот пароль, это затруднит восстановление конфигурации системы.

   Если вы не хотите защищать конфигурацию системы паролем, установите флажок **Я предпочитаю не использовать пароль конфигурации системы и понимаю, что конфигурация системы не будет зашифрована**.

   Нажмите **Продолжить**.

6. На странице **Назначение пароля для защиты данных сервера мобильной связи** введите пароль для шифрования расследований. Он нужен системному администратору для доступа к данным мобильного сервера в случае восстановления системы или при добавлении дополнительных мобильных серверов в систему.

   Этот пароль необходимо хранить в надежном месте. Если этого не сделать, вам может не удаться восстановить данные мобильного сервера.

   Если вы не хотите защищать расследования паролем, установите флажок **Я не хочу использовать пароль для защиты данных сервера мобильной связи и понимаю, что расследования не будут зашифрованы**.

   Нажмите **Продолжить**.

7. На странице **Укажите параметры сервера записи** задайте различные параметры для сервера:
    1. В поле **Имя сервера записи** введите имя сервера записи. По умолчанию будет указано имя компьютера.
    2. В поле **Адрес сервера управления** будет отображен адрес и номер порта сервера управления: localhost:80.
    3. В поле **Выберите расположение мультимедийной базы данных** выберите местоположение, в которое вы хотите сохранить видеозапись. Milestone рекомендует сохранять видеозаписи на носителе, отличном от того, на котором установлено программное обеспечение, и не на системном диске. По умолчанию выбран диск с максимальным объемом свободного места.
    4. В поле **Время хранения для видеозаписей** укажите, как долго требуется хранить видеозаписи. Допустимы значения от 1 до 365,000 дней; по умолчанию время хранения составляет 7 дней.
    5. Нажмите **Продолжить**.

8. На странице **Выберите шифрование** можно настроить защиту потоков обмена данными:

   - Между серверами записи, серверами Data Collector и сервером управления

     Чтобы включить шифрование для внутренних потоков обмена данными, выберите сертификат в разделе **Сертификат сервера**.

     > Если настроено шифрование подключений от сервера записи к серверу управления, необходимо также настроить шифрование подключений от сервера управления к серверу записи.

   - Между сервером записи и клиентами

     Чтобы включить шифрование между сервером записи и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат потоковых мультимедиа**.

   - Между мобильным сервером и клиентами

     Чтобы включить шифрование между мобильным сервером и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат мобильных потоковых мультимедиа**.

   - Между сервером событий и компонентами, которые обмениваются данными с этим сервером

     Чтобы включить шифрование между сервером событий и компонентами, которые обмениваются данными с этим сервером, включая LPR Server, выберите сертификат в разделе **Сервер событий и расширения**.

   Можно использовать один файл сертификата для всех компонентов системы или разные файлы в зависимости от конкретных компонентов.

   Дополнительные сведения о подготовке системы к безопасному обмену данными см.:

   - Защищенное соединение (объяснение) на стр. 162
   - Руководство Milestone по сертификатам

   Включить шифрование также можно после установки из Server Configurator с помощью значка Management Server Manager на панели задач в области уведомлений.

9. На странице **Выберите расположение файла и язык продукта** выберите следующее:

    1. В поле **Расположение файла** выберите папку для установки программы.

    > Если какой-либо продукт VMS Milestone XProtect уже установлен на компьютере, это поле неактивно. В поле отображается место установки компонента.

    2. В поле **Язык продукта** выберите язык установки продукта XProtect.
    3. Нажмите **Установить**.

    Программное обеспечение будет установлено. Если они еще не установлены на данном компьютере, будут автоматически установлены Microsoft® SQL Server® Express и Microsoft IIS.

10. Вам может быть предложено перезагрузить компьютер. После перезагрузки, в зависимости от параметров безопасности, может появиться одно или несколько предупреждений Windows о безопасности. Примите их, установка будет завершена.

11. По завершении установки будет показан список установленных приложений.

    Нажмите **Продолжить** для добавления аппаратного обеспечения и пользователей.

    > Если вы нажмете кнопку **Закрыть**, мастер настройки не будет запускаться, и сразу откроется окно XProtect Management Client. Настроить систему, например добавить аппаратное обеспечение и пользователей, можно в Management Client.

12. На странице **Введите имена и пароли пользователей аппаратного обеспечения** укажите учетные данные для доступа к аппаратному обеспечению, если вы изменили заводские настройки.

    Программа установки проведет в сети поиск этого оборудования, а также оборудования с заводскими учетными данными.

    Нажмите кнопку **Продолжить** и подождите, пока система выполнит поиск оборудования.

13. На странице **Выберите аппаратное обеспечение для добавления в систему** укажите оборудование, которое нужно добавить в систему. Нажмите кнопку **Продолжить** и подождите, пока система добавит оборудование.

14. На странице **Настройка устройств** можно присвоить устройствам удобные имена. Чтобы переименовать устройство, нажмите значок редактирования рядом с его именем. Указанное имя будет добавлено в качестве префикса.

    Развернув узел оборудования, можно включить или выключить те или иные устройства, например камеры, динамики или микрофоны.

    По умолчанию камеры включены, а динамики и микрофоны выключены.

    Нажмите кнопку **Продолжить** и подождите, пока система настроит оборудование.

15. На странице **Добавить пользователей** можно добавить в систему пользователей. Это могут быть пользователи Windows или базовые пользователи. Пользователям можно назначить роли администраторов и операторов.

    Укажите параметры пользователя и нажмите кнопку **Добавить**.

    По окончании добавления пользователей нажмите кнопку **Продолжить**.

16. По завершении установки и начальной настройки появится страница **Настройка завершена** со следующей информацией:

    - список устройств, добавленных в систему;
    - Список пользователей, добавленных в систему
    - адреса XProtect Web Client и клиента XProtect Mobile, которые можно сообщить пользователям.

    После того как вы нажмете кнопку **Закрыть**, откроется окно XProtect Smart Client и система будет готова к работе.

Установка системы — вариант «Один компьютер»

В варианте **Один компьютер** все серверные и клиентские компоненты устанавливаются на текущем компьютере.

Milestone рекомендует перед установкой внимательно ознакомиться со следующим разделом: Перед началом установки на стр. 151.

Для установок с поддержкой FIPS нельзя обновить VMS XProtect, если поддержка FIPS включена в операционной системе Windows. Перед установкой отключите политику безопасности FIPS для Windows на всех компьютерах, входящих в состав VMS, включая компьютер с SQL Server. Однако при обновлении с версии VMS XProtect 2020 R3 и более поздних отключать FIPS не нужно. Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

После первоначальной установки можно продолжить работу с мастером настройки. В зависимости от аппаратного обеспечения и конфигурации сервер записи выполняет сканирование сети для поиска аппаратного обеспечения. Затем можно выбрать аппаратные устройства для добавления в систему. Камеры предварительно настроены в представлениях, кроме того, вы можете включить другие устройства, такие как микрофон и динамики. Пользователей можно добавлять в систему с ролью оператора или администратора. После установки откроется XProtect Smart Client, и система будет готова к работе.

Кроме того, если закрыть мастер установки, откроется XProtect Management Client, где можно внести настройки вручную, например добавить в систему аппаратные устройства и пользователей.

Если вы переходите с предыдущей версии продукта, система не выполняет поиск оборудования и не создает новые представления и профили пользователей.

1. Загрузите программное обеспечение из Интернета (https://www.milestonesys.com/downloads/) и запустите файл `Milestone XProtect VMS Products 2024 R1 System Installer.exe`.
2. Установщик будет распакован. В зависимости от параметров безопасности, появятся одно или несколько предупреждений Windows®. Для продолжения распаковки файлов установки необходимо положительно ответить на каждое предупреждение.
3. По завершении появится мастер установки **Milestone XProtect VMS**.
    1. Выберите **Язык** для установки (это не то же самое, что язык системы после установки; его можно будет выбрать позже). Нажмите **Продолжить**.
    2. Прочитайте *Лицензионное соглашение с конечным пользователем Milestone*. Установите отметку **Я принимаю условия лицензионного соглашения** и нажмите **Продолжить**.
    3. На странице **Параметры конфиденциальности** укажите, хотите ли вы делиться данными об использовании, и нажмите **Продолжить**.

Если система должна соответствовать требованиям GDPR Евросоюза, не включайте сбор данных. Дополнительные сведения о защите данных и сборе данных по использованию см. в руководстве по конфиденциальности GDPR.

Режим конфиденциальности всегда можно изменить. Также см. Системные настройки (диалоговое окно опций).

4. В поле **Укажите или выберите путь к файлу лицензии** введите путь к файлу лицензии, предоставленному поставщиком XProtect. Также можно перейти к расположению файла или щелкнуть ссылку **XProtect Essential+** для загрузки бесплатного файла лицензии. Сведения об ограничениях для бесплатного продукта XProtect Essential+ см. здесь: Сравнение продуктов на стр. 127. Перед продолжением система проверит файл лицензии. Нажмите **Продолжить**.

4. Выберите **Один компьютер**.

   Отобразится перечень компонентов для установки (данный перечень нельзя редактировать). Нажмите **Продолжить**.

5. На странице **Назначить пароль для конфигурации системы** введите пароль для защиты конфигурации системы. Этот пароль потребуется вам при восстановлении или расширении системы (например, при добавлении кластеров).

   Очень важно сохранить этот пароль и держать его в надежном месте. Если вы забудете этот пароль, это затруднит восстановление конфигурации системы.

   Если вы не хотите защищать конфигурацию системы паролем, установите флажок **Я предпочитаю не использовать пароль конфигурации системы и понимаю, что конфигурация системы не будет зашифрована**.

   Нажмите **Продолжить**.

6. На странице **Назначение пароля для защиты данных сервера мобильной связи** введите пароль для шифрования расследований. Он нужен системному администратору для доступа к данным мобильного сервера в случае восстановления системы или при добавлении дополнительных мобильных серверов в систему.

   > Этот пароль необходимо хранить в надежном месте. Если этого не сделать, вам может не удаться восстановить данные мобильного сервера.

   Если вы не хотите защищать расследования паролем, установите флажок **Я не хочу использовать пароль для защиты данных сервера мобильной связи и понимаю, что расследования не будут зашифрованы**.

   Нажмите **Продолжить**.

7. На странице **Укажите параметры сервера записи** задайте различные параметры для сервера:

   1. В поле **Имя сервера записи** введите имя сервера записи. По умолчанию будет указано имя компьютера.
   2. В поле **Адрес сервера управления** будет отображен адрес и номер порта сервера управления: localhost:80.
   3. В поле **Выберите расположение мультимедийной базы данных** выберите местоположение, в которое вы хотите сохранить видеозапись. Milestone рекомендует сохранять видеозаписи на носителе, отличном от того, на котором установлено программное обеспечение, и не на системном диске. По умолчанию выбран диск с максимальным объемом свободного места.
   4. В поле **Время хранения для видеозаписей** укажите, как долго требуется хранить видеозаписи. Допустимы значения от 1 до 365,000 дней; по умолчанию время хранения составляет 7 дней.
   5. Нажмите **Продолжить**.

8. На странице **Выберите шифрование** можно настроить защиту потоков обмена данными:

   - Между серверами записи, серверами Data Collector и сервером управления

     Чтобы включить шифрование для внутренних потоков обмена данными, выберите сертификат в разделе **Сертификат сервера**.

     > Если настроено шифрование подключений от сервера записи к серверу управления, необходимо также настроить шифрование подключений от сервера управления к серверу записи.

   - Между сервером записи и клиентами

     Чтобы включить шифрование между сервером записи и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат потоковых мультимедиа**.

   - Между мобильным сервером и клиентами

     Чтобы включить шифрование между мобильным сервером и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат мобильных потоковых мультимедиа**.

   - Между сервером событий и компонентами, которые обмениваются данными с этим сервером

     Чтобы включить шифрование между сервером событий и компонентами, которые обмениваются данными с этим сервером, включая LPR Server, выберите сертификат в разделе **Сервер событий и расширения**.

   Можно использовать один файл сертификата для всех компонентов системы или разные файлы в зависимости от конкретных компонентов.

   Дополнительные сведения о подготовке системы к безопасному обмену данными см.:

   - Защищенное соединение (объяснение) на стр. 162
   - Руководство Milestone по сертификатам

   Включить шифрование также можно после установки из Server Configurator с помощью значка Management Server Manager на панели задач в области уведомлений.

9. На странице **Выберите расположение файла и язык продукта** выберите следующее:

    1. В поле **Расположение файла** выберите папку для установки программы.

    > Если какой-либо продукт VMS Milestone XProtect уже установлен на компьютере, это поле неактивно. В поле отображается место установки компонента.

    2. В поле **Язык продукта** выберите язык установки продукта XProtect.
    3. Нажмите **Установить**.

    Программное обеспечение будет установлено. Если они еще не установлены на данном компьютере, будут автоматически установлены Microsoft® SQL Server® Express и Microsoft IIS.

10. Вам может быть предложено перезагрузить компьютер. После перезагрузки, в зависимости от параметров безопасности, может появиться одно или несколько предупреждений Windows о безопасности. Примите их, установка будет завершена.

11. По завершении установки будет показан список установленных приложений.

    Нажмите **Продолжить** для добавления аппаратного обеспечения и пользователей.

    > Если вы нажмете кнопку **Закрыть**, мастер настройки не будет запускаться, и сразу откроется окно XProtect Management Client. Настроить систему, например добавить аппаратное обеспечение и пользователей, можно в Management Client.

12. На странице **Введите имена и пароли пользователей аппаратного обеспечения** укажите учетные данные для доступа к аппаратному обеспечению, если вы изменили заводские настройки.

    Программа установки проведет в сети поиск этого оборудования, а также оборудования с заводскими учетными данными.

    Нажмите кнопку **Продолжить** и подождите, пока система выполнит поиск оборудования.

13. На странице **Выберите аппаратное обеспечение для добавления в систему** укажите оборудование, которое нужно добавить в систему. Нажмите кнопку **Продолжить** и подождите, пока система добавит оборудование.

14. На странице **Настройка устройств** можно присвоить устройствам удобные имена. Чтобы переименовать устройство, нажмите значок редактирования рядом с его именем. Указанное имя будет добавлено в качестве префикса.

    Развернув узел оборудования, можно включить или выключить те или иные устройства, например камеры, динамики или микрофоны.

    По умолчанию камеры включены, а динамики и микрофоны выключены.

    Нажмите кнопку **Продолжить** и подождите, пока система настроит оборудование.

15. На странице **Добавить пользователей** можно добавить в систему пользователей. Это могут быть пользователи Windows или базовые пользователи. Пользователям можно назначить роли администраторов и операторов.

    Укажите параметры пользователя и нажмите кнопку **Добавить**.

    По окончании добавления пользователей нажмите кнопку **Продолжить**.

16. По завершении установки и начальной настройки появится страница **Настройка завершена** со следующей информацией:
    - список устройств, добавленных в систему;
    - Список пользователей, добавленных в систему
    - адреса XProtect Web Client и клиента XProtect Mobile, которые можно сообщить пользователям.

    После того как вы нажмете кнопку **Закрыть**, откроется окно XProtect Smart Client и система будет готова к работе.

Установка системы — вариант «Пользовательская»

В варианте **Пользовательская** устанавливается сервер управления. Вы можете выбрать и другие компоненты сервера и клиента, которые необходимо установить на текущий компьютер. По умолчанию сервер записи не выбран в списке компонентов. В дальнейшем вы можете установить компоненты системы, которые не были выделены, на другие компьютеры в зависимости от выбранных вами параметров. Дополнительные сведения о компонентах системы и их роли приведены в разделе Обзор продуктов на стр. 37. Установка на другие компьютеры осуществляется с помощью веб-страницы загрузки сервера управления, которая называется Download Manager. Дополнительные сведения об установке с помощью Download Manager приведены в разделе Download Manager/веб-страница загрузки на стр. 202.

Milestone рекомендует перед установкой внимательно ознакомиться со следующим разделом: Перед началом установки на стр. 151.

Для установок с поддержкой FIPS нельзя обновить VMS XProtect, если поддержка FIPS включена в операционной системе Windows. Перед установкой отключите политику безопасности FIPS для Windows на всех компьютерах, входящих в состав VMS, включая компьютер с SQL Server. Однако при обновлении с версии VMS XProtect 2020 R3 и более поздних отключать FIPS не нужно. Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

1. Загрузите программное обеспечение из Интернета (https://www.milestonesys.com/downloads/) и запустите файл `Milestone XProtect VMS Products 2024 R1 System Installer.exe`.
2. Установщик будет распакован. В зависимости от параметров безопасности, появятся одно или несколько предупреждений Windows®. Для продолжения распаковки файлов установки необходимо положительно ответить на каждое предупреждение.
3. По завершении появится мастер установки **Milestone XProtect VMS**.
    1. Выберите **Язык** для установки (это не то же самое, что язык системы после установки; его можно будет выбрать позже). Нажмите **Продолжить**.
    2. Прочитайте *Лицензионное соглашение с конечным пользователем Milestone*. Установите отметку **Я принимаю условия лицензионного соглашения** и нажмите **Продолжить**.
    3. На странице **Параметры конфиденциальности** укажите, хотите ли вы делиться данными об использовании, и нажмите **Продолжить**.

        Если система должна соответствовать требованиям GDPR Евросоюза, не включайте сбор данных. Дополнительные сведения о защите данных и сборе данных по использованию см. в руководстве по конфиденциальности GDPR.

        Режим конфиденциальности всегда можно изменить. Также см. Системные настройки (диалоговое окно опций).

    4. В поле **Укажите или выберите путь к файлу лицензии** введите путь к файлу лицензии, предоставленному поставщиком XProtect. Также можно перейти к расположению файла или щелкнуть ссылку **XProtect Essential+** для загрузки бесплатного файла лицензии. Сведения об ограничениях для бесплатного продукта XProtect Essential+ см. здесь: Сравнение продуктов на стр. 127. Перед продолжением система проверит файл лицензии. Нажмите **Продолжить**.

4. Выберите **Пользовательская**. Появится список компонентов, которые можно установить. За исключением сервера управления, все перечисленные компоненты необязательны. Сервер записи и мобильный сервер по умолчанию не выбраны. Выберите компоненты системы, которые вы хотите установить, и нажмите **Продолжить**.

   Для правильной работы системы установите хотя бы один экземпляр XProtect API Gateway.

   Далее описаны шаги по установке всех компонентов системы. При использовании распределенной системы установите несколько компонентов системы на этом компьютере, а остальные — на других компьютерах. Если вам не удается определить шаг установки, скорее всего, вы не выбрали установку системного компонента, к которому относится эта страница. В таком случае перейдите к следующему шагу. Также см. Установка с помощью Download Manager (объяснение) на стр. 184, Установка сервера записи с помощью Download Manager на стр. 185 и Автоматическая установка с помощью оболочки командной строки (объяснение) на стр. 193.

5. Страница **Выберите веб-сайт IIS для использования с вашей системой XProtect** отображается только в том случае, если на компьютере доступно несколько веб-сайтов IIS. Необходимо выбрать веб-сайт, который будет использоваться с вашей системой XProtect. Выберите веб-сайт с привязкой HTTPS. Нажмите **Продолжить**.

   Будут установлены службы Microsoft® IIS, если они еще не установлены на этом компьютере.

6. На странице **ВыборMicrosoft SQL Server** выберите нужный вариант SQL Server. Также см. Варианты SQL Server при пользовательской установке на стр. 183. Нажмите **Продолжить**.

   Если на локальном компьютере отсутствует SQL Server, вы можете установить Microsoft SQL Server Express. Однако в больших распределенных системах обычно используется выделенный SQL Server.

7. На странице **Выбрать базу данных** (отображается, если вы выбрали существующий вариант SQL Server) выберите или создайте базу данных SQL Server для хранения конфигурации системы. Если вы выбрали существующую базу данных SQL Server, выберите **Сохранить** или **Перезаписать** существующие данные. При обновлении выберите сохранение существующих данных, чтобы не потерять конфигурацию системы. Также см. Варианты SQL Server при пользовательской установке на стр. 183. Нажмите **Продолжить**.

8. На странице **Параметры базы данных** выберите один из вариантов: **Разрешить программе установки создать или повторно создать базу данных** или **Использовать предварительно созданную базу данных**.
9. Чтобы базы данных создавались с нуля или создавались заново в автоматическом режиме, выберите вариант **Разрешить программе установки создать или повторно создать базу данных** и нажмите **Продолжить**.
10. Чтобы использовать настроенные для конкретной цели базы данных или уже созданные базы данных, выберите вариант **Использовать предварительно созданную базу данных**. После этого откроется страница **Расширенная установка базы данных**.
11. На странице **Расширенная установка базы данных** укажите сервер и название базы данных для компонентов XProtect.
12. Выберите один из вариантов: **Аутентификация с аккаунтом Windows, не доверять сертификату сервера (рекомендуется)**, **Аутентификация с аккаунтом Windows, доверять сертификату сервера** или **Интеграция с Azure Active Directory, не доверять сертификату сервера (рекомендуется)**.

   В зависимости от выбранного типа аутентификации учетная запись, которая будет использоваться для установки, должна быть создана в Azure AD или Windows AD. Для этих учетных записей не поддерживается многофакторная аутентификация.

   Вариант **(не доверять сертификату сервера)** рекомендуется для аутентификации с аккаунтом Windows и является обязательным для интеграции с Azure Active Directory. Таким образом обеспечивается проверка сертификатов сервера перед установкой. Дополнительные сведения о недопустимых сертификатах сервера можно найти в файле журнала установки. Если вы выбрали вариант **Аутентификация с аккаунтом Windows, доверять сертификату сервера**, проверка сертификатов сервера пропускается.

13. Нажмите значок, чтобы проверить соединение. По нажатии значка также выполняется проверка сертификатов сервера.
14. Нажмите кнопку **Продолжить**.

15. На странице **Назначить пароль для конфигурации системы** введите пароль для защиты конфигурации системы. Этот пароль потребуется вам при восстановлении или расширении системы (например, при добавлении кластеров).

    Очень важно сохранить этот пароль и держать его в надежном месте. Если вы забудете этот пароль, это затруднит восстановление конфигурации системы.

    Если вы не хотите защищать конфигурацию системы паролем, установите флажок **Я предпочитаю не использовать пароль конфигурации системы и понимаю, что конфигурация системы не будет зашифрована**.

    Нажмите **Продолжить**.

16. На странице **Назначение пароля для защиты данных сервера мобильной связи** введите пароль для шифрования расследований. Он нужен системному администратору для доступа к данным мобильного сервера в случае восстановления системы или при добавлении дополнительных мобильных серверов в систему.

    Этот пароль необходимо хранить в надежном месте. Если этого не сделать, вам может не удаться восстановить данные мобильного сервера.

    Если вы не хотите защищать расследования паролем, установите флажок **Я не хочу использовать пароль для защиты данных сервера мобильной связи и понимаю, что расследования не будут зашифрованы**.

    Нажмите **Продолжить**.

17. На странице **Выберите учетную запись службы для сервера записи** выберите **Эта предопределенная учетная запись** или **Эта учетная запись**.

    При необходимости введите пароль.

    Имя пользователя для учетной записи должно быть одним словом. Использование пробелов запрещено.

    Нажмите **Продолжить**.

18. На странице **Укажите параметры сервера записи** задайте различные параметры для сервера:
    1. В поле **Имя сервера записи** введите имя сервера записи. По умолчанию будет указано имя компьютера.
    2. В поле **Адрес сервера управления** будет отображен адрес и номер порта сервера управления: localhost:80.
    3. В поле **Выберите расположение мультимедийной базы данных** выберите местоположение, в которое вы хотите сохранить видеозапись. Milestone рекомендует сохранять видеозаписи на носителе, отличном от того, на котором установлено программное обеспечение, и не на системном диске. По умолчанию выбран диск с максимальным объемом свободного места.
    4. В поле **Время хранения для видеозаписей** укажите, как долго требуется хранить видеозаписи. Допустимы значения от 1 до 365,000 дней; по умолчанию время хранения составляет 7 дней.
    5. Нажмите **Продолжить**.

19. На странице **Выберите шифрование** можно настроить защиту потоков обмена данными:

    - Между серверами записи, серверами Data Collector и сервером управления

      Чтобы включить шифрование для внутренних потоков обмена данными, выберите сертификат в разделе **Сертификат сервера**.

      > Если настроено шифрование подключений от сервера записи к серверу управления, необходимо также настроить шифрование подключений от сервера управления к серверу записи.

    - Между сервером записи и клиентами

      Чтобы включить шифрование между сервером записи и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат потоковых мультимедиа**.

    - Между мобильным сервером и клиентами

      Чтобы включить шифрование между мобильным сервером и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат мобильных потоковых мультимедиа**.

    - Между сервером событий и компонентами, которые обмениваются данными с этим сервером

      Чтобы включить шифрование между сервером событий и компонентами, которые обмениваются данными с этим сервером, включая LPR Server, выберите сертификат в разделе **Сервер событий и расширения**.

    Можно использовать один файл сертификата для всех компонентов системы или разные файлы в зависимости от конкретных компонентов.

    Дополнительные сведения о подготовке системы к безопасному обмену данными см.:

    - Защищенное соединение (объяснение) на стр. 162
    - Руководство Milestone по сертификатам

    Включить шифрование также можно после установки из Server Configurator с помощью значка Management Server Manager на панели задач в области уведомлений.

20. На странице **Выберите расположение файла и язык продукта** выберите **Расположение файлов** для файлов программы.

    Если какой-либо продукт VMS Milestone XProtect уже установлен на компьютере, это поле неактивно. В поле отображается место установки компонента.

21. В поле **Язык продукта** выберите язык установки продукта XProtect. Нажмите **Установить**.

    Программное обеспечение будет установлено. По завершении установки будет выведен список успешно установленных компонентов системы. Нажмите кнопку **Закрыть**.

22. Вам может быть предложено перезагрузить компьютер. После перезагрузки, в зависимости от параметров безопасности, может появиться одно или несколько предупреждений Windows о безопасности. Примите их, установка будет завершена.

23. Настройте систему в Management Client. См. раздел Список задач первоначальной настройки на стр. 210.

24. В зависимости от выбранного вами варианта установите остальные компоненты системы на другие компьютеры с помощью Download Manager. См. раздел Установка с помощью Download Manager (объяснение) на стр. 184.

Варианты SQL Server при пользовательской установке

Выберите SQL Server и базу данных, которые вы хотите использовать, из предложенных ниже вариантов.

Варианты SQL Server:

- **Установить Microsoft® SQL Server® Express на этом компьютере**: Этот вариант отображается только в том случае, если на компьютере отсутствует SQL Server.
- **Использовать SQL Server на этом компьютере**: Этот вариант отображается только в том случае, если на компьютере есть SQL Server.
- **Выберите SQL Server в вашей сети с помощью операции поиска**: Обеспечивает поиск всех установок SQL Server, которые можно обнаружить в вашей подсети.
- **Выберите SQL Server в вашей сети**: Позволяет ввести адрес SQL Server (имя хоста или IP-адрес), который не удается найти с помощью функции поиска.

Варианты базы данных SQL Server:

- **Создать базу данных**: Преимущественно используется для новых установок.
- **Использовать существующую базу данных**: Преимущественно используется для обновления существующих установок. Milestone рекомендует повторно использовать существующую базу данных SQL Server для сохранения имеющейся информации, чтобы не потерять конфигурацию системы. Вы также можете переписать информацию в базе данных SQL Server.

Установка новых компонентов XProtect

Установка с помощью Download Manager (объяснение)

Если вы хотите установить компоненты системы на компьютеры, на которых не установлен сервер управления, установить эти компоненты через веб-сайт загрузки Management Server Download Manager.

1. С компьютера, где установлен Management Server, перейдите на веб-страницу загрузки Management Server. В меню **Пуск** Windows выберите **Milestone** > **Страница ресурсов для администратора** и запишите или скопируйте веб-адрес, который потребуется вам в дальнейшем при установке компонентов системы на другие компьютеры. Как правило, этот адрес следующий: *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Войдите в систему на этих компьютерах, чтобы установить один или несколько компонентов системы:
   - Recording Server (Дополнительные сведения приведены в Установка сервера записи с помощью Download Manager на стр. 185 и Автоматическая установка сервера записи на стр. 194.)
   - Management Client (Дополнительные сведения приведены в разделе Установка Management Client с помощью Download Manager на стр. 185.)
   - Smart Client
   - Event Server Не забудьте перезапустить шлюз API после установки. В случае последующего переименования компьютера вам придется перезапустить шлюз API.

     > ⚠ Если вы устанавливаете Event Server в среде, совместимой с FIPS, перед установкой необходимо отключить режим Windows FIPS 140-2.

   - Log Server (Дополнительные сведения приведены в разделе Автоматическая установка сервера регистрации на стр. 197.)
   - Mobile Server (Дополнительные сведения приведены в руководстве по эксплуатации сервера XProtect Mobile)
3. Откройте веб-браузер, введите адрес страницы загрузки Management Server в адресную строку и загрузите соответствующую программу установки.
4. Запустите программу установки.

Если вы сомневаетесь в правильности выбранных параметров и настроек на отдельных этапах установки, см. Установка системы — вариант «Пользовательская» на стр. 176.

Установка Management Client с помощью Download Manager

Если в системе XProtect работает несколько администраторов, или вы планируете управлять системой XProtect с нескольких компьютеров, вы можете установить Management Client, следуя приведенным ниже инструкциям.

Management Client всегда устанавливается на сервере управления.

1. С компьютера, где установлен Management Server, перейдите на веб-страницу загрузки Management Server. В меню **Пуск** Windows выберите **Milestone** > **Страница ресурсов для администратора** и запишите или скопируйте веб-адрес, который потребуется вам в дальнейшем при установке компонентов системы на другие компьютеры. Как правило, этот адрес следующий: *http://[management server address]/installation/Admin/default-en-US.htm*.

   Войдите в систему компьютера, на который требуется установить компонент системы.
2.

1. Откройте веб-браузер и введите адрес страницы загрузки Management Server в адресную строку, затем нажмите клавишу ВВОД.
3. Нажмите **Все языки** для установщика Management Client. Запустите загруженный файл.
4. Нажимайте **Да** в ответ на все предупреждения. Начнется распаковка.
5. Выберите язык установщика. Нажмите **Продолжить**.
6. Ознакомьтесь и примите условия лицензионного соглашения. Нажмите **Продолжить**.
7. Выберите расположение файла и язык продукта. Нажмите **Установить**.
8. Установка завершена. Отобразится список успешно установленных компонентов. Нажмите кнопку **Закрыть**.
9. Чтобы открыть Management Client, нажмите на значок на рабочем столе.
10. Отобразится диалоговое окно входа в Management Client.
11. Укажите имя хоста или IP-адрес своего сервера управления в поле **Компьютер**.
12. Выберите аутентификацию, введите имя пользователя и пароль. Нажмите **Подключить**. Произойдет запуск Management Client.

    Чтобы получить подробную информацию об опциях Management Client и возможностях системы, нажмите на вкладку **Справка** в меню инструментов.

Установка сервера записи с помощью Download Manager

Если компоненты вашей системы распределены по отдельным компьютерам, вы можете установить серверы записи, следуя приведенным ниже инструкциям.

Если был выбран тип установки **Один компьютер**, то сервер записи уже установлен. Если вам требуется дополнительная емкость, вы можете использовать те же инструкции для добавления других серверов записи.

Если вам требуется установить сервер записи обработки отказа, см. Установка сервера записи обработки отказа с помощью Download Manager на стр. 189.

1. С компьютера, где установлен Management Server, перейдите на веб-страницу загрузки Management Server. В меню **Пуск** Windows выберите **Milestone** > **Страница ресурсов для администратора** и запишите или скопируйте веб-адрес, который потребуется вам в дальнейшем при установке компонентов системы на другие компьютеры. Как правило, этот адрес следующий: *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Войдите в систему компьютера, на который требуется установить компонент системы.
3. Откройте веб-браузер и введите адрес страницы загрузки Management Server в адресную строку, затем нажмите клавишу ВВОД.
4. Загрузите программу установки сервера записи, выбрав **Все языки** под **Программа установки сервера записи**. Сохраните программу установки или запустите ее прямо с веб-страницы.
5. Выберите нужный **язык** во время установки. Нажмите **Продолжить**.
6. На экране **Выбор типа установки** выберите:

   Обычная, чтобы установить сервер записи со значениями по умолчанию, или

   Пользовательская, чтобы установить сервер записи с настраиваемыми значениями.

7. На странице **Укажите параметры сервера записи** задайте различные параметры для сервера:
    1. В поле **Имя сервера записи** введите имя сервера записи. По умолчанию будет указано имя компьютера.
    2. В поле **Адрес сервера управления** будет отображен адрес и номер порта сервера управления: localhost:80.
    3. В поле **Выберите расположение мультимедийной базы данных** выберите местоположение, в которое вы хотите сохранить видеозапись. Milestone рекомендует сохранять видеозаписи на носителе, отличном от того, на котором установлено программное обеспечение, и не на системном диске. По умолчанию выбран диск с максимальным объемом свободного места.
    4. В поле **Время хранения для видеозаписей** укажите, как долго требуется хранить видеозаписи. Допустимы значения от 1 до 365,000 дней; по умолчанию время хранения составляет 7 дней.
    5. Нажмите **Продолжить**.
8. Страница **IP-адрес сервера записи** отображается только в том случае, если вы выбрали тип установки **Пользовательская**. Укажите количество серверов записи, которые вы хотите установить на этом компьютере. Нажмите **Продолжить**.
9. На странице **Выберите учетную запись службы для сервера записи** выберите **Эта предопределенная учетная запись** или **Эта учетная запись**.

    При необходимости введите пароль.

    > Имя пользователя для учетной записи должно быть одним словом. Использование пробелов запрещено.

    Нажмите **Продолжить**.

10. На странице **Выберите шифрование** можно настроить защиту потоков обмена данными:

    - Между серверами записи, серверами Data Collector и сервером управления

      Чтобы включить шифрование для внутренних потоков обмена данными, выберите сертификат в разделе **Сертификат сервера**.

      > Если настроено шифрование подключений от сервера записи к серверу управления, необходимо также настроить шифрование подключений от сервера управления к серверу записи.

    - Между сервером записи и клиентами

      Чтобы включить шифрование между сервером записи и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат потоковых мультимедиа**.

    - Между мобильным сервером и клиентами

      Чтобы включить шифрование между мобильным сервером и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат мобильных потоковых мультимедиа**.

    - Между сервером событий и компонентами, которые обмениваются данными с этим сервером

      Чтобы включить шифрование между сервером событий и компонентами, которые обмениваются данными с этим сервером, включая LPR Server, выберите сертификат в разделе **Сервер событий и расширения**.

    Можно использовать один файл сертификата для всех компонентов системы или разные файлы в зависимости от конкретных компонентов.

    Дополнительные сведения о подготовке системы к безопасному обмену данными см.:

    - Защищенное соединение (объяснение) на стр. 162
    - Руководство Milestone по сертификатам

    Включить шифрование также можно после установки из Server Configurator с помощью значка Management Server Manager на панели задач в области уведомлений.

11. На странице **Выберите расположение файла и язык продукта** выберите **Расположение файлов** для файлов программы.

    Если какой-либо продукт VMS Milestone XProtect уже установлен на компьютере, это поле неактивно. В поле отображается место установки компонента.

12. В поле **Язык продукта** выберите язык установки продукта XProtect. Нажмите **Установить**.

    Программное обеспечение будет установлено. По завершении установки будет выведен список успешно установленных компонентов системы. Нажмите кнопку **Закрыть**.

13. После установки сервера записи вы можете проверить его статус с помощью значка Recording Server Manager на панели задач и настроить его в Management Client. Дополнительные сведения приведены в разделе Список задач первоначальной настройки на стр. 210.

Установка сервера записи обработки отказа с помощью Download Manager

Если вы используете рабочие группы, выберите другой вариант установки для серверов записи обработки отказа (см. Установка в рабочих группах на стр. 201).

1. С компьютера, где установлен Management Server, перейдите на веб-страницу загрузки Management Server. В меню **Пуск** Windows выберите **Milestone** > **Страница ресурсов для администратора** и запишите или скопируйте веб-адрес, который потребуется вам в дальнейшем при установке компонентов системы на другие компьютеры. Как правило, этот адрес следующий: *http://[management server address]/installation/Admin/default-en-US.htm*.

   Войдите в систему компьютера, на который требуется установить компонент системы.

2. Откройте веб-браузер и введите адрес страницы загрузки Management Server в адресную строку, затем нажмите клавишу ВВОД.

3. Загрузите программу установки сервера записи, выбрав **Все языки** под **Программа установки сервера записи**. Сохраните программу установки или запустите ее прямо с веб-страницы.
4. Выберите нужный **язык** во время установки. Нажмите **Продолжить**.
5. На странице **Выбор типа установки** выберите **Резерв**, чтобы установить сервер записи в качестве сервера обработки отказа.

6. На странице **Укажите параметры сервера записи** задайте различные параметры для сервера. Имя сервера записи обработки отказа, адрес сервера управления и путь к базе данных мультимедиа. Нажмите **Продолжить**.
7. На странице **Выбор учетной записи службы для сервера записи** и при установке сервера записи обработки отказа необходимо использовать определенную учетную запись пользователя под именем **Данная учетная запись**. Будет создана соответствующая учетная запись пользователя. При необходимости введите пароль и подтвердите его. Нажмите **Продолжить**.

8. На странице **Выберите шифрование** можно настроить защиту потоков обмена данными:

   - Между серверами записи, серверами Data Collector и сервером управления

     Чтобы включить шифрование для внутренних потоков обмена данными, выберите сертификат в разделе **Сертификат сервера**.

     > Если настроено шифрование подключений от сервера записи к серверу управления, необходимо также настроить шифрование подключений от сервера управления к серверу записи.

   - Между сервером записи и клиентами

     Чтобы включить шифрование между сервером записи и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат потоковых мультимедиа**.

   - Между мобильным сервером и клиентами

     Чтобы включить шифрование между мобильным сервером и клиентскими компонентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат мобильных потоковых мультимедиа**.

   - Между сервером событий и компонентами, которые обмениваются данными с этим сервером

     Чтобы включить шифрование между сервером событий и компонентами, которые обмениваются данными с этим сервером, включая LPR Server, выберите сертификат в разделе **Сервер событий и расширения**.

   Можно использовать один файл сертификата для всех компонентов системы или разные файлы в зависимости от конкретных компонентов.

   Дополнительные сведения о подготовке системы к безопасному обмену данными см.:

   - Защищенное соединение (объяснение) на стр. 162
   - Руководство Milestone по сертификатам

   Включить шифрование также можно после установки из Server Configurator с помощью значка Management Server Manager на панели задач в области уведомлений.

9. На странице **Выберите расположение файла и язык продукта** выберите **Расположение файлов** для файлов программы.

   > Если какой-либо продукт VMS Milestone XProtect уже установлен на компьютере, это поле неактивно. В поле отображается место установки компонента.

10. В поле **Язык продукта** выберите язык установки продукта XProtect. Нажмите **Установить**.

    Программное обеспечение будет установлено. По завершении установки будет выведен список успешно установленных компонентов системы. Нажмите кнопку **Закрыть**.

11. После установки сервера записи обработки отказа вы можете проверить его статус с помощью значка Failover Server на панели задач и настроить его в Management Client. Дополнительные сведения приведены в разделе Список задач первоначальной настройки на стр. 210.

Установка VMS XProtect с использованием нестандартных портов

Для установки VMS XProtect требуются конкретные порты. В частности, Management Server и API Gateway работают в IIS, поэтому должны быть доступны определенные порты. В этом разделе описывается установка VMS XProtect и использование нестандартных портов в IIS. Это также применимо, когда устанавливается только API Gateway.

Обзор всех портов, используемых VMS, см. в руководстве администратора VMS XProtect (https://doc.milestonesys.com/2024r1/ru-RU/portal/htm/chapter-page-mc-administrator-manual.htm).

Если в системе еще не установлены службы IIS, программа установки VMS XProtect устанавливает их и использует стандартный веб-сайт с портами по умолчанию.

Если вы не хотите использовать VMS XProtect по умолчанию, сначала установите IIS. При необходимости добавьте новый веб-сайт или продолжите работу, используя стандартный веб-сайт.

Добавьте привязку HTTPS, если ее нет, и выберите действующий сертификат на компьютере (его нужно будет выбрать во время установки VMS XProtect). Измените номера портов в привязках HTTP и HTTPS на доступные порты по вашему выбору.

Запустите программу установки VMS XProtect и выберите тип установки **Пользовательская**.

Во время установки появится страница **Выберите веб-сайт IIS для использования с вашей системой XProtect**, если доступно несколько веб-сайтов. Необходимо выбрать веб-сайт, который будет использоваться с вашей системой XProtect. Программа установки использует измененные номера портов.

Автоматическая установка с помощью оболочки командной строки (объяснение)

Благодаря автоматической установке системные администраторы могут устанавливать и обновлять программное обеспечение VMS XProtect и Smart Client в крупномасштабной сети без участия конечных пользователей и с минимальным вмешательством в их работу.

Программы установки VMS XProtect и Smart Client установщики (EXE-файлы) отличаются аргументами командной строки. Для них предусмотрены собственные наборы параметров командной строки, которые можно вызвать непосредственно в оболочке командной строки или с помощью файла аргументов. В оболочке командной строки параметры командной строки также можно использовать при работе с программами установки.

Вы можете комбинировать программы установки XProtect и их параметры командной строки с инструментами для распространения и установки программного обеспечения в автоматическом режиме, такими как Microsoft System Center Configuration Manager (SCCM, также известный как ConfigMgr). Дополнительные сведения о таких инструментах можно найти на сайте производителя. Для удаленной установки и обновления VMS XProtect, комплектов драйверов и Smart Client также можно использовать Milestone Software Manager. Дополнительные сведения см. в руководстве администратора Milestone Software Manager.

Параметры командной строки и файлы аргументов

Во время автоматической установки можно задать параметры, имеющие непосредственное отношение к различным компонентам системы VMS и их внутреннему взаимодействию, с помощью параметров командной строки и файлов аргументов. Параметры командной строки и файлы аргументов рекомендуется использовать только для новых установок, так как при обновлении нельзя изменить параметры командной строки.

Чтобы просмотреть доступные параметры командной строки и создать файл аргументов для программы установки, в оболочке командной строки перейдите в каталог, в котором находится программа установки, и введите следующую команду:

```
[NameOfExeFile].exe --generateargsfile=[path]
```

Пример:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

В сохраненном файле аргументов (Arguments.xml) каждый параметр командной строки сопровождается описанием, объясняющим его назначение. Вы можете изменить файл аргументов и сохранить его, чтобы значения параметров командной строки соответствовали вашим требованиям к установке.

Если вы хотите использовать файл аргументов вместе с программой установки, воспользуйтесь параметром командной строки `--arguments` и введите следующую команду:

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

Пример:

```
Milestone XProtect VMS Products 2024 R1 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

Параметры командной строки

В оболочке командной строки программы установки также можно комбинировать с параметрами командной строки. Параметры командной строки влияют на выполнение команды.

Чтобы увидеть полный список параметров командной строки, в оболочке командной строки перейдите в каталог, где находится программа установки, и введите `[NameOfExeFile].exe --help`. Для успешной установки укажите значение для обязательных параметров командной строки.

В одной команде можно одновременно использовать параметры и опции командной строки. Используйте параметр командной строки `--parameters` и отделяйте каждый параметр с помощью двоеточия (:). В примере ниже `--quiet`, `--showconsole` и `--parameters` являются опциями командной строки, а `ISFAILOVER` и `RECORDERNAME` — параметрами командной строки:

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

Автоматическая установка сервера записи

При автоматической установке вы не получаете уведомления о завершении операции. Чтобы получить уведомление, включите в команду параметр командной строки `--showconsole`. После завершения установки на панели задач появится значок Milestone XProtect Recording Server.

В приведенных ниже примерах команд текст внутри квадратных скобок ([ ]) и сами квадратные скобки необходимо заменить на реальные значения. Пример: вместо «[путь]» можно ввести `d:\program files\`, `d:\record\` или `\\network-storage-02\surveillance`. Воспользуйтесь параметром командной строки `--help`, чтобы узнать о допустимых форматах каждого значения параметра командной строки.

1. Войдите в систему компьютера, на который требуется установить компонент Recording Server.
2. Откройте веб-браузер и введите адрес страницы загрузки Management Server, предназначенной для администраторов, в адресную строку, затем нажмите клавишу ВВОД.

   Как правило, этот адрес следующий: `http://[адрес сервера управления]:[порт]/installation/Admin/default-en-US.htm`.
3. Загрузите программу установки сервера записи, выбрав **Все языки** под **Программа установки сервера записи**.

4. Откройте предпочитаемую оболочку командной строки. Чтобы открыть командную строку Windows, откройте меню «Пуск» и введите **cmd**.
5. Перейдите в каталог с загруженной программой установки.
6. Продолжите установку в соответствии с одним из двух приведенных ниже сценариев:

Сценарий 1. Обновление установленной системы или установка на сервер компонента Management Server со значениями по умолчанию

- Введите следующую команду, после чего начнется установка.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

Сценарий 2. Установка в распределенной системе

1. Введите следующую команду, чтобы создать файл аргументов с параметрами командной строки.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=
[path]
```

2. Откройте файл аргументов (Arguments.xml) по указанному пути и при необходимости измените значения параметров командной строки.

Убедитесь, что заданы действительные значения параметров командной строки SERVERHOSTNAME и SERVERPORT. В противном случае установка не завершится.

4. Сохраните файл аргументов.
5. Вернитесь в оболочку командной строки и введите указанную ниже команду для установки в соответствии со значениями параметров командной строки, указанными в файле аргументов.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --arguments=
[path]\[filename]
```

Автоматическая установка XProtect Smart Client

При автоматической установке вы не получаете уведомления о завершении операции. Чтобы получить уведомление, включите в команду параметр командной строки `--showconsole`. После завершения установки на рабочем столе появится ярлык XProtect Smart Client.

В приведенных ниже примерах команд текст внутри квадратных скобок ([ ]) и сами квадратные скобки необходимо заменить на реальные значения. Пример: вместо «[путь]» можно ввести `d:\program files\`, `d:\record\` или `\\network-storage-02\surveillance`. Воспользуйтесь параметром командной строки `--help`, чтобы узнать о допустимых форматах каждого значения параметра командной строки.

1. Откройте веб-браузер и введите адрес страницы загрузки Management Server, предназначенной для конечных пользователей, в адресную строку, затем нажмите клавишу ВВОД.

   Как правило, этот адрес следующий: `http://[адрес сервера управления]:[порт]/installation/default-en-US.htm`.

2. Загрузите программу установки XProtect Smart Client, выбрав **Все языки** под **Программа установки XProtect Smart Client**.

3. Откройте предпочитаемую оболочку командной строки. Чтобы открыть командную строку Windows, откройте меню «Пуск» и введите **cmd**.

4. Перейдите в каталог с загруженной программой установки.

5. Продолжите установку в соответствии с одним из двух приведенных ниже сценариев:

   Сценарий 1. Обновление существующей установки или установка со значениями параметров командной строки по умолчанию

   - Введите следующую команду, после чего начнется установка.

     ```
     "XProtect Smart Client 2024 R1 Installer.exe" --quiet
     ```

   Сценарий 2. Установка с настраиваемыми значениями параметров командной строки с помощью XML-файла аргументов в качестве входных данных

   1. Введите следующую команду, чтобы создать XML-файл аргументов с параметрами командной строки.

      ```
      "XProtect Smart Client 2024 R1 Installer.exe" --generateargsfile=[path]
      ```

   2. Откройте файл аргументов (Arguments.xml) по указанному пути и при необходимости измените значения параметров командной строки.

   3. Сохраните файл аргументов.

   4. Вернитесь в оболочку командной строки и введите указанную ниже команду для установки в соответствии со значениями параметров командной строки, указанными в

файле аргументов.

```
"XProtect Smart Client 2024 R1 Installer.exe" --quiet --arguments=
[path]\[filename]
```

Автоматическая установка сервера регистрации

При автоматической установке вы не получаете уведомления о завершении операции. Чтобы получить уведомление, включите в команду параметр командной строки `--showconsole`.

В приведенных ниже примерах команд текст внутри квадратных скобок ([ ]) и сами квадратные скобки необходимо заменить на реальные значения. Пример: вместо «[путь]» можно ввести `d:\program files\`, `d:\record\` или `\\network-storage-02\surveillance`. Воспользуйтесь параметром командной строки `--help`, чтобы узнать о допустимых форматах каждого значения параметра командной строки.

1. Войдите в систему компьютера, на который требуется установить компонент Log Server.
2. Откройте веб-браузер и введите адрес страницы загрузки Management Server, предназначенной для администраторов, в адресную строку, затем нажмите клавишу ВВОД.

   Как правило, этот адрес следующий: `http://[адрес сервера управления]:[порт]/installation/Admin/default-en-US.htm`.
3. Загрузите программу установки сервера регистрации, выбрав **Все языки** под **Программа установки сервера регистрации**.
4. Откройте предпочитаемую оболочку командной строки. Чтобы открыть командную строку Windows, откройте меню «Пуск» и введите **cmd**.
5. Перейдите в каталог с загруженной программой установки.
6. Продолжите установку в соответствии с одним из двух приведенных ниже сценариев:

   Сценарий 1. Обновление существующей установки или установка со значениями параметров командной строки по умолчанию

   - Введите следующую команду, после чего начнется установка.

     ```
     "XProtect Log Server 2024 R1 Installer x64.exe" --quiet --showconsole
     ```

Сценарий 2. Установка с настраиваемыми значениями параметров командной строки с помощью XML-файла аргументов в качестве входных данных

1. Введите следующую команду, чтобы создать XML-файл аргументов с параметрами командной строки.

   ```
   "XProtect Log Server 2024 R1 Installer x64.exe" --generateargsfile=
   [path]
   ```

2. Откройте файл аргументов (Arguments.xml) по указанному пути и при необходимости измените значения параметров командной строки.
3. Сохраните файл аргументов.
4. Вернитесь в оболочку командной строки и введите указанную ниже команду для установки в соответствии со значениями параметров командной строки, указанными в файле аргументов.

   ```
   "XProtect Log Server 2024 R1 Installer x64.exe" --quiet --arguments=
   [path]\[filename] --showconsole
   ```

Автоматическая установка с помощью выделенной учетной записи

Если вы хотите установить VMS XProtect без участия пользователя, запустите программу установки со значениями аргументов, указанными в таблице ниже. Перед установкой создайте XML-файл аргументов и сохраните его.

Аргумент	Описание
`--quiet`	Выполняет автоматическую установку.
`--arguments`	Путь к XML-файлу аргументов с полной конфигурацией. Возможные пути: `C:\Arguments.xml`.
`--license`	Путь к файлу лицензии.

Использование выделенной учетной записи службы

Описание составлено с учетом особенностей использования выделенной учетной записи службы для обеспечения комплексной безопасности. Службы работают под выделенной учетной записью

независимо от того, какой пользователь вошел в систему. Убедитесь, что у этой учетной записи есть все необходимые разрешения, в том числе разрешения на выполнение задач и доступ к сети, файлам и общим папкам.

Для следующих разделов в XML-файле аргументов необходимо указать служебную учетную запись:

SERVICEACCOUNT
SERVICEACCOUNT_NONLOC

Пароль для служебной учетной записи указывается в виде простого текста и задается как значение следующего раздела:

ENCRYPTEDPASSWORD

Пример командной строки для запуска установки в автоматическом режиме:

```
"Milestone XProtect VMS Products 2023 R2 System Installer.exe" --quiet --
arguments=C:\Arguments.xml --license=C:\M01-C01-231-01-ABCDEF.lic
```

Пример: Файл аргументов на основе использования выделенной служебной учетной записи

```
<?xml version="1.0" encoding="utf-8"?>
<CommandLineArguments xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:milestone-systems">
  <InstallEnvironment>
    <Parameters>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>USERACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT_NONLOC</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>sampleaccountpasswordplaintext</Value>
        <Key>ENCRYPTEDPASSWORD</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>%PROGRAMFILES%\Milestone</Value>
        <Key>TARGETDIR</Key>
```

```
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsXPCO</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsDPInstaller</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>false</Value>
        <Key>LEGACY</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>yes</Value>
        <Key>SQL-KEEP-DATA</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>no</Value>
        <Key>SQL-CREATE-DATABASE</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>True</Value>
        <Key>IS_EXTERNALLY_MANAGED</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_MS</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IDP;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IDP</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IM;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IM</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_ES</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_
LogServerV2;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated;Application
Name=Surveillance_LogServerV2</Value>
        <Key>SQL_CONNECTION_STRING_LOG</Key>
      </KeyValueParametersOfStringString>
    </Parameters>
  </InstallEnvironment>
</CommandLineArguments>
```

Предварительные условия, которые необходимо выполнить перед установкой:

- Необходимо создать учетную запись службы, а также учетную запись, используемую для установки.
- Служебная учетная запись должна использоваться для входа в систему и запуска в качестве службы на компьютере, на котором выполняется установка. См. раздел Вход в качестве службы.
- Необходимо создать базы данных, которые будет использовать XProtect, и присвоить им имена в XML-файле аргументов. Например:

Имя базы данных
`Surveillance`
`Surveillance_IDP`
`Surveillance_IM`
`Surveillance_LogServerV2`

- Базы данных должны быть настроены в соответствии со следующим списком:

Конфигурация базы данных
Сортировка по умолчанию устанавливается как «`SQL_Latin1_General_CP1_CI_AS`»
`ALLOW_SNAPSHOT_ISOLATION` устанавливается как `ON`
`READ_COMMITTED_SNAPSHOT` устанавливается как `ON`

- Необходимо выполнить вход в систему Microsoft® SQL Server® с помощью служебной учетной записи и учетной записи, используемой для установки, на всех базах данных. В каждой базе нужно создать пользователя, который будет членом роли db_owner в базах данных.

Установка в рабочих группах

Если вместо домена и сервера Active Directory используется рабочая группа, выполните следующие действия при установке.

Все компьютеры распределенной системы должны входить в домен или рабочую группу.

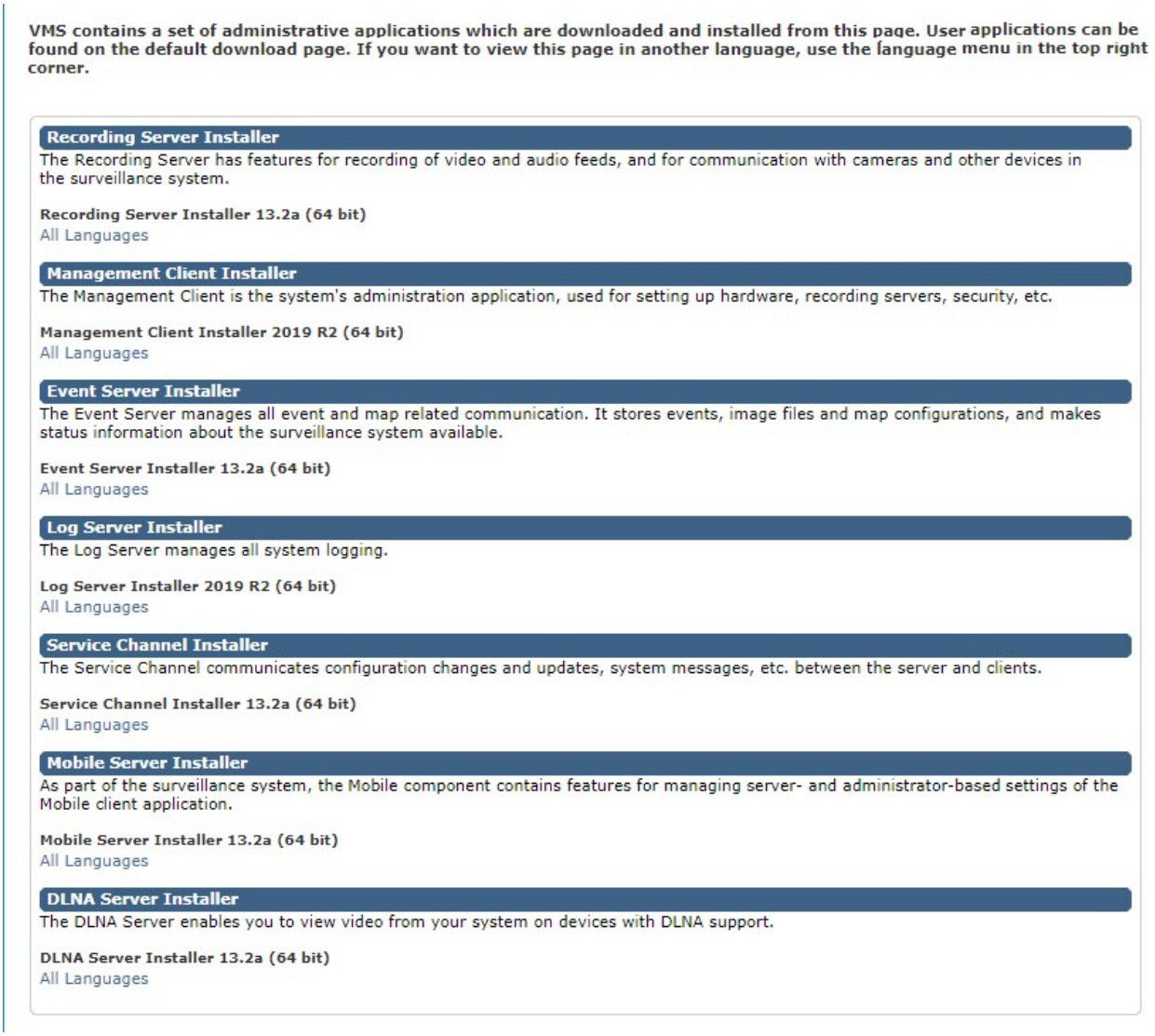
1. Войдите в Windows. Используемая здесь учетная запись пользователя будет добавлена на роль администратора XProtect во время установки.

   Убедитесь, что на всех компьютерах в системе используется одна и та же учетная запись.

2. В зависимости от ваших задач запустите установку сервера управления или сервера записи и выберите **Пользовательская**.
3. В зависимости от выбора на шаге 2 выберите установку службы Management Server или Recording Server с помощью общей учетной записи администратора.
4. Завершите установку.
5. Повторите шаги 1–4, чтобы установить все остальные системы, которые необходимо подключить. Все они должны быть установлены с использованием одной и той же системной учетной записи.

Download Manager/веб-страница загрузки

Сервер управления содержит встроенную веб-страницу. На этой странице администраторы и конечные пользователи могут загружать и устанавливать необходимые компоненты системы XProtect из любого места — как локально, так и удаленно.



На веб-странице может отображаться два набора данных, оба на языке, используемом по умолчанию в установленной системе:

- Одна веб-страница предназначена для **администраторов**, с ее помощью они могут загружать и устанавливать основные компоненты системы. Чаще всего веб-страница автоматически загружается в конце установки сервера управления, и на ней отображается содержимое по умолчанию. На сервере управления можно открыть веб-страницу из меню Windows **Пуск**. Для этого выберите **Программы** > **Milestone** > **Административная страница установки**. Также можно ввести URL-адрес:

  http://[адрес сервера управления]:[порт]/installation/admin/

  [адрес сервера управления] — это IP-адрес или имя хоста сервера управления. [порт] — это номер порта, который IIS будет использовать на сервере управления.

- Другая веб-страница предназначена для конечных **пользователей**, с ее помощью обеспечивается доступ к приложениям клиента с конфигурацией по умолчанию. На сервере управления можно открыть веб-страницу из меню Windows **Пуск**. Для этого выберите **Программы** > **Milestone** > **Общедоступная страница установки**. Также можно ввести URL-адрес:

  http://[адрес сервера управления]:[порт]/installation/

  [адрес сервера управления] — это IP-адрес или имя хоста сервера управления. [порт] — это номер порта, который IIS будет использовать на сервере управления.

Эти две веб-страницы по умолчанию содержат определенную информацию, поэтому их можно использовать сразу же после установки. Администратор может настроить отображение содержимого веб-страниц с помощью Download Manager. Также можно перемещать компоненты между двумя версиями веб-страницы. Чтобы переместить компонент, нажмите его правой кнопкой мыши и выберите версию веб-страницы, на которую вы хотите переместить компонент.

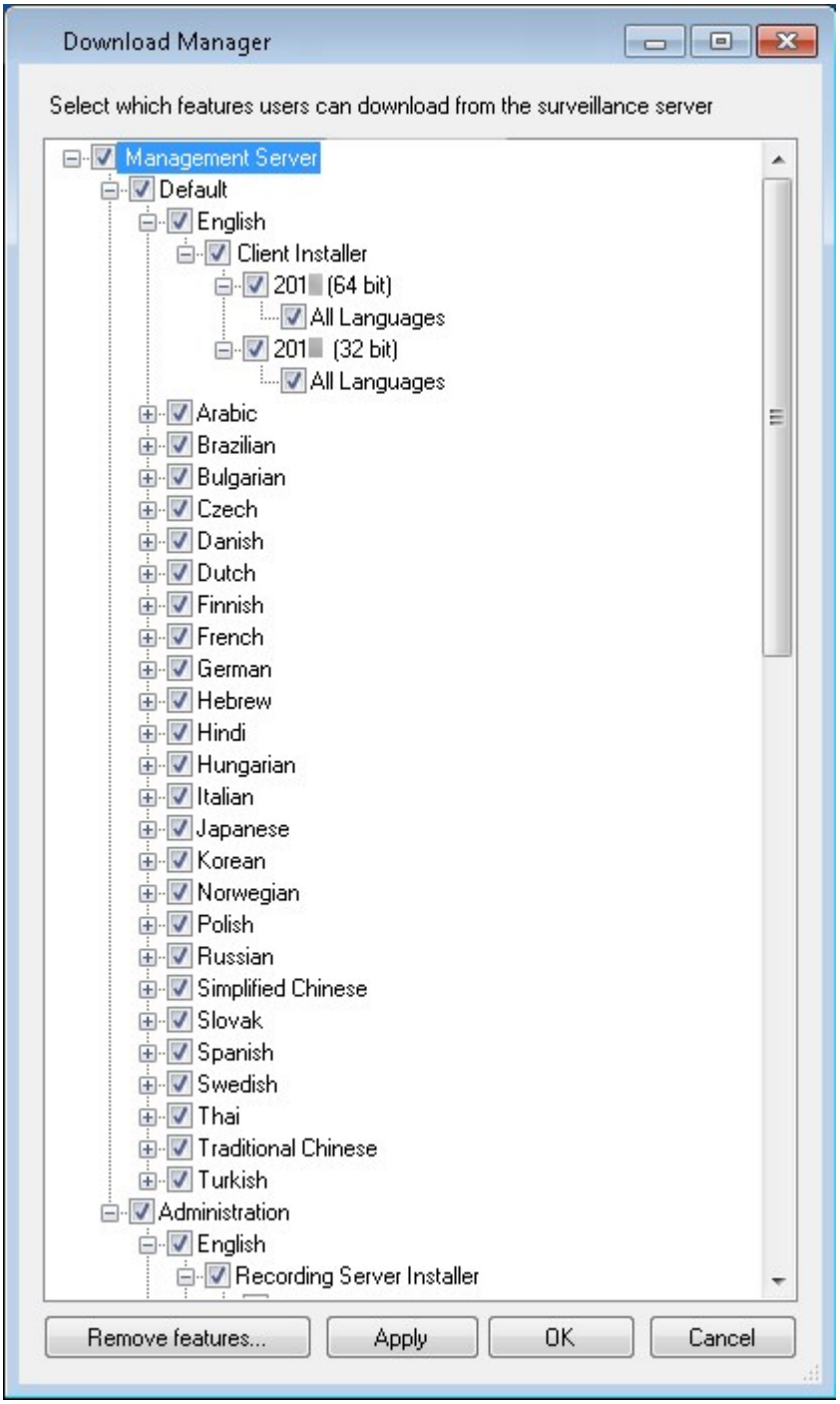
Несмотря на то, что вы можете контролировать, какие компоненты пользователи могут загружать и устанавливать в Download Manager, вы не можете управлять разрешениями пользователей. Такие разрешения определяются ролями, заданными в Management Client.

На сервере управления можно открыть XProtect Download Manager из меню Windows **Пуск**. Для этого выберите **Программы** > **Milestone** > **XProtect Download Manager**.

Стандартная конфигурация Download Manager

Download Manager имеет стандартную конфигурацию. Это гарантирует, что пользователи вашей организации могут сразу же получить доступ к стандартным компонентам.

Стандартная конфигурация обеспечивает установку по умолчанию с доступом к загрузке дополнительных компонентов. Как правило, доступ к веб-странице осуществляется с компьютера с установленным сервером управления. Однако вы также можете получить доступ к веб-странице с других компьютеров.



- Первый уровень: Продукт XProtect
- Второй уровень: Две версии веб-страницы. **По умолчанию** — это версия веб-страницы, которую просматривают конечные пользователи. **Администрирование** — это версия веб-страницы, которую просматривают системные администраторы
- Третий уровень: Языки, на которых доступна веб-страница

- Четвертый уровень: Компоненты, которые уже доступны или могут быть доступны пользователям.
- Пятый уровень: Конкретные версии каждого компонента, которые уже доступны или могут быть доступны пользователям.
- Шестой уровень: Языковые версии компонентов, которые уже доступны или могут быть доступны пользователям.

Благодаря тому, что изначально доступны только стандартные компоненты, причем исключительно на том же языке, что и установленная система, сокращается время установки и экономится место на сервере. Нет необходимости хранить компонент или языковую версию на сервере, если они не используются.

Вы можете сделать доступными дополнительные компоненты или языки, а также скрыть или удалить ненужные компоненты или языки при необходимости.

Стандартные программы установки Download Manager (пользователь)

Следующие компоненты по умолчанию доступны для самостоятельной установки с веб-страницы загрузки сервера управления, предназначенной для пользователей (под управлением Download Manager):

- Серверы записи, включая серверы записи обработки отказа Изначально серверы записи обработки отказа загружаются и устанавливаются как серверы записи. Уже непосредственно в процессе установки вы указываете, что вам нужен сервер записи обработки отказа.
- Management Client
- XProtect Smart Client
- Сервер событий, используемый совместно с функцией карты
- Сервер регистрации, используемый для обеспечения функций, которые требуются для регистрации системной информации
- Сервер XProtect Mobile
- Для вашей организации могут быть доступны и другие варианты.

Дополнительные сведения об установке комплектов драйверов приведены в разделе Обязательная загрузка программы установки комплекта драйверов на стр. 208.

Добавление/публикация компонентов программы установки Download Manager

Чтобы нестандартные компоненты и новые версии стали доступны на странице загрузки сервера управления, необходимо выполнить две процедуры.

Сначала добавьте новые и/или нестандартные компоненты в Download Manager. С помощью этой системы настройте компоненты, которые должны быть доступны в различных языковых версиях веб-страницы.

Перед установкой новых компонентов следует закрыть Download Manager, если система открыта.

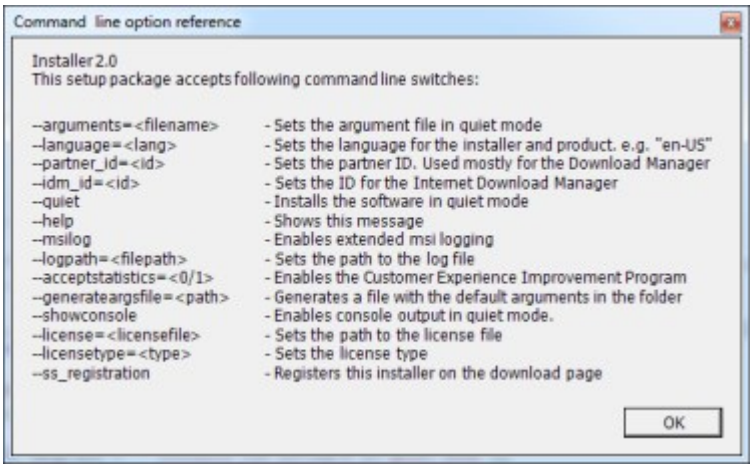
Добавление новых/нестандартных файлов в Download Manager:

1. Используя компьютер, на который вы загрузили компоненты, откройте меню **Пуск** Windows, *Командная строка*.
2. В *командной строке* введите имя файла (*.exe*) с:[пробел]--*ss_registration*.

   Пример: *MilestoneXProtectRecordingServerInstaller_x64.exe --ss_registration*

   Файл будет добавлен в папку Download Manager, но не установлен на текущем компьютере.

Чтобы узнать о командах программы установки, в *командной строке* введите [пробел]--*help*, после чего появится следующее окно:



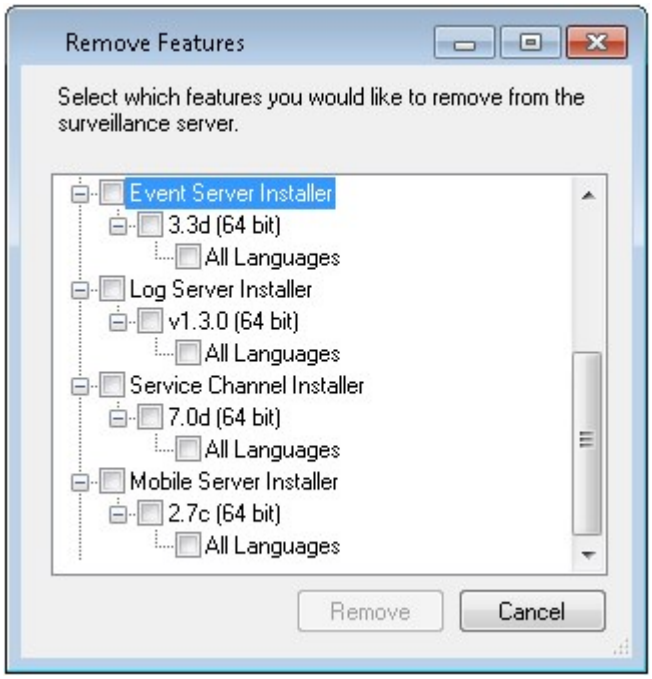
После установки новых компонентов они будут по умолчанию выбраны в Download Manager и сразу же станут доступны пользователям на веб-странице. Вы можете отобразить или скрыть функции на веб-странице в любой момент, установив или сняв соответствующие флажки в дереве Download Manager.

Последовательность отображения компонентов на веб-странице можно изменить. В дереве Download Manager перетащите элементы компонента и переместите их в нужное положение.

Скрытие/удаление компонентов программы установки Download Manager

Доступно три варианта:

- **Скрыть компоненты** с веб-страницы, сняв флажки в дереве Download Manager. Компоненты остаются на сервере управления. Вы можете быстро сделать их доступными, установив соответствующие флажки в дереве Download Manager.
- **Удалить установленные компоненты** с сервера управления. Компоненты удалятся из папки Download Manager, при этом установочные файлы будут храниться в папке `C:\Program Files (x86)\Milestone\XProtect Download Manager`, так что вы сможете переустановить их снова, если потребуется.
    1. В Download Manager нажмите **Удалить компоненты**.
    2. В окне **Удалить компоненты** выберите компоненты, которые вы хотите удалить.



    3. Нажмите **ОК**, затем **Да**.
- **Удалить установочные файлы ненужных компонентов** с сервера управления. Это поможет сэкономить место на сервере, если известно, что ваша организация не будет использовать определенные компоненты.

Обязательная загрузка программы установки комплекта драйверов

Комплект драйверов устройств (содержит драйверы устройств), включенный в первоначальную установку, не входит в Download Manager. Если вам потребуется переустановить комплект драйверов или сделать доступной программу установки комплекта драйверов, сначала добавьте или опубликуйте последнюю версию программы установки комплекта драйверов в Download Manager:

1. Загрузите последнюю версию стандартного комплекта драйверов со страницы загрузки на сайте Milestone (https://www.milestonesys.com/downloads/).
2. На этой же странице можно загрузить комплект драйверов для старых устройств. Чтобы проверить, используют ли ваши камеры драйверы из комплекта драйверов для старых устройств, перейдите на этот сайт (https://www.milestonesys.com/community/business-partner-tools/device-packs/).
3. Чтобы добавить/опубликовать в Download Manager, вызовите его с помощью команды *--ss_registration*.

Если вы не подключены к сети, можно переустановить весь сервер записи с помощью Download Manager. Установочные файлы для сервера записи хранятся локально на вашем компьютере, таким образом, переустановка комплекта драйверов выполняется автоматически.

Файлы журнала установки и устранение неполадок

Во время установки, обновления или удаления записи регистрируются в различных файлах журнала установки: в основной файл журнала установки `installer.log` и в файлы журналов, относящиеся к различным устанавливаемым компонентам системы. Все записи журнала сопровождаются метками времени. Самые последние записи содержатся в конце файлов журнала.

Все файлы журналов установки можно найти в папке `C:\ProgramData\Milestone\Installer\`. Файлы журнала с именами *I.log или *I[integer].log — это файлы журнала, содержащие информацию о новых установках или обновлениях. Файлы журнала с именами *U.log или *U[integer].log — это файлы журнала, содержащие информацию об удаленных компонентах. Если вы приобрели сервер с уже установленной системой XProtect от партнера Milestone, файлы журнала установки могут отсутствовать.

Файлы журнала содержат информацию о параметрах и опциях командной строки, которые использовались во время установки, обновления или удаления. Чтобы найти информацию об используемых параметрах командной строки в файлах журнала, выполните поиск по **Command Line:** или **Parameter '** в зависимости от файла журнала.

При диагностике и устранении неполадок рекомендуется в первую очередь изучить основной файл журнала установки installer.log. Если во время установки возникли какие-либо исключения, ошибки или предупреждения, информация о них содержится в журнале. Выполните поиск по словам **exception**, **error** или **warning**. «Код завершения: 0» означает успешную установку. «Код завершения: 1» означает, что установку выполнить не удалось. Информация, содержащаяся в файлах журнала, поможет вам найти подходящее решение в MilestoneKnowledge Base. Если вам не удается справиться самостоятельно, свяжитесь с партнером Milestone и предоставьте ему соответствующие файлы журнала установки.

Конфигурация

Список задач первоначальной настройки

В приведенном ниже контрольном списке перечислены первоначальные задачи по настройке системы. Некоторые из них, возможно, были решены при установке.

Выполненный контрольный список сам по себе не гарантирует, что система в точности соответствует требованиям организации. Для того, чтобы система соответствовала требованиям организации, Milestone рекомендует осуществлять непрерывный мониторинг и корректировку системы.

Например, после запуска системы полезно протестировать и скорректировать настройки чувствительности к обнаружению движений различных камер в различных физических условиях: днем и ночью, а также при ветре и в безветренную погоду.

Другим примером настроек, которые можно изменить в зависимости от потребностей организации, является комплекс правил, определяющих большинство выполняемых системой действий, в том числе — когда следует начинать запись видео.

Шаг	Описание
☑	Первоначальная установка системы завершена. См. раздел Установка новой системы XProtect на стр. 164.
☑	Замените пробный код лицензии на программное обеспечение на постоянный (при необходимости). См. раздел Изменение кода лицензии на программное обеспечение на стр. 140.
☑	Войдите в Management Client. См. раздел Вход в систему (объяснение) на стр. 33.
☐	Убедитесь, что настройки хранилища каждого сервера записи отвечают вашим потребностям. См. раздел Хранение и архивирование (объяснение) на стр. 64.
☐	Убедитесь, что настройки архивирования каждого сервера записи отвечают вашим потребностям. См. раздел Свойства окна «Параметры хранения и записи» на стр. 454.

Шаг	Описание
☐	Определите, какое оборудование, камеры или видеокодеры нужно подключить к каждому серверу записи. См. раздел Добавление оборудования на стр. 232.
☐	Настройте отдельные камеры каждого сервера записи. См. раздел Камеры (узел «Устройства») на стр. 474.
☐	Включите хранилище и архивирование для отдельных камер или для группы камер. Для этого используются настройки отдельных камер или группы устройств. См. раздел Подключение устройства или группы устройств к хранилищу на стр. 217.
☐	Включите и настройте устройства. См. раздел Устройства (раздел «Устройства») на стр. 472.
☐	Поведение системы в значительной степени определяется правилами. Именно правила устанавливают, когда камеры должны начинать запись, когда PTZ-камера (поворотная камера с трансфокатором) должна осуществлять патрулирование, а также когда следует отправлять уведомления. Создайте правила. См. раздел Правила и события (объяснение) на стр. 88.
☐	Добавьте правила в систему. См. раздел Роли и разрешения роли (объяснение) на стр. 78.
☐	Назначьте пользователям или группам пользователей роли. См. раздел Назначение ролям пользователей и групп и их удаление из ролей на стр. 313.
☐	Активируйте лицензии. См. раздел Интерактивная активация лицензии на стр. 138 или Автономная активация лицензий на стр. 138.

Дополнительные сведения о настройке системы на панели **Навигация по сайту** см. в разделе Панель «Навигация по сайту» на стр. 416.

Серверы записи

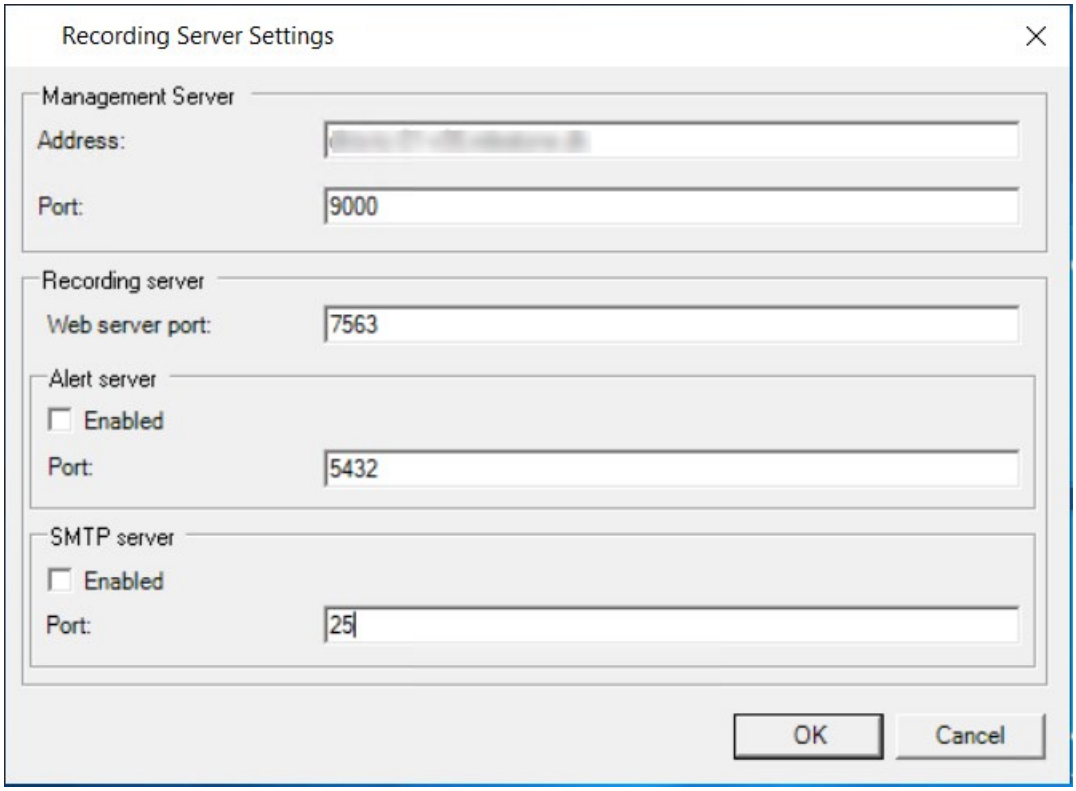
Изменение или проверка правильности основных настроек сервера записи

Если в Management Client не перечислены все установленные вами серверы записи, наиболее вероятная причина заключается в том, что в процессе установки были неправильно заданы параметры (например, IP-адрес или имя хоста сервера управления).

Для установки параметров серверов управления не требуется переустанавливать сервера записи, но можно изменить основные настройки или проверить их правильность:

1. На компьютере, на котором работает сервер записи, нажмите значок **Сервер записи** в области уведомлений правой кнопкой мыши.
2. Выберите пункт **Остановить службу Recording Server**.
3. Повторно нажмите значок **сервера управления** правой кнопкой мыши и выберите **Восстановить конфигурацию**.

   Откроется окно **Настройки сервера записи**.



4. Проверьте правильность следующих настроек или проверьте их правильность:
   - **Сервер управления**: **Адрес**: Укажите IP-адрес или имя хоста сервера управления, к которому должен быть подключен сервер записи.
   - **Сервер управления**: **Порт**: Укажите номер порта, который должен использоваться для связи с сервером управления. При необходимости этот параметр можно изменить, но номер порта должен всегда совпадать с номером порта, настроенным на сервере управления. См. раздел Порты, используемые системой на стр. 109.
   - **Сервер записи**: **Порт веб-сервера**: Укажите номер порта, который должен использоваться для связи с веб-сервером сервера записи. См. раздел Порты, используемые системой на стр. 109.
   - **Сервер записи**: **Порт сервера оповещения**: Включите и укажите номер порта, который должен использоваться для связи с сервером оповещения сервера записи, ожидающим получения сообщений о событиях от устройств. См. раздел Порты, используемые системой на стр. 109.
   - **Сервер SMTP**: **Порт**: Включите и укажите номер порта, который должен использоваться для связи со службой SMTP (простой протокол передачи почты) сервера записи. См. раздел Порты, используемые системой на стр. 109.
5. Нажмите кнопку **OK**.
6. Для повторного запуска службы Recording Server нажмите значок **Сервер записи** правой кнопкой мыши и выберите пункт **Запустить службу Recording Server**.

> Остановка службы Recording Server означает, что, пока вы проверяете правильность основных настроек сервера записи или меняете их, запись и просмотр видео в режиме реального времени невозможны.

Регистрация сервера записи

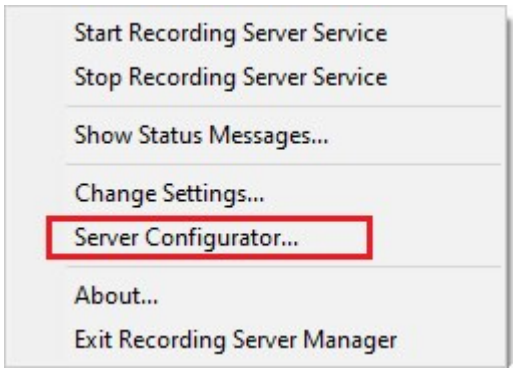
В большинстве случаев устанавливаемый сервер записи регистрируется автоматически. Регистрировать сервер вручную требуется в следующих случаях:

- Если вы заменили сервер записи
- Если сервер записи был установлен в автономном режиме, а затем добавлен к серверу управления
- Если сервер записи не использует порты по умолчанию. Если номера портов зависят от настроек шифрования. Дополнительные сведения приведены в разделе Порты, используемые системой на стр. 109

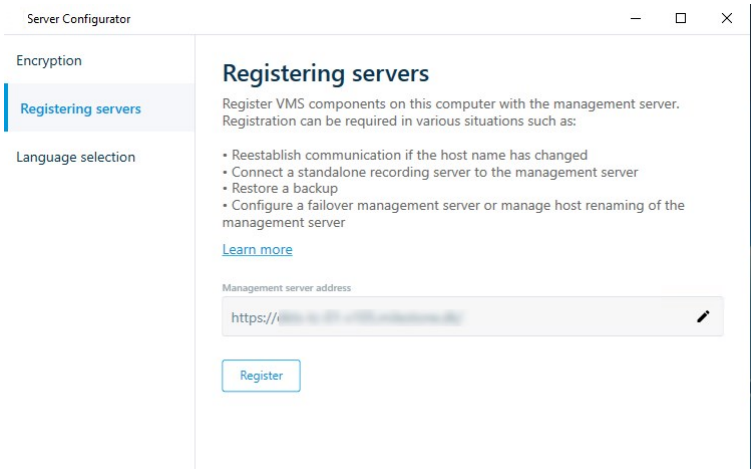
- Автоматическая регистрация завершилась сбоем, например после изменения адреса сервера управления, изменения имени компьютера с сервером записи или после включения или отключения параметров шифрования для связи с сервером. Дополнительные сведения о внесении изменений в адрес сервера управления приведены в разделе Изменение имени хоста компьютера с сервером управления.

При регистрации сервера записи его необходимо настроить так, чтобы он подключался к серверу управления. Компонентом сервера управления, который отвечает за регистрацию, является служба Authorization Server.

1. Откройте Server Configurator из меню «Пуск» или с помощью значка сервера записи на панели задач.



2. Выберите пункт **Регистрация серверов** в Server Configurator .



3. Проверьте правильность адреса сервера управления и схему (HTTP или HTTPS), к которым вы хотите подключить серверы на компьютере, а затем нажмите кнопку **Зарегистрировать**.

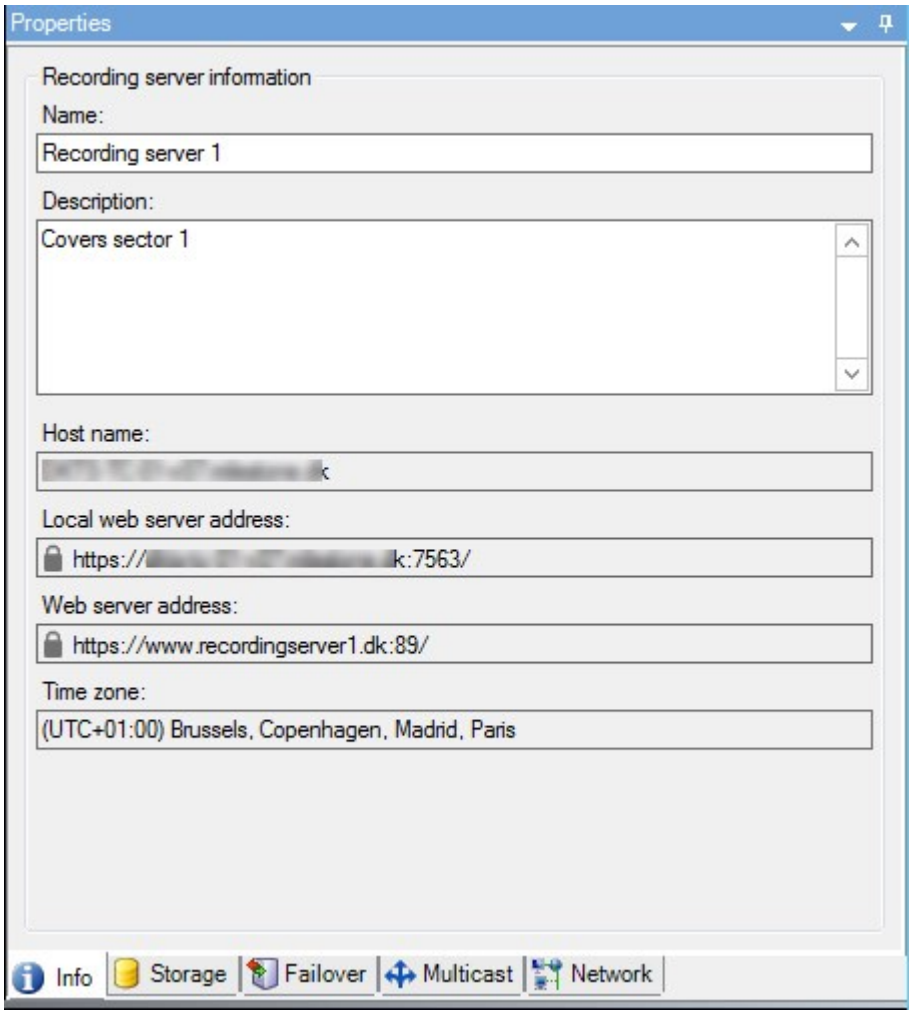
Отобразится подтверждение с сообщением об успешной регистрации сервера управления.

Также см. Замена сервера записи на стр. 372.

Просмотр состояния шифрования при подключении к клиентам

Для того чтобы проверить, использует ли сервер записи шифрование подключений:

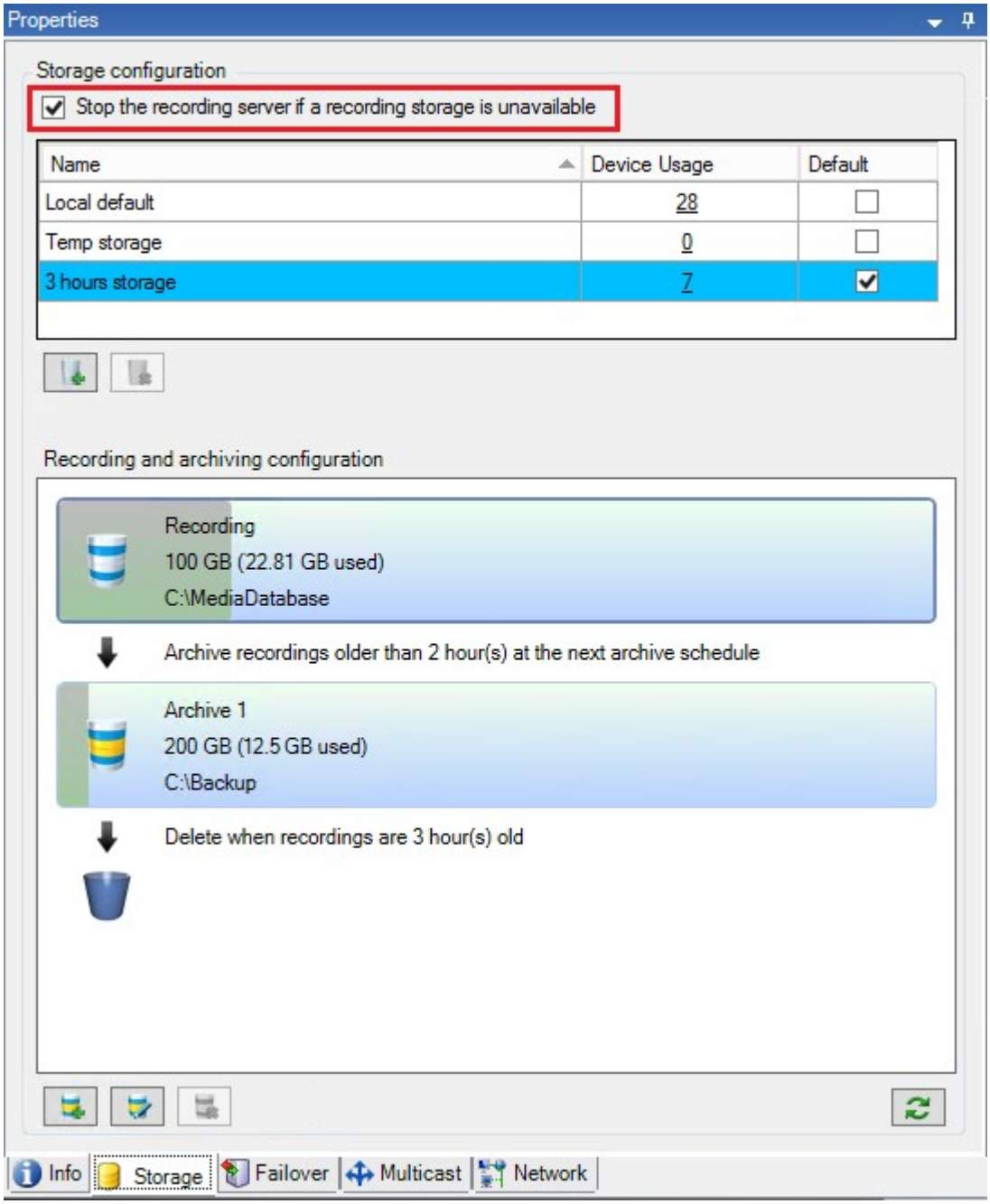
1. Откройте Management Client.
2. На панели **Навигация по сайту** выберите пункт **Серверы** > **Серверы записи**. Откроется список серверов записи.
3. На панели **Обзор** выберите требуемый сервер записи и перейдите на вкладку **Сведения**. Если включено шифрование подключений к клиентам и серверам, которые получают потоки данных от сервера записи, перед локальным адресом веб-сервера и дополнительным адресом веб-сервера отображается значок замка.



Указание действий, выполняемых при недоступности хранилища записей

По умолчанию сервер записи продолжает работать, даже если хранилище записей становится недоступным. Если в системе настроено использование серверов записи обработки отказа, можно указать, что сервер записи должен прекратить работу, а серверы отказоустойчивости — взять на себя его функции:

1. В разделе соответствующего сервера записи перейдите на вкладку **Хранилище**.
2. Включите параметр **Останавливать сервер записи при недоступности хранилища**.



Добавление нового хранилища

При добавлении нового хранилища всегда создается одно хранилище записей с предварительно определенной базой данных записей под названием **Запись**. Переименовать базу данных невозможно. Помимо хранилища записей хранилище может содержать ряд архивов.

1. Для добавления дополнительного хранилища к выбранному серверу записи нажмите кнопку  , расположенную под списком **Конфигурация хранилища**. Откроется диалоговое окно **Настройки хранилища и записи**.
2. Выберите требуемые параметры (см. Свойства окна «Параметры хранения и записи» на стр. 454).
3. Нажмите кнопку **OK**.

Теперь в новом хранилище можно создавать архивы.

Создание архива в хранилище

По умолчанию в хранилище нет архивов, но их можно создать по мере необходимости.

1. Выберите соответствующее хранилище в списке **Настройки записи и архивирования**.
2. Нажмите кнопку  под списком **Настройки записи и архивирования**.
3. В диалоговом окне **Настройки архива** задайте требуемые параметры (см. раздел Свойства окна «Настройки архива» на стр. 456).
4. Нажмите кнопку **OK**.

Подключение устройства или группы устройств к хранилищу

После настройки хранилища для сервера записи его можно включить для отдельных устройств (например, камер, микрофонов или динамиков) либо для группы устройств. Также можно выбрать области хранилища сервера записи, которые нужно использовать для отдельного устройства или группы.

1. Откройте список **Устройства** и выберите пункт **Камеры**, **Микрофоны** или **Динамики** (в зависимости от ситуации).
2. Выберите устройство или группу устройств.
3. Откройте вкладку **Запись**.
4. В области **Хранилище** выберите пункт **Выбрать**.
5. В открывшемся диалоговом окне выберите базу данных, в которой нужно хранить записи устройства, и нажмите кнопку **OK**.
6. На панели инструментов нажмите кнопку **Сохранить**.

При нажатии номера уровня использования устройства в области хранилища на вкладке «Хранилище» сервера записи устройство отобразится в открывающемся отчете.

Отключенные устройства

Отключенные устройства по умолчанию не отображаются на панели **Обзор**.

Чтобы вывести на экран все отключенные устройства, вверху панели **Обзор** нажмите **Фильтр**, чтобы открыть вкладку **Фильтр**, и выберите **Показать отключенные устройства**.

Чтобы снова скрыть отключенные устройства, снимите флажок **Показать отключенные устройства**.

Изменение настроек для выбранного хранилища или архива

1. Для изменения хранилища выберите его базу данных записей в списке **Настройки записи и архивирования**. Для изменения архива выберите базу данных архива.
2. Нажмите кнопку  **Изменить хранилище записей** под списком **Настройки записи и архивирования**.
3. Внесите изменения в базу данных записей или архив.

В случае изменения максимального размера базы данных система автоматически архивирует записи, превышающие новый лимит. В зависимости от настроек архивирования, она автоматически архивирует записи путем перемещения в следующий архив или удаляет их.

Включение цифровой подписи для экспорта

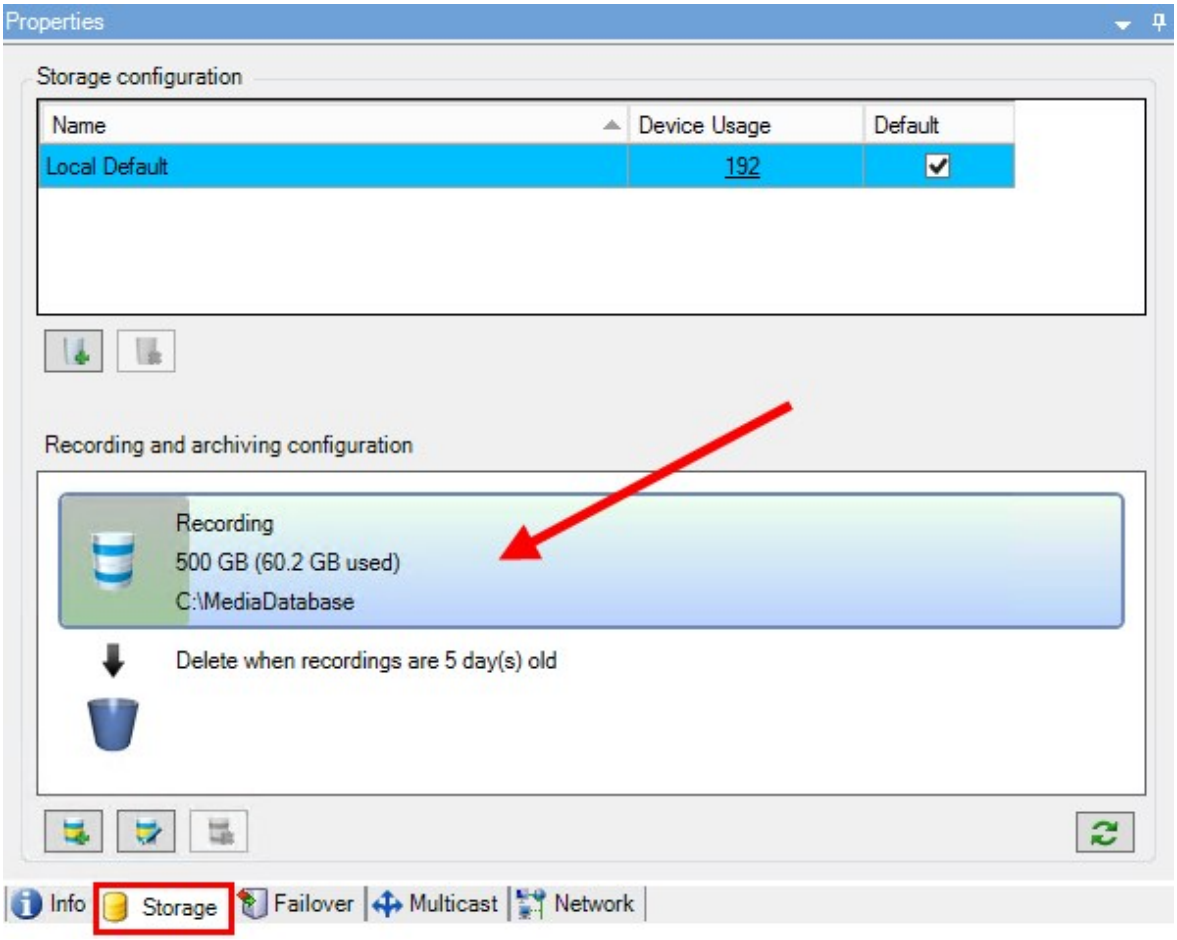
Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Для записанного видео можно включить цифровую подпись: так пользователи клиента смогут убедиться, что с момента записи в него не вносились несанкционированные изменения. Пользователь проверяет аутентичность видео в XProtect Smart Client – Player после его экспорта.

Подпись также необходимо включить в XProtect Smart Client > вкладка **Экспорт** > **Настройки экспорта** > **XProtectФормат** > **Включить цифровую подпись**. В противном случае кнопка **Проверить подписи** в XProtect Smart Client – Player не отображается.

1. На панели **Навигация по сайту** откройте раздел **Серверы**.
2. Нажмите кнопку **Серверы записи**.
3. На панели «Обзор» нажмите сервер записи, для которого требуется включить подпись.

4. В нижней части панели **Свойства** перейдите на вкладку **Хранилище**.



5. В разделе **Настройки записи и архивирования** дважды нажмите горизонтальную полоску, которой соответствует база данных записей. Откроется окно **Настройки хранилища и записи**.
6. Поставьте отметку в поле **Подпись**.
7. Нажмите кнопку **OK**.

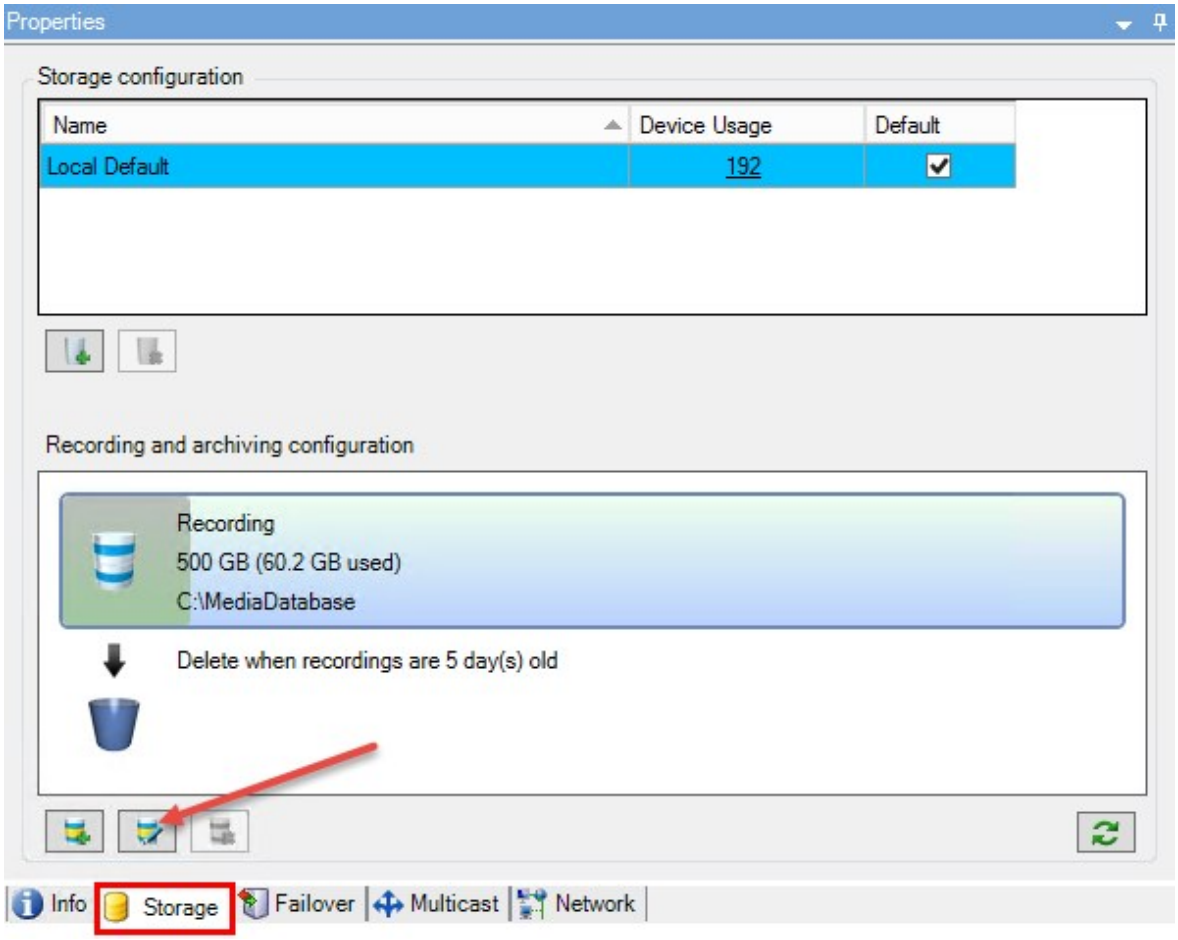
Шифрование записей

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

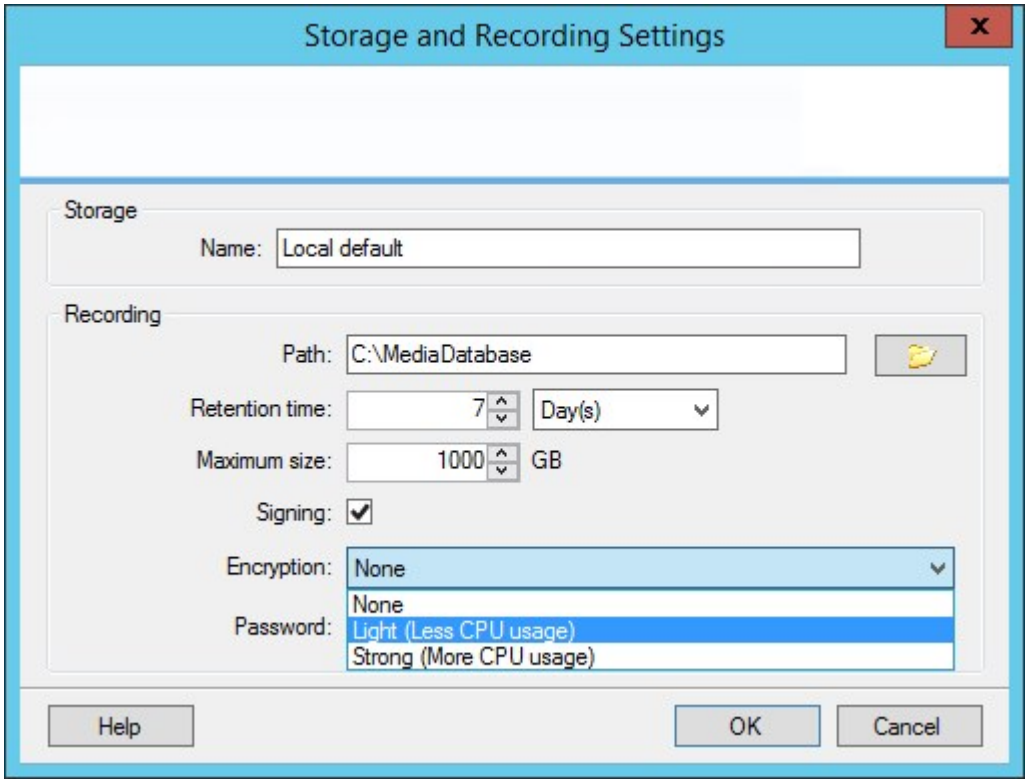
Для защиты записей можно включить шифрование в хранилище и архивах серверов записи. Можно выбрать облегченное или стойкое шифрование. Также при включении шифрования необходимо задать соответствующий пароль.

В зависимости от размера базы данных и производительности диска, включение шифрования или изменение его настроек либо пароля могут занять много времени. Следить за ходом выполнения операций можно в разделе **Текущие задачи**.
Не останавливайте сервер записи, пока выполняется эта задача.

1. Нажмите кнопку **Изменить хранилище записей** под списком **Настройки записи и архивирования**.



2. В открывшемся диалоговом окне укажите уровень шифрования.



3. Вы автоматически перейдете в диалоговое окно **Задать пароль**. Введите пароль и нажмите кнопку **OK**.

Резервное копирование архивных записей

Многие организации выполняют резервное копирование записей с помощью накопителей на магнитных лентах или аналогичных устройств. Детали рабочего процесса разнятся от случая к случаю и зависят от носителей медиаданных, применяемых в организации для хранения резервных копий. Однако полезно запомнить следующее:

Выполняйте резервное копирование архивов, а не баз данных камер

Всегда создавайте резервные копии содержимого архивов, а не баз данных отдельных камер. В случае создания резервных копий содержимого баз данных отдельных камер могут возникнуть нарушения правил совместного использования ресурсов или другие неполадки.

При планировании резервного копирования убедитесь, что задание резервного копирования не пересекается с предусмотренными вами сроками архивирования. Для просмотра расписания архивирования каждого сервера записи в каждой из областей данных откройте вкладку **Хранилище**.

Чтобы архивирование не запустилось в процессе резервного копирования, можно отключить архив, выполнить резервное копирование, а затем вновь подключить архив. Подключение и отключение архивов осуществляется посредством API Gateway.

Для резервного копирования нужных ресурсов важно знать структуру архива

При архивировании записей они хранятся в архиве в виде определенной структуры подкаталогов.

Во всех случаях обычного использования системы структура подкаталогов полностью прозрачна для пользователей системы, когда они просматривают записи при помощи XProtect Smart Client. Это относится как к архивированным, так и к неархивированным записям. Важно знать структуру подкаталогов (см. раздел Структура архива (объяснение) на стр. 69), если вы намерены осуществлять резервное копирование архивированных записей (см. раздел Резервное копирование и восстановление конфигурации системы на стр. 361).

Удаление архива из хранилища

1. Выберите архив в списке **Настройки записи и архивирования**.

   Возможно удалить только последний архив в списке. Архив не должен быть пустым.

2. Нажмите кнопку  , расположенную под списком **Настройки записи и архивирования**.
3. Нажмите кнопку **Да**.

   Применительно к недоступным (например, автономным) архивам, невозможно проверить, содержит ли архив медиаданные с защитой доказательств, но после подтверждения пользователя архив можно удалить.

   Доступные (оперативные) архивы, которые содержат медиаданные с защитой доказательств, удалить невозможно.

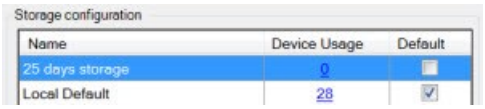
Удаление хранилища

Удалить хранилище по умолчанию или хранилища, которые используются устройствами в качестве хранилища записей при прямой передаче, нельзя.
Это означает, что перед удалением хранилища может потребоваться перенести устройства (см. раздел Move hardware на стр. 373) и еще не архивированные записи в другое хранилище.

1. Для просмотра списка устройств, использующих данное хранилище, нажмите номер уровня использования устройства.

   Если в хранилище имеются данные из устройств, которые были перенесены на другой сервер записи, отобразится предупреждение. Нажмите ссылку, чтобы увидеть список устройств.

2. Выполните шаги, описанные в разделе Перенос неархивированных записей из одного хранилища в другое на стр. 223.
3. Повторяйте операции до тех пор, пока не будут перенесены все устройства.
4. Выберите хранилище, которое вы хотите удалить.



5. Нажмите кнопку , расположенную под списком **Настройки хранилища**.
6. Нажмите кнопку **Да**.

Перенос неархивированных записей из одного хранилища в другое

Перенос записей из одной базы данных прямой записи в другую осуществляется на вкладке устройства **Запись**.

1. Выберите тип устройства. На панели **Обзор** выберите представление транзакции.
2. Откройте вкладку **Запись**. Нажмите **Выбрать** в верхней части области **Хранилище**.
3. Выберите базу данных в диалоговом окне **Выбрать хранилище**.
4. Нажмите кнопку **OK**.
5. В диалоговом окне **Действие с записями** выберите необходимое действие: перемещение существующих, но **не архивированных**, записей в новое хранилище либо их удаление.
6. Нажмите кнопку **OK**.

Привязка серверов записи обработки отказа

На вкладке **Обработка отказа** сервера записи можно выбрать один из трех типов схем обработки отказа:

- Без схемы обработки отказа
- Основная/вспомогательная схема обработки отказа (холодная замена)
- Схема горячей замены

При выборе пункта **b** и **c** необходимо выбрать конкретный сервер/группы. При выборе пункта **b** можно выбрать вспомогательную группу отказоустойчивых серверов. В случае недоступности сервера записи его функции начинает выполнять сервер записи обработки отказа из основной группы отказоустойчивых серверов. Если выбрана вспомогательная группа отказоустойчивых серверов, сервер записи обработки отказа из вспомогательной группы вступает в действие, когда заняты все серверы записи обработки отказа из основной группы отказоустойчивых серверов. Таким образом, риск отсутствия решения по обработке отказа возникает в лишь в том маловероятном случае, когда заняты все серверы записи обработки отказа как в основной, так и во вспомогательной группах отказоустойчивых серверов.

1. На панели **Навигация по сайту** выберите пункт **Серверы** > **Серверы записи**. Откроется список серверов записи.
2. На панели **Обзор** выберите требуемый сервер записи и перейдите на вкладку **Обработка отказа**.
3. При выборе схема обработки отказа возможны следующие варианты:
   - **Нет**
   - **Основная группа отказоустойчивых серверов/Вспомогательная группа отказоустойчивых серверов**
   - **Сервер горячей замены**

   Выбрать одну и ту же группу отказоустойчивых серверов в качестве как основной, так и вспомогательной группы отказоустойчивых серверов нельзя. Также обычные отказоустойчивые серверы, уже включенные в группу отказоустойчивых серверов, нельзя выбрать в качестве серверов горячей замены.
4. Затем нажмите **Дополнительные параметры обработки отказа**. Откроется окно **Дополнительные параметры обработки отказа** со списком всех устройств, подключенных к выбранному серверу записи. Если выбран пункт **Нет**, будут доступны дополнительные параметры обработки отказа. Система сохраняет сведения о выбранных параметрах для последующих схем обработки отказа.
5. Чтобы указать уровень поддержки обработки отказа, выберите **Полная поддержка**, **Только в режиме реального времени** или **Отключено** для каждого устройства из списка. Нажмите кнопку **OK**.
6. В поле **Коммуникационный порт службы обработки отказа (TCP)** отредактируйте номер порта (если это необходимо).

Если поддержка обработки отказа включена, но сервер записи настроен на продолжение работы в случае недоступности хранилища, сервер записи обработки отказа не вступит в действие. Для обеспечения работоспособности поддержки отказоустойчивости необходимо включить параметр **Останавливать сервер записи при недоступности хранилища** на вкладке **Хранилище**.

Включение многоадресной передачи для сервера записи

При обычной передаче данных по сети каждый пакет данных отправляется от одного отправителя к одному получателю. Этот процесс называется одноадресной передачей. При этом при многоадресной передаче один пакет данных (от сервера) можно отправить нескольким получателям (клиентам) из состава группы. Многоадресная передача может помочь сэкономить пропускную способность.

- При использовании **одноадресной передачи** источник должен передавать один поток данных для каждого получателя.
- При использовании **многоадресной передачи** в каждом сетевом сегменте требуется лишь один поток данных

Описываемая в настоящем документе многоадресная передача — это **НЕ** потоковая передача видео с камеры на серверы, а передача видео с серверов клиентам.

При многоадресной передаче вы работаете с определенной группой получателей, исходя из таких параметров, как диапазоны IP-адресов, возможность включения/отключения многоадресной передачи для отдельных камер, возможность задавать максимальный допустимый размер пакета данных (MTU), максимальное количество маршрутизаторов, между которыми должен пересылаться пакет данных (TTL), и так далее.

Потоки многоадресной передачи не шифруются, даже если на сервере записи используется шифрование.

Многоадресную передачу не следует путать с **трансляцией**, при которой данные отправляются всем, кто подключен к сети, даже если эти данные могут быть не актуальны для каждого пользователя:

Имя	Описание
Одноадресная передача	Данные отправляются от одного источника к одному получателю.
Многоадресная передача	Данные отправляются от одного источника к нескольким получателям в рамках четко заданной группы.
Трансляция	Данные отправляются от одного источника каждому, кто подключен к сети. Таким образом, трансляция способна привести к значительному замедлению сетевого обмена данными.

Для использования многоадресной передачи сетевая инфраструктура должна поддерживать стандарт многоадресной передачи по интернет-протоколу IGMP (протокол управления группами в Интернете).

- На вкладке **Многоадресная передача** поставьте отметку в поле **Многоадресная передача**.

Если на одном или нескольких серверах записи уже занят весь диапазон IP-адресов, сначала необходимо освободить несколько IP-адресов для многоадресной передачи и только потом включать многоадресную передачу на дополнительных серверах записи.

Потоки многоадресной передачи не шифруются, даже если на сервере записи используется шифрование.

Включение многоадресной передачи для отдельных камер

Многоадресная передача работает только в том случае, если вы включили ее для соответствующих камер:

1. Выберите сервер записи и необходимую камеру на панели **Обзор**.
2. На вкладке **Клиент** поставьте отметку в поле **Динамическая прямая передача**. Повторите эти действия для всех соответствующих камер.

Потоки многоадресной передачи не шифруются, даже если на сервере записи используется шифрование.

Задайте общедоступный адрес и порт

Если вам требуется получать доступ к VMS с помощью XProtect Smart Client через общедоступную или ненадежную сеть, Milestone рекомендует использовать защищенное VPN-подключение. Это позволит обеспечить защиту обмена данными между XProtect Smart Client и VMS.

Общедоступный IP-адрес сервера записи задается на вкладке **Сеть**.

В чем преимущества общедоступного адреса?

Клиенты могут подключаться из локальной сети или из Интернета, и в любом случае система наблюдения должна предоставлять подходящие адреса, чтобы клиенты могли получить доступ к записанному или транслируемому видео с серверов записи:

- Если клиенты подключаются локально, система наблюдения должна предоставить локальные адреса и номера портов.
- Если клиенты подключаются из Интернета, система наблюдения должна предоставлять общедоступный адрес сервера записи. Это адрес брандмауэра или маршрутизатора NAT (Network Address Translation — преобразование сетевых адресов), кроме того, номер порта также часто отличается. Затем адрес и номер порта могут передаваться на локальный адрес и порт сервера.

1. Для включения общего доступа поставьте отметку в поле **Включить общий доступ**.
2. Задайте общедоступный адрес сервера записи. Введите адрес брандмауэра или NAT-маршрутизатора, чтобы клиенты, получающие доступ к системе наблюдения из Интернета, могли подключаться к серверам записи.
3. Задайте номер общедоступного порта. Желательно, чтобы номера портов, используемые в брандмауэре или NAT-маршрутизаторе, отличались от номеров портов, используемых локально.

Если вы используете общий доступ, настройте брандмауэр или NAT-маршрутизатор таким образом, чтобы запросы, отправляемые на общедоступный адрес и порт, перенаправлялись на локальный адрес и порт соответствующих серверов записи.

Назначение диапазонов локальных IP-адресов

Необходимо задать список диапазонов локальных IP-адресов, которые система наблюдения будет рассматривать как принадлежащие к локальной сети:

- На вкладке **Сеть** выберите **Настроить**

Применение фильтров в дереве устройств

Если у вас много зарегистрированных устройств, дерево устройств на панели **Обзор** может стать очень большим. В дереве устройств можно применять фильтры, чтобы быстрее находить устройства, с которыми вы работаете.

Задав критерии фильтрации, уникальные для нескольких конкретных устройств, можно создать список, в котором будут отображаться только эти устройства.

Применение фильтров в дереве устройств

- В верхней части панели **Обзор** нажмите **Фильтр** чтобы перейти на вкладку **Фильтр**.
- В поле **Укажите данные для фильтрации устройств** введите один или несколько критериев и нажмите кнопку **Применить фильтр** для фильтрации списка устройств.

Характеристики критериев фильтрации

Критерии фильтрации применяются к значениям полей имени устройства, краткого имени устройства, адреса оборудования (IP-адреса), идентификатора устройства и идентификатора оборудования.

При применении фильтров к значениям полей идентификатора оборудования и идентификатора устройства частичные совпадения с фильтром не отображаются. Таким образом, при применении фильтров к идентификатору оборудования и идентификатору устройства необходимо указывать идентификатор полностью и точно.

Частичные совпадения с фильтрами отображаются для значений полей имени устройства, краткого имени устройства и адреса оборудования. Поэтому, применительно к критерию фильтрации «камер», будут отображены все устройства, в имени устройства которых содержится слово «камера».

Критерии фильтрации нечувствительны к регистру: результаты фильтрации по словам «камера» и «Камера» будут одинаковыми.

Использование нескольких критериев фильтрации

Для более точной фильтрации дерева устройств можно задать несколько критериев фильтрации. При применении фильтра считается, что все заданные критерии фильтрации объединены оператором «И», то есть суммируются.

Например, если введены два критерия фильтрации: «камера» и «склад», в списке будут отображены все устройства, в имени которых содержатся слова «камера» и «склад», но не будут отображены устройства, в имени которых содержатся слова «камера» и «парковка», а также устройства, в имени которых содержится только слово «камера».

Если вы задали слишком ограничительный фильтр, удалите каждый отдельный критерий фильтрации из поля фильтра, чтобы расширить диапазон фильтрации. При удалении критериев фильтр автоматически применяется к дереву устройств.

Сброс фильтра

При удалении всех критериев фильтрации из поля фильтра данные панели **Обзор**сбрасываются, и на ней вновь отображаются все устройства.

Также чтобы сбросить фильтр и снять отметку в поле **Показывать отключенные устройства**, можно нажать клавишу **F5**.

Отключенные устройства

Отключенные устройства по умолчанию не отображаются на панели **Обзор**.

Чтобы вывести на экран все отключенные устройства, вверху панели **Обзор** нажмите **Фильтр**, чтобы открыть вкладку **Фильтр**, и выберите **Показать отключенные устройства**.

Чтобы снова скрыть отключенные устройства, снимите флажок **Показать отключенные устройства**.

Серверы записи обработки отказа

Настройка и включение серверов записи обработки отказа

Если сервер обработки отказа отключен, его необходимо включить, иначе он не сможет заменить стандартные серверы записи.

Чтобы включить сервер записи обработки отказа и изменить его основные свойства, выполните следующие действия:

1. На панели **Навигация по сайту** выберите **Серверы** > **Серверы отказоустойчивости**. Откроется список установленных серверов записи обработки отказа и групп отказоустойчивых серверов.
2. На панели **Обзор** выберите нужный сервер записи обработки отказа.
3. Нажмите правой кнопкой мыши и выберите **Включено**. Сервер записи обработки отказа включен.
4. Чтобы изменить свойства сервера записи обработки отказа, перейдите на вкладку **Информация**.
5. После этого перейдите на вкладку **Сеть**. Здесь указывается общедоступный IP-адрес сервера записи обработки отказа и другие параметры. Данный пункт актуален, если вы используете NAT (Network Address Translation — преобразование сетевых адресов) и переадресацию портов. Дополнительные сведения приведены на вкладке **Сеть** стандартного сервера записи.
6. На панели **Навигация по сайту** выберите пункт **Серверы** > **Серверы записи**. Выберите сервер записи, для которого вы хотите настроить резервирование, и назначьте серверы записи обработки отказа (см. Вкладка «Обработка отказа» (сервер записи) на стр. 458).

Чтобы узнать статус сервера записи обработки отказа, наведите курсор на значок Failover Recording Server Manager на панели задач в области уведомлений. Появится всплывающая подсказка, содержащая текст, введенный в поле «Описание» для сервера записи обработки отказа. Таким образом можно определить, функции какого сервера записи будет брать на себя сервер записи обработки отказа.

Сервер записи обработки отказа регулярно проверяет связь с сервером управления. Это позволяет убедиться, что он подключен к сети и при необходимости можно запросить и получить конфигурацию стандартных серверов записи. Если заблокировать проверку связи, сервер записи обработки отказа не сможет заменить стандартные серверы записи.

Объединение серверов записи обработки отказа в группу холодной замены

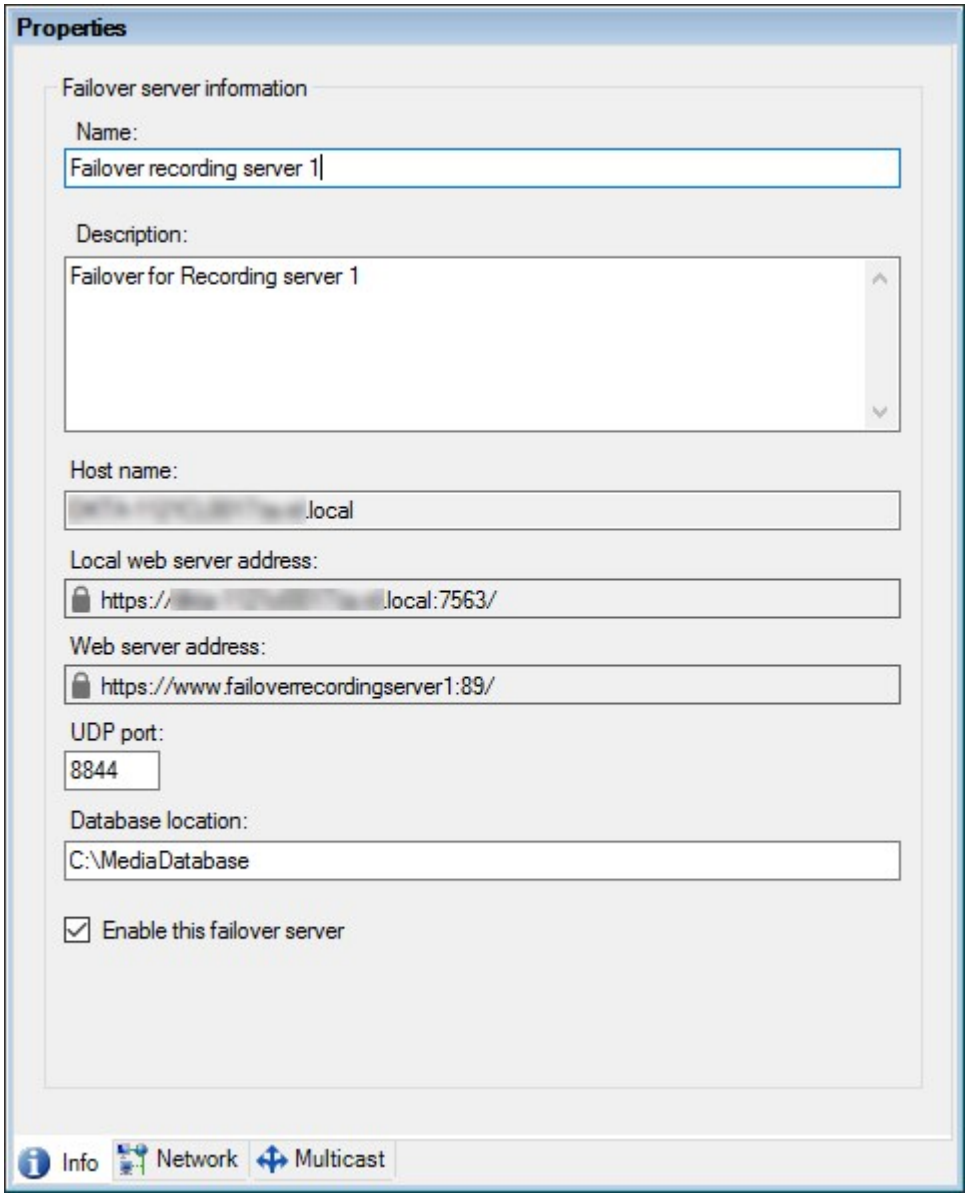
1. Выберите **Серверы** > **Серверы отказоустойчивости**. Откроется список установленных серверов записи обработки отказа и групп отказоустойчивых серверов.
2. На панели **Обзор** правой кнопкой мыши нажмите верхний узел **Резервные группы** и нажмите **Добавить группу**.
3. Укажите имя (в данном примере *Группа отказоустойчивых серверов 1*) и описание новой группы (необязательно). Нажмите кнопку **OK**.
4. Правой кнопкой мыши нажмите только что созданную группу (*Группа отказоустойчивых серверов 1*). Выберите **Изменить состав группы**. Откроется окно **Выбор состава группы**.
5. Перетащите выбранные серверы записи обработки отказа с левой части на правую или используйте соответствующие кнопки перемещения. Нажмите кнопку **OK**. Выбранные серверы записи обработки отказа теперь входят в созданную вами группу (*Группа отказоустойчивых серверов 1*).
6. Откройте вкладку **Последовательность**. Используйте кнопки **Вверх** и **Вниз**, чтобы установить внутреннюю последовательность серверов записи обработки отказа в группе.

Просмотр статуса шифрования сервера записи обработки отказа

Чтобы узнать, использует ли ваш сервер записи обработки отказа шифрование, выполните следующие действия:

1. На панели **Навигация по сайту** выберите **Серверы** > **Серверы отказоустойчивости**. Откроется список серверов записи обработки отказа.
2. На панели **Обзор** выберите требуемый сервер записи и перейдите на вкладку **Сведения**. Если включено шифрование подключений к клиентам и серверам, которые получают потоки данных от сервера записи, перед локальным адресом веб-сервера и дополнительным адресом

веб-сервера отображается значок замка.



Просмотр сообщений о состоянии

1. На сервере записи обработки отказа правой кнопкой мыши нажмите значок **Milestone Failover Recording Serverслужбы**.
2. Выберите **Просмотр сообщений о статусе**. Откроется окно **Сообщения о состоянии сервера отказоустойчивости**, в котором будут перечислены сообщения о состоянии с метками времени.

Просмотр информации о версии

Информация о точной версии **Failover Recording Serverслужбы** пригодится, если вам потребуется обратиться в службу поддержки.

1. На сервере записи обработки отказа правой кнопкой мыши нажмите значок **Milestone Failover Recording Serverслужбы**.
2. Выберите **О службе**.
3. Откроется небольшое диалоговое окно, где будет указана точная версия данной **Failover Recording Serverслужбы**.

Оборудование

Добавление оборудования

В системе предусмотрено несколько способов добавления оборудования на серверы записи.

> Если оборудование находится за маршрутизатором с поддержкой NAT или брандмауэром, может потребоваться указать другой номер порта и настроить на маршрутизаторе/брандамауэре сопоставление порта и IP-адреса, используемого оборудованием.

Мастер **добавления оборудования** обнаруживает оборудование, такое как камеры и видеокодеры, в сети и добавляет его на серверы записи в системе. Этот мастер также помогает добавлять серверы дистанционной записи для конфигураций Milestone Interconnect. Добавлять оборудование можно только на **один сервер записи** за раз.

1. Для доступа к разделу **Добавление оборудования** нажмите требуемый сервер записи правой кнопкой мыши и выберите **Добавить оборудование**.
2. Выберите один из вариантов мастера (см. ниже) и следуйте отображаемым на экране инструкциям.
3. После установки оборудование и связанные с ним устройства станут видны на панели **Обзор**.

> При первом добавлении отдельных типов оборудования потребуется выполнить предварительную настройку. Так, при добавлении такого оборудования отображается дополнительный мастер **Предварительная настройка аппаратных устройств**. Дополнительные сведения приведены в разделе Предварительная настройка оборудования (объяснение) на стр. 60.

Добавление оборудования (диалоговое окно)

Оборудование — это:

- Физический модуль, напрямую подключенный к серверу записи системы наблюдения по протоколу IP (например, камера, видеокодер, модуль ввода/вывода)
- Сервер записи на удаленном объекте в схеме Milestone Interconnect

Дополнительные сведения о добавлении оборудования в систему см. в разделе Добавление оборудования на стр. 232.

Имя	Описание
Экспресс (рекомендуется)	Система автоматически сканирует локальную сеть сервера записи в поисках нового оборудования. Поставьте отметку в поле **Отобразить оборудование, запущенное на других серверах записи**, чтобы увидеть, запущено ли найденное оборудование на других серверах записи. Этот параметр можно использовать при каждом добавлении к сети нового оборудования, которое требуется использовать в системе. Этот вариант невозможно использовать для добавления удаленных систем в схемах Milestone Interconnect. Для добавления оборудования, поддерживающего как HTTP, так и HTTPS, выполните обнаружение оборудования типа **Экспресс** с включенным переключателем **HTTPS (защищенный)**, а затем — с включенным переключателем **HTTP (незащищенный)**.
Сканирование диапазона адресов	Система сканирует сеть в поисках соответствующего оборудования и удаленных систем Milestone Interconnect • имена и пароли пользователей оборудования. Не требуется, если оборудование использует имена и пароли пользователей из заводских настроек • драйверы • Диапазоны IP-адресов (только для IPv4) • номер порта (значение по умолчанию = 80) Этот вариант подходит для случаев, когда требуется сканировать только часть сети (например, при расширении системы).

Имя	Описание
Ручной	Укажите сведения о каждой единице оборудования и удаленных систем Milestone Interconnect по отдельности. Данный способ подходит для случаев, когда вы добавляете лишь несколько единиц оборудования и знаете их IP-адреса и имена и пароли соответствующих пользователей, или если камера не поддерживает функцию автоматического обнаружения.
Оборудование с удаленным подключением	Система выполняет сканирование в поисках оборудования, подключенного через удаленно подключенный сервер. Этот вариант можно использовать, если вы установили серверы, например, для мгновенного подключения камер Axis One-click. Этот вариант невозможно использовать для добавления удаленных систем в схемах Milestone Interconnect.

Включение/отключение оборудования

По умолчанию добавляемое оборудование **включено**.

Определить, включено или отключено оборудование, можно следующим образом:

 Включено
 Отключено

Для отключения добавленного оборудования (например, по причинам, связанным с лицензиями или производительностью):

1. Откройте раздел сервера записи и нажмите оборудование, которое вы хотите отключить, правой кнопкой мыши.
2. Выберите **Включено** для выделения или снятия выделения.

Изменение оборудования

Нажмите добавленное оборудование правой кнопкой мыши и выберите **Изменить оборудование**, чтобы изменить настройки сети и аутентификации пользователей для оборудования в Management Client.

Изменить оборудование (диалоговое окно)

Применительно к определенному оборудованию, диалоговое окно **Изменить оборудование** можно использовать для применения настроек непосредственно к аппаратному устройству.

Если поставлена отметка в поле **Изменить настройки Management Client**, в диалоговом окне **Изменить оборудование** отображаются настройки, используемые Management Client для подключения к оборудованию. Для правильного добавления аппаратного устройства в систему задайте те же настройки, которые были использованы для подключения к предусмотренному производителем интерфейсу настройки оборудования:

Имя	Описание
Имя	Отображает имя оборудования вместе с определенным для него IP-адресом (в скобках).
URL оборудования	Веб-адрес предусмотренного производителем интерфейса настройки оборудования, как правило, содержащий IP-адрес этого оборудования. Укажите допустимый адрес в вашей сети.
Имя пользователя	Имя пользователя, используемое для подключения к оборудованию. Указанное здесь имя пользователя не меняет имя пользователя на самом аппаратном устройстве. Поставьте отметку в поле **Изменить Management Client и настройки оборудования**, чтобы изменить настройки на поддерживаемых аппаратных устройствах.
Пароль	Пароль, используемый для подключения к оборудованию. Указанный здесь пароль не меняет пароль на самом аппаратном устройстве. Поставьте отметку в поле **Изменить Management Client и настройки оборудования**, чтобы изменить настройки на поддерживаемых аппаратных устройствах.

Имя	Описание
	Сведения о том, как изменить пароли на нескольких аппаратных устройствах, см. в разделе Изменение пароля на аппаратных устройствах на стр. 241. Как системный администратор, вы должны предоставить другим пользователям разрешение на просмотр пароля в Management Client. Дополнительные сведения см. в пункте Настройки роли раздела «Оборудование».

Если поставлена отметка в поле **Изменить Management Client и настройки оборудования** (для поддерживаемого оборудования), в диалоговом окне **Изменить оборудование** отображаются настройки, которые напрямую применяются к аппаратному устройству:

Применение настроек с помощью этой кнопки-переключателя приводит к перезаписи настроек на аппаратном устройстве. При применении настроек подключение оборудования к серверу записи будет ненадолго разорвано.

Имя	Описание
Имя	Отображает имя оборудования вместе с определенным для него IP-адресом (в скобках).
Конфигурация сети	Сетевые настройки оборудования. Для изменения сетевых настроек нажмите Настройка на стр. 236.
Настройка	Выберите интернет-протокол (для поддерживаемых аппаратных устройств) в раскрывающемся списке **Версия интернет-протокола**. • Для IPv4 значения должны быть указаны в следующем формате: **(0-999).(0-999).(0-999).(0-999)** • Для IPv6 значения должны быть указаны в виде восьми групп шестнадцатеричных цифр, отделенных друг от друга двоеточием. Маска подсети должна представлять собой число в диапазоне **0-128**.

Имя	Описание
	С помощью кнопки **Проверить** можно определить, имеется ли в настоящее время в системе другое устройство, использующее введенный IP-адрес. При этом с помощью кнопки **Проверить** не удастся выявить конфликты с аппаратными устройствами, которые выключены, находятся за пределами системы VMS XProtect или временно не отвечают.
Имя пользователя	Имя и уровень пользователя, используемые для подключения к оборудованию. Выберите другого пользователя в раскрывающемся списке и добавьте новый пароль с помощью описанного ниже поля **Пароль**. Добавляйте или удаляйте пользователей с помощью подчеркнутых действий, расположенных в нижней части раздела **Аутентификация** (см. раздел Добавить пользователя на стр. 238 или Удалить пользователей на стр. 238). Выбор пользователя, который не находится на максимальном уровне пользователя, предусмотренном производителем, может привести к тому, что некоторые функции будут недоступны.
Пароль	Пароль, используемый для подключения к оборудованию. Для просмотра вводимого текста можно воспользоваться кнопкой **Показать**. При изменении пароля обратитесь к документации производителя, чтобы получить сведения о правилах использования пароля для конкретного аппаратного устройства, или воспользуйтесь кнопкой **Сгенерировать пароль**, чтобы автоматически сгенерировать пароль, отвечающий требованиям. Сведения о том, как изменить пароли на нескольких аппаратных устройствах, см. в разделе Изменение пароля на аппаратных устройствах на стр. 241. Как системный администратор, вы должны предоставить другим пользователям

Имя	Описание
	разрешение на просмотр пароля в Management Client. Дополнительные сведения см. в пункте Настройки роли раздела «Оборудование».
Добавить пользователя	Нажмите подчеркнутую ссылку **Добавить**, чтобы открыть диалоговое окно **Добавить пользователя** и добавить пользователя к аппаратному устройству. При добавлении пользователя он автоматически становится активным пользователем, причем введенные ранее учетные данные перезаписываются. При создании пароля обратитесь к документации производителя, чтобы получить сведения о правилах использования пароля для конкретного аппаратного устройства, или воспользуйтесь кнопкой **Сгенерировать пароль**  , чтобы автоматически сгенерировать пароль, отвечающий требованиям. Будет автоматически выбран максимальный уровень пользователя, заданный на аппаратном устройстве. Менять **Уровень пользователя**, заданный по умолчанию, не рекомендуется. Выбор **Уровня пользователя**, который отличается от максимального уровня, предусмотренного производителем, может привести к тому, что некоторые функции будут недоступны.
Удалить пользователей	Нажмите подчеркнутую ссылку **Удалить**, чтобы открыть диалоговое окно **Удалить пользователей** и удалить пользователей из аппаратного устройства. Удалить пользователя, который в настоящее время является активным, невозможно. Чтобы задать нового пользователя, воспользуйтесь описанным выше диалоговым окном **Добавить пользователя**, а затем удалите старого пользователя.

Включение/отключение отдельных устройств

По умолчанию **камеры включены**.

По умолчанию **микрофоны, динамики, метаданные, вводы** и **выводы отключены**.

Это означает, что для использования в системе микрофоны, динамики, метаданные, вводы и выводы необходимо включить отдельно. Такая особенность обусловлена тем, что системы наблюдения основаны на камерах, а использование микрофонов и т. п. в значительной степени зависит от потребностей каждой организации.

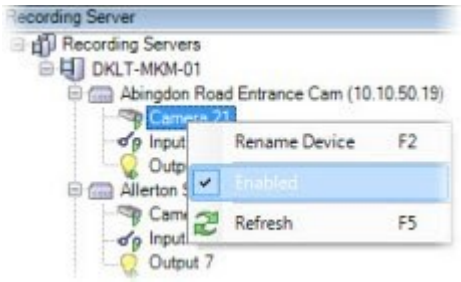
Определить, включены или отключены устройства, можно следующим образом (на примерах показан вывод):

 Отключено

 Включено

Этот способ включения/отключения используется для камер, микрофонов, динамиков, метаданных, вводов и выводов.

1. Откройте раздел сервера записи и устройства. Нажмите устройство, которое требуется включить, правой кнопкой мыши.
2. Выберите **Включено** для выделения или снятия выделения.



Настройка защищенного подключения к оборудованию

Настроить защищенное HHTPS-подключение между оборудованием и сервером записи можно при помощи протокола SSL (протокола защищенных соединений).

Перед выполнением описанных ниже действий обратитесь к поставщику своих камер, чтобы получить сертификат для оборудования, и загрузите его в оборудование:

1. На панели **Обзор** нажмите сервер записи правой кнопкой мыши и выберите нужное оборудование.

2. На вкладке **Настройки** включите HTTPS. По умолчанию этот параметр отключен.

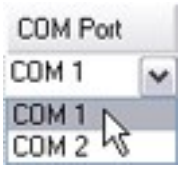
3. Введите порт сервера записи, используемый для HTTPS-подключения. Номер порта должен соответствовать порту, заданному на главной странице устройства.
4. Внесите необходимые изменения и сохраните их.

Включение функции PTZ на видеокодере

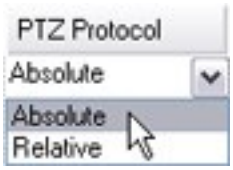
Для включения возможности использования PTZ-камер (поворотных камер с трансфокатором) на видеокодере выполните следующие действия на вкладке **PTZ**:

1. В списке устройств, подключенных к видеокодеру, поставьте отметку в поле **PTZ** для соответствующих камер:

2. В столбце **Идентификатор PTZ-устройства** проверьте правильность идентификатора каждой камеры.
3. В столбце **COM-порт** выберите COM-порты (порты последовательной передачи данных) видеокодера, которые будут применяться для управления функцией PTZ:



4. В столбце **PTZ-протокол** выберите схему позиционирования, которую вы хотите использовать:



   - **Абсолютная**: При использовании элементов управления PTZ-камерой операторами она перемещается относительно фиксированного положения (часто называемого исходным положением камеры)
   - **Относительная**: При использовании элементов управления PTZ-камерой операторами она перемещается относительно своего текущего положения

   Содержание столбца **PTZ-протокол** в значительной степени зависит от оборудования. Для некоторого оборудования предусмотрены от 5 до 8 протоколов. Также см. документацию по камере.

5. На панели инструментов нажмите кнопку **Сохранить**.

6. Теперь можно задать исходные предустановки и настройки патрулирования каждой PTZ-камеры:
   - Добавить исходную предустановку (тип 1)
   - Добавление профиля патрулирования

Изменение пароля на аппаратных устройствах

> Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Пароли на нескольких аппаратных устройствах можно изменить в рамках одной операции.

В общем случае, поддерживаемые устройства включают модели производства Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision, а также аппаратные устройства, совместимые с ONVIF, однако в пользовательском интерфейсе точно показано, поддерживается ли модель. Также узнать, поддерживается ли модель, можно на нашем веб-сайте: https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Применительнокустройствам,которыенеподдерживаютуправлениепаролямина устройстве,необходимоизменитьпарольаппаратногоустройстванаегове б-странице,азатемвручнуювестиновыйпарольвManagementClient.Дополнительные сведенияприведеныврazделеИзменениеоборудованиянастр.234.

Можно выбрать один из следующих вариантов:

- Предоставить системе возможность генерирования отдельных паролей для каждого аппаратного устройства. Система создает пароли, исходя из требований производителя аппаратных устройств.

- Использовать один пользовательский пароль для всех аппаратных устройств. При применении новых паролей связь аппаратных устройств с сервером записи ненадолго прерывается. После применения новых паролей на экране отображается результат по каждому аппаратному устройству. Если при выполнении операции произошел сбой, отображается причина сбоя (если аппаратное устройство поддерживает такую информацию). Из мастера можно создать отчет об успешных и безуспешных изменениях пароля. Кроме того, результаты фиксируются в **Журналах сервера**.

  > Применительно к аппаратным устройствам с драйверами ONVIF и несколькими учетными записями пользователей, изменять пароли из ПО для управления видео может только администратор XProtect с соответствующими разрешениями для соответствующего аппаратного устройства.

Требования:

- Аппаратное устройство должно поддерживать управление паролями устройства, которое осуществляет Milestone.

Действия:

1. На панели **Навигация по сайту** выберите раздел **Серверы записи**.
2. На панели «Обзор» нажмите соответствующий сервер записи или оборудование правой кнопкой мыши.
3. Выберите пункт **Изменить пароль аппаратного устройства**. Откроется мастер.
4. Введите пароль с использованием строчных и прописных букв, цифр и следующих символов: **! ( ) * - . _**

   Максимальная длина пароля — 64 символа.

   > Максимальная длина пароля для камеры Bosch FLEXIDOME IP outdoor 5000 MP NDN-50051 —19 символов.

5. Для завершения изменений следуйте инструкциям на экране.

   > В поле **Последнее изменение пароля** отображается метка времени последней смены пароля в соответствии с локальными параметрами времени компьютера, с которого выполнялась смена пароля.

6. На последней странице отображается результат. Если система не смогла обновить пароль, нажмите **Сбой** рядом с именем аппаратного устройства, чтобы выяснить причину.

7. Также можно нажать кнопку **Распечатать отчет**, чтобы ознакомиться с полным списком успешных и безуспешных изменений.
8. Если вы хотите изменить пароль на аппаратных устройствах, на которых произошел сбой, нажмите кнопку **Повторить попытку**, и мастер начнет процесс для этих устройств заново.

> Если вы нажмете кнопку **Повторить попытку**, вы не сможете вернуться к отчету, созданному при первом запуске мастера.

> Вследствие ограничений, обусловленных требованиями безопасности, некоторые аппаратные устройства могут стать недоступны на определенный период времени при нескольких последовательных безуспешных попытках изменить пароль. Ограничения, обусловленные требованиями безопасности, варьируются в зависимости от конкретного производителя.

Обновление прошивки на аппаратных устройствах

> Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Management Client позволяет обновить прошивку оборудования, добавленного в ПО для управления видео. Вы можете обновить прошивку для нескольких аппаратных устройств одновременно, если они совместимы с одним файлом прошивки.

В пользовательском интерфейсе показано, поддерживает ли модель обновление прошивки. Также узнать, поддерживается ли модель, можно на веб-сайте: Milestone https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Если аппаратные устройства не поддерживают обновление прошивки, ее необходимо обновить с веб-страницы устройства.

При обновлении прошивки связь аппаратных устройств с сервером записи ненадолго прерывается.

После обновления прошивки на экране отображается результат по каждому аппаратному устройству. Если при выполнении операции произошел сбой, отображается причина сбоя (если аппаратное устройство поддерживает такую информацию). Кроме того, результаты фиксируются в **Журналах сервера**.

Применительно к аппаратным устройствам с драйверами ONVIF и несколькими учетными записями пользователей, обновлять прошивку из ПО для управления видео может только администратор XProtect с административными разрешениями для соответствующего аппаратного устройства.

Требования:

- Модель аппаратного устройства поддерживает обновление прошивки, выполняемое Milestone.

Действия:

1. На панели **Навигация по сайту** выберите раздел **Серверы записи**.
2. На панели «Обзор» нажмите соответствующий сервер записи или оборудование правой кнопкой мыши.
3. Выберите пункт **Обновить прошивку оборудования**. Откроется мастер.
4. Для завершения изменений следуйте инструкциям на экране.

   Обновление нескольких аппаратных устройств возможно, только если они совместимы с одним и тем же файлом прошивки. Оборудование, добавленное при помощи драйвера ONVIF, находится не в разделе своего производителя, а в разделе **Прочее**.

6. На последней странице отображается результат. Если система не смогла обновить прошивку, нажмите **Сбой** рядом с именем аппаратного устройства, чтобы выяснить причину.

Milestone не несет ответственность за неисправность аппаратного устройства при выборе несовместимого файла прошивки или несовместимого аппаратного устройства.

Добавление и настройка внешнего IDP

1. В Management Client выберите пункт **Инструменты** > **Параметры**, а затем перейдите на вкладку **Внешний IDP**.
2. В разделе **Внешний IDP** выберите **Добавить**. Обратите внимание, что можно добавить только однин внешний IDP.
3. Введите информацию для внешнего IDP. Дополнительные сведения о требуемой информации см. в разделе Внешний IDP.

Сведения о регистрации заявок из внешнего IDP, которые вы хотите использовать в ПО для управления видео, см. в разделе Регистрация заявок из внешнего IDP.

Устройства — группы

Добавление группы устройств

1. На панели **Обзор** нажмите тип устройств, для которого требуется создать группу устройств, правой кнопкой мыши.
2. Выберите пункт **Добавить группу устройств**.
3. В диалоговом окне **Добавить группу устройств** укажите имя и описание новой группы устройств:

   Описание появляется, когда вы задерживаете курсор мыши над группой устройств в списке групп устройств.

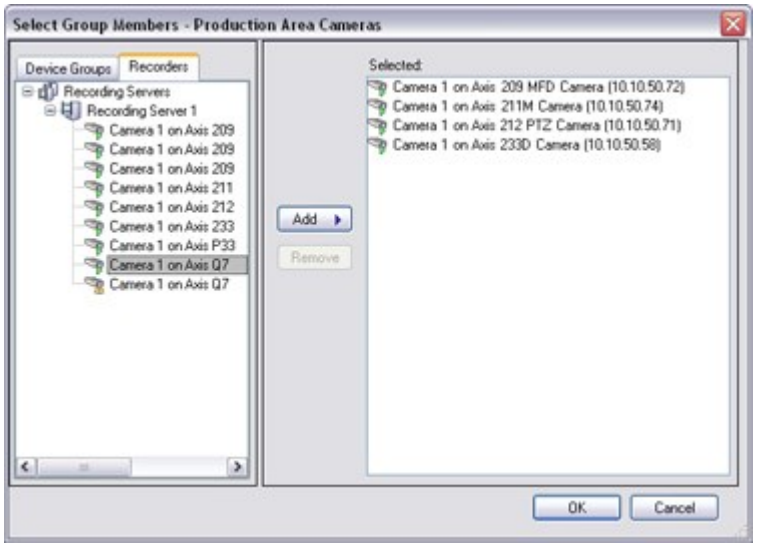
4. Нажмите кнопку **OK**. В списке появится папка, которой соответствует новая группа устройств.
5. Продолжите указывать устройства, которые необходимо включить в группу устройств (см. раздел Указание устройств, которые необходимо включить в группу устройств на стр. 245).

Указание устройств, которые необходимо включить в группу устройств

1. На панели **Обзор** нажмите папку соответствующей группы устройств правой кнопкой мыши.
2. Выберите пункт **Изменить состав группы устройств**.
3. В окне **Выбрать состав группы** перейдите на одну из вкладок, чтобы найти устройство.

   Устройство может входить в состав нескольких групп устройств.

4. Выберите устройства, которые требуется включить в состав группы, и нажмите кнопку **Добавить** либо дважды нажмите устройство:



5. Нажмите кнопку **OK**.

6. Если вы превысили лимит в 400 устройств на группу, можно добавить группы устройств в качестве подгрупп других групп устройств:

Отключенные устройства

Отключенные устройства по умолчанию не отображаются на панели **Обзор**.

Чтобы вывести на экран все отключенные устройства, вверху панели **Обзор** нажмите **Фильтр**, чтобы открыть вкладку **Фильтр**, и выберите **Показать отключенные устройства**.

Чтобы снова скрыть отключенные устройства, снимите флажок **Показать отключенные устройства**.

Указание общих свойств для всех устройств в группе

При помощи групп устройств можно задавать общие свойства для всех устройств из состава конкретной группы:

1. На панели **Обзор** нажмите группу устройств.

   На вкладках панели **Свойства** перечислены и сгруппированы **все свойства, которые доступны во всех устройствах из состава группы**.

2. Задайте необходимые общие свойства.

   На вкладке **Настройки** можно переключаться между настройками **всех** устройств и настройками отдельных устройств.

3. На панели инструментов нажмите кнопку **Сохранить**. Настройки будут сохранены на отдельных устройствах, а не в группе устройств.

Отключенные устройства

Отключенные устройства по умолчанию не отображаются на панели **Обзор**.

Чтобы вывести на экран все отключенные устройства, вверху панели **Обзор** нажмите **Фильтр**, чтобы открыть вкладку **Фильтр**, и выберите **Показать отключенные устройства**.

Чтобы снова скрыть отключенные устройства, снимите флажок **Показать отключенные устройства**.

Включение/отключение устройств с помощью групп устройств

Включать/отключать устройства можно только с помощью настроенного оборудования. За исключением случаев, когда камеры включены/отключены вручную в мастере добавления оборудования, по умолчанию камеры включены, а все другие устройства отключены.

Отключенные устройства по умолчанию не отображаются на панели **Обзор**.

Чтобы вывести на экран все отключенные устройства, вверху панели **Обзор** нажмите **Фильтр**, чтобы открыть вкладку **Фильтр**, и выберите **Показать отключенные устройства**.

Чтобы снова скрыть отключенные устройства, снимите флажок **Показать отключенные устройства**.

Чтобы найти включаемое или отключаемое устройств в группах устройств:

1. Выберите устройство на панели **Навигация по сайту**.
2. На панели **Обзор** откройте соответствующую группу и найдите устройство.
3. Нажмите устройство правой кнопкой мши и выберите пункт **Перейти к оборудованию**.
4. Нажмите значок «плюс», чтобы просмотреть все устройства на оборудовании.
5. Нажмите включаемое/отключаемое устройство правой кнопкой мыши и выберите пункт **Включено**.

Устройства — параметры камеры

Просмотр или изменение настроек камеры

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. Откройте вкладку **Настройки**.

Вы можете просматривать или изменять следующие настройки:

- Частота кадров по умолчанию
- Разрешение
- Сжатие
- Максимальное количество кадров между ключевыми кадрами
- Отображение даты/времени/текста на экране для выбранной камеры или для всех камер из группы

Содержимое вкладки **Настройки** определяется драйверами камер. Драйвера зависят от типа камеры.

Для камер, которые поддерживают несколько типов потоков (например, MJPEG и MPEG-4/H.264/H.265), можно использовать многопоточную передачу; см. раздел Управление многопоточной передачей на стр. 255.

Предв. просмотр

При изменении настройки можно быстро проверить последствия изменения, если включена панель **Предварительный просмотр**.

- Чтобы включить **Предварительный просмотр**, выберите меню **Просмотр**, а затем —пункт **Окно предварительного просмотра**.

Для контроля последствий изменения частоты кадров панель **Предварительный просмотр** использовать невозможно, так как в уменьшенном изображении на панели **Предварительный просмотр** используется другая частота кадров, задаваемая в диалоговом окне **Параметры**.

Производительность

Если изменить настройки **Максимальное количество кадров между ключевыми кадрами** и **Режим максимального количества кадров между ключевыми кадрами**, это может привести к снижению производительности некоторых функций в XProtect Smart Client. Например, XProtect Smart Client требует наличия ключевого кадра для запуска показа видео, поэтому длительный период между ключевыми кадрами приводит к более длительному запускуXProtect Smart Client.

Добавление оборудования

Дополнительные сведения о добавлении оборудования в систему см. в разделе Добавление оборудования на стр. 232.

Включение и отключение поддержки объектива типа «рыбий глаз»

По умолчанию поддержка объектива типа «рыбий глаз» отключена.

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Объектив типа «рыбий глаз»** поставьте или снимите отметку в поле **Включить поддержку объектива типа «рыбий глаз»**.

Задайте параметры объектива типа «рыбий глаз»

1. На вкладке **Объектив типа «рыбий глаз»** укажите тип объектива.
2. Выберите физическое положение/ориентацию камеры из списка **Положение/ориентация камеры**.
3. Выберите номер зарегистрированного паноморфного объектива (RPL) из списка **Номер RPL системы ImmerVision Enables® panomorph**.

   Это обеспечивает идентификацию и правильную настройку объектива, используемого с камерой. Как правило, номер RPL находится на самом объективе или на его упаковочной коробке. Сведения об объективах ImmerVision panomorph и объективах RPL см. на веб-сайте компании ImmerVision (https://www.immervisionenables.com/).

   При выборе профиля объектива **Общее устранение искажений** обязательно задайте требуемое **Поле обзора**.

Устройства — запись

Включение/отключение записи

По умолчанию запись включена. Для включения/отключения записи:

1. На панели **Навигация по сайту** выберите **Серверы записи**.
2. Выберите соответствующее устройство на панели **Обзор**.
3. На вкладке **Запись** поставьте или снимите отметку в поле **Запись**.

> Для записи данных с камеры необходимо включить запись для устройства. При отключении записи для устройства правило, которое задает условия начала записи, перестает действовать.

Включение записи на связанных устройствах

Применительно к камерам можно включить запись на связанных устройствах, например микрофонах, подключенных к тому же серверу записи. Это означает, что связанное устройство ведет запись, когда камера ведет запись.

По умолчанию запись на связанных устройствах для новых камер включена, но при необходимости ее можно отключить. По умолчанию для уже занесенных в систему камер отметка снята.

1. На панели **Навигация по сайту** выберите **Серверы записи**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Запись** поставьте или снимите отметку в поле **Запись на связанных устройствах**.
4. На вкладке **Клиент** укажите устройства, которые связаны с этой камерой.

Если вы хотите включить запись на связанных устройствах, подключенных к другому серверу записи, необходимо создать правило.

Ручное управление записью

Параметр **Остановить запись вручную через** включен по умолчанию, а время записи составляет пять минут. Это сделано для того, чтобы система автоматически останавливала все сеансы записи, запущенные пользователями XProtect Smart Client.

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор**.
3. На вкладке **Запись** поставьте или снимите отметку в поле **Остановить запись вручную через**.

Если вы включили этот параметр, задайте время записи. Заданное количество минут должно быть достаточным для того, чтобы соответствовать требованиям различных сценариев записи вручную без чрезмерной нагрузки на систему.

Добавлять к ролям:

В пункте **Роли** на вкладке **Устройство** необходимо предоставить пользователям клиента разрешение на ручные запуск и остановку записи на каждой камере.

Использовать в ролях:

События, которые можно использовать при создании правил для ручного управления записью:

- Ручная запись начата
- Ручная запись остановлена

Указание частоты кадров при записи

Для формата JPEG можно задать частоту кадров при записи.

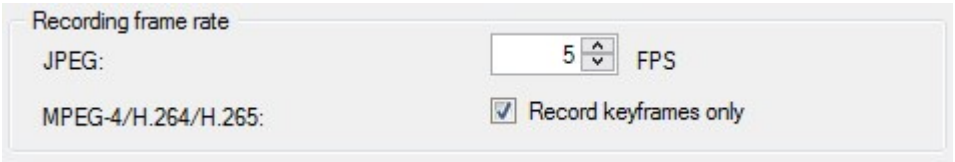
1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор**.
3. На вкладке **Запись**, в поле **Частота кадров при записи: (JPEG)**, выберите или введите частоту кадров при записи (количество кадров в секунду (FPS)).

Включение записи ключевых кадров

Для потоков в формате MPEG-4/H.264/H.265 можно включить запись ключевых кадров. Это означает, что, в зависимости от настроек правил, система переключается между записью только ключевых кадров и записью всех кадров.

Например, для экономии места в хранилище можно разрешить системе записывать ключевые кадры, когда в области обзора нет движений, а при обнаружении движений — переключаться на запись всех кадров.

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор**.
3. На вкладке **Запись** поставьте отметку в поле **Записывать только ключевые кадры**.



4. Настройте правило, активирующее данную функцию (см. раздел Действия и останавливающие действия).

Включение записи на связанных устройствах

Применительно к камерам можно включить запись на связанных устройствах, например микрофонах, подключенных к тому же серверу записи. Это означает, что связанное устройство ведет запись, когда камера ведет запись.

По умолчанию запись на связанных устройствах для новых камер включена, но при необходимости ее можно отключить. По умолчанию для уже занесенных в систему камер отметка снята.

1. На панели **Навигация по сайту** выберите **Серверы записи**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Запись** поставьте или снимите отметку в поле **Запись на связанных устройствах**.
4. На вкладке **Клиент** укажите устройства, которые связаны с этой камерой.

Если вы хотите включить запись на связанных устройствах, подключенных к другому серверу записи, необходимо создать правило.

Сохранение и получение дистанционной записи

Для сохранения всех удаленных записей в случае проблем с сетью можно включить автоматическое получение записей после восстановления подключения.

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор**.
3. В разделе **Дистанционные записи** выберите пункт **Автоматически получить дистанционные записи при восстановлении подключения**. Будет включено автоматическое получение записей после восстановления подключения.

> Параметр удаленного хранения доступен только в том случае, если выбранная камера поддерживает локальное хранение данных, или если камера функционирует в схеме Milestone Interconnect.

Место, из которого выполняется получение записей, определяется типом выбранного оборудования:

- Применительно к камере с локальным хранилищем записей, получение записей выполняется из локального хранилища записей камеры
- Применительно к удаленной системе Milestone Interconnect, получение записей выполняется из серверов записи удаленных систем

Следующие функции можно использовать независимо от автоматического получения записей:

- Ручная запись
- Правило **Получение и хранение дистанционных записей из <устройств>**
- Правило **Получение и хранение дистанционных записей между <временем начала и временем окончания> с<устройств>**

Удаление записей

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор** и перейдите на вкладку **Запись**.
3. Чтобы удалить все записи для устройства или группы устройств, нажмите кнопку **Удалить все записи**.

Этот способ можно использовать, только если все устройства в группе добавлены к одному и тому же серверу. Защищенные данные не удаляются.

Устройства — потоковая передача

Адаптивное потоковое воспроизведение (объяснение)

Адаптивное потоковое воспроизведение — это метод потоковой передачи, который используется при отображении нескольких видеопотоков в режиме реального времени в одном представлении. Эта функция позволяет автоматически выбирать транслируемые видеопотоки с оптимальным разрешением для элементов просмотра. Адаптивное потоковое воспроизведение снижает нагрузку на сеть, расширяет возможности декодирования и повышает производительность клиентского компьютера.

Максимально близкое соответствие доступных видеопотоков для разрешения, требуемого элементом представления, можно настроить при включении адаптивного воспроизведения в XProtect Smart Client. Дополнительные сведения приведены в разделе Включить адаптивное потоковое воспроизведение.

В XProtect Smart Client адаптивное потоковое воспроизведение можно применять в режиме реального времени и в режиме воспроизведения. В мобильных клиентах оно доступно только в режиме реального времени.

При применении в режиме воспроизведения метод потоковой передачи данных называется адаптивным воспроизведением. Дополнительные сведения приведены в разделе Адаптивное воспроизведение (объяснение) на стр. 253

Адаптивное воспроизведение (объяснение)

Адаптивное воспроизведение — это настройка, которая позволяет использовать адаптивную потоковую передачу данных в режиме воспроизведения.

Адаптивное воспроизведение требует наличия двух потоков записи — основного и вспомогательного. Если в Management Client включены оба потока, оба потока будут вести запись.

- Если вы воспроизводите видео за определенный период до того, как настроили вспомогательную запись, будет воспроизводиться только основная запись.
- Если вы воспроизводите видео, записанное после того, как настроили вспомогательную запись, видео будет воспроизводиться из основной либо вспомогательной записи, в зависимости от того, какой из вариантов лучше соответствует размеру представления клиента.

Доступность

> Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Включить адаптивное потоковое воспроизведение

Включить адаптивное воспроизведение вместе с адаптивным потоковым воспроизведением можно на вкладке **Дополнительно** в разделе **Smart ClientПрофили**, причем оно должно быть включено и в XProtect Smart Client в разделе **Настройки** > **Дополнительно** > **Адаптивное потоковое воспроизведение**. Дополнительные сведения о включении адаптивного потокового воспроизведения в XProtect Smart Client см. в Включить адаптивное потоковое воспроизведение.

Записи на периметре

При необходимости записи на периметре можно использовать для адаптивного воспроизведения. С помощью записей на периметре можно просматривать эпизоды потока с другим, как правило, более высоким разрешением, чем в остальной части потока. Например, основной поток можно записывать с низким разрешением и объединять его с записями, полученными из источника с высоким разрешением. При обзоре данных можно включить объединенные записи на периметре.

Записи на периметре хранятся в базе медиаданных, а разрешение этих записей задается на отдельных камерах.

Разрешение воспроизводимого видео

При использовании адаптивного воспроизведения разрешение воспроизводимого видео определяется текущим разрешением основной и вспомогательной записей. Так, выбор основного или вспомогательного потока при воспроизведении зависит от разрешения, заданного для соответствующих потоков записи.

Добавление потока

Потоки, добавленные для записи, можно просматривать в режиме прямой передачи и в режиме воспроизведения.

Также записанное видео можно просматривать в вашем элементе представления, если включено адаптивное потоковое воспроизведение. Адаптивное потоковое воспроизведение в режиме воспроизведения называется адаптивным воспроизведением.

1. На вкладке **Потоки** нажмите **Добавить**. В список будет добавлен второй поток.
2. В столбце **Имя** измените имя потока. Имя отобразится в XProtect Smart Client.
3. В столбце **Режим трансляции** укажите, когда требуется потоковая трансляция:
    - **Всегда**: поток передается, даже если пользователи XProtect Smart Client не запрашивают его
    - **Никогда**: поток отключен. Используйте этот вариант только для потоков записи: например, если вы хотите получить запись высокого качества и сэкономить пропускную способность
    - **При необходимости**: поток запускается по запросу клиента или если предусмотрена запись потока

4. В столбце **Поток трансляции по умолчанию** выберите, какой из потоков должен использоваться по умолчанию, если клиент не запрашивает конкретный поток, а адаптивное потоковое воспроизведение отключено.
5. В столбце **Поток записи** выберите **Основной** или **Вспомогательный**. Для адаптивного воспроизведения необходимо создать поток каждого типа. Источником воспроизводимого видео является основной видеопоток, а вспомогательное потоковое воспроизведение активируется при необходимости. Всегда необходимо иметь основной поток записи. Кроме того, поток, заданный в качестве **Основного**, используется в различных контекстах, например для обнаружения движений и для экспорта из XProtect Smart Client.
6. В разделе **Поток воспроизведения по умолчанию** выберите, какой из потоков используется по умолчанию. Поток по умолчанию будет передаваться клиенту, если не настроено адаптивное воспроизведение.
7. В столбце **Использовать локальные записи** поставьте отметку в поле, если вы хотите использовать локальные записи. Дополнительные сведения о локальных записях см. в разделе Записи на периметре на стр. 254.
8. Нажмите **Сохранить**.

Если вы не хотите, чтобы потоки запускались до тех пор, пока один из пользователей не начнет просмотр видео в режиме трансляции, можно изменить **Правило начала передачи по умолчанию**, чтобы поток запускался по запросу после наступления заранее определенного события **Запрос клиента на передачу в режиме трансляции**.

Управление многопоточной передачей

Просмотр видео в режиме реального времени и воспроизведение записанного видео не требуют одинакового качества видео и частоты кадров.

Изменение потока, который используется для записи

При адаптивное воспроизведении запись должна выполняться в два потока: основной и вспомогательный. Для прямой потоковой передачи можно настроить и использовать столько потоков трансляции, сколько поддерживает камера.

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Потоки** выберите поток, который необходимо использовать для записи.

4. Выберите соответствующий параметр в списке **Режим трансляции**. Параметры **При необходимости**, **Всегда** и **Никогда** указывают, когда поток должен применяться к клиенту. Если от клиента ничего не требуется, для записи будет использоваться поток, в поле **Поток трансляции по умолчанию** которого поставлена отметка.
5. Для записи одного потока выберите пункт **Основной** или **Вспомогательный** в списке **Запись**.
6. Для использования адаптивного воспроизведения настройте два потока и задайте один из них в качестве **Основного**, а другой — в качестве **Вспомогательного**.
7. Для записи потока выберите пункт **Основной** или **Вспомогательный** в списке **Запись**.

Ограничение передачи данных

Можно настроить комплекс условий, при котором видеопотоки будут передаваться при их просмотре клиентом.

С целью управления потоковой передачей и ограничения излишнего объема передаваемых данных потоковая передача не начинается, когда выполнены следующие условия:

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. В списке **Режим трансляции** на вкладке **Потоки** выберите пункт **При необходимости**.
4. На вкладке **Запись** снимите отметку в поле **Запись**.
5. На вкладке **Движение** снимите отметку в поле **Обнаружение движений**.

Если эти условия выполнены, видеопотоки будут передаваться только при их просмотре клиентом.

Примеры

Пример 1. Видео в режиме трансляции и записанное видео:

- Для просмотра видео **в режиме реального времени** ваша организация может предпочесть формат H.264 с высокой частотой кадров
- Для воспроизведения **записанного** видео ваша организация может предпочесть формат MJPEG с пониженной частотой кадров (для экономии пространства на диске)

Пример 2. Локальное и удаленное видео в режиме реального времени:

- Для просмотра **видео в режиме реального времени с локально подключенной рабочей точки** ваша организация может предпочесть формат H.264 с высокой частотой кадров (для получения максимально возможного качества видеоизображения)
- Для просмотра **видео в режиме реального времени с удаленно подключенной рабочей точки** ваша организация может предпочесть формат MJPEG с пониженной частотой кадров и качеством (чтобы сохранить пропускную способность сети)

Пример 3. Адаптивное потоковое воспроизведение:

- Для просмотра **видео в режиме реального времени и снижения нагрузки на центральный и графический процессоры компьютера XProtect Smart Client** ваша организация может предпочесть несколько потоков в формате H.264/H.265, передаваемых с различными разрешениями, чтобы соответствовать разрешению, которое требуется XProtect Smart Client при использовании адаптивного потокового воспроизведения. Дополнительные сведения приведены в разделе Профили Smart Client (узел «Клиент») на стр. 512.

> Если включить параметр **Многоадресная прямая передача** на вкладке **Клиент** камеры (см. раздел Вкладка «Клиент» (устройства)), он будет работать только с видеопотоком по умолчанию.

Даже если камеры поддерживают многопоточную передачу, некоторые возможности многопоточной передачи в различных камерах могут отличаться. Дополнительные сведения см. в документации по камере.

Чтобы выяснить, поддерживает ли камера различные типы потоков, просмотрите раздел **Вкладка «Настройки» (устройства)**.

Устройства — хранение

Управление буферизацией перед событием

Камеры, микрофоны и динамики поддерживают буферизацию перед событием. Применительно к динамикам, потоки отправляются только при использовании функции **Разговор через динамик** пользователем XProtect Smart Client. Так, в зависимости от того, как настроен запуск записи потоков из динамиков, буферизация перед событием незначительна либо отсутствует.

В большинстве случаев запись через динамики можно настроить так, чтобы она начиналась при использовании функции **Разговор через динамик** пользователем XProtect Smart Client. В таких случаях предварительный буфер в динамике отсутствует.

> Для использования функции буферизации перед событием устройства должны быть включены и отправлять поток в систему.

Включение и отключение буферизации перед событием

По умолчанию буферизация перед событием включена, размер предварительного буфера составляет три секунды, а данные сохраняются в память.

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор**.
3. На вкладке **Запись** поставьте или снимите отметку в поле **Буферизация перед событием**.

4. На вкладке **Клиент** укажите устройства, которые связаны с этой камерой.

Указание места хранения и размера предварительного буфера

При буферизации перед событием временные записи хранятся в памяти или на диске:

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор** и перейдите на вкладку **Запись**.
3. В списке **Местонахождение** выберите пункт **Память** или **Диск** и укажите количество секунд.
4. Если задаваемый размер предварительного буфера превышает 15 секунд, выберите **Диск**.

Указываемое количество секунд должно быть достаточно большим, чтобы отвечать требованиям для различных правил записи.

Если изменить местонахождение на **Память**, система автоматически уменьшит размер буфера до 15 секунд.

Использование буферизации перед событием в правилах

При создании правил запуска записи можно указать, что запись должна начинаться за некоторое время до фактического события (буферизация перед событием).

Пример: В приведенном ниже правиле указано, что камера должна начинать запись за 5 секунд до обнаружения движений.

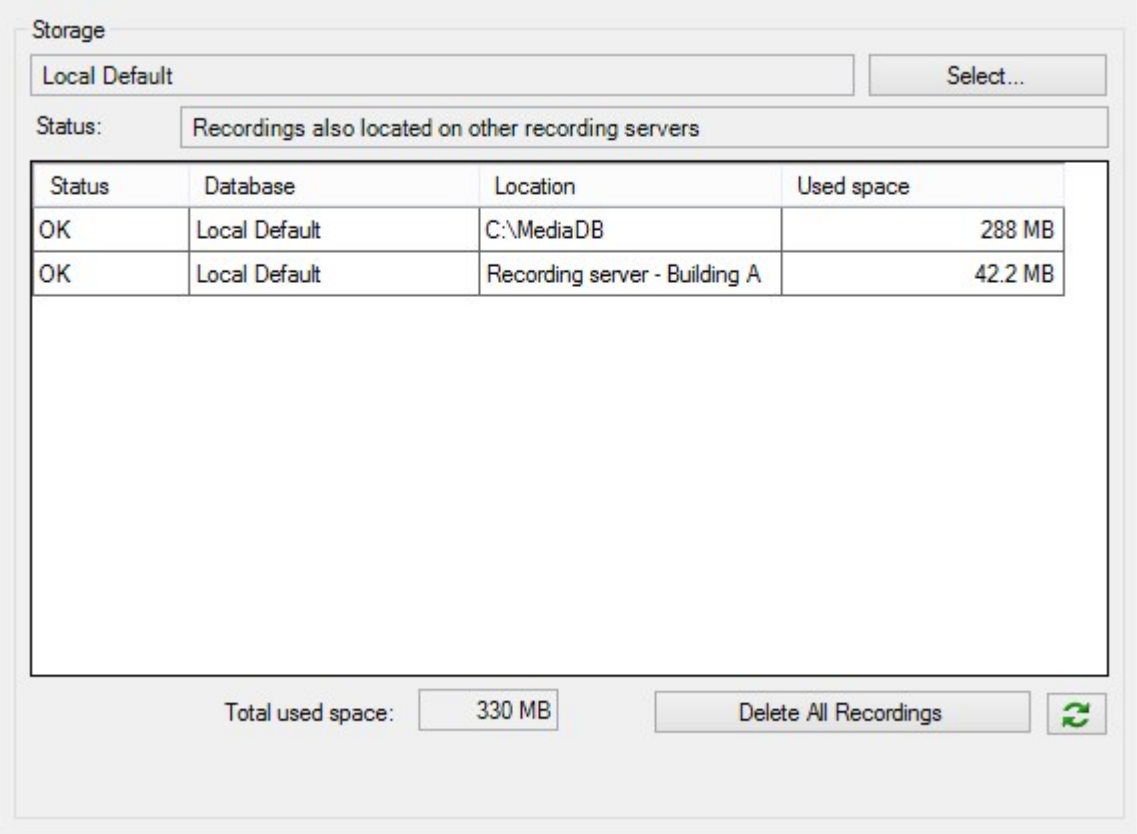
Для использования в правиле функции записи с буферизацией перед событием необходимо включить буферизацию перед событием на записывающем устройстве и указать такой размер предварительного буфера, который будет не меньше размера из правила.

Мониторинг состояния баз данных устройств

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор** и перейдите на вкладку **Запись**.

В разделе **Хранилище** можно осуществлять мониторинг и управление базами данных устройства или группы устройств, добавленных к одному и тому же серверу записи.

Над таблицей указаны сведения о выбранной базе данных и ее состоянии. В этом примере выбрана база данных **Локальная по умолчанию**, ее состояние — **Также записи существуют на других серверах записи**. Другой сервер — это сервер записи в здании A.



Возможные состояния выбранной базы данных

Имя	Описание
Также записи существуют на других серверах записи	База данных активна и работает, а ее записи расположены в хранилищах на других серверах записи.
Также архивы расположены в старом хранилище	База данных активна и работает, а ее архивы расположены в других хранилищах.
Активно	База данных активна и работает.
Данные для некоторых выбранных устройств перемещаются в другое местоположение	База данных активна и работает, а система переносит данные одного или нескольких выбранных устройств группы из одного местоположения в другое.

Имя	Описание
Данные этого устройства перемещаются в другое местоположение	База данных активна и работает, а система переносит данные выбранного устройства из одного местоположения в другое.
Информация недоступна в режиме обработки отказа	Система не может собирать сведения о состоянии базы данных, когда база данных находится в режиме обработки отказа.

Ниже в этом окне расположены сведения о состоянии каждой базы данных (**ОК**, **Автономный режим** или **Старое хранилище**), ее местонахождении и занимаемом пространстве.

Если все серверы подключены к сети, в поле **Общий объем используемого пространства** отображаются сведения об общем объеме пространства, используемого для всего хранилища.

Сведения о настройке хранилища см. в разделе Вкладка «Хранилище» (сервер записи).

Перенос устройств из одного хранилища в другое

> При выборе нового местонахождения для хранения записей существующие записи не переносятся. Они остаются в своем текущем местонахождении, и к ним применяются условия, заданные настройками связанного с ними хранилища.

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующее устройство на панели **Обзор** и перейдите на вкладку **Запись**.
3. Нажмите **Выбрать** в разделе **Хранилище**, чтобы выбрать хранилище записей, в котором будут храниться записи ваших устройств.

Архивирование записей будет выполняться в соответствии с настройками выбранного вами хранилища.

Устройства — обнаружение движений

Обнаружение движений (объяснение)

Настройка обнаружения движений — это один из ключевых элементов системы: Настройки обнаружения движений определяют, когда система создает события обнаружения движений, а также, как правило, когда ведется запись видео.

Подбор максимально эффективной конфигурации обнаружения движений для каждой камеры поможет избежать, например, сохранения ненужных записей. В зависимости от физического местонахождения камеры может быть полезно протестировать настройки обнаружения движений в различных физических условиях: например, днем и ночью, а также при ветре и в безветренную погоду.

Можно задать параметры объема изменений в поле обзора камеры, которые будут рассмотрены как движение. Например, можно задать интервалы при анализе обнаружения движений и области в поле обзора, движение в которых следует игнорировать. Также можно отрегулировать точность обнаружения движений и, тем самым, нагрузку на системные ресурсы.

Качество изображения

Перед настройкой обнаружения движений для камеры Milestone рекомендует настроить качество ее изображения, например, параметры разрешения, видеокодека и потока. Это можно сделать на вкладке **Настройки** в окне **Свойства** устройства. Если позднее вы измените параметры качества изображения, обязательно протестируйте настройки обнаружения движений.

Маски конфиденциальности

Если вы задали области с постоянными масками конфиденциальности, обнаружение движений в этих областях не осуществляется.

Включение и отключение обнаружения движений

Задайте для камер параметр обнаружения движений, используемый по умолчанию

1. В меню **Инструменты** нажмите **Параметры**.
2. На вкладке **Общая информация**, в разделе **Автоматически включать новые камеры при добавлении**, поставьте отметку в поле **Обнаружение движений**.

Включите или отключите обнаружение движений для конкретной камеры.

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Движение** поставьте или снимите отметку в поле **Обнаружение движений**.

При отключении обнаружения движений для камеры ее правила, основанные на обнаружении движений, перестают действовать.

Включение или отключение аппаратного ускорения

При добавлении камеры по умолчанию включено аппаратно-ускоренное декодирование видео при обнаружении движений. Сервер записи использует ресурсы графического процессора (если они доступны). Это позволяет уменьшить нагрузку на графический процессор во время анализа движений и повысить общую производительность сервера записи.

Включение или отключение аппаратного ускорения

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Движение** в разделе **Аппаратное ускорение** выберите пункт **Автоматически**, чтобы включить аппаратное ускорение, или **Выключено**, чтобы отключить этот параметр.

Использование ресурсов графического процессора

Аппаратно-ускоренное декодирование видео при анализе движений использует ресурсы графического процессора на следующих устройствах:

- Центральные процессоры Intel, которые поддерживают технологию Intel Quick Sync
- Графические адаптеры NVIDIA®, подключенные к серверу записи

Балансировка нагрузки и производительности

Балансировка нагрузки между различными серверами осуществляется автоматически. В разделе **Системный монитор** > **Пороговые значения системного монитора** можно проверить, находится ли текущий уровень загрузки ресурсов графического процессора NVIDIA, связанный с анализом движений, в заданных пределах. Применяются следующие показатели нагрузки на графический процессор NVIDIA:

- Декодирование NVIDIA
- Память NVIDIA
- Визуализация NVIDIA

> Если нагрузка слишком велика, можно добавить к серверу записи ресурсы графического процессора: для этого необходимо установить несколько графических адаптеров NVIDIA. Milestone не рекомендует пользоваться адаптерами NVIDIA в конфигурации SLI.

NVIDIA предлагает продукты с разными вычислительными возможностями.

Для аппаратного ускорения декодирования при обнаружении движений с помощью графических процессоров NVIDIA необходимы вычислительные возможности версии 6.x (Pascal) или выше.

- Узнать о вычислительных способностях вашего продукта NVIDIA можно на сайте NVIDIA (https://developer.nvidia.com/cuda-gpus/).
- Чтобы узнать, используется ли аппаратное ускорение для обнаружения движений на видео для конкретной камеры, включите ведение журнала в файле журнала сервера записи. Задайте уровень **Отладка**, и диагностические данные будут фиксироваться в файле DeviceHandling.log. В журнале используется следующая модель:
  [время] [274] ОТЛАДКА – [guid] [имя] Настроенное декодирование: Автоматически: Фактическое декодирование: Intel/NVIDIA

Версия ОС сервера записи и поколение графического процессора могут влиять на производительность аппаратно-ускоренного обнаружения движений на видео. Как правило, на устаревших версиях ограничением является распределение памяти графического процессора (как правило, лимит находится в диапазоне от 0,5 ГБ до 1,7 ГБ).

Системы на базе Windows 10 / Server 2016 и графические адаптеры 6-го поколения (Skylake) или более новые способны выделять графическому процессору 50 % и более системной памяти, тем самым устраняя такое ограничение или уменьшая его влияние.

Графические процессоры Intel 6-го поколения обеспечивают аппаратно-ускоренное декодирование формата H.265, поэтому производительность этих версий графических процессоров сопоставима с форматом H.264.

Включение ручной регулировки чувствительности при анализе движений

Настройка чувствительности определяет, **насколько должен измениться каждый пиксель** на изображении, чтобы оно рассматривалось как движение.

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Движение** поставьте отметку в поле **Ручная регулировка чувствительности**.

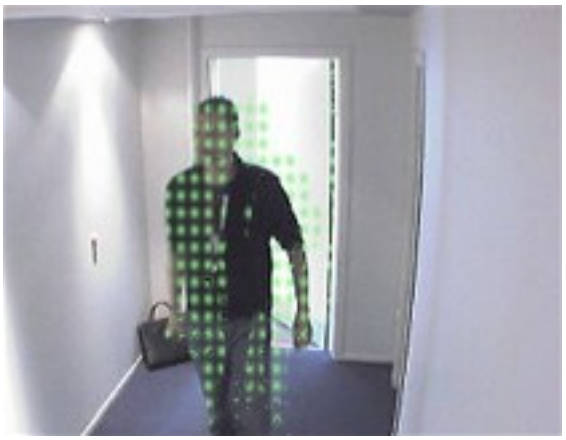
4. Для задания более высокого уровня чувствительности переместите ползунок влево, а для задания более низкого уровня чувствительности — вправо.

   Чем **выше** уровень чувствительности, тем меньшее изменение допускается в каждом пикселе, прежде чем оно будет рассмотрено как движение.

   Чем **ниже** уровень чувствительности, тем большее изменение допускается в каждом пикселе, прежде чем оно будет рассмотрено как движение.

   Пиксели, в которых обнаружено движение, выделены зеленым цветом в поле предварительного просмотра.

5. Выберите положение ползунка, при котором выделены только те случаи обнаружения, которые вы рассматриваете как движение.



Сравнить и установить точный параметр чувствительности камер можно с помощью числа в правой части ползунка.

Указание порогового значения при анализе движений

Пороговое значение обнаружения движений определяет, **сколько пикселей** в изображении должно измениться, чтобы оно рассматривалось как движение.

1. Для задания более высокого уровня подвижности переместите ползунок влево, а для задания более низкого уровня подвижности — вправо.
2. Выберите положение ползунка, при котором обнаруживаются только те случаи обнаружения, которые рассматриваются как движение.

Черной вертикальной линией на панели индикации движений отображается пороговое значение при обнаружении движений: Когда обнаруженное движение превышает выбранный пороговый уровень, цвет панели меняется с зеленого на красный, что сигнализирует о наличии движения.

Панель обнаружения движений: цвет меняется с зеленого на красный при превышении порогового значения, что сигнализирует о наличии движения.

Указание областей, исключаемых при обнаружении движений

Все настройки можно задать для группы камер, но исключенные области, как правило, задаются только для конкретной камеры.

> Также при обнаружении движений исключаются области с постоянными масками конфиденциальности. Для их отображения поставьте отметку в поле **Показать маски конфиденциальности**.

Отключение обнаружения движений в определенных областях помогает избежать обнаружения ненужных движений, например, если в поле обзора камеры находится область с деревом, качающимся на ветру, или с машинами, регулярно проезжающими на заднем плане.

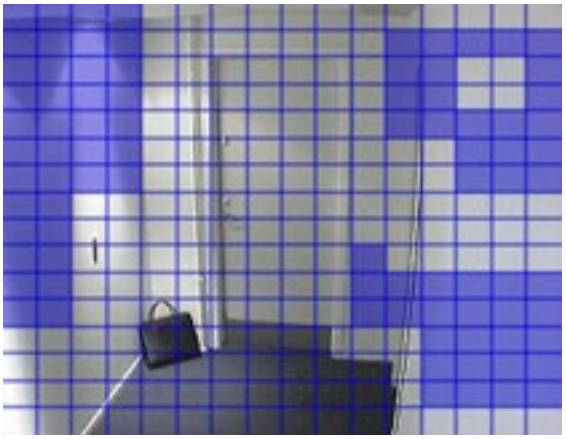
При использовании исключенных областей в PTZ-камерах и повороте, наклоне или изменения масштаба камеры исключенная область **не** перемещается, так как она зафиксирована на изображении с камеры, а не на объекте.

1. Для использования исключенных областей поставьте отметку в поле **Использовать исключенные области**.

   На изображение в поле предварительного просмотра наложена сетка, части которой можно выбирать.

2. Для задания исключенных областей нажмите левую кнопку мыши и перемещайте курсор мыши над требуемыми областями поля предварительного просмотра. Для снятия выделения части сетки нажмите правую кнопку мыши.

Можно задать неограниченное количество исключенных областей. Исключенные области отображаются голубым цветом:



Исключенные области голубого цвета отображаются только в поле предварительного просмотра на вкладке **Движение**, но не в других полях предварительного просмотра в Management Client и не в клиентах с правом доступа.

Устройства — сброс элементов представления

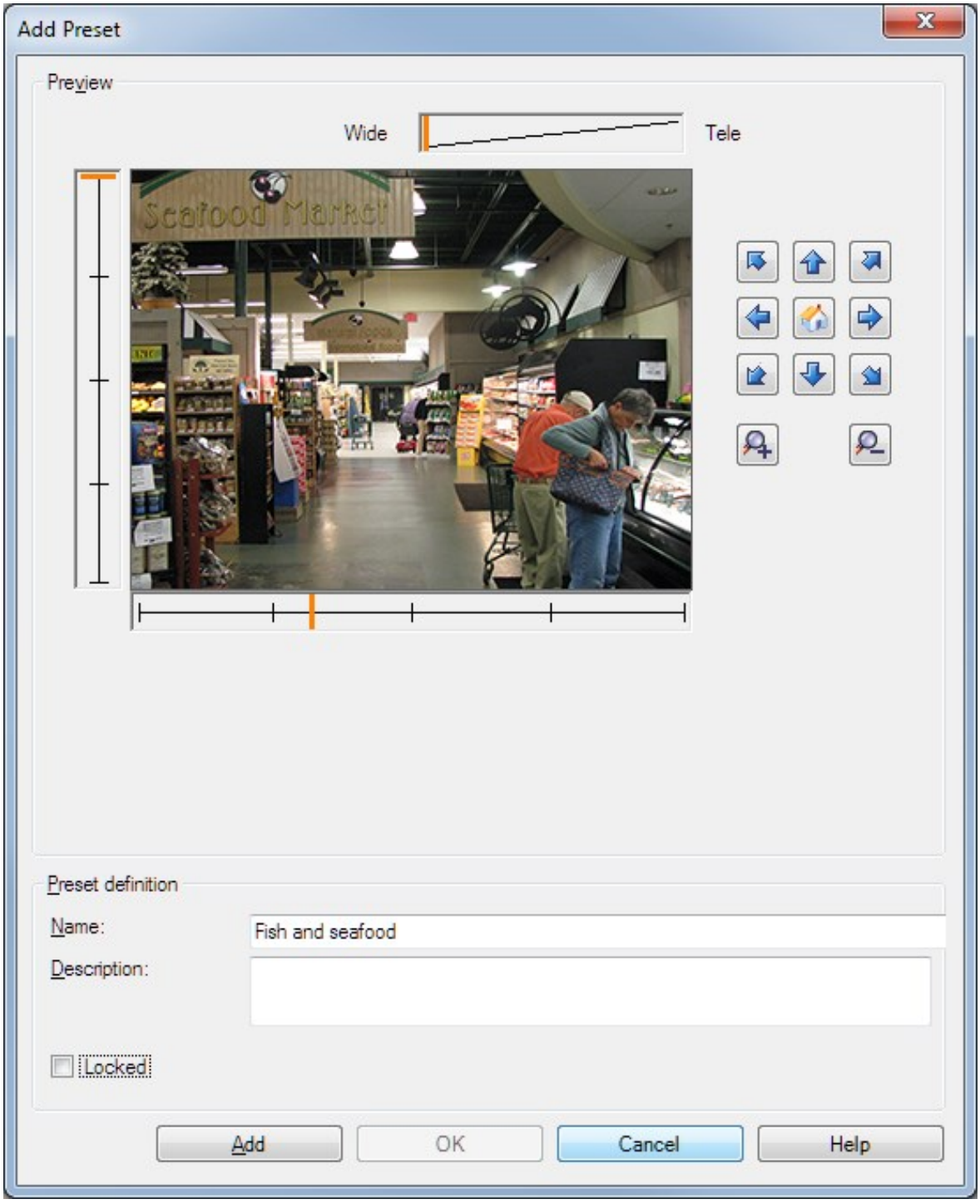
Исходная предустановка «Исходное положение»

Определите **исходную** предустановку PTZ-камеры на главной странице камеры. Возможности PTZ, доступные на странице камеры, зависят от модели.

Добавление исходной предустановки (тип 1)

Чтобы добавить исходную предустановку камеры:

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Предустановки** нажмите кнопку **Новая**. Откроется окно **Добавить предустановку**:



4. В окне **Добавить предустановку** отображается изображение для предварительного просмотра при прямой передаче с камеры. Используйте кнопки навигации и (или) ползунки, чтобы перевести камеру в необходимое положение.
5. Задайте имя исходной предустановки в поле **Имя**.
6. Кроме того, в поле **Описание** можно ввести описание исходной предустановки.
7. Выберите пункт **Заблокировано**, если вы хотите заблокировать исходную предустановку. Впоследствии разблокировать предустановку смогут только пользователи с соответствующими разрешениями.
8. Чтобы задать предустановки, нажмите **Добавить**. Добавьте необходимое количество предустановок.
9. Нажмите кнопку **ОК**. Окно **Добавить предустановку** закроется, а положение будет добавлено в расположенный на вкладке **Предустановки** список доступных для камеры исходных предустановок.

Использование исходных предустановок из камеры (тип 2)

В качестве альтернативы заданию исходных предустановок в системе, для некоторых PTZ-камер их можно задавать непосредственно на камере. Обычно это можно сделать на веб-странице настроек конкретного продукта.

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Предустановки** выберите пункт **Использовать предустановки из устройства**, чтобы импортировать предустановки в систему.

   Заданные для камеры предустановки удаляются и влияют на заданные правила и расписания патрулирования, а также удаляют предустановки, доступные для пользователей XProtect Smart Client.
4. Нажмите кнопку **Удалить**, чтобы удалить предустановки, которые не нужны пользователям.
5. Нажмите кнопку **Изменить**, если вы хотите изменить отображаемое имя предустановки (см. раздел Переименование исходной предустановки (только тип 2)).
6. Если впоследствии потребуется изменить предустановки, задаваемые на устройстве, внесите изменения на камере, а затем повторите импорт.

Назначение исходной предустановки камеры по умолчанию

При необходимости можно задать одну из исходных предустановок PTZ-камеры в качестве предустановки по умолчанию.

Исходная предустановка по умолчанию эффективна, поскольку по ней можно задавать правила, в рамках которых PTZ-камера должна перемещаться в положение по умолчанию в определенных обстоятельствах, например после завершения управления PTZ-камерой в ручном режиме.

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Предустановки** в разделе **Исходные предустановки** выберите предустановку из списка заранее определенных исходных предустановок.
4. Поставьте отметку в поле **Предустановка по умолчанию**, расположенном под списком.

В качестве исходной предустановки по умолчанию может быть задана только одна исходная предустановка.

Если в разделе **Параметры** > **Общие** выбран пункт **Использовать предустановку по умолчанию как исходное PTZ-положение**, исходная предустановка по умолчанию будет использоваться вместо заданного исходного положения PTZ-камеры.

Указание предустановки по умолчанию в качестве исходного PTZ-положения

Пользователи Management Client и XProtect Smart Client, обладающие необходимыми пользовательскими разрешениями, могут настроить систему таким образом, чтобы она использовала исходную предустановку по умолчанию вместо исходного положения для PTZ-камер, у которых в клиенте есть кнопка **Исходное положение**.

Для камеры необходимо задать исходную предустановку по умолчанию. Если исходная предустановка по умолчанию не задана, при нажатии кнопки **Исходное положение** в клиенте ничего не произойдет.

Включение настроек исходного PTZ-положения

1. Выберите раздел **Инструменты** > **Параметры**.

2. На вкладке **Общая информация**, в группе **Сервер записи**, выберите пункт **Использовать предустановку по умолчанию как исходное PTZ-положение**.

3. Задайте исходную предустановку в качестве исходной предустановки по умолчанию для камеры.

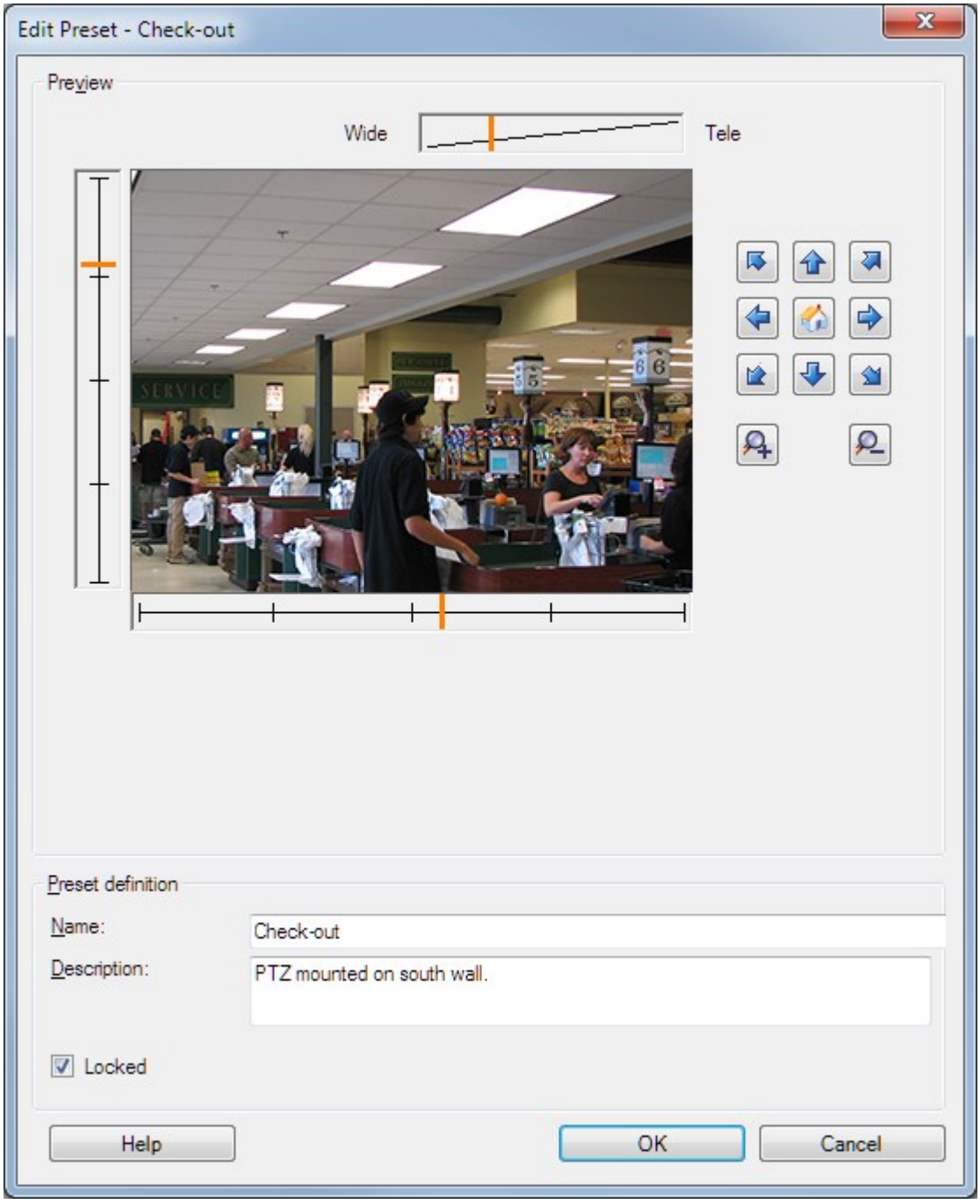
Сведения о задании исходной предустановки см. в разделе Назначение исходной предустановки камеры по умолчанию на стр. 268

Также см. Параметры системы (диалоговое окно «Опции») на стр. 417

Изменение исходной предустановки камеры (только тип 1)

Для изменения существующей исходной предустановки, заданной в системе:

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Предустановки** в разделе «Исходные предустановки» выберите исходную предустановку из списка предустановок, доступных для камеры.
4. Нажмите **Изменить**. Откроется окно **Изменить предустановку**:

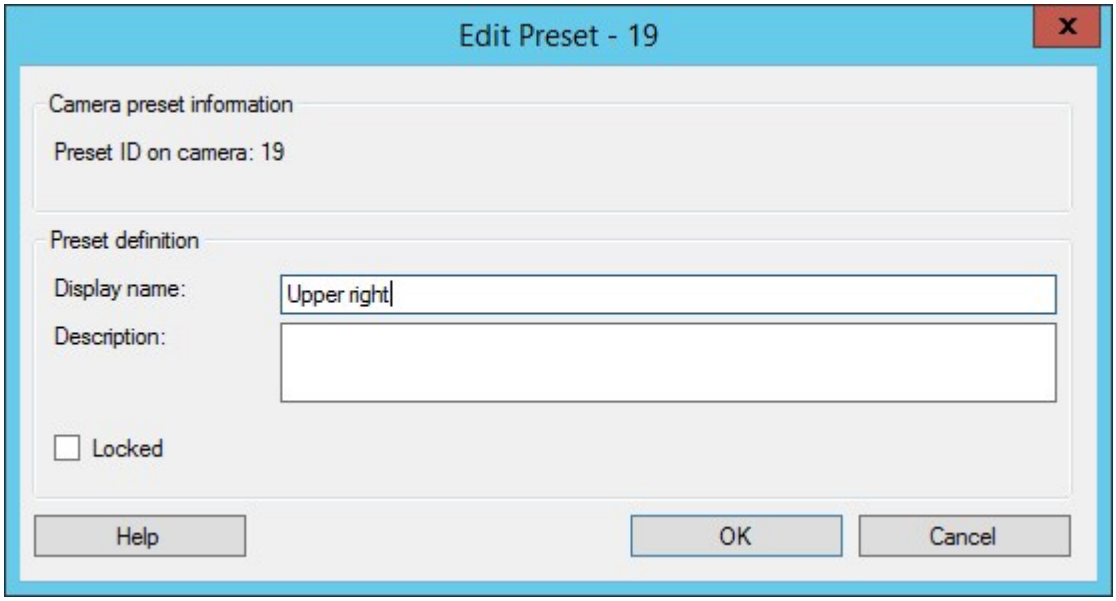


5. В окне **Изменить предустановку** отображается видео, в режиме реального времени поступающее из исходной предустановки. Воспользуйтесь кнопками навигации и (или) ползунками, чтобы изменить исходную предустановку.
6. При необходимости измените имя/номер и описание исходной предустановки.
7. Выберите пункт **Заблокировано**, если вы хотите заблокировать исходную предустановку. Впоследствии разблокировать предустановку смогут только пользователи с соответствующими разрешениями.
8. Нажмите кнопку **OK**.

Переименование исходной предустановки камеры (только тип 2)

Для изменения имени исходной предустановки, заданного в камере:

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Предустановки** выберите исходную предустановку из списка предустановок, доступных для камеры.
4. Нажмите **Изменить**. Откроется окно **Изменить предустановку**:



5. При необходимости измените имя и добавьте описание исходной предустановки.

6. Выберите пункт **Заблокировано**, если требуется заблокировать имя предустановки. Заблокировать имя предустановки можно для того, чтобы у пользователей в XProtect Smart Client или пользователей с ограниченными разрешениями в системе безопасности не было возможности изменить имя предустановки или удалить ее. Заблокированные предустановки обозначены следующим значком:  . Разблокировать имя предустановки смогут только пользователи с соответствующими разрешениями.
7. Нажмите кнопку **OK**.

Тестирование исходной предустановки (только тип 1)

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Предустановки** выберите исходную предустановку из списка исходных предустановок, доступных для камеры.
4. Нажмите **Активировать**.
5. Камера перемещается в выбранную исходную предустановку.

Устройства — патрулирование

Профили патрулирования и патрулирование вручную (объяснение)

Профили патрулирования представляют собой наборы параметров патрулирования. В частности, в этих профилях можно задать порядок перемещения камеры между стандартными позициями и время нахождения в каждой из них. Можно создать неограниченное количество профилей патрулирования и использовать их в правилах. Например, можно создать правило, указывающее, что один профиль патрулирования следует использовать в рабочие часы в дневное время, а другой — ночью.

Патрулирование вручную

Перед применением профиля патрулирования в правиле можно протестировать этот профиль с помощью функции патрулирования вручную. Также патрулирование вручную можно использовать для того, чтобы взять на себя патрулирование вместо другого пользователя или переключиться из режима патрулирования, активируемого при срабатывании правил, при условии, что вы обладаете более высоким PTZ-приоритетом.

Если камера уже выполняет патрулирование или контролируется другим пользователем, вы сможете начать патрулирование вручную только в том случае, если обладаете более высоким приоритетом.

Если вы приступаете к патрулированию вручную в то время, как камера уже выполняет патрулирование по заданным правилам, система возвратится в этот режим после выключения функции патрулирования вручную. Если другой пользователь выполняет патрулирование вручную, но вы обладаете более высоким приоритетом и сами приступаете к патрулированию вручную, патрулирование вручную другого пользователя не будет возобновлено.

Если вы не остановите патрулирование вручную, оно будет выполняться до тех пор, пока не будет задействовано патрулирование по правилам, или контроль над ним не получит пользователь с более высоким приоритетом. По завершении патрулирования по правилам система возвращает вам право патрулирования вручную. Если другой пользователь приступает к патрулированию вручную, ваше патрулирование вручную останавливается и в дальнейшем не возобновляется.

Когда вы останавливаете патрулирование вручную, и для профиля патрулирования задано конечное положение, камера возвращается в это положение.

Добавление профиля патрулирования

До начала работы с патрулированием необходимо задать не менее двух исходных предустановок камеры на вкладке **Предустановки**; см. раздел Добавление исходной предустановки (тип 1).

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Патрулирование** нажмите **Добавить**. Откроется диалоговое окно **Добавить профиль**.
4. В диалоговом окне **Добавить профиль** задайте имя профиля патрулирования.
5. Нажмите кнопку **OK**. Кнопка неактивна, если имя не является уникальным.

Новый профиль патрулирования добавлен в список **Профиль**. Теперь можно задать исходные предустановки и другие настройки профиля патрулирования.

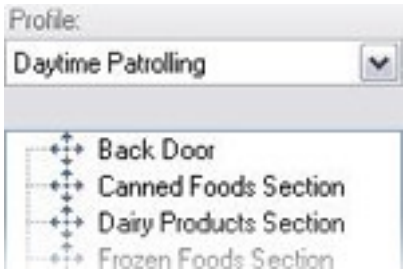
Указание исходных предустановок в профиле патрулирования

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Патрулирование** выберите профиль патрулирования в списке **Профиль**:

4. Нажмите кнопку **Добавить**.

5. В диалоговом окне **Выбрать исходную предустановку** выберите исходные предустановки для профиля патрулирования:

6. Нажмите кнопку **OK**. Выбранные исходные предустановки будут добавлены в список исходных предустановок профиля патрулирования:



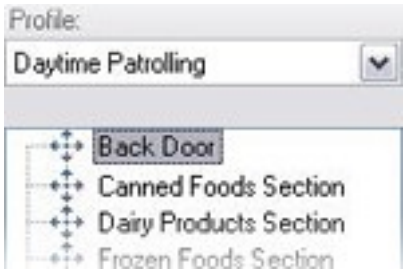
7. При патрулировании в соответствии с профилем патрулирования камера использует исходную предустановку в верхней части списка в качестве первой точки остановки. Вторая точка остановки — это вторая сверху исходная предустановка, и так далее.

Указание времени нахождения в каждой исходной предустановке

При патрулировании PTZ-камера по умолчанию останавливается на 5 секунд в каждой исходной предустановке, указанной в профиле патрулирования.

Для изменения длительности в секундах выполните следующие действия:

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Патрулирование** выберите профиль патрулирования в списке **Профиль**.
4. Выберите исходную предустановку, для которой требуется изменить время:



5. Укажите время в поле **Время на позиции (с)**.
6. При необходимости повторите эти операции для других исходных предустановок.

Пользовательская настройка переходов (PTZ-камера)

По умолчанию перемещение камеры из одной стандартной позиции в другую (**переход**) занимает три секунды. В течение этого времени на камере по умолчанию отключено обнаружение движений, так как в противном случае камера, вероятнее всего, будет обнаруживать ненужное движение при перемещении между исходными предустановками.

Настроить скорость переходов можно только в том случае, если камера поддерживает PTZ-поиск и относится к типу камер, в которых исходные предустановки настраиваются и хранятся на сервере системы (PTZ-камера типа 1). В противном случае ползунок **Скорость** будет неактивен.

Можно настроить следующие параметры:

- Приблизительное время перехода
- Скорость движения камеры во время перехода

Для настройки переходов между различными исходными предустановками:

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Патрулирование** в списке **Профиль** выберите профиль патрулирования.
4. Поставьте отметку в поле **Настроить переходы**.

   Указатели переходов добавляются к списку исходных предустановок.
5. Выберите переход из списка.

6. В поле **Ожидаемое время (с)** укажите приблизительное время перехода (в секундах).

7. Для задания скорости перехода воспользуйтесь ползунком **Скорость**. Когда ползунок находится в крайнем правом положении, камера движется со скоростью, заданной по умолчанию. Чем больше ползунок сдвинут влево, тем медленнее движется камера во время выбранного перехода.
8. Повторите описанные действия для других переходов.

Указание конечного положения при патрулировании

Камеру можно настроить таким образом, чтобы при патрулировании она перемещалась в конкретную исходную предустановку в соответствии с конечными точками выбранного профиля патрулирования.

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Патрулирование** в списке **Профиль** выберите соответствующий профиль патрулирования.
4. Поставьте отметку в поле **Перейти к определенному положению по завершении**. Откроется диалоговое окно **Выберите предустановку**.
5. Выберите конечное положение и нажмите кнопку **ОК**.

   > В качестве конечного положения можно выбирать любые из исходных предустановок камеры, а не только исходные предустановки, используемые в профиле патрулирования.

6. Выбранное конечное положение будет добавлено в список профилей.

После завершения патрулирования в соответствии с выбранным профилем патрулирования камера перемещается в заданное конечное положение.

Резервирование и освобождение сеансов PTZ

В зависимости от типа используемой системы наблюдения может быть возможно резервирование сеансов PTZ.

Администраторы с достаточными разрешениями в системе безопасности для запуска зарезервированного сеанса PTZ могут запустить PTZ-камеру в этом режиме. Это не позволяет другим пользователям взять на себя управление камерой. В рамках зарезервированного сеанса PTZ стандартная система PTZ-приоритетов не принимается во внимание, чтобы пользователи с более высоким PTZ-приоритетом не смогли прервать сеанс.

Во время зарезервированного сеанса PTZ управлять камерой можно через XProtect Smart Client и Management Client.

Резервирование сеанса PTZ полезно в тех случаях, когда вам требуется внести срочные обновления, провести обслуживание PTZ-камеры или скорректировать ее предустановки, избежав вмешательства других пользователей.

Резервирование сеанса PTZ

1. На панели **Навигация по сайту** выберите пункт **Устройства**, а затем — **Камеры**.
2. Выберите соответствующую PTZ-камеру на панели **Обзор**.
3. На вкладке **Предустановки** выберите сеанс PTZ и нажмите кнопку **Зарезервировано**.

> Начать зарезервированный сеанс PTZ нельзя, если камерой управляет пользователь с более высоким приоритетом, либо если она уже зарезервирована другим пользователем.

Освобождение сеанса PTZ

Кнопка **Освободить** позволяет освободить текущий сеанс PTZ, чтобы камерой мог управлять другой пользователь. При нажатии кнопки **Освободить** сеанс PTZ немедленно прекращается и становится доступным для первого пользователя, который приступит к работе с камерой.

Администраторы с разрешением системы безопасности **Освободить сеанс PTZ** наделены правом в любой момент времени освободить зарезервированный сеанс PTZ других пользователей. Данная функция полезна в случаях, когда требуется выполнить обслуживание PTZ-камеры или ее предустановок, либо если другие пользователи случайно заблокировали камеру в экстренных ситуациях.

Время ожидания в сеансах PTZ

Пользователи Management Client и XProtect Smart Client с необходимыми пользовательскими разрешениями могут вручную прерывать сеансы патрулирования PTZ-камер.

Можно указать, сколько времени должно пройти, прежде чем для всех PTZ-камер в системе будет возобновлено обычное патрулирование:

1. Выберите пункт **Инструменты** > **Опции**.
2. В окне **Параметры**, на вкладке **Общая информация** выберите промежуток времени в следующих списках:
   - Список **Время ожидания для сеансов PTZ вручную** (значение по умолчанию — 15 секунд).
   - Список **Время ожидания для приостановленных сеансов патрулирования** (значение по умолчанию — 10 минут).
   - Список **Время ожидания для зарезервированных сеансов PTZ** (значение по умолчанию — 1 час).

   Эти настройки применяются ко всем PTZ-камерам в вашей системе.

Время ожидания можно изменить отдельно для каждой камеры.

1. В области **Навигация по сайту** выберите пункт **Камера**.
2. На панели «Обзор» выберите камеру.
3. На вкладке **Общие** выберите промежуток времени в следующих списках:
   - Список **Время ожидания для сеанса PTZ вручную** (значение по умолчанию — 15 секунд).
   - Список **Время ожидания для приостановленного сеанса патрулирования** (значение по умолчанию — 10 минут).
   - Список **Время ожидания для зарезервированного сеанса PTZ** (значение по умолчанию — 1 час).

   Эти настройки применяются только к конкретной камере.

Устройства — события для правил

Добавление или удаление события для устройства

Добавление события

1. На панели **Обзор** выберите устройство.
2. Перейдите на вкладку **События** и нажмите **Добавить**. Откроется окно **Выбрать инициирующее событие**.
3. Выберите событие. За один раз можно выбрать только одно событие.
4. Если требуется просмотреть полный список событий, чтобы добавить уже добавленные события, выберите пункт **Показать уже добавленные события**.
5. Нажмите кнопку **ОК**.
6. На панели инструментов нажмите кнопку **Сохранить**.

Удаление события

Удаление события отражается на всех правилах, в которых оно используется.

1. На панели **Обзор** выберите устройство.
2. Перейдите на вкладку **События** и нажмите **Удалить**.

Задайте свойства события

Можно задать свойства для каждого добавленного вами события. Количество свойств зависит от устройства и от события. Для того чтобы событие сработало надлежащим образом, некоторые (или все) свойства должны быть заданы одинаково и на устройстве, и на вкладке **События**.

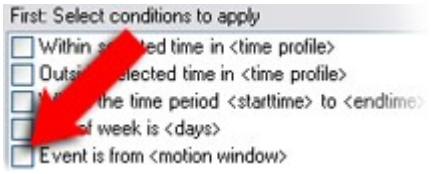
Использование нескольких экземпляров события

Для того чтобы задать различные свойства для различных экземпляров события, событие можно добавить несколько раз.

Ниже приведен пример для камер.

Пример: Вы настроили в камере два окна движения и назвали их A1 и A2. Вы добавили два экземпляра события «Начало движения (аппаратное)». В свойствах одного экземпляра вы задали использование окна движения A1. В свойствах другого экземпляра вы задали использование окна движения A2.

При использовании события в правиле можно указать, что для срабатывания правила событие должно быть основано на движении, обнаруженном в конкретном окне:



Устройства — маски конфиденциальности

Включение/отключение конфиденциальной маскировки

По умолчанию функция конфиденциальной маскировки отключена.

Для включения/отключения функции конфиденциальной маскировки для камеры:

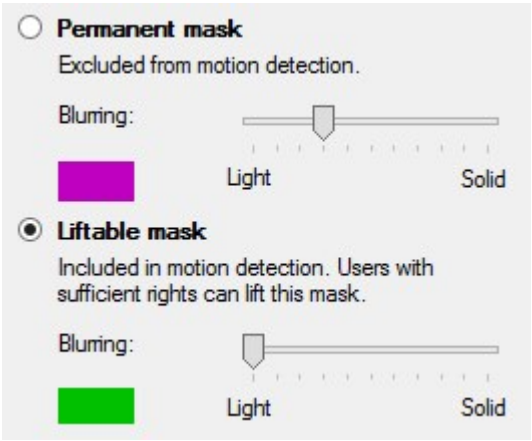
1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. На вкладке **Конфиденциальная маскировка** снимите или поставьте отметку в поле **Конфиденциальная маскировка**.

> В схеме Milestone Interconnect центральный объект игнорирует маски конфиденциальности, установленные на удаленном объекте. Если вы хотите применить одинаковые маски конфиденциальности, их необходимо повторно задать на центральном объекте.

Настройка масок конфиденциальности

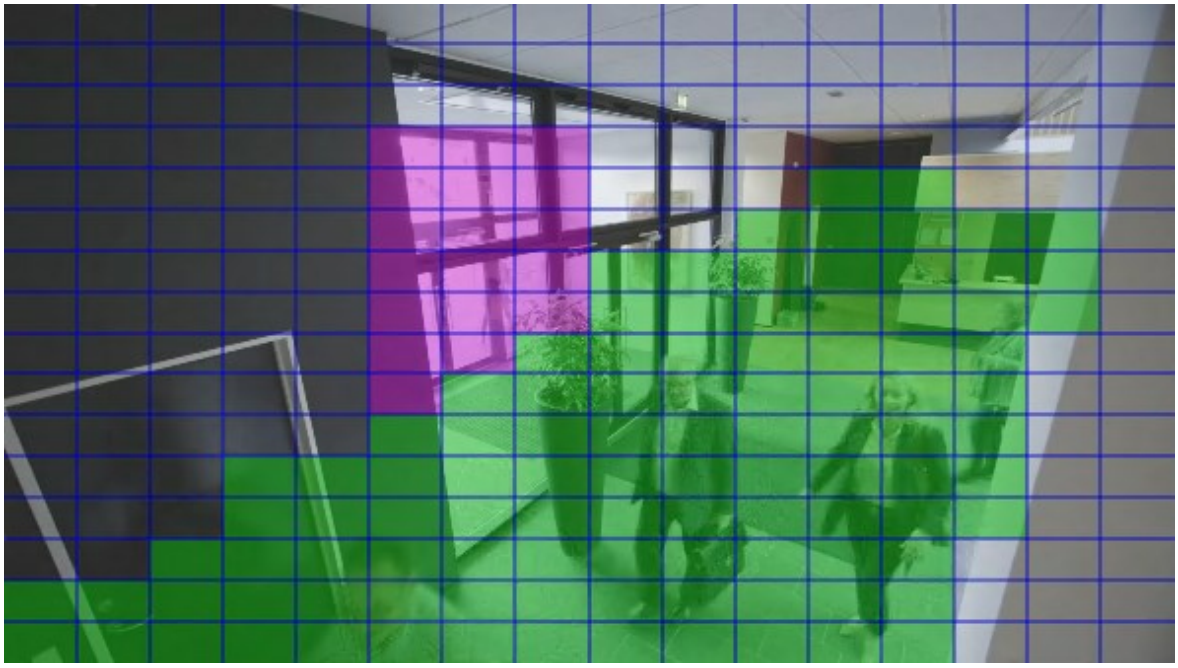
При включении функции конфиденциальной маскировки на вкладке **Конфиденциальная маскировка** к окну предварительного просмотра камеры добавляется сетка.

1. На панели **Навигация по сайту** выберите пункт **Устройства**.
2. Выберите соответствующую камеру на панели **Обзор**.
3. Для того чтобы закрыть область маской конфиденциальности, сначала выберите пункт **Постоянная маска** или **Съемная маска** на вкладке **Конфиденциальная маскировка**, чтобы задать требуемый тип маски.



4. Расположите курсор мыши в области предварительного просмотра. Нажмите ее левой кнопкой мыши для выбора ячейки сетки. Нажмите ее правой кнопкой мыши для очистки ячейки сетки.

5. Можно задать требуемое количество областей конфиденциальной маскировки. Области с постоянными масками конфиденциальности выделены фиолетовым цветом, а области со съемными масками конфиденциальности — зеленым цветом.



6. Укажите, как закрытые области должны отображаться при показе видео клиентам. С помощью ползунков этот параметр можно задать в диапазоне от небольшой размытости до сплошной, непрозрачной маски.

> Также постоянные маски конфиденциальности отображаются на вкладке **Движение**.

7. В XProtect Smart Client убедитесь, что маски конфиденциальности отображаются в соответствии с заданными параметрами.

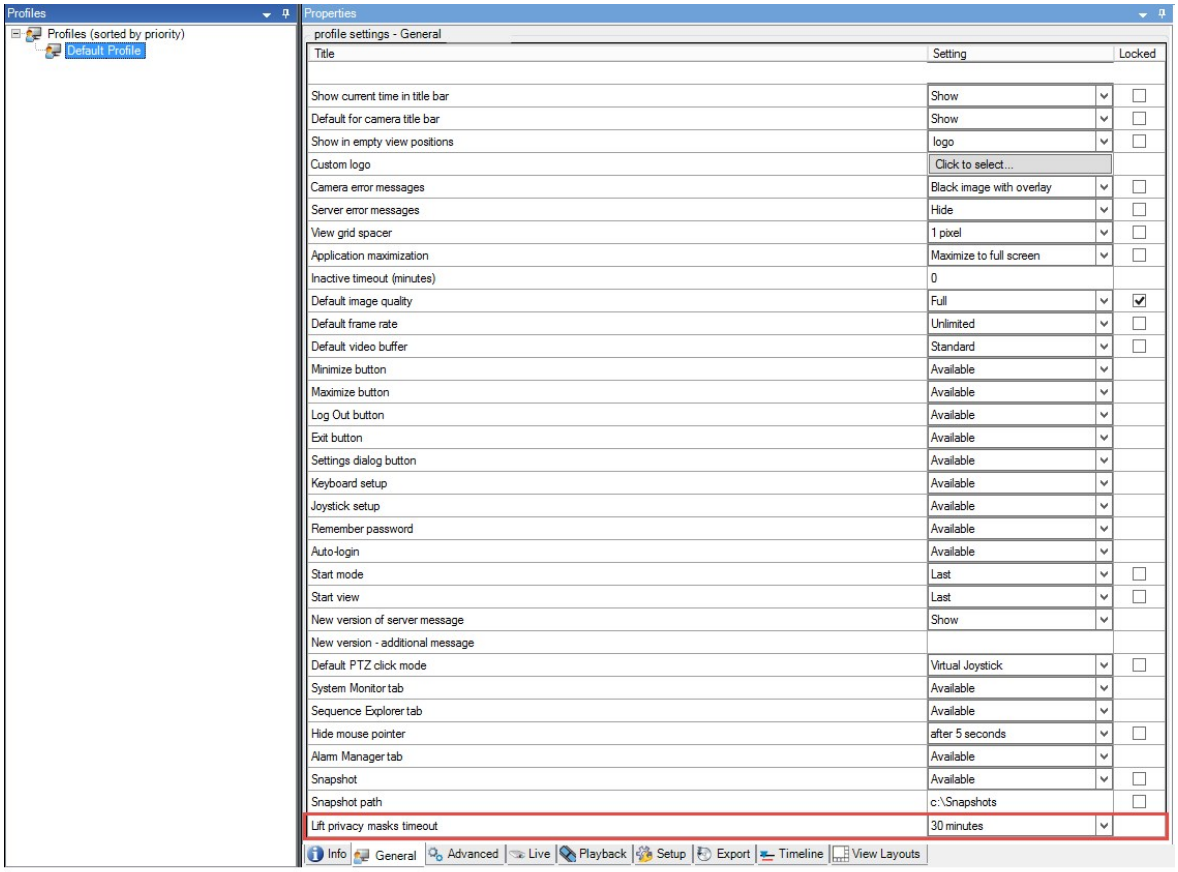
Изменение времени ожидания для съемных масок конфиденциальности

По умолчанию маски конфиденциальности в XProtect Smart Client снимаются на 30 минут, после чего автоматически применяются повторно. Однако этот параметр можно изменить.

> При изменении времени ожидания обязательно делайте это для профиля Smart Client, связанного с ролью, которой разрешено снимать маски конфиденциальности.

Для изменения времени ожидания:

1. В разделе **Smart ClientПрофили** выберите соответствующий профиль Smart Client.
2. На вкладке **Общая информация** найдите пункт **Время ожидания при снятии масок конфиденциальности**.



3. Выберите одно из двух значений:
   - **2 минуты**
   - **10 минут**
   - **30 минут**
   - **1 час**
   - **2 часа**
   - **До выхода из системы**
4. Нажмите **Сохранить**.

Предоставление пользователям разрешения снимать маски конфиденциальности

По умолчанию пользователям не предоставлены разрешения снимать маски конфиденциальности в XProtect Smart Client.

Для включения/отключения разрешения:

1. На панели **Навигация по сайту** выберите пункт **Безопасность**, а затем — **Роли**.
2. Выберите роль, которой требуется предоставить разрешение снимать маски конфиденциальности.
3. На вкладке **Общая безопасность** выберите пункт **Камеры**.
4. В пункте **Разрешение снимать маски безопасности** поставьте отметку в поле **Разрешить**.

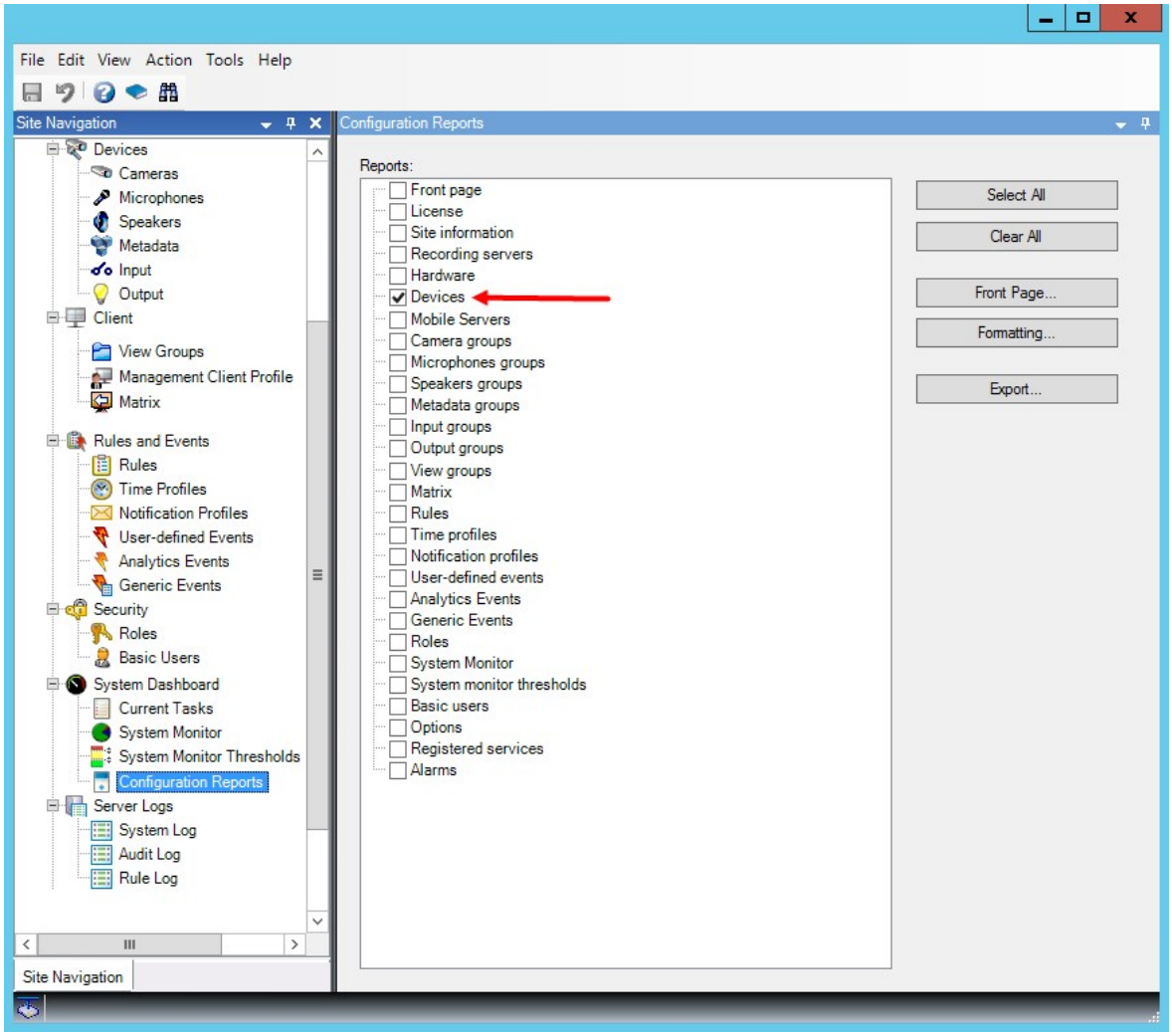
Пользователи, которым назначена эта роль, смогут снимать съемные маски безопасности для себя, а также давать разрешение на снятие масок другим пользователям XProtect Smart Client.

Создание отчета о настройках конфиденциальной маскировки

В отчете об устройствах содержится информация о текущих настройках конфиденциальной маскировки для камер.

Для настройки отчета:

1. На панели **Навигация по сайту** выберите пункт **Информационная панель системы**.
2. В разделе **Отчёты о конфигурации** выберите отчет **Устройства**.



3. При необходимости можно изменить титульный лист и форматирование отчета.
4. Нажмите кнопку **Экспортировать**: система создаст отчет в виде PDF-файла.

Дополнительные сведения об отчетах см. в разделе Печать отчета с конфигурацией системы на стр. 326.

Клиенты

Группы представлений (объяснение)

Способ, с помощью которого система отображает видео с одной или нескольких камер клиентов, называется представлением. Группа представлений — это контейнер для одной или нескольких логических групп таких представлений. В клиентах группа представлений отображается как раскрываемая папка, из которой пользователи могут выбрать группу и представление для просмотра:

Пример из XProtect Smart Client: Стрелкой обозначается группа представлений, которая содержит логическую группу (называемую «Вспомогательные объекты») с тремя представлениями.

По умолчанию каждая роль, заданная в Management Client, также создается как группа представлений. При добавлении роли в Management Client роль по умолчанию отображается как группа представлений, доступная для использования в клиентах.

- Группу представлений на основе роли можно закрепить за пользователями/группами с соответствующей ролью. Эти разрешения группы представлений можно изменить путем внесения последующих изменений в настройки роли.
- Группа представлений на основе роли использует имя этой роли.

  Пример: При создании роли с именем **Формирование службы безопасности** она будет отображаться в XProtect Smart Client как группа представлений под названием **Формирование службы безопасности**.

  В дополнение к группам представлений, создаваемым при добавлении ролей, можно создать любое количество других групп представлений. Также группы представлений можно удалять, включая созданные автоматически при добавлении ролей
- Даже если при каждом добавлении роли создается новая группа представлений, группы представлений не обязаны соответствовать ролям. При необходимости любые из групп представлений можно добавлять, переименовывать или удалять.

> В случае переименования группы представлений уже подключенные пользователи клиентов должны выйти из системы и войти в нее вновь, чтобы увидеть новое имя.

Добавление группы представлений

1. Нажмите раздел **Группы представлений** правой кнопкой мыши и выберите пункт **Добавить группу представлений**. Откроется диалоговое окно **Добавить группу представлений**.
2. Введите имя и, при необходимости, описание новой группы представлений, а затем нажмите кнопку **OK**.

Роли не смогут использовать только что добавленную группу представлений, пока не будут заданы такие разрешения. Если указано, какие из ролей могут использовать только что добавленную группу представлений, пользователи клиента, которые уже подключены и имеют соответствующие роли, должны выйти из системы и войти в нее повторно, прежде чем смогут увидеть эту группу представлений.

Профили Smart Client

Добавление и настройка профиля Smart Client

Перед настройкой профиля Smart Client его необходимо создать.

1. Правой кнопкой мыши нажмите **Smart ClientПрофили**.
2. Выберите **Добавить профиль Smart Client**.
3. В диалоговом окне **Добавить профиль Smart Client** введите имя и описание нового профиля и нажмите **OK**.
4. На панели **Обзор** выберите созданный профиль, чтобы настроить его.
5. Настройте параметры на одной, нескольких или всех доступных вкладках и нажмите **OK**.

Копирование профиля Smart Client

Если у вас есть профиль Smart Client с нестандартными параметрами или разрешениями, и вам требуется похожий профиль, удобнее скопировать уже существующий профиль и внести в него незначительные изменения, нежели создавать заново.

1. Нажмите **Smart ClientПрофили**, правой кнопкой мыши нажмите профиль на панели **Обзор**, затем выберите **Копировать профиль Smart Client**.
2. В появившемся диалоговом окне задайте для скопированного профиля новое уникальное имя и описание. Нажмите кнопку **OK**.
3. На панели **Обзор** выберите созданный профиль, чтобы настроить его. Настройте параметры на одной, нескольких или всех доступных вкладках. Нажмите кнопку **OK**.

Создание и настройка профилей Smart Client, ролей и профилей времени

Для работы с профилями Smart Client важно понимать связь между профилями Smart Client, ролями и профилями времени:

- Профили Smart Client предназначены для настройки прав пользователей в XProtect Smart Client.
- Роли связаны с параметрами безопасности в клиентах, MIP SDK и т.д.
- Профили времени связаны с параметрами времени двух типов профилей.

Вместе эти три функции обеспечивают уникальные возможности контроля и настройки разрешений пользователей XProtect Smart Client.

Пример: В рамках XProtect Smart Client предполагается наличие пользователя, которому разрешено просматривать видео в режиме реального времени (без воспроизведения) с выбранных камер и только в стандартное рабочее время (с 8:00 до 16:00). Возможна следующая настройка:

1. Создайте профиль Smart Client и задайте подходящее имя. Например, **Только для режима «Наблюдение»**.
2. Укажите необходимые параметры прямой передачи/воспроизведения для профиля **Только для режима «Наблюдение»**.
3. Создайте профиль времени и задайте подходящее имя. Например, **Только в дневное время**.
4. Укажите желаемый период времени для профиля **Только в дневное время**.
5. Создайте новую роль и задайте подходящее имя. Например, **Охрана (выбранные камеры)**.
6. Укажите, какие камеры можно использовать для роли **Охрана (выбранные камеры)**.
7. Назначьте профиль **Только для режима «Наблюдение»** Smart Client и профиль времени **Только в дневное время** роли **Охрана (выбранные камеры)**, чтобы связать эти три элемента.

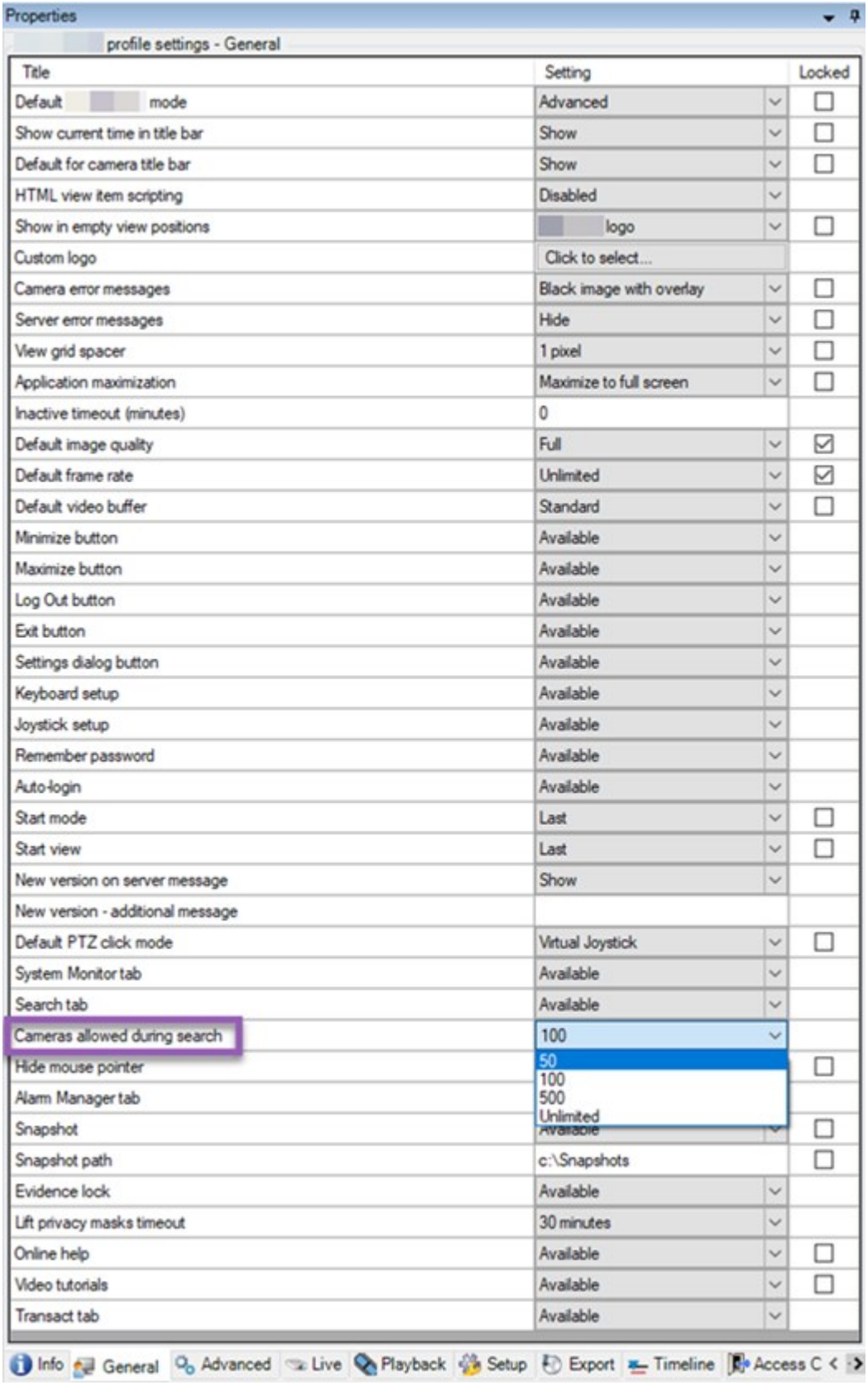
Благодаря комбинации этих трех функций вы можете получить оптимальный результат, а также легко выполнить точную настройку и регулировку. Процесс настройки можно выполнить в другом порядке. Так, сначала можно создать роль, затем профиль Smart Client и профиль времени, или же выполнить настройку в любом удобном для вас порядке.

Настройка количества камер, разрешенных во время поиска

Количество камер, которые операторы могут добавить при поиске, настраивается в XProtect Smart Client. Значение по умолчанию — **100**. При превышении установленного предела по количеству камер оператор получает предупреждение.

1. В XProtect Management Client разверните узел **Клиент** > **Smart ClientПрофили**.
2. Выберите необходимый профиль.

3. Перейдите на вкладку **Общая информация**.


Properties
profile settings - General
Title
Setting
Locked
Default mode
Advanced
Show current time in title bar
Show
Default for camera title bar
Show
HTML view item scripting
Disabled
Show in empty view positions
logo
Custom logo
Click to select...
Camera error messages
Black image with overlay
Server error messages
Hide
View grid spacer
1 pixel
Application maximization
Maximize to full screen
Inactive timeout (minutes)
0
Default image quality
Full
Default frame rate
Unlimited
Default video buffer
Standard
Minimize button
Available
Maximize button
Available
Log Out button
Available
Exit button
Available
Settings dialog button
Available
Keyboard setup
Available
Joystick setup
Available
Remember password
Available
Auto-login
Available
Start mode
Last
Start view
Last
New version on server message
Show
New version - additional message
Default PTZ click mode
Virtual Joystick
System Monitor tab
Available
Search tab
Available
Cameras allowed during search
100
50
100
500
Unlimited
Hide mouse pointer
Alarm Manager tab
Snapshot
Snapshot path
c:\Snapshots
Evidence lock
Available
Lift privacy masks timeout
30 minutes
Online help
Available
Video tutorials
Available
Transact tab
Available
Info
General
Advanced
Live
Playback
Setup
Export
Timeline
Access C

4. В разделе **Камеры, разрешенные во время поиска** выберите одно из следующих значений:
    - **50**
    - **100**
    - **500**
    - **Без ограничений**
5. Сохраните изменения.

Изменение настроек экспорта по умолчанию

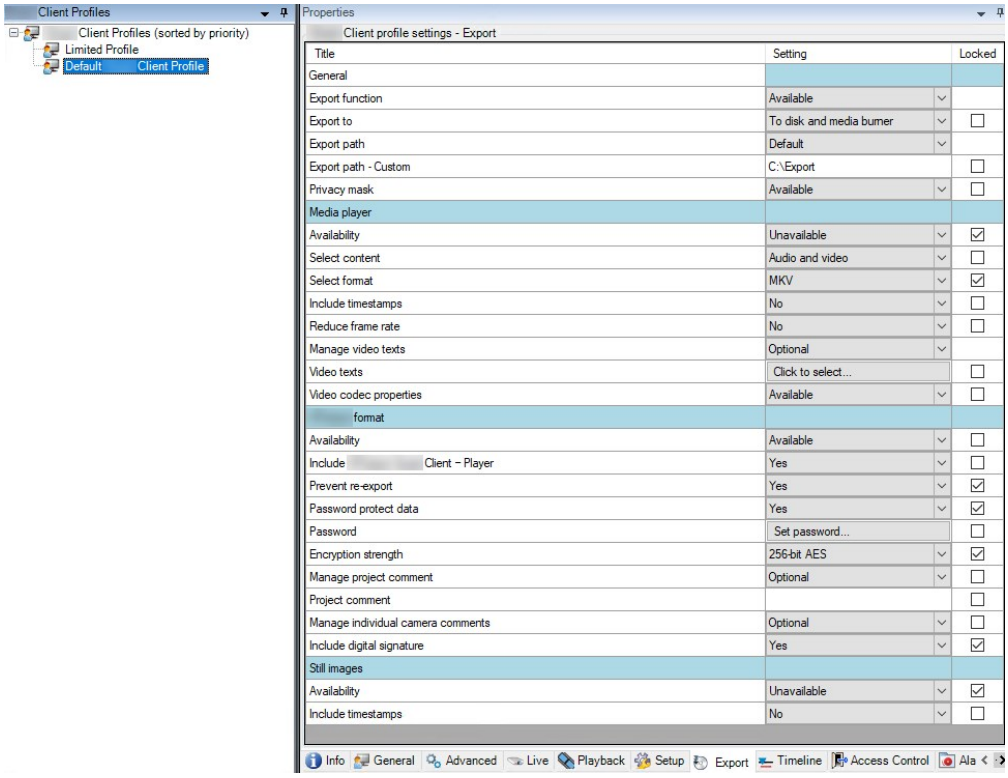
При установке системы VMS XProtect настройки экспорта, определяющие параметры экспорта в XProtect Smart Client, по умолчанию ограничены, чтобы обеспечить максимальный уровень безопасности. Эти настройки можно изменить, расширив возможности операторов.

Параметры по умолчанию

- XProtect является единственным доступным форматом
    - Повторный экспорт заблокирован
    - Операции экспорта защищены паролем
    - Шифрование с помощью алгоритма AES с 256-разрядным ключом
    - Добавлены цифровые подписи
- Экспорт в формат MKV или AVI недоступен
- Экспорт кадров недоступен

Действия:

1. В XProtect Management Client разверните узел **Клиент** > **Smart ClientПрофили**.
2. Выберите **Профиль Smart Client по умолчанию**.
3. На панели **Свойства** перейдите на вкладку **Экспорт**.



4. Чтобы активировать запрещенный формат в XProtect Smart Client, найдите соответствующий параметр и выберите **Доступно**.
5. Чтобы предоставить операторам право изменять настройки в XProtect Smart Client, снимите флажок **Заблокировано** для соответствующего параметра.
6. При необходимости измените другие параметры.
7. (необязательно) Войдите в XProtect Smart Client и убедитесь, что параметры применены.

Профили Management Client

Добавление и настройка профиля Management Client

Если вы не хотите использовать профиль по умолчанию, сначала создайте профиль Management Client, а затем настройте его.

1. Правой кнопкой мыши нажмите **Management ClientПрофили**.
2. Выберите **Добавить профиль Management Client**.
3. В диалоговом окне **Добавить профиль Management Client** введите имя и описание нового профиля и нажмите **OK**.
4. На панели **Обзор** выберите созданный профиль, чтобы настроить его.
5. На вкладке **Профиль** выберите функции профиля Management Client или отмените выбранные функции.

Копирование профиля Management Client

Если у вас есть настроенный профиль Management Client, параметры которого необходимо использовать повторно, вы можете скопировать уже существующий профиль и внести в него незначительные изменения вместо того, чтобы создавать профиль заново.

1. Нажмите **Management ClientПрофиль**, правой кнопкой мыши нажмите профиль на панели **Обзор**, затем выберите **Копировать профиль Management Client**.
2. В появившемся диалоговом окне задайте для скопированного профиля новое уникальное имя и описание. Нажмите кнопку **OK**.
3. На панели **Обзор** выберите профиль и перейдите на вкладку **Информация** или вкладку **Профиль**, чтобы выполнить настройку.

Управление отображением функций в профиле Management Client

Привяжите профили Management Client к ролям, чтобы в интерфейсе были доступны только функции, необходимые соответствующим ролям администраторов.

Привязка профиля Management Client к роли

1. Разверните узел **Безопасность** и выберите **Роли**.
2. На вкладке **Информация** в окне **Параметры ролей** привяжите профиль к роли. Дополнительные сведения см. в разделе Вкладка «Информация» (роли).

Управление общим доступом к функциям системы в зависимости от роли

Профили Management Client обеспечивают только визуальное представление функциональности системы, не предоставляя доступа к ней.

Чтобы настроить общий доступ к функциям системы для роли, выполните следующие действия:

1. Разверните узел **Безопасность** и выберите **Роли**.
2. Откройте вкладку **Общий уровень безопасности** и установите соответствующие флажки. Дополнительные сведения приведены в разделе Вкладка «Общая безопасность» (роли) на стр. 563.

На вкладке **Общий уровень безопасности** включите разрешение безопасности **Подключение**, чтобы предоставить всем ролям доступ к Management Server.

Кроме встроенной роли администратора, добавлять, редактировать или удалять профили Management Client на сервере управления могут только те пользователи, у которых есть право **Управление безопасностью**, назначенное на вкладке **Общий уровень безопасности**.

Ограничение на отображение функций для профиля

Вы можете изменить настройки видимости всех элементов Management Client. По умолчанию профиль Management Client имеет доступ к просмотру всех функций в Management Client.

1. Разверните узел «Клиент» и выберите «Профили Management Client».
2. Выберите профиль и откройте вкладку «Профиль».
3. Снимите флажки с соответствующих функций, чтобы они не отображались в Management Client у пользователей Management Client с ролью, привязанной к профилю Management Client.

Matrix

Получатели Matrix и Matrix (объяснение)

Matrix — это функция удаленного распределения видеоданных.

Получатель Matrix — это компьютер с XProtect Smart Client, который задан в качестве получателя Matrix в Management Client.

При использовании Matrix можно передавать видео с любой камеры в сети любому активному получателю Matrix.

Для просмотра списка получателей Matrix, добавленных в Management Client, откройте раздел **Клиент** на панели **Навигация по сайту**, а затем выберите **Matrix**. На панели **Свойства** отобразится список конфигураций Matrix.

В Management Client необходимо добавить каждого получателя Matrix, который должен получать активированное при помощи Matrix видео.

Указание правил для отправки видео получателям Matrix

Для отправки видео получателям Matrix необходимо включить получателя Matrix в правило, активирующее передачу видео связанному получателю Matrix. Для этого:

1. На панели **Навигация по сайту** откройте раздел **Правила и события** > **Правила**. Нажмите раздел **Правила** правой кнопкой мыши, чтобы открыть мастер **Управление правилом**. На первом этапе выберите тип правила, а на втором этапе — условие.
2. На третьем этапе мастера **Управление правилом** (**Этап 3. Действия**) выберите действие **Задать Matrix для просмотра <устройств>**.
3. Нажмите ссылку Matrix в исходном описании правила.
4. В диалоговом окне **Выбрать конфигурацию Matrix** выберите соответствующего получателя-Matrix и нажмите кнопку **OK**.
5. Нажмите ссылку **Устройства** в исходном описании правила и выберите камеры, которые должны отправлять видео получателю-Matrix, а затем нажмите кнопку **OK** для подтверждения выбора.
6. Нажмите кнопку **Готово**, если правило готово, либо задайте дополнительные действия и (или) завершающее действие.

При удалении получателя-Matrix любое правило, включающее этого получателя-Matrix, перестает действовать.

Добавление получателей Matrix

Для добавления существующего получателя Matrix в Management Client:

1. Откройте раздел **Клиенты**, а затем выберите пункт **Matrix**.
2. Нажмите раздел **MatrixКонфигурации** правой кнопкой мыши и выберите пункт **ДобавитьMatrix**.
3. Заполните поля в диалоговом окне **ДобавитьMatrix**.
    1. В поле **Адрес** введите IP-адрес или имя хоста необходимого получателя Matrix.
    2. В поле **Порт** введите номер порта, используемый системой получателя Matrix.
4. Нажмите кнопку **OK**.

Теперь можно использовать получателя Matrix в правилах.

Система не проверяет, правилен ли указанный номер порта или пароль, или соответствует ли указанный номер порта, пароль или тип реальному получателю Matrix. Убедитесь, что введена правильная информация.

Отправка одного и того же видео в несколько представлений XProtect Smart Client

Одно и то же видео можно отправлять в несколько положений Matrix в нескольких представлениях XProtect Smart Client, при условии, что положения Matrix этих представлений используют одинаковый номер порта и пароль:

1. В XProtect Smart Client создайте соответствующие представления и положения Matrix, которые используют одинаковый номер порта и пароль.
2. В Management Client добавьте соответствующий XProtect Smart Client в качестве получателя-Matrix.
3. Получателя-Matrix можно включать в правило.

Правила и события

Добавление правил

Для добавления правил используется мастер **Управление правилом**, в котором приведены только значимые параметры.

Благодаря мастеру в правиле будут отражены все необходимые элементы. На основе содержимого правила мастер автоматически предлагает подходящие завершающие действия (то есть то, что должно произойти, когда правило перестает применяться). Таким образом, вы не сможете непреднамеренно создать правило, которое никогда не завершится.

События

При добавлении правила на основе событий можно выбрать различные типы событий.

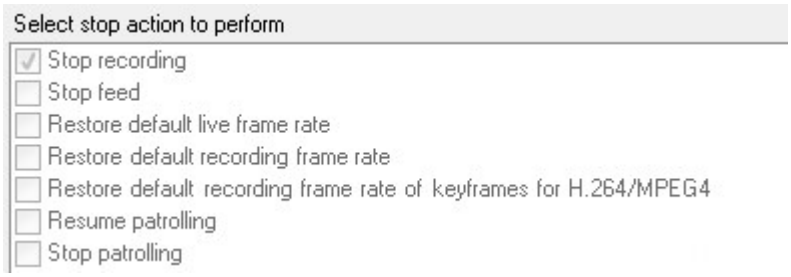
- Общие сведения и описание типов доступных событий приведены в разделе Обзор событий.

Действия и завершающие действия

При создании правил можно выбирать различные действия.

Некоторые из действий требуют наличия завершающих действия. Например, если выбрать действие **Начать запись**, запись начинается и, теоретически, продолжается бесконечно. В связи с этим для действия **Начать запись** имеется обязательное завершающее действие под названием **Остановить запись**.

Мастер **Управление правилом** следит за тем, чтобы всегда были заданы обязательные завершающие действия:



Выбор завершающих действий. При рассмотрении следующего примера обратите внимание на обязательное завершающее действие (выбрано и отображается бледным цветом), неприменимые завершающие действия (отображаются бледным цветом), а также необязательные завершающие действия (могут быть выбраны).

- Общие сведения о доступных действиях и завершающих действиях приведены в разделе Действия и завершающие действия .

Создание правила

1. Нажмите пункт **Правила** правой кнопкой мыши и выберите > **Добавить правило**. Откроется мастер **Управлением правилом**. Мастер поможет задать содержимое правила.
2. Введите имя и описание нового правила в полях **Имя** и **Описание** соответственно.
3. Выберите для правила соответствующий тип условия: правило, выполняющее одно или несколько действий при наступлении определенного события, или правило, выполняющее одно или несколько действий при указании конкретного периода времени.
4. Нажмите кнопку **Далее**, чтобы перейти ко второму этапу мастера. На втором этапе мастера задайте для правила дополнительные условия.

5. Выберите одно или несколько условий, например **День недели: <день>**:

Измените описание правила в нижней части окна мастера на основе выбранных значений:

Нажмите подчеркнутые пункты, выделенные **жирным курсивом**, чтобы задать для них точное содержимое. Например, при нажатии ссылки **дни** в нашем примере можно выбрать один или несколько дней недели, в которые должно применяться правило.

6. Задайте точные условия и нажмите кнопку **Далее**, чтобы перейти к следующему этапу мастера и выбрать действия, которые должно охватывать правило. В зависимости от содержимого и степени сложности правила может потребоваться указать сведения о дополнительных этапах (например, завершающие события и завершающие действия). Например, если правило предусматривает, что устройство должно выполнить определенное действие в заданный интервал времени (например, в четверг с 08:00 до 10:30), в мастере может отобразиться запрос на указание действия, которое должно быть выполнено по истечении интервала.
7. По умолчанию правило активно после создания, если соблюдены заданные условия. Если вы не хотите, чтобы правило сразу же становилось активным, снимите отметку в поле **Активно**.
8. Нажмите кнопку **Готово**.

Проверка правил

Вы можете проверить содержимое отдельного правила или всех правил одним действием. При создании правил мастер **Управление правилом** следит за тем, чтобы все элементы правила были допустимыми.

Но если правило создано давно, один или несколько его элементов могут быть затронуты другими настройками, и правило может перестать работать. Например, если правило активируется определенным профилем времени, оно перестанет работать, если этот профиль времени будет удален или у вас больше не будет прав доступа к нему. Иногда такие нежелательные последствия настройки трудно заметить.

Проверка правил помогает отслеживать правила, которые могли быть затронуты изменениями. Проверка осуществляется на индивидуальной основе, и каждое правило проверяется само по себе. Проверить несколько правил путем их сравнения друг с другом нельзя (например, чтобы выяснить, противоречит ли одно правило другому), даже если использовать функцию **Проверить все правила**.

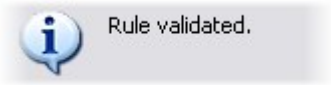
Проверка правила

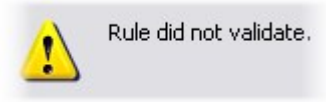
1. Откройте пункт **Правила** и выберите правило, которое требуется проверить.
2. Нажмите правило правой кнопкой мыши и выберите пункт **Проверить правило.**
3. Нажмите кнопку **OK**.

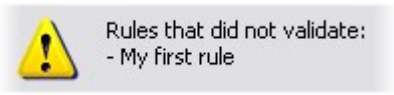
Проверьте все правила

1. Нажмите пункт **Правила** правой кнопкой мыши и выберите **Проверить все правила**.
2. Нажмите кнопку **OK**.

В диалоговом окне отобразится сообщения со сведениями о том, успешно ли завершилась проверка правил. Если вы решили проверить несколько правил, и одно или несколько правил не прошли проверку, в диалоговом окне будут приведены имена соответствующих правил.







Невозможно выявить случаи, когда правило не работает из-за настройки требований, не связанных с самим правилом. Например, если правило указывает, что запись должна включаться при обнаружении движений определенной камерой, оно успешно пройдет проверку, если элементы правила будут настроены правильно, даже если для соответствующей камеры будет отключено обнаружение движений, которое включено на уровне камеры, а не при помощи правил.

Изменение, копирование и переименование правила

1. На панели **Обзор** нажмите соответствующее правило правой кнопкой мыши.
2. Выберите один из вариантов:

   Изменить правило, **Копировать правило** или **Переименовать правило**. Откроется мастер **Управление правилом**.
3. Если выбрать пункт **Копировать правило**, откроется мастер, в котором отображается копия выбранного правила. Нажмите кнопку **Готово**, чтобы создать копию.
4. При выборе пункта **Изменить правило** откроется мастер, и вы можете внести изменения. Нажмите кнопку **Готово**, чтобы принять изменения.
5. При выборе пункта **Переименовать правило** можно изменить текст в имени правила.

Деактивация и активация правила

Система применяет правило при выполнении заданных условий. Это означает, что правило становится активно. При необходимости правила можно деактивировать. При деактивации правила система не применяет правило, даже если выполнены его условия. Деактивированное правило можно активировать позднее.

Деактивация правила

1. На панели **Навигация по сайту** выберите правило.
2. Снимите отметку в поле **Активно** на панели **Свойства**.
3. Нажмите кнопку **Сохранить** на панели инструментов.
4. Значок с красным символом «X» указывает на то, что правило деактивировано в списке **Правила**:

Активация правила

Для повторной активации правила выберите его, а затем поставьте отметку в поле **Активировать** и сохраните настройку.

Указание профиля времени

1. В списке **Профили времени** нажмите пункт **Профили времени** правой кнопкой мыши и выберите **Добавить профиль времени**. Откроется окно **Профиль времени**.
2. В окне **Профиль времени** введите имя нового профиля времени в поле **Имя**. Кроме того, можно ввести описание нового профиля времени в поле **Описание**.

3. В календаре окна **Профиль времени** выберите **День**, **Неделя** или **Месяц**, а затем нажмите область календаря правой кнопкой мыши и выберите **Добавить разовое время** или **Добавить повторяющееся время**.
4. Укажите периоды времени для профиля времени и нажмите кнопку **OK** в окне **Профиль времени**. Система добавит новый профиль времени в список **Профили времени**. Если в дальнейшем потребуется изменить или удалить профиль времени, это можно сделать в списке **Профили времени**.

Добавить разовое время

При выборе пункта **Добавить разовое время** откроется окно **Выбрать время**:

Формат времени и даты в вашей системе может отличаться.

1. В окне **Выбрать время** укажите **Время начала** и **Время окончания**. Если время должно охватывать целые дни, поставьте отметку в поле **Весь день**.
2. Нажмите кнопку **OK**.

Добавить повторяющееся время

При выборе пункта **Добавить повторяющееся время** откроется окно **Выбрать повторяющееся время**:

1. В поле **Выбрать время** укажите интервал времени, периодичность повторения и интервал повторения.
2. Нажмите кнопку **OK**.

Профиль времени может содержать несколько периодов времени. Если в профиль времени необходимо включить дополнительные периоды времени, добавьте другое разовое время или повторяющееся время.

Повторяющееся время

При задании выполнения действия на основе подробного, повторяющегося расписания.

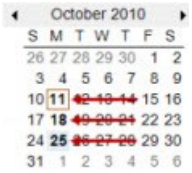
Пример:

- Еженедельно по вторникам каждый 1 час между 15:00 и 15:30
- В 15 день каждые 3 месяца в 11:45
- Ежедневно каждый 1 час между 15:00 и 19:00

Время основано на параметрах локального времени сервера, на котором установлен Management Client.

Изменение профиля времени

1. На панели **Обзор**, в списке **Профили времени**, нажмите соответствующий профиль времени правой кнопкой мыши и выберите пункт **Изменить профиль времени**. Откроется окно **Профиль времени**.
2. Внесите в профиль времени необходимые изменения. После внесения изменений в профиль времени нажмите кнопку **OK** в окне **Профиль времени**. Вы вернетесь в список **Профили времени**.



В окне **Информация о профиле времени** можно внести необходимые изменения в профиль времени. Не забывайте о том, что профиль времени может содержать несколько периодов времени, а периоды времени могут повторяться. В небольшом окне обзора месяца в правом верхнем углу представлено общее представление о периодах времени, которые охватывает профиль времени: даты с указанными моментами времени выделены жирным шрифтом.

В этом примере даты, выделенные жирным шрифтом, указывают, что вы задали периоды времени нескольких дней, а также что вы задали повторяющийся момент времени по понедельникам.

Создание профилей продолжительности светового дня

1. Откройте папку **Правила и события** > **Профили времени**.
2. В списке **Профили времени** нажмите пункт **Профили времени** правой кнопкой мыши и выберите **Добавить профиль продолжительности светового дня**.
3. В окне **Профиль продолжительности светового дня** перейдите к расположенной ниже таблице свойств, чтобы указать необходимую информацию. Для работы в переходный период между светлым и темным временем суток можно настроить смещение времени активации и деактивации профиля. Время и название месяца отображаются на языке, используемом в вашем компьютере/настройках региона.
4. Для просмотра местонахождения введенных географических координат на карте нажмите кнопку **Показать положение в браузере**. Откроется браузер, в котором можно увидеть их местонахождение.
5. Нажмите кнопку **OK**.

Свойства профиля продолжительности светового дня

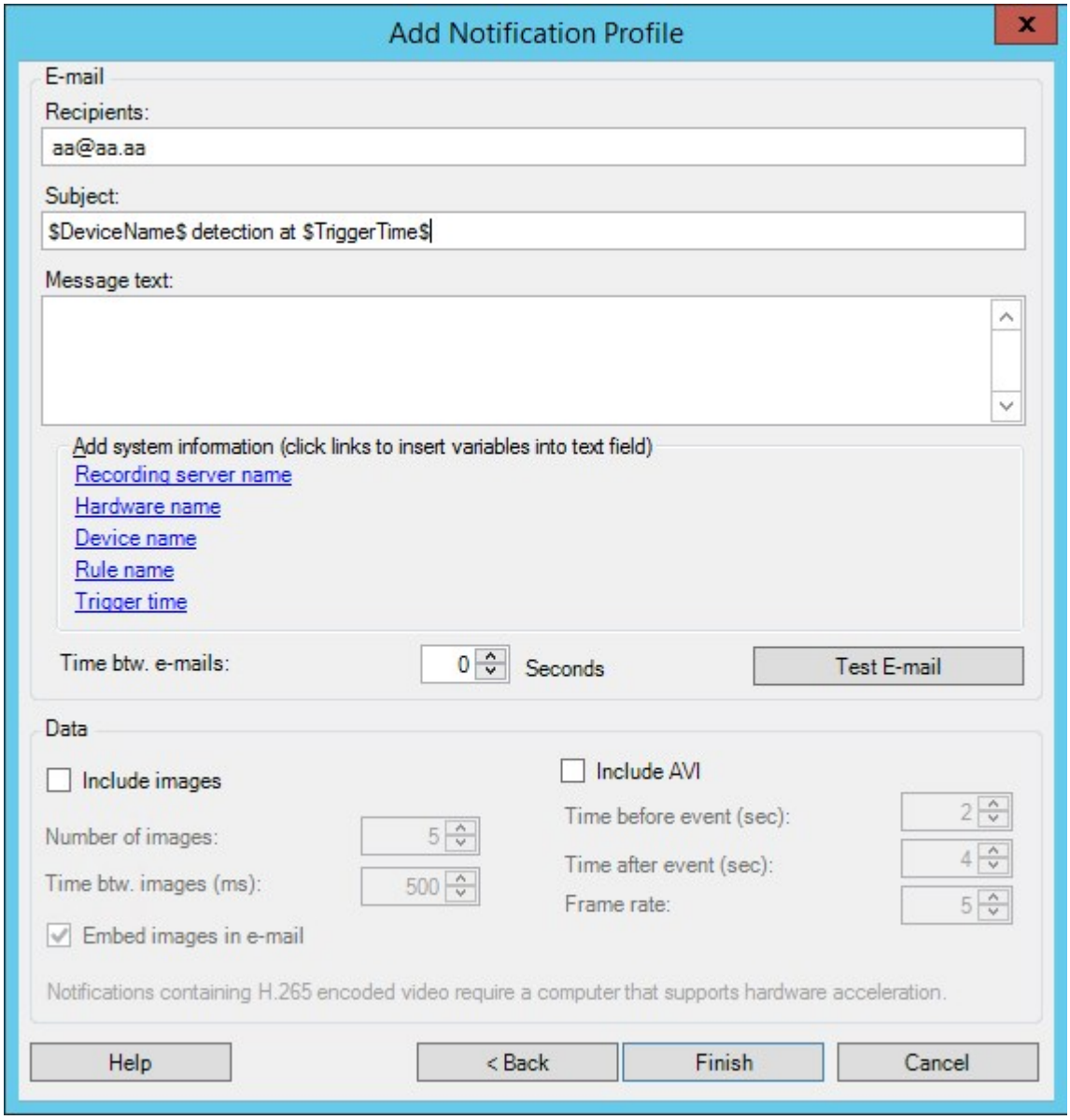
Имя	Описание
Имя	Имя профиля.
Описание	Описание профиля (необязательно).
Координаты	Географические координаты, отражающие физическое местонахождение камер, закрепленных за профилем.
Смещение времени восхода Солнца	Количество минут (+/-), на которое момент активации профиля смещается временем восхода Солнца.
Смещение времени захода Солнца	Количество минут (+/-), на которое момент деактивации профиля смещается временем захода Солнца.
Часовой пояс	Часовой пояс, в котором находятся камеры.

Добавление профилей уведомления

Перед созданием профилей уведомлений необходимо задать настройки почтового сервера для уведомлений по электронной почте. Дополнительные сведения см. в разделе Требования для создания профилей уведомлений.

1. Откройте раздел **Правила и события**, нажмите пункт **Профили уведомлений** правой кнопкой мыши и выберите > **Добавить профиль уведомлений**. Откроется мастер **Добавить профиль уведомлений**.
2. Введите имя и описание. Нажмите **Далее**.

3. Укажите получателя, тему, текст сообщения и время между электронными письмами:



4. Для отправки тестового уведомления по электронной почте указанным получателям нажмите кнопку **Протестировать электронное письмо**.

5. Для включения кадров изображений до сигнала тревоги выберите пункт **Включить изображения** и укажите количество изображений, время между изображениями, а также следует ли вставлять изображения в текст электронных писем.

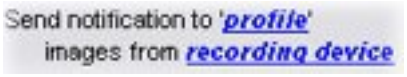
6. Для включения видеоклипов в формате AVI выберите пункт **Включить AVI** и укажите время до события и после него, а также частоту кадров.

> Для уведомлений, содержащих видео с использованием стандарта кодирования H.265, требуется поддержка аппаратного ускорения на компьютере.

7. Нажмите кнопку **Готово**.

Активация уведомлений по электронной почте на основе правил

1. Нажмите пункт **Правила** правой кнопкой мыши, а затем выберите > **Добавить правило** или **Изменить правило**.
2. В мастере **Управление правилом** нажмите **Далее**, чтобы перейти к списку **Выбрать выполняемые действия**, и выберите пункт **Отправить уведомление в <профиль>**.
3. Выберите соответствующий профиль уведомлений, а также камеры, с которых необходимо взять записи, которые будут включены в уведомления для отправки по электронной почте в рамках этого профиля.



Включить записи в отправляемые по электронной почте уведомления профиля можно только в том случае, если запись действительно ведется. Если требуется, чтобы уведомления по электронной почте сопровождались кадрами из видео или видеоклипами в формате AVI, убедитесь, что в правиле задано выполнение записи. Приведенный ниже пример взят из правила, которое включает как действие **Начать запись**, так и действие **Отправить уведомление**:

Добавление пользовательского события

> Независимо от того, как будут использованы пользовательские события, их необходимо добавлять при помощи Management Client.

1. Откройте раздел **Правила и события** > **Пользовательские события**.
2. На панели **Обзор** нажмите раздел **События** правой кнопкой мыши и выберите **Добавить пользовательское событие**.
3. Введите имя нового пользовательского события и нажмите кнопку **OK**. Только что добавленное пользовательское событие появится в списке на панели **Обзор**.

Теперь пользователь может активировать пользовательское событие вручную в XProtect Smart Client, если у него имеются соответствующие разрешения.

Удаление пользовательского события отразится на всех правилах с этим событием. Кроме того, удаленное пользовательское событие перестанет отображаться в XProtect Smart Client только после того, как пользователи XProtect Smart Client выйдут из системы.

Переименование пользовательского события

В случае переименования пользовательского события уже подключенные пользователи XProtect Smart Client должны выйти из системы и войти в нее вновь, чтобы увидеть новое имя.

1. Откройте раздел **Правила и события** > **Пользовательские события**.
2. На панели **Навигация по сайту** выберите пользовательское событие.
3. На панели **Свойства** замените существующее имя.
4. На панели инструментов нажмите кнопку **Сохранить**.

Добавление и изменение события аналитики

Добавление события аналитики

1. Откройте раздел **Правила и события**, нажмите пункт **События аналитики** правой кнопкой мыши и выберите **Добавить новое**.
2. В окне **Свойства** введите имя события в поле **Имя**.
3. При необходимости введите описание в поле **Описание**.
4. На панели инструментов нажмите кнопку **Сохранить**. Для тестирования допустимости события нажмите кнопку **Протестировать событие**. Можно неоднократно исправлять ошибки, выявленные при тесте, а также запускать тест необходимое количество раз и на любом этапе процесса.

Изменение события аналитики

1. Нажмите существующее событие аналитики для просмотра окна **Свойства**, в котором можно изменять соответствующие поля.
2. Для тестирования допустимости события нажмите кнопку **Протестировать событие**. Можно неоднократно исправлять ошибки, выявленные при тесте, а также запускать тест необходимое количество раз и на любом этапе процесса.

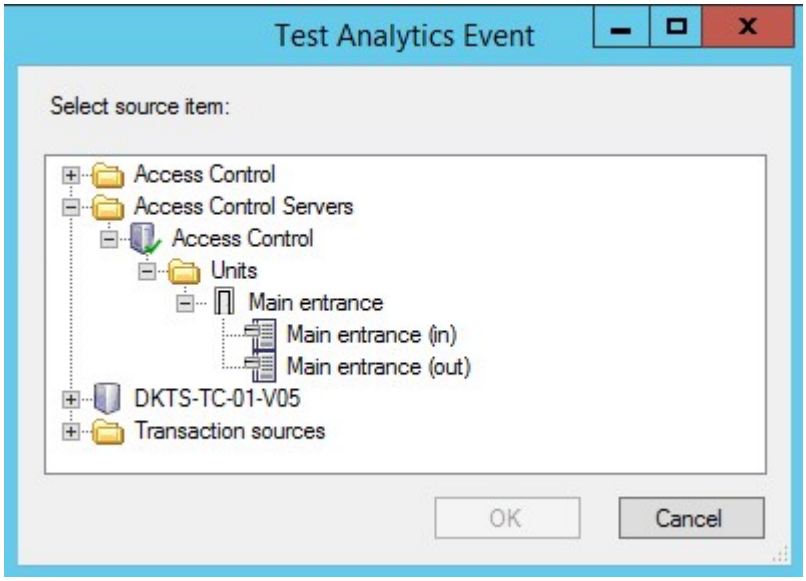
Изменение настроек аналитического события

На панели инструментов перейдите в раздел **Инструменты** > **Параметры** > вкладка **События аналитики**, чтобы изменить соответствующие настройки.

Тестирования события аналитики

После создания события аналитики можно протестировать требования (см. раздел Добавление и изменение события аналитики на стр. 307), например убедиться, что функция событий аналитики включена в Management Client.

1. Выберите существующее событие аналитики.
2. В разделе «Свойства» нажмите кнопку **Протестировать событие**. Откроется окно, в котором отображаются все возможные источники событий.



3. Выберите источник тестового события (например, камеру). Окно закроется, и откроется новое окно с указанием четырех условий, которые должны быть выполнены для срабатывания события аналитики.

В качестве дополнительного теста в XProtect Smart Client можно проверить, было ли событие аналитики отправлено на сервер событий. Для этого откройте XProtect Smart Client и просмотрите событие на вкладке **Диспетчер сигналов тревоги**.

Добавление типичного события

Можно задать типичные события, чтобы помочь ПО для управления видео распознавать конкретные строки в TCP- или UPD-пакетах из внешней системы. На основе типичного события Management Client можно настроить для активации событий, например для начала записи или отправки сигналов тревоги.

Требования
Включение типичных событий и указание допустимых исходных мест назначения. Дополнительные сведения приведены в разделе Вкладка «Типичные события» (параметры) на стр. 436.

Для добавления типичного события:

1. Откройте раздел **Правила и события**.
2. Нажмите раздел **Типичные события** правой кнопкой мыши и выберите пункт **Добавить новое**.
3. Введите необходимую информацию и свойства. Дополнительные сведения приведены в разделе Типичные события и источники данных (свойства) на стр. 558.
4. (дополнительно) Для проверки правильности поискового выражения введите строку поиска в поле **Проверить соответствие выражения строке события**, которое соответствует ожидаемым пакетам:
   - **Соответствует** — строка соответствует поисковому выражению
   - **Не соответствует** — поисковое выражение неверно. Внесите изменения и повторите попытку

В XProtect Smart Client можно проверить, получены ли типичные события сервером событий. Это можно сделать в разделе **Список сигналов тревоги** на вкладке **Диспетчер сигналов тревоги**, выбрав пункт **События**.

Аутентификация

Регистрация заявок от внешнего IDP

1. В Management Client выберите пункт **Инструменты** > **Параметры**, а затем перейдите на вкладку **Внешний IDP**.
2. В разделе **Внешний IDP** выберите **Добавить**.

3. В разделе **Зарегистрированные заявки** выберите пункт **Добавить**.
4. Введите информацию о заявке. Дополнительные сведения см. в разделе Регистрация заявок.

Привязка заявок от внешнего IDP к ролям в XProtect

На сайте внешнего IDP администратор должен создать заявки, состоящие из имени и значения. Впоследствии заявка привязывается к роли в ПО для управления видео, и привилегии пользователя будут определяться этой ролью.

Заявки, которые вы хотите использовать в ролях, необходимо добавить в конфигурацию IDP, прежде чем их можно будет выбрать в ролях. Заявки можно добавить на вкладке **Внешний IDP** диалогового окна **Параметры**. Вкладка «Внешний IDP» (параметры) на стр. 425. Если заявка не добавлена в конфигурацию IDP, вы не сможете выбрать ее в ролях.

При использовании заявок для привязки пользователей внешнего IDP к ролям VMS пользователи внешнего IDP фактически не добавляются к ролям, как обычные базовые пользователи или пользователи AD. Вместо этого они динамически связываются с каждым новым сеансом на основе своих текущих заявок.

1. На панели **Навигация по сайту** в Management Client откройте раздел **Безопасность** и выберите пункт **Роли**.
2. Выберите роль, затем перейдите на вкладку **Внешний IDP** и выберите **Добавить**.
3. Выберите внешнего IDP и имя заявки, а затем введите стоимость заявки.

   Имя заявки следует указывать именно так, как оно указано в информации от внешнего IDP.

4. Нажмите **OK**.

При удалении внешнего IDP также удаляются все пользователи, подключенные к ПО для управления видео через внешнего IDP. Все зарегистрированные заявки, подключенные к внешнему IDP, удаляются, а также удаляются любые привязки к ролям.

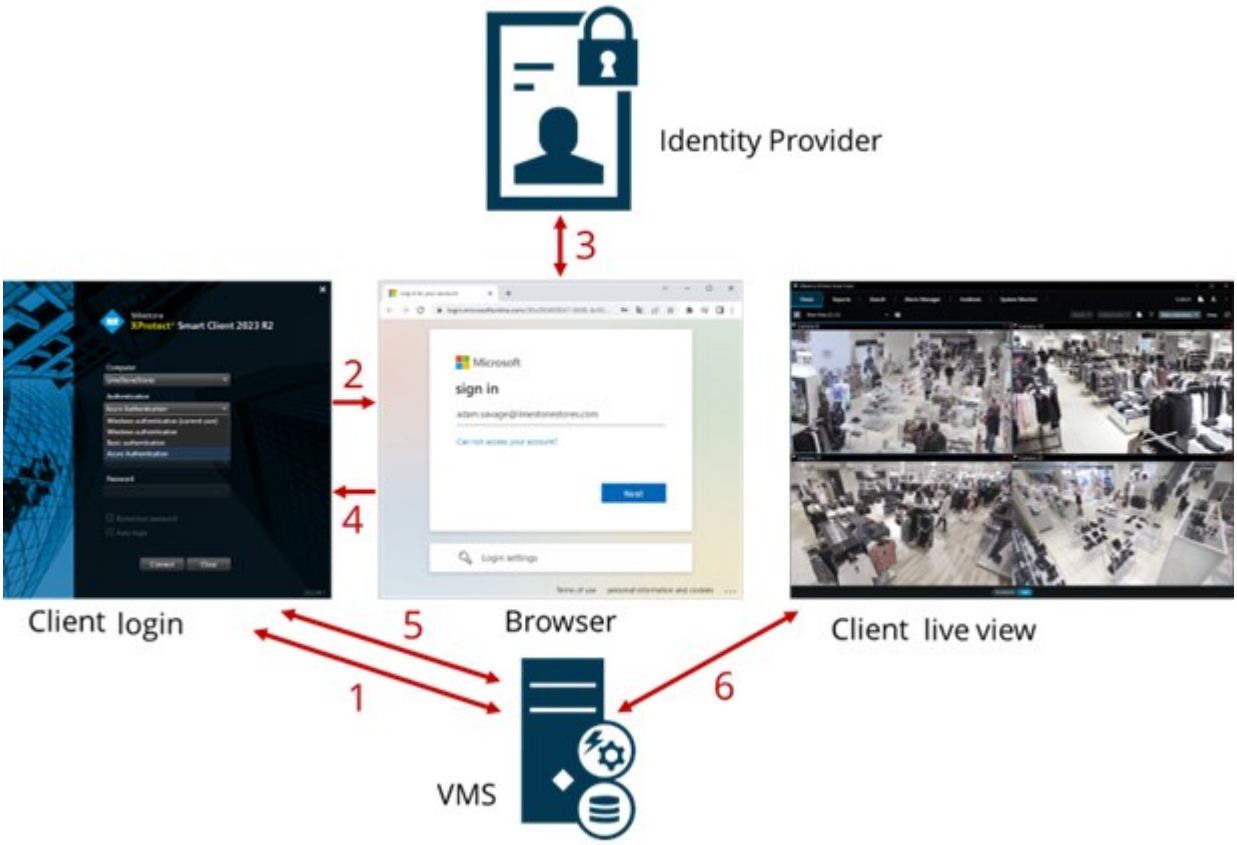
В разделе **Эффективные роли** можно получить обзор динамической роли пользователей внешнего IDP. Это участие в роли, основанное на последнем сеансе входа в систему пользователя внешнего IDP. Дополнительные сведения приведены в разделе Просмотр эффективных ролей на стр. 313.

Войдите систему через внешнего IDP

При помощи внешнего IDP можно войти в клиент XProtect Smart Client, XProtect Management Client, XProtect Web Client и XProtect Mobile.

Аутентификация внешнего IDP

На следующем рисунке представлен обзор процесса аутентификации внешнего IDP. Для иллюстрации процесса аутентификации в потоке используется Microsoft Entra ID (Azure).



1. В поле **Компьютер** в XProtect Smart Client или XProtect Management Client введите адрес компьютера VMS XProtect и выберите внешний IDP в разделе **Аутентификация**. Поля **Имя пользователя** и **Пароль** отключены.
2. Нажмите **Подключить**, чтобы открыть страницу аутентификации внешнего IDP в браузере.
3. На странице аутентификации введите свой адрес электронной почты и нажмите **Далее**.
4. Введите свой пароль и нажмите кнопку входа.
5. Когда вы получите подтверждение того, что аутентификация пользователя прошла успешно, можно закрыть браузер. Клиент VMS продолжает обычный процесс входа в систему, по завершении отображается клиент, и вы входите в систему.

Дополнительные сведения о регистрации в XProtect Web Client см. в разделе Регистрация в системе, а о регистрации в XProtect Mobile — в разделе Регистрация в приложении XProtect Mobile.

В разделе **Инструменты** > **Параметры** > **Внешний IDP** можно настроить имя внешнего IDP, которое отображается в списке **Аутентификация**.

Если внешний IDP отключен в результате, например, восстановления или изменения пароля, вариант регистрации в системе с помощью внешнего IDP в списке **Аутентификация** будет недоступен. Кроме того, если внешний IDP отключен, секрет клиента, полученный от внешнего IDP, перестает отображаться в поле **Секрет клиента** на вкладке **Внешний IDP** в разделе **Инструменты** > **Параметры**.

Безопасность

Добавление правила и его настройка

1. Откройте раздел **Безопасность** и нажмите пункт **Роли** правой кнопкой мыши.
2. Выберите **Добавить роль**. Откроется диалоговое окно **Добавить роль**.
3. Введите имя и описание новой роли и нажмите кнопку **OK**.
4. Новая роль будет добавлена в список **Роли**. По умолчанию с новой ролью не связаны никакие пользователи/группы, но с ней связан ряд профилей по умолчанию.
5. Для выбора различных профилей Smart Client и Management Client, профилей защиты доказательств или профилей времени выберите выпадающие списки.
6. Теперь роли можно назначить пользователей/группы, а также указать, к каким из функций системы они могут получать доступ.

Дополнительные сведения приведены в разделах Назначение ролям пользователей и групп и их удаление из ролей на стр. 313 и Роли (узел «Безопасность») на стр. 561.

Копирование, переименование или удаление роли

Копирование роли

Если у вас имеется роль со сложными настройками и (или) разрешениями, и вам требуется аналогичная или почти аналогичная роль, удобнее скопировать уже существующую роль и внести в нее незначительные изменения, чем создавать роль заново.

1. Откройте раздел **Безопасность**, выберите пункт **Роли**, нажмите соответствующую роль правой кнопкой мыши и выберите пункт **Копировать роль**.
2. В открывшемся диалоговом окне задайте для скопированной роли новое уникальное имя и

описание.

3. Нажмите кнопку **OK**.

Переименование роли

Переименование роли не приводит к изменению имени группы представлений, основанной на этой роли.

1. Откройте раздел **Безопасность** и нажмите пункт **Роли** правой кнопкой мыши .
2. Нажмите требуемую роль правой кнопкой мыши и выберите пункт **Переименовать роль**.
3. В открывшемся диалоговом окне измените имя роли.
4. Нажмите кнопку **OK**.

Удаление роли

1. Откройте раздел **Безопасность** и выберите пункт **Роли**.
2. Нажмите ненужную роль правой кнопкой мыши и выберите пункт **Удалить роль**.
3. Нажмите кнопку **Да**.

Удаление роли не приводит к удалению группы представлений, основанной на этой роли.

Просмотр эффективных ролей

Функция эффективных ролей позволяет просматривать все роли выбранного пользователя или группы. Данная функция полезна при использовании групп и представляет собой единственный способ увидеть, участником каких ролей является конкретный пользователь.

1. Откройте окно **Эффективные роли**, развернув раздел **Безопасность**, а затем нажмите пункт **Роли** правой кнопкой мыши и выберите **Эффективные роли**.
2. Если вам требуется информация о базовом пользователе, введите его имя в поле **Имя пользователя**. Нажмите кнопку **Обновить**, чтобы отобразить роли пользователя.
3. Если используются пользователи или группы Windows в Active Directory, нажмите кнопку обзора **«...»**. Выберите тип объекта, введите имя и нажмите кнопку **OK**. Автоматически отобразятся роли пользователя.

Назначение ролям пользователей и групп и их удаление из ролей

Для назначения пользователей или группы Windows или базовых пользователей, а также их удаления из роли:

1. Откройте раздел **Безопасность** и выберите пункт **Роли**. Затем выберите требуемую роль на панели **Обзор**:
2. На панели **Свойства** перейдите на вкладку **Пользователи и группы** в нижней части окна.
3. Нажмите **Добавить**, выберите **Пользователь Windows** или**Базовый пользователь**.

Назначение роли пользователей и групп Windows

1. Выберите пункт **Пользователь Windows**. Откроется диалоговое окно **Выбрать пользователей**, **Компьютеры и группы**:
2. Убедитесь, что указан требуемый тип объекта. Если, например, требуется добавить компьютер, нажмите **Типы объектов** и выберите пункт **Компьютер**. Также убедитесь, что в поле **Из этого местонахождения** указан требуемый домен. В противном случае нажмите **Местонахождения**, чтобы найти требуемый домен.
3. В окне **Укажите выбираемые имена объектов** введите соответствующие имена пользователей, инициалы или другие типы идентификаторов, которые может распознавать Active Directory. Чтобы убедиться, что Active Directory распознает введенные вами имена или инициалы, воспользуйтесь функцией **Проверить имена**. В качестве альтернативы, воспользуйтесь функцией **«Дополнительно...»**, чтобы найти пользователей или группы.
4. Нажмите кнопку **ОК**. Теперь выбранные пользователи/группы добавлены в расположенный на вкладке **Пользователи и группы** список пользователей, которых вы назначили выбранной роли. Можно добавить больше пользователей и групп, если ввести несколько имен, разделенных точкой с запятой (;).

Назначение роли базовых пользователей

1. Выберите пункт **Базовый пользователь**. Откроется диалоговое окно **Выбрать базовых пользователей для добавления к роли**:
2. Выберите базовых пользователей, которых вы хотите назначить этой роли.
3. Дополнительно: Нажмите кнопку **Новый**, чтобы создать нового базового пользователя.
4. Нажмите кнопку **ОК**. Теперь выбранные базовые пользователи добавлены в расположенный на вкладке **Пользователи и группы** список базовых пользователей, которых вы назначили выбранной роли.

Удаление пользователей и групп из роли

1. На вкладке **Пользователи и группы** выберите пользователя или группу, которых необходимо удалить, и нажмите кнопку **Удалить** в нижней части вкладки. При необходимости можно выбрать несколько пользователей или групп либо сочетание групп и отдельных пользователей.
2. Подтвердите, что вы хотите удалить выбранных пользователей и (или) группы. Нажмите кнопку **Да**.

Также у пользователя могут быть роли, заданные при помощи членства в группах. В таком случае отдельного пользователя удалить из роли невозможно. Также члены групп могут иметь роли как отдельные лица. Чтобы определить, какие роли имеются у пользователей, групп или отдельных членов групп, воспользуйтесь функцией **Просмотреть эффективные роли**.

Создание базовых пользователей

В VMS Milestone XProtect существует два типа учетных записей пользователей: базовый пользователь и пользователь Windows.

Базовыми пользователями являются учетные записи пользователей, создаваемые в VMS Milestone XProtect. Это специальная системная учетная запись пользователя, предусматривающая аутентификацию на основе пароля и имени базового пользователя для отдельных пользователей.

Пользователи Windows — это учетные записи пользователей, добавляемые через Microsoft Active Directory.

Между базовыми пользователями и пользователями Windows есть несколько различий:

- Аутентификация базовых пользователей выполняется по комбинации имени пользователя и пароля, они создаются только для одной системы или сайта. Учтите, что даже если у базового пользователя на одном федеративном сайте то же имя и пароль, что у базового пользователя на другом федеративном сайте, базовый пользователь имеет доступ только к сайту, на котором он был создан.
- Аутентификация пользователей Windows в основана на имени для входа Windows, и они привязаны к компьютеру.

Настройка параметров входа в систему для базовых пользователей

Задать параметры входа в систему для базовых пользователей можно в файле JSON, который находится здесь: `\\Program Files\Milestone\Management Server\IIS\IDP\appsettings.json`.

В этом файле можно задать следующие параметры:

LoginSettings	
"ExpireTimeInMinutes": 5	Задает период времени (в минутах), по истечении которого сеанс прекращается, если пользователь неактивен.
LockoutSettings	

"LockoutTimeSpanInMinutes": 5	Задает продолжительность периода блокировки пользователя.
"MaxFailedAccessAttempts": 5	Задает количество предоставляемых пользователю попыток входа в систему, после которых он будет заблокирован.
PasswordSettings	
"RequireDigit": true	Определяет, требуется ли включать в пароль цифры (от 0 до 9).
"RequireLowercase": true	Определяет, требуется ли включать в пароль строчные буквы.
"RequireNonAlphanumeric": true	Определяет, требуется ли включать в пароль специальные символы (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/).
"RequireUppercase": true	Определяет, требуется ли включать в пароль прописные буквы.
"RequiredLength": 8	Задает обязательное количество символов в пароле. Минимальная длина пароля — {0} символов, а максимальная длина пароля — 255 символов.
"RequiredUniqueChars": 1	Задает минимальное обязательное количество уникальных символов в пароле. Например, если требуемое количество уникальных символов — 2, то пароли вида aaaaaa, aa, a, b, bb или bbbbbbb будут считаться недопустимыми. При этом пароли вида abab, abc, aaab и так далее будут допустимыми, так как в пароле есть не менее двух уникальных символов. Увеличение количества уникальных символов в пароле повышает его надежность, так как в нем будут отсутствовать легко угадываемые повторяющиеся последовательности.

Для создания в системе базового пользователя:

1. Разверните узел **Безопасность** > **Базовые пользователи**.
2. На панели **Базовые пользователи** щелкните правой кнопкой мыши и выберите **Создать базового пользователя**.

3. Укажите имя пользователя и пароль. Повторите пароль, чтобы убедиться, что ввели его правильно.

   Пароль должен отвечать требованиям к сложности, как определено в файле **appsettings.json** (см. Настройка параметров входа в систему для базовых пользователей на стр. 315).

4. Укажите, должен ли базовый пользователь сменить пароль при следующем входе в систему. Milestone рекомендует установить этот флажок, чтобы базовые пользователи могли задавать собственные пароли при первом входе в систему.

   Снимите этот флажок, только если создаете базовых пользователей, которым запрещено менять пароли. К таким базовым пользователям относятся, например, системные пользователи, которые используются для аутентификации служб серверов и встраиваемых расширений.

5. Укажите состояние базового пользователя: **Включено** или **Заблокировано**.

6. Нажмите кнопку **OK**, чтобы создать базового пользователя.

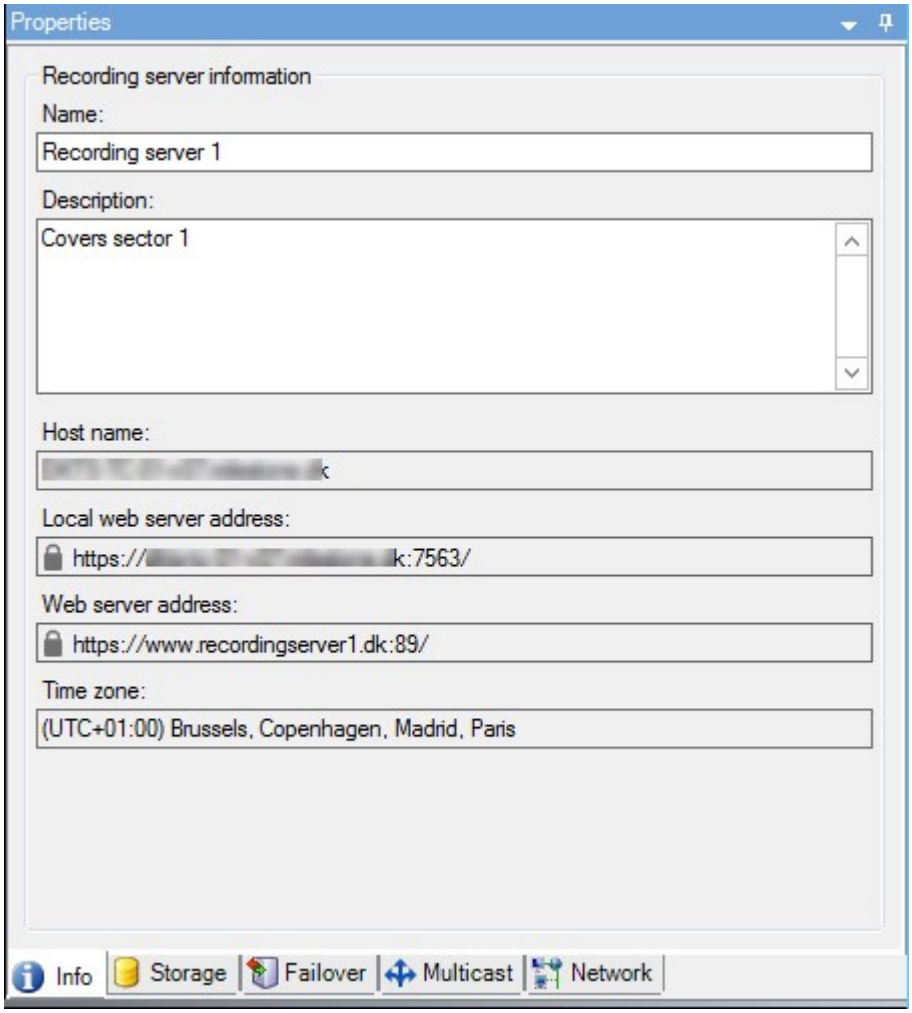
Просмотр состояния шифрования при подключении к клиентам

Для того чтобы проверить, использует ли сервер записи шифрование подключений:

1. Откройте Management Client.

2. На панели **Навигация по сайту** выберите пункт **Серверы** > **Серверы записи**. Откроется список серверов записи.

3. На панели **Обзор** выберите требуемый сервер записи и перейдите на вкладку **Сведения**.
   Если включено шифрование подключений к клиентам и серверам, которые получают потоки данных от сервера записи, перед локальным адресом веб-сервера и дополнительным адресом веб-сервера отображается значок замка.



Информационная панель системы

Просмотр задач, выполняющихся на серверах записи

В окне **Текущие задачи** показан обзор текущих задач для выбранного сервера записи. Если вы запустили задачу, которая занимает много времени и выполняется в фоновом режиме, вы можете открыть окно **Текущие задачи** и проверить ход ее выполнения. К длительным задачам, запускаемым пользователем, относятся, например, обновления прошивки и перемещение оборудования. В окне доступна информация о времени начала, примерном времени завершения и ходе выполнения задачи.

Если задача выполняется ненадлежащим образом, возможной причиной могут быть оборудование или сеть. Например, причиной может быть остановка сервера, возникновение ошибки на сервере, недостаточная пропускная способность или прерывание подключения.

1. На панели **Навигация по сайту** выберите пункт **Информационная панель системы** > **Текущие задачи**.
2. Выберите сервер записи, чтобы просмотреть его текущие задачи.

Сведения в окне **Текущие задачи** не обновляются динамически. Это скорее снимок состояния текущих задач на момент открытия окна. Если окно оставалось открытым в течение какого-то времени, обновите данные, нажав кнопку **Обновить** в нижнем правом углу окна.

Системный монитор (объяснение)

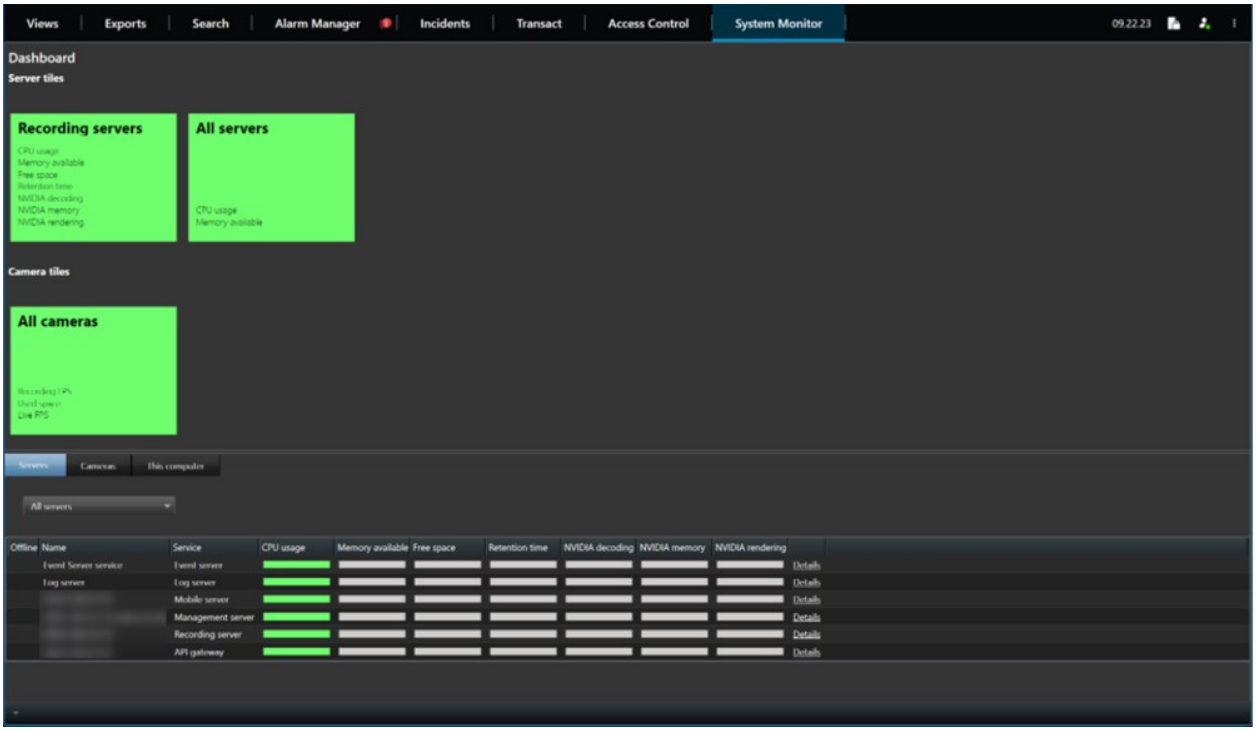
Функция системного монитора требует, чтобы была запущена служба Data Collector, и работает только на компьютерах, в которых используется григорианский (западный) календарь.

Информационная панель системного монитора (объяснение)

В **информационной панели системного монитора** представлен обзор работоспособности вашей VMS-системы. Состояние оборудование визуально представлено плитками и их цветами: зеленый (выполняется), желтый (предупреждение) и красный (критическое состояние). На плитках также могут отображаться значки ошибок или предупреждений в случае неисправности одной или нескольких единиц оборудования.

По умолчанию система отображает плитки, обозначающие **Серверы записи**, **Все серверы** и **Все камеры**. Кроме того, можно настроить параметры мониторинга плиток, используемых по умолчанию, а также создать новые плитки. Например, можно настроить плитки, обозначающие отдельный сервер, отдельную камеру, группу камер или группу серверов.

Параметры мониторинга — это, например, уровень использования центрального процессора или объем памяти, доступной для сервера. Плитка отслеживает только добавленные в нее параметры мониторинга. Дополнительные сведения приведены в разделах Добавление новой плитки камеры или сервера в информационную панель системного монитора на стр. 323, Изменение плитки камеры или сервера в информационной панели системного монитора на стр. 323 и Удаление плитки камеры или сервера из информационной панели системного монитора на стр. 324.



Пороговые значения системного монитора (объяснение)

Используя пороговые значения системного монитора, можно задать и скорректировать пороговые значения изменения состояния оборудования, визуально отображаемого на плитках в **информационной панели системного монитора**. Например, при изменении состояния загрузки ЦП сервера с нормального (зеленый цвет) на состояние предупреждения (желтый цвет) или с состояния предупреждения (желтый цвет) на критическое состояние (красный цвет).

Для оборудования одного и того же типа в системе настроены пороговые значения по умолчанию, поэтому можно приступать к мониторингу состояния системного оборудования сразу же после установки системы и добавления оборудования. Можно настроить пороговые значения для отдельных серверов, камер, дисков и хранилищ. Сведения об изменении пороговых значений см. в разделе Изменение пороговых значений, задающих моменты изменения состояния оборудования на стр. 324.

Чтобы состояние **Критическое** или **Предупреждение** не отображалось в случаях, когда уровень использования системного оборудования или нагрузки на него достигает высокого порогового значения лишь на несколько секунд, используйте **Интервал расчета**. При правильно заданном интервале расчета вы не будете получать ложные оповещения о превышении пороговых значений. Вам будут приходить оповещения только о постоянно возникающих проблемах, (например, об использовании центрального процессора или потреблении памяти).

Также можно настроить правила (см. раздел Правила (объяснение)), которые будут выполнять конкретные действия или активировать сигналы тревоги, при переходе порогового значения из одного состояния в другое.

Просмотрите текущее состояние оборудования и при необходимости устраните неполадки.

В **информационной панели системного монитора** представлен обзор работоспособности вашей VMS-системы. Состояние оборудование визуально представлено плитками и их цветами: зеленый (выполняется), желтый (предупреждение) и красный (критическое состояние). На плитках также могут отображаться значки ошибок или предупреждений в случае неисправности одной или нескольких единиц оборудования.

Пороговые значения для этих трех состояний задаются пользователем. Дополнительные сведения приведены в разделе Изменение пороговых значений, задающих моменты изменения состояния оборудования на стр. 324.

Информационная панель системного монитора позволяет ответить на такие вопросы, как: Работают ли все службы серверов и камеры? Достаточен ли уровень использования центрального процессора и доступной памяти различных серверов для того, чтобы вся нужная информация записывалась и была доступной для просмотра?

1. На панели **Навигация по сайту** выберите **Информационная панель системы** > **Системный монитор**.
2. Если все плитки зеленого цвета, и на них отсутствуют значки предупреждения или ошибки, все параметры мониторинга и все серверы и камеры, обозначаемые плитками, работают нормально.
   Если на одной или нескольких плитках есть значок предупреждения или ошибки, или если они полностью желтого или красного цвета, выберите одну из этих плиток для устранения неполадок.
3. В списке оборудования с параметрами мониторинга (в нижней части окна) найдите неработающее оборудование. Поместите курсор мыши над значком красного креста рядом с названием оборудования, чтобы прочитать, в чем состоит проблема.
4. При желании можно выбрать пункт **Сведения** справа от названия оборудования, чтобы узнать, как давно возникла проблема. Включите сбор исторических данных, чтобы наблюдать за состоянием оборудования в динамике по времени. Дополнительные сведения приведены в разделе Сбор исторических данных о состояниях оборудования на стр. 322.
5. Найдите способ решить проблему. Например, перезагрузка компьютера, перезагрузка службы сервера, замена неисправного оборудования и так далее.

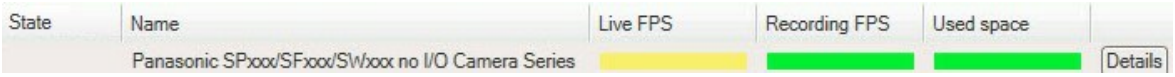
Просмотр исторических данных о состоянии оборудования и печать отчета

При помощи функции **Системный монитор** можно получить комплексное представление о работоспособности программной системы для управления видео. Кроме того, можно получить данные за длительный период.

Бывают ли ситуации, в которых уровни использования центрального процессора, пропускной способности или другого оборудования достигают опасных значений? Найдите ответ на этот вопрос с помощью системного монитора и решите, требуется ли обновить оборудование или приобрести новое, чтобы проблема не повторялась.

Не забудьте включить сбор исторических данных. См. раздел Сбор исторических данных о состояниях оборудования на стр. 322.

1. На панели **Навигация по сайту** выберите **Информационная панель системы** > **Системный монитор**.
2. В окне **Системный монитор** выберите плитку с оборудованием, в отношении которого требуется получить исторические данные о работоспособности, или выберите сервер или камеру в нижней части окна.
3. Выберите пункт **Подробнее** справа от названия соответствующего сервера или камеры.



4. Применительно к серверам, выберите пункт **История** справа от названия оборудования, которое требуется проанализировать. Применительно к камерам, нажмите на ссылку.
5. Если требуется распечатать отчет, выберите значок «PDF».

Создать исторические отчеты можно только с данными того сервера записи, на котором в настоящий момент находится оборудование.

Если вы получаете доступ к данным системного монитора из операционной системы сервера, может появляться сообщение о **конфигурации усиленной безопасности Internet Explorer**. Перед продолжением выполните инструкции по добавлению страницы **системного монитора** в **зону надежных сайтов**.

Сбор исторических данных о состояниях оборудования

Сбор исторических данных о системном оборудовании можно включить для создания графиков с состоянием оборудования в динамике по времени и печати отчета. Дополнительные сведения приведены в разделе Просмотр исторических данных о состоянии оборудования и печать отчета на стр. 321.

1. На панели **Навигация по сайту** выберите **Информационная панель системы** > **Системный монитор**.
2. В окне **Системный монитор** выберите пункт **Настроить**.

3. В открывшемся окне **Настроить информационную панель** выберите пункт **Собирать исторические данные**.
4. Выберите интервал выборки. Чем короче интервал, тем значительнее нагрузка на базу данных SQL Server, пропускную способность или другое оборудование. Также интервал выборки исторических данных определяет степень детализации графиков.

Добавление новой плитки камеры или сервера в информационную панель системного монитора

Если вы хотите отслеживать камеры или серверы небольшими группами в зависимости от их физического местонахождения или отслеживать оборудование с различными параметрами мониторинга, в окно **Системный монитор** можно добавить дополнительные плитки.

1. На панели **Навигация по сайту** выберите **Информационная панель системы** > **Системный монитор**.
2. В окне **Системный монитор** выберите пункт **Настроить**.
3. В открывшемся окне **Настройка информационной панели** выберите пункт **Новая** в разделе **Плитки сервера** или **Плитки камеры**.
4. В окне **Новая плитка сервера/новая плитка камеры** выберите камеры или серверы, которые требуется отслеживать.
5. В разделе **Параметры мониторинга** поставьте или снимите отметки в полях параметров, которые необходимо добавить к плитке или удалить из нее.
6. Нажмите **OK**. Теперь новая плитка сервера или камеры добавлена к плиткам, отображаемым в информационной панели.

Изменение плитки камеры или сервера в информационной панели системного монитора

Если вы хотите отслеживать камеры или серверы с использованием других параметров мониторинга, их можно скорректировать.

1. На панели **Навигация по сайту** выберите **Информационная панель системы** > **Системный монитор**.
2. В окне **Системный монитор** выберите пункт **Настроить**.
3. В открывшемся окне **Настроить информационную панель** выберите плитку, которую необходимо изменить, в разделе **Плитки сервера** или **Плитки камеры**, а затем выберите пункт **Изменить**.
4. В окне **Изменить плитку сервера/камеры в информационной панели** выберите все камеры или серверы, группу камер или серверов или отдельные камеры или серверы, параметры

мониторинга которых требуется изменить.

5. В разделе **Параметры мониторинга** выберите параметры, которые требуется отслеживать.
6. Нажмите **OK**.

Удаление плитки камеры или сервера из информационной панели системного монитора

Если вам больше не требуется отслеживать оборудование, представленного плиткой, ее можно удалить.

1. На панели **Навигация по сайту** выберите **Информационная панель системы** > **Системный монитор**.
2. В окне **Системный монитор** выберите пункт **Настроить**.
3. В открывшемся окне **Настроить информационную панель** выберите плитку, которую необходимо изменить, в разделе **Плитки сервера** или **Плитки камеры**.
4. Выберите **Удалить**.

Изменение пороговых значений, задающих моменты изменения состояния оборудования

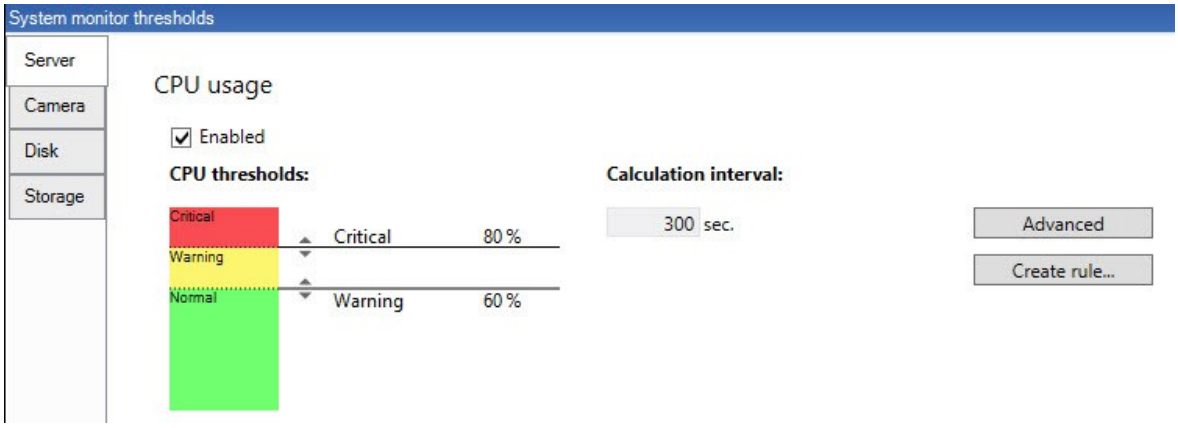
Можно изменить пороговые значения, задающие моменты перехода оборудования на **Информационной панели системного монитора** из одного из трех состояний в другое. Дополнительные сведения приведены в разделе Пороговые значения системного монитора (объяснение) на стр. 320.

Пороговые значения можно изменять для различных типов оборудования. Дополнительные сведения приведены в разделе Пороговые значения системного монитора (узел «Информационная панель системы») на стр. 629.

По умолчанию в системе настроено отображение пороговых значений для всех единиц одного и того же типа оборудования (например, всех камер или серверов). Пороговые значения по умолчанию можно изменить.

Также можно задать пороговые значения для отдельных серверов, камер или набора этих устройств, чтобы, например, в некоторых камерах использовалась более высокая **Частота кадров трансляции** или **Частота кадров записи**, чем в других камерах.

1. На панели **Навигация по сайту** выберите **Информационная панель системы** > **Пороговые значения системного монитора**.
2. Поставьте отметку в поле **Включено** для соответствующего оборудования, если она еще не поставлена. На приведенном ниже рисунке показан пример.



3. Потяните ползунок регулятора порогового значения вверх или вниз, чтобы уменьшить или увеличить пороговое значение. Для каждой единицы оборудования, отображаемой в регуляторе порогового значения, имеются два ползунка, разделяющие состояния **Нормальное**, **Предупреждение** и **Критическое**.
4. Введите значение интервала расчета или оставьте значение по умолчанию.
5. Если необходимо задать значения для отдельных единиц оборудования, выберите пункт **Дополнительно**.
6. Если необходимо задать правила для определенных событий или в рамках конкретных интервалов времени, выберите пункт **Создать правило**.
7. Завершите установку пороговых значений и интервалов расчета, а затем выберите пункт **Файл** > **Сохранить** в меню.

Просмотр защиты доказательств в системе

В разделе **Защита доказательств** узла **Информационная панель системы** содержится обзор всех защищенных данных текущей системы наблюдения.

Найдите защиту доказательств, применив фильтр по автору или времени создания.

1. На панели **Навигация по сайту** выберите пункт **Информационная панель системы** > **Защита доказательств**.
2. Изучите обзорный раздел и найдите соответствующую защиту доказательств. Различные метаданные, связанные с защитой доказательств, можно использовать для применения фильтров и сортировки.

Вся информация, отображаемая в окне **Защита доказательств**, представляет собой снимки. Нажмите F5 для обновления информации.

Печать отчета с конфигурацией системы

При установке и настройке ПО для управления видео (VMS) вы задаете много параметров: возможно, их потребуется задокументировать. Кроме того, по прошествии времени бывает трудно вспомнить, какие именно параметры вы изменяли с момента установки и первоначальной настройки или даже за последние месяцы. Именно поэтому в системе есть возможность напечатать отчет со всеми настроенными параметрами.

При создании отчета о конфигурации (в формате PDF) в него можно добавить любые существующие элементы системы. Например, можно включить в него сведения о лицензиях, настройках устройств, настройках сигналов тревоги, а также многое другое. Для создания отчета, соответствующего требованиям GDPR, можно включить параметр **Исключить конфиденциальные данные** (он включен по умолчанию). Также можно настроить шрифт, формат страницы и титульный лист.

1. Откройте раздел **Информационная панель системы** и выберите пункт **Отчеты о конфигурации**.
2. Выберите элементы, которые требуется включить в отчет или исключить из него.
3. **Дополнительно**: Если вы решили включить титульный лист, выберите пункт **Титульный лист**, чтобы настроить информацию, отображаемую на титульном листе. В появившемся окне укажите необходимые сведения.
4. Выберите пункт **Форматирование** для настройки шрифта, размера страницы и полей. В появившемся окне выберите требуемые настройки.
5. Когда подготовка к экспорту будет завершена, нажмите кнопку **Экспортировать** и выберите имя отчета и место его сохранения.

Отчеты о конфигурации могут создавать только пользователи с административными разрешениями в программной системе для управления видео.

Метаданные

Отображение или скрытие категорий поиска по метаданным и фильтров поиска

Пользователи XProtect Management Client, имеющие административные разрешения, могут отображать или скрывать используемые по умолчанию категории поиска по метаданным в Milestone и фильтры поиска в XProtect Smart Client. По умолчанию эти категории поиска и фильтры поиска скрыты. Их полезно отображать, если система видеонаблюдения соответствует требованиям (см. раздел Требования для поиска по метаданным на стр. 636).

Эта настройка влияет на всех пользователей XProtect Smart Client.

Эта настройка не влияет на видимость:

- Других, не связанных с метаданными категорий поиска и фильтров поиска Milestone, например **Движение**, **Отметки**, **Сигналы тревоги** и **События**.
- Сторонние категории поиска и фильтры поиска

1. На панели **Навигация по сайту** XProtect Management Client выберите пункт **Использование метаданных**> **Поиск метаданных**.
2. На панели **Поиск по метаданным** выберите категорию поиска, для которой требуется изменить настройки видимости.
3. Чтобы отобразить категорию поиска или фильтр поиска, поставьте отметку в соответствующем поле. Чтобы скрыть категорию поиска или фильтр поиска, снимите отметку.

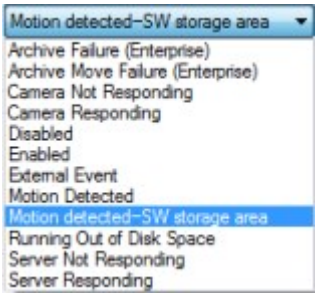
Сигналы тревоги

Добавление сигнала тревоги

Чтобы задать сигнал тревоги, необходимо создать определение тревоги. В нем указывается, к примеру, что активирует сигнал тревоги, инструкции для оператора, а также информация о том, что останавливает сигнал тревоги или когда это происходит. Дополнительные сведения о настройках приведены в разделе Определения тревог (узел «Сигналы тревоги»).

1. На панели **Навигация по сайту** разверните узел **Сигналы тревоги** и нажмите **Определение тревоги** правой кнопкой мыши.
2. Выберите **Добавить новые**.

3. Заполните перечисленные свойства:
   - **Имя**: Введите имя определения сигнала тревоги. Имя определения тревоги отображается, если определение тревоги находится в списке.
   - **Инструкции**: Здесь можно написать инструкции для оператора, который получит сигнал тревоги.
   - **Событие срабатывания**: С помощью раскрывающихся меню выберите тип события и сообщение, которое будет отображаться при срабатывании сигнала тревоги.

     Список возможных событий срабатывания. Выделенный вариант создан и настроен с помощью событий аналитики.
   - **Источники**: Выберите камеры или другие устройства, события которых будет активировать сигнал тревоги. Возможные варианты зависят от типа выбранного вами события.
   - **Профиль времени**: Чтобы активировать сигнал тревоги в определенный интервал времени, установите переключатель, а затем выберите профиль времени в раскрывающемся меню.
   - **На основе события**: чтобы активировать определение тревоги по событию, установите переключатель и укажите событие, запускающее определение тревоги. Также укажите событие, которое отключает определение тревоги.
4. В раскрывающемся меню **Ограничение по времени** задайте период времени, в течение которого оператор должен предпринять необходимые действия.
5. В раскрывающемся меню **События запущены** задайте событие, которое должно сработать по истечении установленного времени.
6. Настройте дополнительные параметры, такие как связанные камеры и первоначальный владелец сигнала тревоги.

Изменение разрешений для отдельных определений тревог

Если вы хотите, чтобы только определенные пользователи могли просматривать сигналы тревоги и управлять ими, измените разрешения для определения тревоги в XProtect Management Client. Таким образом обеспечиваются следующие условия:

- Пользователи получают только актуальные для них сигналы.
- Неавторизованные пользователи не могут реагировать на сигналы тревоги.

Используйте роли для объединения пользователей, которые наделяются одинаковыми правами для определений тревог.

Чтобы изменить разрешения для определения тревоги, выполните следующие действия:

1. На панели **Навигация по сайту** разверните узел **Безопасность** и выберите роль, разрешения которой вы хотите изменить.
2. Откройте вкладку **Сигналы тревоги** и разверните узел **Определения тревоги**, чтобы просмотреть список заданных вами сигналов тревоги.
3. Выберите определение тревоги, чтобы изменить соответствующие разрешения.

Включение шифрования

Включить шифрование при передаче на сервер управления и из него

Можно настроить шифрование обмена данными между сервером управления и службой Data Collector, присоединяемой при наличии удаленного сервера следующего типа:

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Если в системе есть несколько серверов записи или удаленных серверов, шифрование необходимо включить для всех таких серверов.

При настройке шифрования для группы серверов его необходимо включить, используя сертификат, принадлежащий тому же сертификату ЦС, или, если шифрование отключено, отключить его на всех компьютерах в группе серверов.

Предварительные условия

- Для сертификата аутентификации сервера необходимо настроить доверие на компьютере, где размещается сервер управления.

Прежде всего, включите шифрование на сервере управления.

Действия:

1. На компьютере с установленным сервером управления откройте **Server Configurator** из:

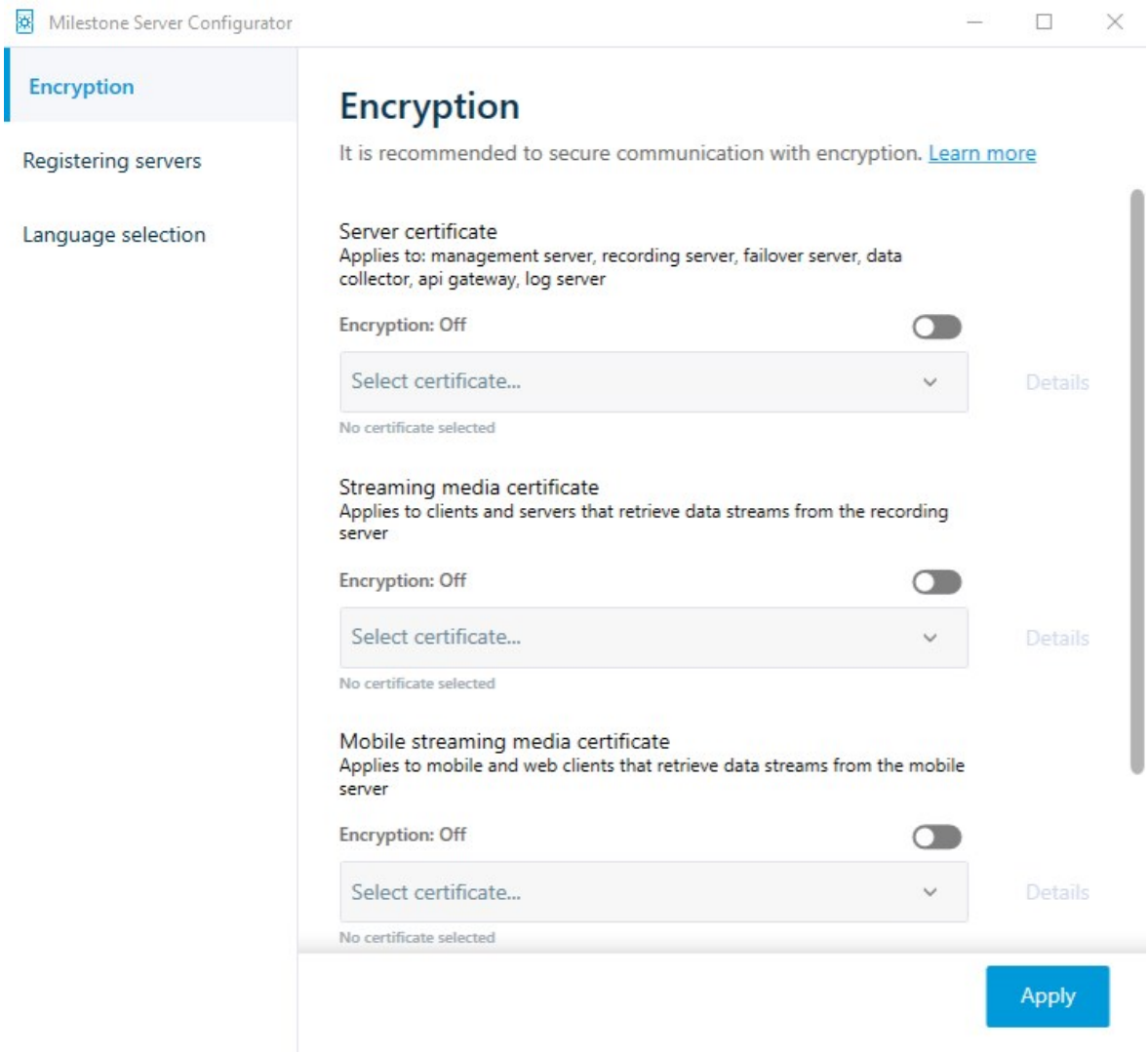
   - меню «Пуск» Windows

   или

   - Management Server Manager, щелкнув значок Management Server Manager на панели задач компьютера правой кнопкой мыши.

2. В **Server Configurator** в разделе **Сертификат сервера** включите **Шифрование**.
3. Нажмите **Выбрать сертификат**, чтобы открыть список с уникальными именами субъектов сертификатов с закрытыми ключами, которые установлены на локальном компьютере в хранилище сертификатов Windows.
4. Выберите сертификат для шифрования обмена данными между сервером записи, сервером управления, сервером отказоустойчивости и Data Collector server.

   Выберите **Сведения**, чтобы просмотреть информацию о выбранном сертификате из хранилища сертификатов Windows.



5. Нажмите кнопку **Применить**.

Чтобы завершить настройку шифрования, выполните следующий шаг — обновите параметры шифрования на каждом сервере записи и каждом сервере, где установлена Data Collector (Event Server, Log Server, LPR Server, и Mobile Server).

Дополнительные сведения приведены в разделе Включить шифрование сервера для серверов записи или удаленных серверов на стр. 331.

Включить шифрование сервера для серверов записи или удаленных серверов

Вы можете настроить шифрование двусторонних подключений между сервером управления и сервером записи или другими удаленными серверами, использующими Data Collector.

Если в системе есть несколько серверов записи или удаленных серверов, шифрование необходимо включить для всех таких серверов.

Дополнительные сведения см. в руководстве по сертификатам, посвященном защите систем XProtect VMS.

При настройке шифрования для группы серверов его необходимо включить, используя сертификат, принадлежащий тому же сертификату ЦС, или, если шифрование отключено, отключить его на всех компьютерах в группе серверов.

Предварительные условия

- Включено шифрование на сервере управления, см. Включить шифрование при передаче на сервер управления и из него на стр. 329.

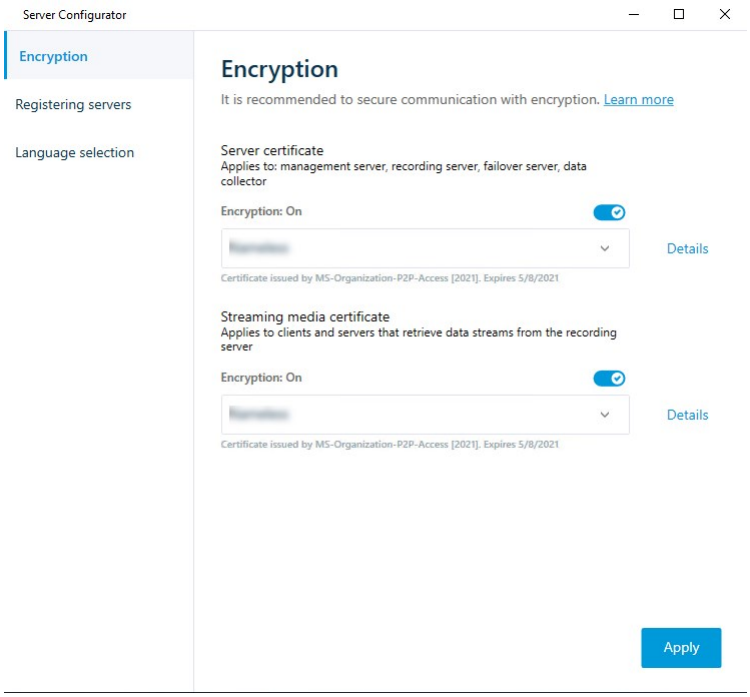
1. На компьютере с Management Server или Recording Server откройте **Server Configurator** из:
   - меню «Пуск» Windows

   или

   - диспетчера серверов, щелкнув значок этого диспетчера на панели задач компьютера правой кнопкой мыши.
2. В **Server Configurator** в разделе **Сертификат сервера** включите **Шифрование**.
3. Нажмите **Выбрать сертификат**, чтобы открыть список с уникальными именами субъектов сертификатов с закрытыми ключами, которые установлены на локальном компьютере в хранилище сертификатов Windows.
4. Выберите сертификат для шифрования обмена данными между сервером записи, сервером управления, сервером отказоустойчивости и сервером Data Collector.

   Выберите **Сведения**, чтобы просмотреть информацию о выбранном сертификате из хранилища сертификатов Windows.

   Пользователю сервиса Recording Server предоставлен доступ к закрытому ключу. Для этого сертификата необходимо настроить доверие на всех клиентах.



5. Нажмите кнопку **Применить**.

Когда вы примените сертификаты, сервер записи будет остановлен и перезапущен. Остановка службы Recording Server означает, что, пока вы проверяете правильность или изменяете основные настройки сервера записи, запись и просмотр видео в режиме реального времени невозможны.

Включить шифрование сервера событий

Можно настроить шифрование двусторонних подключений между сервером событий и компонентами, обменивающимися данными с сервером событий, включая LPR Server.

При настройке шифрования для группы серверов его необходимо включить, используя сертификат, принадлежащий тому же сертификату ЦС, или, если шифрование отключено, отключить его на всех компьютерах в группе серверов.

Предварительные условия

- Для сертификата аутентификации сервера необходимо настроить доверие на компьютере, где размещается сервер событий.

Прежде всего, включите шифрование на сервере событий.

Действия:

1. На компьютере с установленным сервером событий откройте **Server Configurator** из:

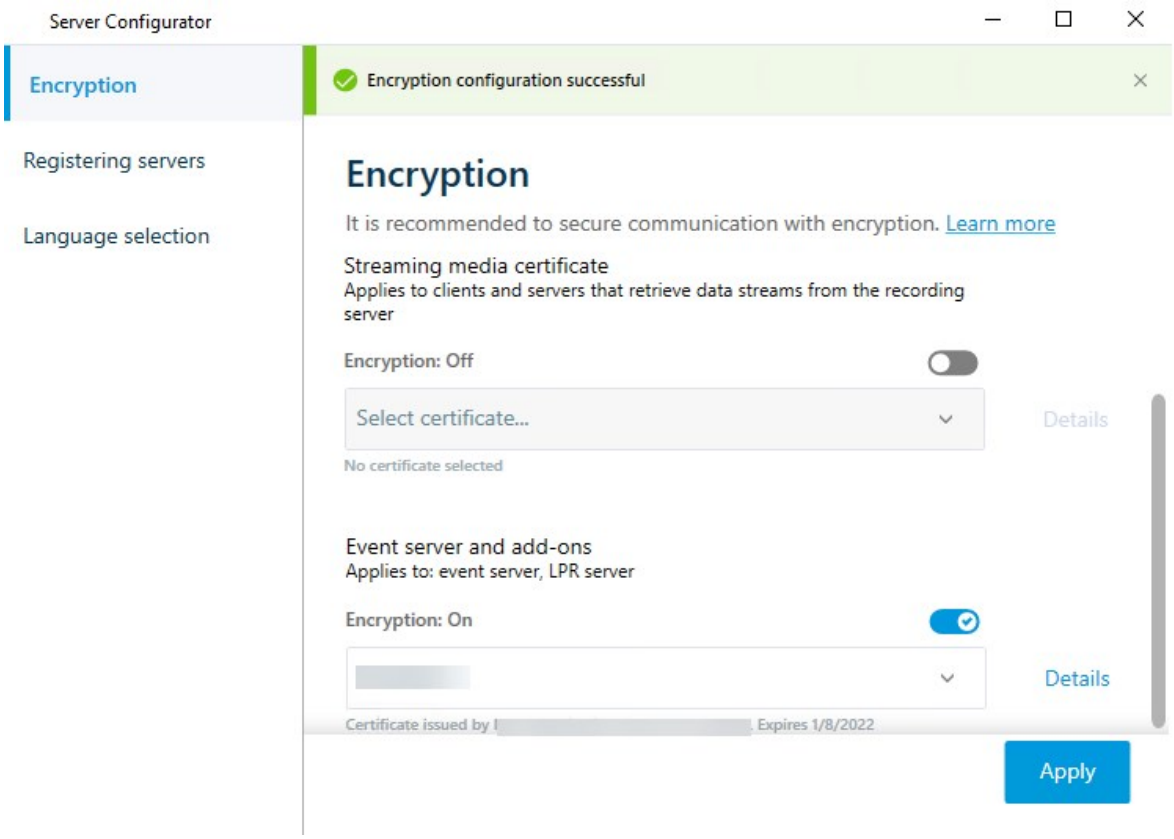
   - меню «Пуск» Windows

   или

   - Event Server, щелкнув значок Event Server на панели задач компьютера правой кнопкой мыши.

2. В **Server Configurator** в разделе **Сервер событий и надстройки** включите **Шифрование**.
3. Нажмите **Выбрать сертификат**, чтобы открыть список с уникальными именами субъектов сертификатов с закрытыми ключами, которые установлены на локальном компьютере в хранилище сертификатов Windows.
4. Выберите сертификат для шифрования обмена данными между сервером событий и связанными надстройками.

   Выберите **Сведения**, чтобы просмотреть информацию о выбранном сертификате из хранилища сертификатов Windows.



5. Нажмите кнопку **Применить**.

Чтобы завершить настройку шифрования, выполните следующий шаг — обновите параметры шифрования для каждого связанного расширения LPR Server.

Включить шифрование для клиентов и серверов

Можно настроить шифрование подключений с сервера записи на клиенты и серверы, осуществляющие потоковую передачу данных с сервера записи.

> При настройке шифрования для группы серверов его необходимо включить, используя сертификат, принадлежащий тому же сертификату ЦС, или, если шифрование отключено, отключить его на всех компьютерах в группе серверов.

Предварительные условия

- Для используемого сертификата аутентификации сервера необходимо настроить доверие на всех компьютерах, где выполняются службы, получающие потоки данных с сервера записи.
- XProtect Smart Client и все службы, получающие потоки данных с сервера записи, должны иметь версию 2019 R1 или более позднюю.
- Может потребоваться обновить некоторые сторонние решения, созданные с помощью версий MIP SDK, предшествующих 2019 R1.

Действия:

1. На компьютере с установленным сервером записи откройте **Server Configurator** из:
   - меню «Пуск» Windows

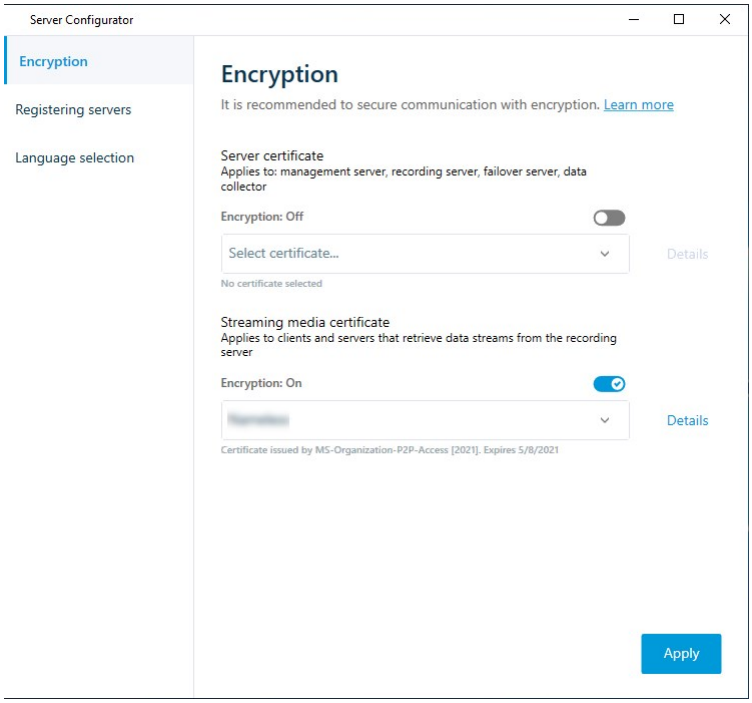
   или

   - Recording Server Manager, щелкнув значок Recording Server Manager на панели задач компьютера правой кнопкой мыши.
2. В **Server Configurator** в разделе **Сертификат потоковых мультимедиа** включите **Шифрование**.
3. Нажмите **Выбрать сертификат**, чтобы открыть список с уникальными именами субъектов сертификатов с закрытыми ключами, которые установлены на локальном компьютере в хранилище сертификатов Windows.
4. Выберите сертификат для шифрования обмена данными между клиентами и серверами, получающими потоки данных с сервера записи.

   Выберите **Сведения**, чтобы просмотреть информацию о выбранном сертификате из хранилища сертификатов Windows.

   Пользователю сервиса Recording Server предоставлен доступ к закрытому ключу. Для этого

сертификата необходимо настроить доверие на всех клиентах.



5. Нажмите кнопку **Применить**.

Когда вы примените сертификаты, сервер записи будет остановлен и перезапущен. Остановка службы Recording Server означает, что, пока вы проверяете правильность или изменяете основные настройки сервера записи, запись и просмотр видео в режиме реального времени невозможны.

Чтобы узнать, как проверить, использует ли сервер записи шифрования, см. раздел Просмотр состояния шифрования при подключении к клиентам.

Включить шифрование на мобильном сервере

Для использования протокола HTTPS для обмена данными между мобильным сервером, клиентами и службами необходимо установить на сервере действительный сертификат. Этот сертификат подтверждает, что владелец сертификата имеет право на создание защищенных подключений.

Дополнительные сведения см. в руководстве по сертификатам, посвященном защите систем XProtect VMS.

При настройке шифрования для группы серверов его необходимо включить, используя сертификат, принадлежащий тому же сертификату ЦС, или, если шифрование отключено, отключить его на всех компьютерах в группе серверов.

Сертификаты, выпущенные центром сертификации (ЦС), представляют собой цепочку сертификатов, и в корне этой цепочки находится корневой сертификат ЦС. Когда устройство или браузер получают этот сертификат, они сравнивают его корневой сертификат с сертификатами, предустановленными в ОС (Android, iOS, Windows и т.д.). Если корневой сертификат указан в списке предустановленных сертификатов, ОС сообщает пользователю, что подключение к серверу достаточно безопасно. Эти сертификаты выдаются по доменному имени и не бесплатны.

Действия:

1. На компьютере с установленным мобильным сервером откройте **Server Configurator** из:
   - меню «Пуск» Windows

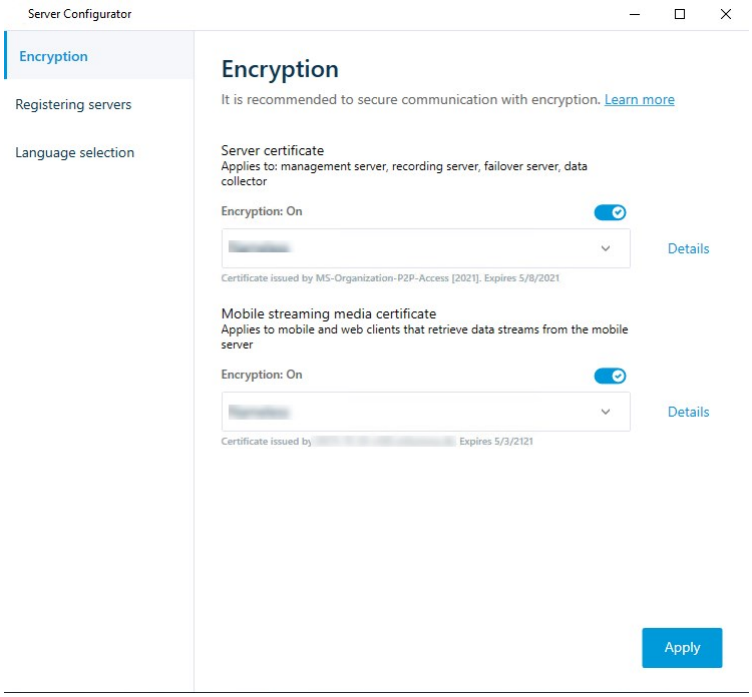
   или

   - Mobile Server Manager, щелкнув значок Mobile Server Manager на панели задач компьютера правой кнопкой мыши.
2. В **Server Configurator** в разделе **Сертификат мобильных потоковых мультимедиа** включите **Шифрование**.
3. Нажмите **Выбрать сертификат**, чтобы открыть список с уникальными именами субъектов сертификатов с закрытыми ключами, которые установлены на локальном компьютере в хранилище сертификатов Windows.
4. Выберите сертификат для шифрования обмена данными клиента XProtect Mobile и XProtect Web Client с мобильным сервером.

   Выберите **Сведения**, чтобы просмотреть информацию о выбранном сертификате из хранилища сертификатов Windows.

   Пользователю сервиса Mobile Server предоставлен доступ к закрытому ключу. Для этого

сертификата необходимо настроить доверие на всех клиентах.



5. Нажмите кнопку **Применить**.

После применения сертификатов служба Mobile Server будет перезапущена.

Milestone Federated Architecture

Настройка системы для работы с федеративными сайтами

Чтобы подготовить систему к работе с Milestone Federated Architecture, необходимо задать определенные параметры при установке сервера управления. В зависимости от настройки ИТ-инфраструктуры вы можете выбрать один из трех вариантов.

Вариант 1. Подключение сайтов из одного домена (с помощью общего пользователя домена)

Перед установкой сервера управления создайте общего пользователя домена и назначьте его администратором на всех серверах, входящих в иерархию федеративных сайтов. Способ установления связи между сайтами зависит от созданной учетной записи пользователя.

Учетная запись пользователя Windows

1. Запустите установку продукта на сервере, который будет использоваться в качестве сервера управления, и выберите тип установки **Пользовательская**.
2. Выберите установку службы Management Server с помощью учетной записи пользователя. Выбранная учетная запись пользователя должна иметь статус учетной записи администратора на всех серверах управления. Во время установки других серверов управления в иерархии федеративных сайтов используйте ту же учетную запись пользователя.
3. Завершите установку. Повторите шаги 1–3, чтобы установить другие системы, которые вы хотите добавить в иерархию федеративных сайтов.
4. Добавьте сайт в иерархию (см. Добавление сайтов в иерархию на стр. 340).

Встроенная учетная запись пользователя Windows (сетевая служба)

1. Запустите установку продукта на первом сервере, который будет использоваться в качестве сервера управления, и выберите **Один компьютер** или **Пользовательская**. В этом случае сервер управления устанавливается с помощью учетной записи сетевой службы. Повторите этот шаг для всех сайтов в иерархии федеративных сайтов.
2. Войдите на сайт, который вы хотите использовать в качестве центрального в иерархии федеративных сайтов.
3. В Management Client разверните узел **Безопасность** > **Роли** > **Администраторы**.
4. На вкладке **Пользователи и группы** нажмите **Добавить** и выберите **Пользователь Windows**.
5. В диалоговом окне в качестве типа объекта выберите **Компьютеры**, введите имя сервера федеративного сайта и нажмите **OK**, чтобы добавить сервер в роль **Администратор** на центральном объекте. Повторяйте этот шаг до тех пор, пока не добавите все федеративные сайты, после чего выйдите из приложения.
6. Выполните вход на каждый федеративный сайт и добавьте следующие серверы в роль **Администратор**, аналогично описанному выше:
   - сервер родительского сайта;
   - серверы дочерних сайтов, которые вы хотите подключить к этому федеративному сайту.
7. Добавьте сайт в иерархию (см. Добавление сайтов в иерархию на стр. 340).

Вариант 2. Подключение сайтов из разных доменов

Чтобы установить связь с сайтами разных доменов, убедитесь, что это эти домены доверяют друг другу. Настройте доверие доменов в конфигурации доменов Microsoft Windows. После настройки доверия между разными доменами на каждом сайте в иерархии федеративных сайтов выполните действия, описанные в варианте 1. Дополнительные сведения о настройке доверенных доменов приведены на сайте Microsoft (https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/).

Milestone рекомендует использовать Milestone Interconnect для создания связанных систем с несколькими сайтами и несколькими доменами.

Вариант 3. Подключение сайтов в рабочих группах

При установлении связи между сайтами в рабочих группах одна и та же учетная запись администратора должна присутствовать на всех серверах, подключаемых в иерархии федеративных сайтов. Учетную запись администратора необходимо настроить до начала установки системы.

1. Войдите в систему **Windows**, используя учетную запись администратора.
2. Запустите установку продукта и выберите тип настройки **Пользовательская**.
3. Выберите установку службы Management Server с помощью учетной записи администратора.
4. Завершите установку. Повторите шаги 1–4, чтобы установить все остальные системы, которые необходимо подключить. Для установки всех этих систем необходимо использовать одну учетную запись администратора.
5. Добавьте сайт в иерархию (см. Добавление сайтов в иерархию на стр. 340).

Milestone рекомендует использовать Milestone Interconnect для создания связанных систем с несколькими сайтами, если эти сайты не являются частью домена.

Объединять домены и рабочие группы нельзя. Не подключайте сайты из домена к сайтам из рабочей группы и наоборот.

Добавление сайтов в иерархию

В процессе расширения системы можно добавлять сайты на верхний и дочерние уровни при условии правильной настройки системы.

При добавлении небезопасного сайта в Milestone Federated Architecture, убедитесь, что включен параметр **Разрешить незащищенные соединения с сервером** в разделе **Инструменты** > **Опции** > **Общие настройки** в Management Client.

1. Откройте панель **Иерархия федеративных сайтов**.
2. Выберите сайт, для которого нужно добавить дочерний сайт, нажмите правой кнопкой мыши и выберите **Добавить сайт в иерархию**.
3. Введите URL-адрес запрашиваемого сайта в окне **Добавить сайт в иерархию** и нажмите **ОК**.

4. Родительский сайт направляет запрос на установление связи с дочерним сайтом. Спустя некоторое время связь между двумя сайтами отобразится на панели **Иерархия федеративных сайтов**.
5. Если вы можете установить связь с дочерним сайтом без получения согласия администратора дочернего сайта, перейдите к шагу 7.

   Если **нет**, для дочернего сайта появится значок ожидания подтверждения  , который будет активен до тех пор, пока администратор этого сайта не подтвердит запрос.
6. Убедитесь, что администратор дочернего сайта подтвердил запрос на установление связи с родительским сайтом (см. Принять добавление в иерархию на стр. 341).
7. Будет создана новая связь между родительским и дочерним сайтом, а на панели **Иерархия федеративных сайтов** обновится значок  для нового дочернего сайта.

Принять добавление в иерархию

Если дочерний сайт получает запрос на связь от потенциального родительского сайта, администратор которого не имеет соответствующего разрешения на работу с дочерним сайтом, появится значок ожидания подтверждения  .

Чтобы подтвердить запрос, выполните следующие действия:

1. Войдите на сайт.
2. На панели **Иерархия федеративных сайтов** правой кнопкой мыши нажмите нужный объект и выберите **Принять добавление в иерархию**.

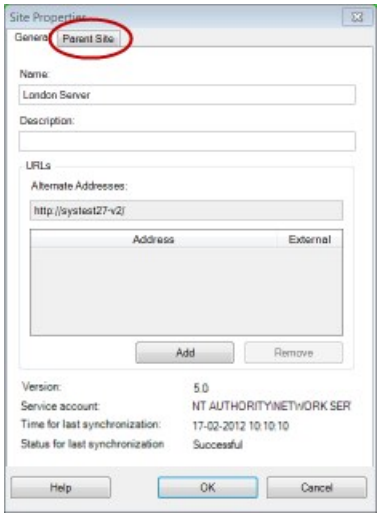
   Если на сайте выполняется версия XProtect Expert, нажмите сайт на панели **Навигация по сайту** правой кнопкой мыши.
3. Нажмите кнопку **Да**.
4. Будет создана новая связь между родительским и дочерним сайтом, а на панели **Иерархия федеративных сайтов** обновится значок  для выбранного сайта.

> Изменения, которые вносятся в дочерние сайты, удаленные от родительского сайта, будут отражены на панели **Иерархия федеративных сайтов** с некоторой задержкой.

Настройка свойств сайта

Вы можете просматривать и в некоторых случаях редактировать свойства главного сайта и его дочерних сайтов.

1. В Management Client на панели **Иерархия федеративных сайтов** выберите соответствующий сайт, нажмите правой кнопкой мыши и выберите **Свойства**.



2. При необходимости измените следующие параметры:

   Вкладка **Общая информация** (см. Вкладка «Общая информация» на стр. 654)

   Вкладка **Родительский сайт** (см. Вкладка «Родительский сайт» на стр. 654) **(доступна только на дочерних объектах)**

   > В связи с особенностями синхронизации для отражения любых изменений, внесенных на удаленных дочерних сайтах, на панели **Навигация по сайту** может потребоваться некоторое время.

Обновление иерархии сайта

Система автоматически синхронизирует иерархию на всех уровнях родительских и дочерних сайтов на регулярной основе. Вы можете выполнить обновление вручную, если хотите, чтобы внесенные изменения оперативно отразились в иерархии. Тогда вам не придется ждать следующей автоматической синхронизации.

Чтобы выполнить обновление вручную, необходимо войти на сайт. При обновлении отражаются только те изменения, которые были сохранены на этом сайте после последней синхронизации. Это означает, что изменения, внесенные ниже по иерархии, могут не отразиться при обновлении вручную, если эти изменения еще не появились на сайте.

1. Войдите на соответствующий сайт.
2. Нажмите правой кнопкой мыши сайт верхнего уровня на панели **Иерархия федеративных сайтов** и выберите **Обновить иерархию сайта**.

   На это потребуется несколько секунд.

Вход на другие сайты в иерархии

Вы можете выполнять вход на другие сайты и управлять ими. Сайт, на который вы вошли, является главным.

1. На панели **Иерархия федеративных сайтов** нажмите правой кнопкой мыши сайт, на который хотите войти.
2. Нажмите **Войти на сайт**.

   Для этого сайта появится Management Client.
3. Введите необходимую информацию для входа и нажмите **OK**.
4. После успешного входа в систему вы можете переходить к управлению сайтом.

Обновление информации о дочерних сайтах

> Этот раздел применим только при работе с XProtect Corporate и XProtect Expert 2014 и более поздних версий.

В крупной среде Milestone Federated Architecture с большим количеством дочерних сайтов общий обзор и поиск контактных данных администраторов каждого дочернего сайта может представлять трудности.

Вы можете добавить дополнительные сведения в каждый дочерний сайт, и эта информация затем будет доступна администраторам центрального объекта.

Чтобы ознакомиться с информацией о сайте, наведите курсор на имя соответствующего сайта на панели **Иерархия федеративных сайтов**. Чтобы обновить информацию о сайте, выполните следующие действия:

1. Войдите на сайт.
2. Откройте панель **Навигация по сайту** и выберите **Сведения о сайте**.
3. Нажмите **Изменить**, чтобы добавить необходимую информацию в каждой категории.

Отключение сайта от иерархии

Если отключить сайт, то связь между ним и родительским сайтом будет прервана. Можно отключать сайты от центрального объекта, от самого сайта или его родительского сайта.

1. На панели **Иерархия федеративных сайтов** нажмите нужный сайт правой кнопкой мыши и выберите **Удалить сайт из иерархии**.
2. Нажмите **Да**, чтобы обновить панель **Иерархия федеративных сайтов**.

   Если у отключенного сайта есть дочерние сайты, он становится новым сайтом верхнего уровня для этой ветви иерархии, а стандартный значок сайта меняется на значок сайта верхнего уровня .
3. Нажмите кнопку **OK**.

Внесенные изменения отразятся в иерархии после обновления вручную или после автоматической синхронизации.

Milestone Interconnect

Добавление удаленного объекта в центральный объект Milestone Interconnect

Чтобы добавить удаленные объекты в центральный объект, используйте мастер **добавления оборудования**.
Требования

- Достаточное количество лицензий на камеры Milestone Interconnect (см. Milestone Interconnect и лицензирование на стр. 103).
- Еще одна настроенная и работающая система XProtect, предусматривающая учетную запись пользователя (базовые пользователи, локальный пользователь Windows или пользователь Windows Active Directory) с разрешениями на устройства, к которым центральная система XProtect Corporate должна иметь доступ
- Сетевое подключение между центральным объектом XProtect Corporate и удаленными объектами с соответствующим доступом или перенаправлением на порты, используемые на удаленных объектах

Добавление удаленного объекта:

1. На центральном объекте разверните узел **Серверы** и выберите **Сервер записи**.
2. На панели **Обзор** разверните соответствующий сервер записи и нажмите правой кнопкой мыши.
3. Выберите **Добавить оборудование**, чтобы запустить соответствующий мастер.
4. На первой странице выберите **Сканирование диапазона адресов** или **Вручную** и нажмите **Далее**.
5. Укажите имена и пароли пользователей. Учетная запись пользователя должна быть предварительно задана в удаленной системе. При необходимости вы можете добавить имена пользователей и пароли, нажав кнопку **Добавить**. После этого нажмите **Далее**.

6. Выберите драйверы, которые будут использоваться при сканировании. В данном случае следует выбрать один из драйверов Milestone. Нажмите **Далее**.
7. Укажите IP-адреса и номера портов, которые необходимо просканировать. По умолчанию используется порт 80. Нажмите **Далее**.

   Дождитесь, когда система обнаружит удаленные объекты. Индикатор состояния отображает ход процесса обнаружения. В случае положительного результата в столбце **Статус** появится сообщение **Успешно**. При неудачной попытке нажмите сообщение **Сбой**, чтобы узнать причину ошибки.
8. Вы можете включить или отключить обнаруженные системы. Нажмите **Далее**.
9. Дождитесь, когда система обнаружит оборудование и получит информацию о конкретном устройстве. Нажмите **Далее**.
10. Вы можете включить или отключить обнаруженное оборудование и устройства. Нажмите **Далее**.
11. Выберите группу по умолчанию. Нажмите кнопку **Готово**.
12. После установки система и ее устройства отобразятся на панели **Обзор**.

    Доступ к камерам и функциям на центральном объекте определяется разрешениями выбранного пользователя на удаленном объекте.

Назначение разрешений

Разрешения для подключенной камеры настраиваются таким же образом, как и для других камер: создается роль и назначается доступ к функциям.

1. На центральном объекте на панели **Навигация по сайту** разверните узел **Безопасность** и выберите **Роли**.
2. На панели «Обзор» правой кнопкой мыши нажмите встроенную роль администратора и выберите **Добавить роль** (см. раздел Добавление роли и управление ролью).
3. Задайте имя роли и настройте ее параметры на вкладке **Устройство** (см. Вкладка «Устройство» (роли)) и вкладке **Удаленные записи** (см. Вкладка «Удаленные записи» (роли)).

Обновление оборудования удаленного объекта

В случае изменения конфигурации удаленного объекта, например добавления или удаления камер и событий, необходимо обновить конфигурацию центрального объекта, чтобы отразить изменения, внесенные в конфигурацию удаленного объекта.

1. На центральном объекте разверните узел **Серверы** и выберите **Сервер записи**.
2. На панели **Обзор** разверните нужный сервер записи и выберите соответствующую удаленную систему. Нажмите ее правой кнопкой мыши.
3. Выберите **Обновить оборудование**. Откроется диалоговое окно **Обновить оборудование**.

4. В диалоговом окне отображаются все изменения (удаленные, обновленные и добавленные устройства) в удаленной системе с момента настройки Milestone Interconnect или последнего обновления. Нажмите **Подтвердить**, чтобы обновить центральный объект с учетом внесенных изменений.

Воспроизведение напрямую с камеры удаленного объекта

Если между центральным объектом и удаленными объектами поддерживается постоянная связь, систему можно настроить таким образом, чтобы пользователи воспроизводили записи напрямую с удаленных объектов. Дополнительные сведения приведены в разделе Настройки Milestone Interconnect (объяснение) на стр. 104.

1. На центральном объекте разверните узел **Серверы** и выберите **Сервер записи**.
2. На панели **Обзор** разверните нужный сервер записи и выберите соответствующую удаленную систему. Выберите соответствующую подключенную камеру.
3. На панели «Свойства» выберите вкладку **Запись**. Затем установите флажок **Воспроизведение записей удаленной системы**.
4. На панели инструментов нажмите кнопку **Сохранить**.

В схеме Milestone Interconnect центральный объект игнорирует маски конфиденциальности, установленные на удаленном объекте. Если вы хотите применить одинаковые маски конфиденциальности, их необходимо повторно задать на центральном объекте.

Получение дистанционных записей с камер удаленного объекта

Если центральный объект **не** имеет постоянного подключения к удаленным объектам, вы можете настроить централизованное хранение дистанционных записей в системе, а также настроить получение дистанционных записей при наличии оптимального сетевого подключения. Дополнительные сведения приведены в разделе Настройки Milestone Interconnect (объяснение) на стр. 104.

Для того чтобы пользователи могли получать записи, необходимо включить это разрешение для соответствующей роли (см. раздел Роли (Безопасность)).

Настройка системы:

1. На центральном объекте разверните узел **Серверы** и выберите **Сервер записи**.
2. На панели **Обзор** разверните нужный сервер записи и выберите соответствующую удаленную систему. Выберите соответствующий удаленный сервер.
3. На панели свойств откройте вкладку **Дистанционное получение** и обновите настройки (см. Вкладка «Дистанционное получение» на стр. 470).

В случае сбоя сетевого подключения центральный объект не сможет записывать эпизоды. Систему можно настроить таким образом, чтобы центральный объект автоматически получал дистанционные записи, относящиеся к периоду отключения, после восстановления сетевого подключения.

1. На центральном объекте разверните узел **Серверы** и выберите **Сервер записи**.
2. На панели **Обзор** разверните нужный сервер записи и выберите соответствующую удаленную систему. Выберите соответствующую камеру.
3. На панели «Свойства» откройте вкладку **Запись** и установите флажок **Автоматически получить дистанционные записи при восстановлении подключения** (см. раздел Сохранение и получение дистанционной записи).
4. На панели инструментов нажмите кнопку **Сохранить**.

Помимо этого, можно использовать правила или запускать получение дистанционных записей с XProtect Smart Client по мере необходимости.

В схеме Milestone Interconnect центральный объект игнорирует маски конфиденциальности, установленные на удаленном объекте. Если вы хотите применить одинаковые маски конфиденциальности, их необходимо повторно задать на центральном объекте.

Настройка реагирования центрального объекта на события, связанные с удаленными объектами

Вы можете использовать события, заданные на удаленных объектах, чтобы запустить правила и сигналы тревоги на центральном объекте. Благодаря этому обеспечивается немедленное реагирование на события, полученные с удаленных объектов. Для этого требуется, чтобы удаленные объекты были подключены и находились в режиме онлайн. Количество и типы событий зависят от событий, настроенных и предварительно заданных на удаленных объектах.

Список поддерживаемых событий доступен на сайте Milestone (https://www.milestonesys.com/).

Предварительно заданные события удалить нельзя.

Требования:

- Если вы хотите использовать пользовательские или активируемые вручную события с удаленных объектов в качестве событий срабатывания, сначала создайте такие события на удаленных объектах.
- Убедитесь, что у вас есть обновленный список событий удаленных объектов (см. Обновление оборудования удаленного объекта на стр. 345).

Добавление пользовательского/активируемого вручную события с удаленного объекта:

1. На центральном объекте разверните узел **Серверы** и выберите **Сервер записи**.
2. На панели «Обзор» выберите соответствующий удаленный сервер и перейдите на вкладку **События**.
3. Список включает предварительно заданные события. Нажмите **Добавить**, чтобы включить в список пользовательские или активируемые вручную события с удаленного объекта.

Используйте событие удаленного объекта для подачи сигнала тревоги на центральном объекте:

1. На центральном объекте разверните узел **Сигналы тревоги** и выберите **Определения тревог**.
2. На панели «Обзор» правой кнопкой мыши нажмите **Определения тревог** и выберите **Добавить новое**.
3. Введите соответствующие значения.
4. В поле **Событие срабатывания** выберите одно из предварительно заданных или пользовательских событий.
5. В поле **Источники** выберите удаленный сервер, соответствующий удаленному объекту, с которого вы хотите получать сигналы тревоги.
6. Завершив работу, сохраните конфигурацию.

Используйте событие удаленного объекта для активации действия на основе правил на центральном объекте:

1. На центральном объекте разверните узел **Правила и события** и выберите **Правила**.
2. На панели «Обзор» правой кнопкой мыши нажмите **Правила** и выберите **Добавить правило**.
3. Откроется мастер, выберите **Выполнить действие применимо к <событие>**.
4. В области **Изменить определение правила** нажмите **Событие** и выберите одно из предварительно заданных или пользовательских событий. Нажмите кнопку **ОК**.
5. Нажмите **устройства/сервер записи/сервер управления** и выберите удаленный сервер, соответствующий удаленному объекту, для которого центральный объект будет запускать действие. Нажмите кнопку **ОК**.
6. Нажмите **Далее**, чтобы перейти на следующую страницу мастера.
7. Выберите условия, которые вы хотите применить к этому правилу. Если вы не выберете никаких условий, правило будет применяться во всех случаях. Нажмите **Далее**.
8. Выберите действие и укажите подробную информацию в области **Изменить определение правила**. Нажмите **Далее**.
9. При необходимости выберите критерий завершения. Нажмите **Далее**.
10. При необходимости выберите действие завершения. Нажмите кнопку **Готово**.

Службы удаленного подключения

Службы удаленного подключения (объяснение)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Службы удаленного подключения включают технологию «Подключение к камере Axis нажатием одной кнопки», разработанную компанией Axis Communications. Благодаря этой функции система может получать видео (и звуковую информацию) с внешних камер в тех случаях, когда брандмауэры и/или сетевые конфигурации маршрутизаторов блокируют установку соединений с такими камерами. Связь осуществляется через безопасные туннельные серверы (ST-серверы). ST-серверы используют VPN. По VPN работают только те устройства, на которых установлен действительный ключ. Таким образом создается безопасный туннель, по которому общедоступные сети могут безопасно обмениваться данными.

С помощью служб удаленного подключения можно:

- редактировать учетные данные в службе контроля Axis;
- добавлять, изменять и удалять ST-серверы;
- регистрировать/отменять регистрацию камер Axis One-click и изменять их;
- просматривать оборудование, связанное с камерой Axis One-Click.

Установка безопасного туннельного сервера для подключения к камере нажатием одной кнопки

Прежде чем использовать функцию «Подключение к камере Axis нажатием одной кнопки», установите подходящую серверную среду безопасного туннелирования. Для работы с безопасным туннельным сервером (ST-сервером) и камерами Axis One-click обратитесь к поставщику системы, чтобы получить необходимые имя пользователя и пароль для служб контроля Axis.

Требования

- Свяжитесь с поставщиком системы, чтобы получить имя пользователя и пароль для служб контроля Axis.
- Убедитесь, что ваши камеры поддерживают систему видеохостинга Axis. Перейдите на сайт Axis, чтобы посмотреть поддерживаемые устройства (https://www.axis.com/products/axis-guardian)
- При необходимости обновите камеры Axis и установите последнюю версию прошивки. Чтобы загрузить прошивку, перейдите на сайт Axis (https://www.axis.com/support/firmware).

1. На главной странице соответствующей камеры перейдите в раздел **Основные настройки**, **TCP/IP** и выберите **Включить AVHS** и **Всегда**.
2. На сервере управления откройте страницу загрузки Milestone (https://www.milestonesys.com/downloads/) и загрузите программное обеспечение **AXIS One-Click**. Запустите программу, чтобы установить подходящую среду безопасного туннеля Axis.

Добавление и изменение безопасных туннельных серверов

Связь между службами удаленного подключения осуществляется через безопасные туннельные серверы (ST-серверы).

1. Выполните одно из следующих действий:
   - Чтобы добавить ST-сервер, правой кнопкой мыши нажмите верхний узел **Безопасные туннельные серверы Axis** и выберите **Добавление «Безопасный туннельный сервер Axis»**.
   - Чтобы изменить ST-сервер, нажмите его правой кнопкой мыши и выберите **Правка «Безопасный туннельный сервер Axis»**.
2. Заполните необходимую информацию в открывшемся окне.
3. Если при установке компонента **Подключение к Axis нажатием одной кнопки**, вы хотите использовать учетные данные, установите флажок **Использовать учетные данные** и введите имя пользователя и пароль, которые используются для компонента **Подключение к Axis нажатием одной кнопки**.
4. Нажмите кнопку **OK**.

Регистрация новой камеры Axis One-click

1. Для регистрации камеры на ST-сервере нажмите ее правой кнопкой мыши и выберите **Регистрация камеры Axis One-Click**.
2. Заполните необходимую информацию в открывшемся окне.
3. Нажмите кнопку **OK**.
4. Теперь камера отображается на соответствующем ST-сервере.

Для камеры может применяться следующая цветовая кодировка:

Цвет	Описание
Красный	Начальное состояние. Камера зарегистрирована, но не подключена к ST-серверу.

Цвет	Описание
Желтый	Камера зарегистрирована. Есть подключение к ST-серверу, но камера не добавлена как оборудование.
Зеленый	Камера добавлена как оборудование. Подключение к ST-серверу может иметься или отсутствовать.

При добавлении новой камеры цвет статуса будет зеленым. Состояние подключения отражается на панели **Обзор** в разделе **Серверы записи**, **Устройства**. На панели **Обзор** камеры можно для удобства объединять в группы. Если вы решили **не** регистрировать камеру в службе контроля Axis на этом этапе, вы можете сделать это позже с помощью контекстного меню (выберите **Правка «Камеры Axis One-click»**).

Интеллектуальные карты

Картографический фон (объяснение)

Чтобы пользователи XProtect Smart Client могли выбрать картографический фон, сначала необходимо настроить картографические фоны в XProtect Management Client.

- **Общая карта мира** — используется стандартный картографический фон XProtect Smart Client. Настройка не требуется. Эту карту можно использовать для общего ориентирования, и она не содержит подробностей, таких как границы стран, города и т. д. При этом она имеет геопространственную привязку, аналогично другим картографическим фонам
- **Bing Maps** — подключение Bing Maps
- **Google Maps** — подключение Google Maps
- **Milestone Map Service** - подключение к поставщику бесплатных карт. После включения Milestone Map Service дополнительная настройка не требуется.

  См. Включить Milestone Map Service

- **OpenStreetMap**– подключение:
  - Коммерческий сервер фрагментов
  - Ваш собственный, локальный или онлайн-сервер фрагментов

  См. Определение сервера фрагментов OpenStreetMap

Для использования Bing Maps и Google Maps требуется подключение к Интернету и платный ключ API, предоставляемый компанией Microsoft или Google.

Milestone Map Service необходим доступ в Интернет.

Для работы OpenStreetMap требуется интернет-доступ за исключением случаев, когда вы используете собственный локальный сервер фрагментов.

Если система должна соответствовать требованиям GDPR, не используйте следующие службы:

- Bing Maps
- Google Maps
- Milestone Map Service

Дополнительные сведения о защите данных и сборе данных по использованию см. в руководстве по конфиденциальности GDPR.

По умолчанию карты Bing и Google отображают вид со спутника (Спутник). Для изменения визуализации в XProtect Smart Client можно менять вид карты, например с гибридного на вид местности.

Включение Bing Maps или Google Maps в Management Client

Чтобы ключ стал доступным для нескольких пользователей, введите его для профиля Smart Client в Management Client. Все пользователи, имеющие доступ к данному профилю, смогут использовать ключ.

Действия:

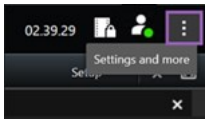
1. В Management Client на панели **Навигация по сайту** выберите **Профили Smart Client**.
2. На панели **Профили Smart Client** выберите соответствующий профиль Smart Client.
3. На панели **Свойства** откройте вкладку **Интеллектуальная карта**:
   - При использовании Bing Maps введите базовый ключ или корпоративный ключ в поле **Ключ Bing Maps**.
   - При использовании Google Maps введите ключ Maps Static API в поле **Закрытый ключ Google Maps**.
4. Если вы не хотите, чтобы операторы XProtect Smart Client использовали другой ключ, установите флажок **Заблокировано**.

Включение Bing Maps или Google Maps в XProtect Smart Client

Если вы хотите, чтобы операторы XProtect Smart Client могли использовать ключ, отличный от ключа профиля Smart Client, введите ключ в настройках XProtect Smart Client.

Действия:

1. В XProtect Smart Client откройте окно **Параметры**.



2. Нажмите **Интеллектуальная карта**.
3. В зависимости от выбранной службы выполните одно из следующих действий:
   - При использовании Bing Maps введите ключ в поле **Ключ Bing Maps**. Также см. Интеграция интеллектуальных карт с Bing Maps (объяснение) на стр. 99.
   - При использовании Google Maps введите ключ в поле **Закрытый ключ Google Maps**. Также см. Интеграция интеллектуальных карт с Google Maps (объяснение) на стр. 98.

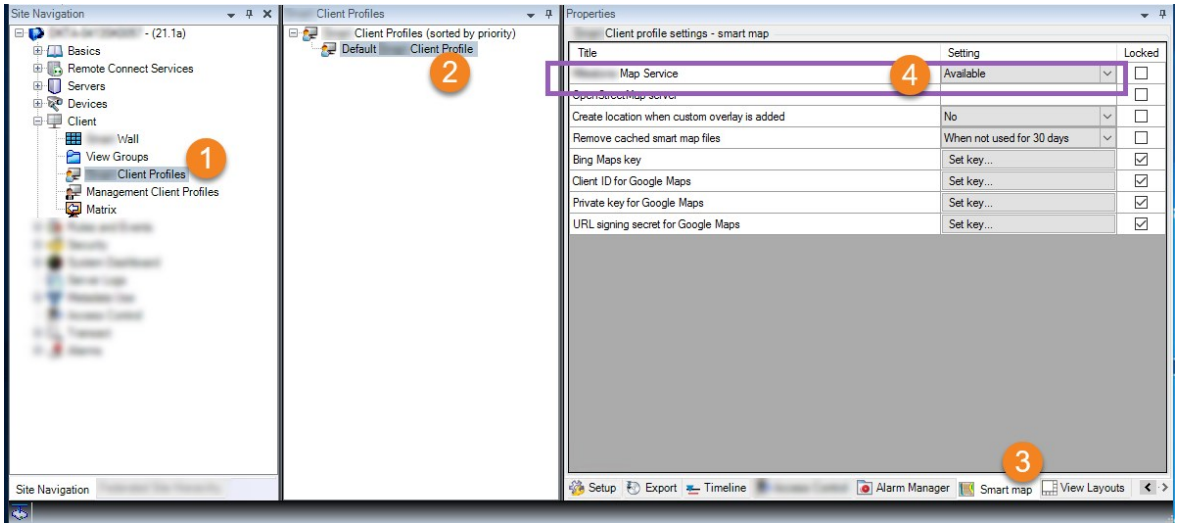
Включить Milestone Map Service

Milestone Map Service — это онлайн-сервис, позволяющий подключиться к серверу фрагментов карт Milestone Systems. Данный сервер фрагментов использует бесплатную картографическую службу.

После включения Milestone Map Service на интеллектуальной карте такая карта будет использовать Milestone Map Service в качестве географического фона.

Действия:

1. На панели **Навигация по сайту** разверните узел **Клиент** и нажмите **Профили Smart Client**.
2. На панели «Обзор» выберите соответствующий профиль Smart Client.
3. На панели **Свойства** перейдите на вкладку **Интеллектуальная карта**.



4. В поле **Milestone Map Service** выберите **Доступно**.
5. Чтобы принудительно применить эту настройку в XProtect Smart Client, установите флажок **Заблокировано**. Теперь операторы XProtect Smart Client не смогут включить или отключить Milestone Map Service.
6. Сохраните изменения.

Также можно включить Milestone Map Service в окне **Параметры** в XProtect Smart Client.

Milestone Map Service необходим доступ в Интернет.

Если вы используете брандмауэр с ограниченным доступом, разрешите доступ к соответствующим доменам. Milestone Map Service может потребоваться разрешение на использование исходящего трафика с помощью maps.milestonesys.com на каждом устройстве, на котором работает Smart Client.

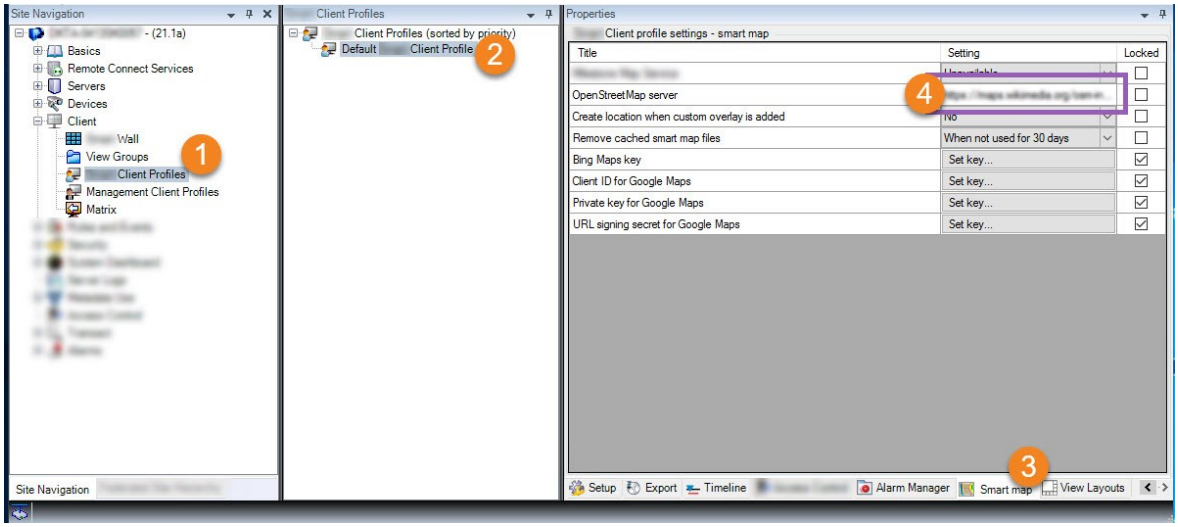
Указание сервера фрагментов OpenStreetMap

При использовании сервиса **OpenStreetMap** в качестве картографического фона для интеллектуальной карты необходимо указать, откуда будут получены фрагменты изображений. Для этого достаточно указать адрес сервера фрагментов. Это может быть коммерческий или локальный сервер фрагментов, если у вашей организации есть собственные карты для таких областей, как аэропорты или гавани.

> Адрес сервера фрагментов также можно указать в окне **Параметры** в XProtect Smart Client.

Действия:

1. На панели **Навигация по сайту** разверните узел **Клиент** и нажмите **Профили Smart Client**.
2. На панели «Обзор» выберите соответствующий профиль Smart Client.
3. На панели **Свойства** перейдите на вкладку **Интеллектуальная карта**.



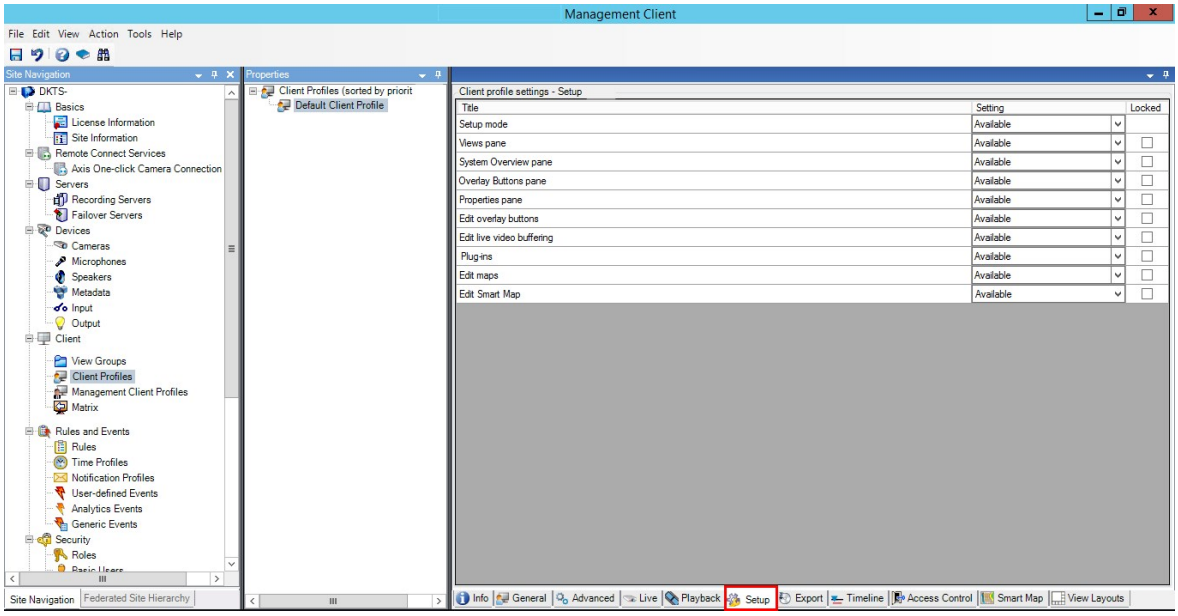
4. В поле **Сервер OpenStreetMap** введите адрес сервера фрагментов.
5. Чтобы принудительно применить эту настройку в XProtect Smart Client, установите флажок **Заблокировано**. Тогда операторы XProtect Smart Client не смогут изменить адрес.
6. Сохраните изменения.

Редактирование интеллектуальных карт

Операторы могут редактировать интеллектуальные карты в XProtect Smart Client в режиме настройки при условии, что включена функция редактирования в Management Client. В противном случае необходимо включить функцию редактирования для соответствующих профилей Smart Client.

Действия:

1. На панели **Навигация по сайту** разверните узел **Клиент**.
2. Нажмите **Smart ClientПрофили**.



3. На панели «Обзор» выберите соответствующий профиль Smart Client.
4. На панели **Свойства** перейдите на вкладку **Настройки**.
5. В списке **Изменить интеллектуальную карту** выберите **Доступно**.
6. Повторите эти шаги для всех соответствующих профилей Smart Client.
7. Сохраните изменения. При следующем входе в систему XProtect Smart Client пользователи, которым назначен выбранный вами профиль Smart Client, смогут редактировать интеллектуальные карты.

Чтобы отключить функцию редактирования, выберите **Недоступно** в списке **Изменить интеллектуальную карту**.

Редактирование устройств на интеллектуальной карте

Включите возможность редактирования устройств для соответствующих ролей, чтобы операторы могли выполнять ряд действий, например:

- размешать устройства ввода или микрофон на интеллектуальной карте;
- корректировать поле обзора камеры на интеллектуальной карте.

Операторам разрешается редактировать следующие типы устройств на интеллектуальных картах:

- Камеры
- Устройства ввода
- Микрофоны

Требования
Перед началом работы убедитесь, что редактирование интеллектуальной карты включено (см. Редактирование интеллектуальных карт на стр. 355). Для этого выберите профиль Smart Client, с которым связана роль оператора.

Действия:

1. Разверните узел **Безопасность** > **Роли**.
2. На панели **Роли** выберите роль нужного оператора.
3. Чтобы предоставить разрешения на редактирование, выполните следующие действия:
    - Откройте вкладку **Общий уровень безопасности**, на панели **Параметры роли** выберите тип устройства (например, **Камеры** или **Устройства ввода**).
    - В столбце **Разрешить** установите флажок **Полный контроль** или **Редактирование**.
4. Сохраните изменения.

Чтобы включить возможность редактирования отдельных устройств, перейдите на вкладку **Устройство** и выберите соответствующее устройство.

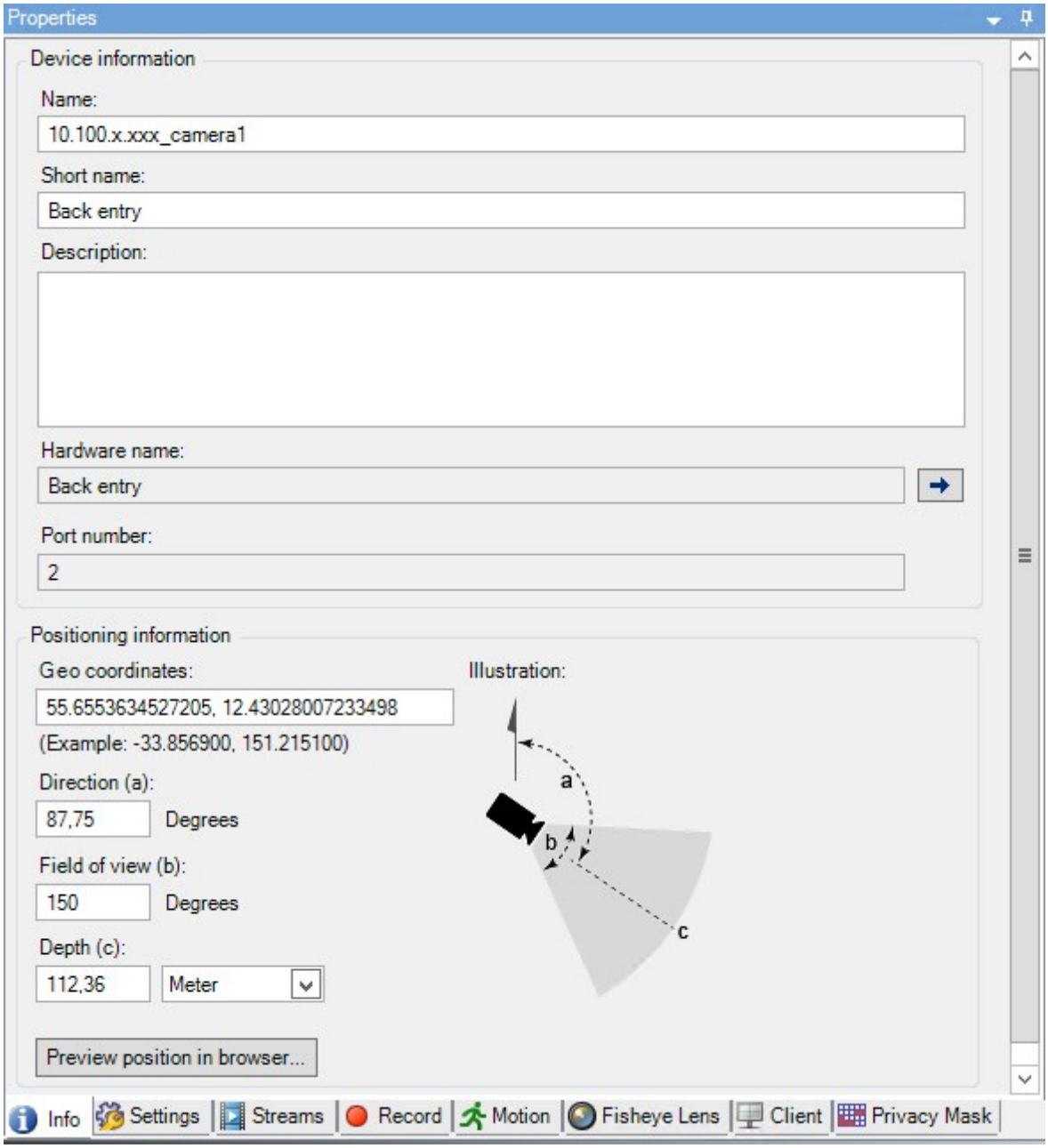
Задание положения устройства и направления камеры, поля обзора, глубины (интеллектуальная карта)

Для обеспечения правильного расположения устройства на интеллектуальной карте можно задать его географические координаты. Для камер можно также задать направление, поле обзора и глубину. При установке любого из вышеперечисленных параметров устройство будет автоматически добавлено на интеллектуальную карту при следующей загрузке интеллектуальной карты в XProtect Smart Client оператором.

Действия:

1. В Management Client разверните узел **Устройства** и выберите тип устройства (например, **Камеры** или **Устройства ввода**).
2. Выберите соответствующее устройство на панели **Устройства**.

3. На вкладке **Информация** прокрутите список вниз до раздела **Информация о местоположении**.



4. В поле **Координаты** укажите значения широты и долготы в указанном порядке. В качестве десятичного разделителя используйте точку, а для разделения широты и долготы — запятую.
   - Для камер:
     1. В поле **Направление** введите значение в диапазоне от 0 до 360 градусов.
     2. В поле **Поле обзора** введите значение в диапазоне от 0 до 360 градусов.
     3. В поле **Глубина** введите значение глубины просмотра в метрах или футах.

5. Сохраните изменения.

Свойства также можно задать на серверах записи.

Настройка интеллектуальной карты с помощью Milestone Federated Architecture

При использовании интеллектуальной карты в Milestone Federated Architecture на карте отображаются все устройства подключенных сайтов. Чтобы настроить интеллектуальную карту в федеративной архитектуре, выполните следующие действия.

Общие сведения о Milestone Federated Architecture приведены в разделе Настройка Milestone Federated Architecture на стр. 105.

1. Перед подключением сайта верхнего уровня к дочерним сайтам убедитесь, что для всех устройств и на всех объектах указаны географические координаты. Географические координаты добавляются автоматически при размещении устройства на интеллектуальной карте в XProtect Smart Client. Их также можно добавить в Management Client вручную с помощью свойств устройства. Дополнительные сведения приведены в разделе Задание положения устройства и направления камеры, поля обзора, глубины (интеллектуальная карта) на стр. 357.
2. Необходимо добавить операторов Smart Client в качестве пользователей Windows на родительском сайте и на всех федеративных сайтах. Кроме того, пользователи Windows должны иметь разрешения на редактирование интеллектуальной карты, как минимум, на сайте верхнего уровня. Это позволит пользователям редактировать интеллектуальную карту сайта верхнего уровня и дочерних сайтов. Далее определите, потребуются ли пользователям Windows разрешения на редактирование интеллектуальных карт на дочерних сайтах. Сначала создайте пользователей Windows в области **Роли** в Management Client. Затем включите возможность редактирования интеллектуальных карт. Дополнительные сведения приведены в разделе Редактирование интеллектуальных карт на стр. 355.
3. На сайте верхнего уровня добавьте дочерние сайты как пользователей Windows в роль с правами администратора. При указании типа объекта установите флажок **Компьютеры**.
4. На каждом дочернем сайте добавьте сайт верхнего уровня в ту же роль с правами администратора, которая используется на сайте верхнего уровня, в качестве пользователя Windows. При указании типа объекта установите флажок **Компьютеры**.
5. Убедитесь, что на сайте верхнего уровня можно просматривать окно **Иерархия федеративных сайтов**. В Management Client перейдите в раздел **Вид** и выберите **Иерархия федеративных сайтов**. Добавьте все дочерние сайты на сайт верхнего уровня. Дополнительные сведения приведены в разделе Добавление сайтов в иерархию на стр. 340.

6. Теперь проверьте работу Milestone Federated Architecture в XProtect Smart Client. Авторизуйтесь на сайте верхнего уровня в качестве администратора или оператора и откройте режим просмотра интеллектуальной карты. Если настройка выполнена корректно, на интеллектуальной карте отобразятся все устройства сайта верхнего уровня и дочерних сайтов. Если вы войдете на один из дочерних сайтов, вы увидите только устройства этого сайта и его дочерних сайтов.

Для изменения параметров устройств на интеллектуальной карте, например элемента представления и угла наклона камеры, требуются соответствующие разрешения на редактирование устройств. Дополнительные сведения приведены в разделе Редактирование устройств на интеллектуальной карте на стр. 356.

Обслуживание

Резервное копирование и восстановление конфигурации системы

Milestone рекомендует регулярно создавать резервные копии конфигурации системы в качестве меры аварийного восстановления.

Шанс потерять данные конфигурации крайне низок, однако это возможно. Крайне важно обеспечить защиту резервных копий с помощью технических или организационных мер.

Резервное копирование и восстановление конфигурации системы (объяснение)

В системе предусмотрена встроенная функция резервного копирования всех конфигураций системы, которые можно задать в Management Client. База данных сервера регистрации и файлы журналов, в том числе файлы контрольного журнала, не включаются в эту резервную копию.

При работе со сложными системами Milestone рекомендует настроить резервное копирование по расписанию. Для этого используется сторонний инструмент: Microsoft® SQL Server Management Studio. Эта резервная копия включает те же данные, что и при резервном копировании вручную.

Во время резервного копирования система продолжает работать в режиме онлайн.

Резервное копирование конфигурации системы может занять некоторое время. Продолжительность резервного копирования зависит от следующих факторов:

- конфигурации системы;
- аппаратного обеспечения;
- типа установки компонентов SQL Server, Event Server и Management Server — на одном сервере или на нескольких серверах.

Во время резервного копирования, выполняемого вручную или по расписанию, происходит очистка файла журнала транзакций базы данных SQL Server. Дополнительные сведения о способах очистки файла журнала транзакций приведены в разделе Журнал транзакций базы данных SQL Server (объяснение) на стр. 151.

При создании резервной копии убедитесь, что вам известны параметры пароля для настройки конфигурации системы.

Для систем, соответствующих требованиям FIPS 140-2, с операциями экспорта и базами данных архивирования мультимедиа из версий VMS XProtect, предшествующих 2017 R1, шифрование которых выполнятся с помощью шифров, не соответствующих FIPS, данные необходимо архивировать там, где к ним можно будет получить доступ после включения FIPS. Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

Выбор общей папки резервного копирования

Перед выполнением резервного копирования и восстановления конфигурации системы необходимо создать папку резервного копирования.

1. Правой кнопкой мыши нажмите значок службы Management Server в области уведомлений и выберите **Выбрать общую папку резервного копирования**.
2. В появившемся окне выберите местонахождение нужного файла.
3. Нажмите **OK** два раза.
4. При запросе на удаление файлов в текущей папке резервного копирования выберите **Да** или **Нет** в зависимости от ваших потребностей.

Резервное копирование конфигурации системы вручную

1. В строке меню выберите **Файл** > **Резервная копия конфигурации**.
2. Ознакомьтесь с примечанием в диалоговом окне и нажмите **Резервное копирование**.
3. Укажите название файла в формате CNF.
4. Укажите путь к папке и нажмите **Сохранить**.
5. Дождитесь окончания резервного копирования и нажмите **Закрыть**.

Все соответствующие файлы конфигурации системы объединяются в один CNF-файл, который сохраняется в указанной папке. Во время резервного копирования файлы резервных копий сначала экспортируются во временную системную папку на сервере управления. Можно выбрать другую временную папку. Для этого правой кнопкой мыши нажмите значок службы Management Server в области уведомлений и выберите «Выбрать общую папку резервного копирования».

Восстановление конфигурации системы из резервной копии вручную

Важно!

- Пользователь, который выполняет установку, и пользователь, который восстанавливает данные, должен быть локальным администратором базы данных SQL Server конфигурации системы на сервере управления **и** в SQL Server.
- Во время восстановления система будет полностью остановлена за исключением серверов записи. Восстановление может занять некоторое время.
- Резервную копию можно восстановить только в той установке системы, в которой она была создана. Убедитесь, что настройки аналогичны тем, которые использовались при создании резервной копии. В противном случае может произойти сбой восстановления.
- Если при восстановлении запрашивается пароль для настройки системы, укажите пароль, который был действителен на момент создания резервной копии. Без этого пароля вы не сможете восстановить конфигурацию из резервной копии.
- Если вы выполняете резервное копирование базы данных SQL Server и восстанавливаете ее в чистую версию SQL Server, то не будут выдаваться сообщения об ошибках базы данных SQL Server. Вы получите только одно общее сообщение об ошибке SQL Server. Чтобы избежать этого, сначала переустановите систему XProtect, используя чистую версию SQL Server, а затем восстановите резервную копию.
- Если во время проверки произошел сбой восстановления, вы можете снова запустить прежнюю конфигурацию, так как она осталась без изменений.
  Если сбой произошел на другом этапе процесса, вы не сможете вернуться к прежней конфигурации.
  Если файл резервной копии не поврежден, вы можете выполнить повторное восстановление.
- Восстановленные данные заменяют текущую конфигурацию. Это означает, что изменения в конфигурации, внесенные после последнего резервного копирования, не сохранятся.
- Журналы, в том числе контрольные, не восстанавливаются.
- После запуска восстановления его нельзя отменить.

Восстановление

1. Правой кнопкой мыши нажмите значок службы Management Server в области уведомлений и выберите **Восстановить конфигурацию**.
2. Прочитайте важное примечание и нажмите **Восстановить**.
3. В открывшемся диалоговом окне перейдите к папке, где хранится файл резервной копии конфигурации системы, выберите его и нажмите **Открыть**.

   Файл резервной копии хранится на компьютере Management Client. Если компонент Management Client установлен на другом сервере, скопируйте файл резервной копии на этот сервер, прежде чем выбрать место

назначения.

4. Откроется окно **Восстановить конфигурацию**. Дождитесь окончания восстановления и нажмите **Закрыть**.

Пароль для настройки системы (объяснение)

Вы можете защитить конфигурацию системы с помощью установки пароля для настройки системы. После установки пароля для настройки системы резервные копии будут защищены этим паролем. Параметры пароля хранятся в защищенной папке на компьютере, на котором установлен сервер управления. Пароль потребуется, чтобы:

- восстановить конфигурацию из резервной копии, которая была создана с использованием параметров пароля, отличных от текущих параметров;
- переместить или установить сервер управления на другой компьютер из-за отказа оборудования (восстановление);
- настроить дополнительный сервер управления в системе с кластеризацией.

Пароль для настройки системы можно задать во время выполнения установки или после ее завершения. Сложность пароля должна соответствовать требованиям Windows, которые определяются политикой Windows для паролей.

Также необходимо учитывать, что системные администраторы должны сохранить этот пароль и держать его в надежном месте. Если вы задали пароль для настройки системы, то при восстановлении резервной копии может потребоваться ввести этот пароль. Без этого пароля вы не сможете восстановить конфигурацию из резервной копии.

Параметры пароля для настройки системы

Параметры пароля для настройки системы можно изменить. Доступны следующие варианты параметров пароля для настройки системы:

- защита конфигурацию системы с помощью установки пароля для настройки системы;
- изменение пароля для настройки системы;
- отказ от использования пароля для настройки системы и удаление всех назначенных ранее паролей.

Изменение параметров пароля для настройки системы

В случае изменения пароля важно, чтобы системные администраторы обеспечивали сохранность паролей, используемых для защиты резервных копий. При восстановлении резервной копии может потребоваться ввести пароль для настройки системы, который был действителен на момент создания резервной копии. Без этого пароля вы не сможете восстановить конфигурацию из резервной копии.

После изменения пароля потребуется также ввести текущий пароль для настройки системы на сервере событий, если сервер управления и сервер событий установлены на разных компьютерах. Дополнительные сведения приведены в разделе Ввод текущего пароля для настройки системы (сервер событий).

Изменения применяются после перезапуска служб сервера управления.

1. Найдите значок сервера управления на панели задач и убедитесь, что служба запущена.
2. Правой кнопкой мыши нажмите значок службы Management Server в области уведомлений и выберите **Изменить параметры пароля для настройки системы**.
3. Откроется окно изменения параметров пароля для настройки системы.

Назначение пароля

1. Введите новый пароль в поле **Новый пароль**.
2. Введите этот же пароль повторно в поле **Подтверждение нового пароля** и нажмите **ВВОД**.
3. Прочтите уведомление и нажмите **Да**, чтобы принять изменения.
4. Дождитесь подтверждения изменений и нажмите **Закрыть**.
5. Изменения применяются после перезапуска служб сервера управления.
6. После перезапуска убедитесь, что сервер управления работает.

Снятие защиты паролем

Если вам не требуется защита паролем, от нее можно отказаться.

1. Установите флажок: **Я предпочитаю не использовать пароль конфигурации системы и понимаю, что конфигурация системы не будет зашифрована** и нажмите **ВВОД**.
2. Прочтите уведомление и нажмите **Да**, чтобы принять изменения.
3. Дождитесь подтверждения изменений и нажмите **Закрыть**.
4. Изменения применяются после перезапуска служб сервера управления.
5. После перезапуска убедитесь, что сервер управления работает.

Ввод параметров пароля для настройки системы (восстановление)

При удалении файла с параметрами пароля (в результате сбоя оборудования или по другим причинам) потребуется указать параметры пароля для настройки системы, чтобы получить доступ к базе данных, содержащей конфигурацию системы. Во время установки на новый компьютер потребуется ввести параметры пароля для настройки системы.

Если файл с параметрами пароля удален или поврежден, а компьютер, на котором работает сервер управления, исправно работает, можно ввести параметры пароля конфигурации системы следующим способ:

1. Найдите значок сервера управления на панели задач.
2. Правой кнопкой мыши нажмите значок службы Management Server в области уведомлений и выберите **Ввести пароль для конфигурации системы**.
3. Откроется окно ввода параметров пароля для настройки системы.

Конфигурация системы защищена паролем

1. Введите пароль в поле **Пароль** и нажмите **ВВОД**.
2. Дождитесь подтверждения правильности пароля. Выберите **Закрыть**.
3. Убедитесь, что сервер управления запущен.

Конфигурация системы не защищена паролем

1. Установите флажок: **В этой системе не используется пароль конфигурации системы** и нажмите **ВВОД**.
2. Дождитесь подтверждения настроек. Выберите **Закрыть**.
3. Убедитесь, что сервер управления запущен.

Резервное копирование конфигурации системы вручную (объяснение)

Если вы хотите вручную выполнить резервное копирование базы данных сервера управления, содержащей конфигурацию системы, убедитесь, что система продолжает работать в режиме онлайн. Имя базы данных сервера управления по умолчанию — **Surveillance**.

Перед началом резервного копирования необходимо учесть следующие моменты:

- Резервную копию базы данных SQL Server нельзя использовать для копирования системных конфигураций в другие системы.
- Резервное копирование базы данных SQL Server может занять некоторое время. Продолжительность зависит от конфигурации системы, аппаратного обеспечения, а также от того, установлены ли SQL Server, сервер управления и Management Client на одном компьютере или нет.
- Журналы, включая контрольные, хранятся в базе данных сервера регистрации. Соответственно, они **не** являются частью резервной копии базы данных сервера управления. Имя базы данных сервера регистрации по умолчанию — **SurveillanceLogServerV2**. Резервное копирование обеих баз данных SQL Server выполняется аналогичным образом.

Резервное копирование и восстановление конфигурации сервера событий (объяснение)

Содержимое конфигурации сервера событий включается в резервное копирование и восстановление конфигурации системы.

При первом запуске сервера событий все файлы конфигурации автоматически перемещаются в базу данных SQL Server. Для применения восстановленной конфигурации к серверу событий не требуется перезапуск. При этом сервер событий может запускать и останавливать внешнее взаимодействие в ходе процесса восстановления конфигурации.

Запланированное резервное копирование и восстановление конфигурации системы (объяснение)

На сервере управления системные настройки хранятся в базе данных SQL Server. Milestone рекомендует регулярно создавать запланированные резервные копии этой базы данных в качестве меры аварийного восстановления. Шанс потерять данные конфигурации системы крайне низок, однако это возможно. Процесс займет не больше минуты. Кроме того, дополнительным преимуществом резервного копирования является очистка журнала транзакций базы данных SQL Server.

Если у вас небольшая система и не требуется запланированное резервное копирование, вы можете создать резервную копию конфигурации системы вручную. Инструкции приведены в разделе Резервное копирование конфигурации системы вручную (объяснение) на стр. 366.

При выполнении резервного копирования/восстановления сервера управления убедитесь, что база данных SQL Server с настройками системы включена в резервную копию/восстановление.

Требования к использованию запланированного резервного копирования и восстановления

Microsoft® SQL Server Management Studio. Этот инструмент можно бесплатно загрузить с веб-сайта (https://www.microsoft.com/downloads/).

Помимо управления SQL Server и базами данных в программе предусмотрены удобные функции резервного копирования и восстановления. Загрузите программу и установите ее на сервер управления.

Запланированное резервное копирование конфигурации системы

1. В меню «Пуск» Windows запустите Microsoft® SQL Server Management Studio.
2. При подключении укажите требуемое имя SQL Server. Используйте учетную запись, под которой вы создали базу данных SQL Server.
    1. Найдите базу данных SQL Server, содержащую полную конфигурацию системы, включая сервер событий, серверы записи, камеры, устройства ввода и вывода, пользователей, правила, профили патрулирования и т.д. Имя этой базы данных SQL по умолчанию — **Surveillance**.
    2. Создайте резервную копию базы данных SQL Server и проверьте следующее:
        - Убедитесь, что выбрана подходящая база данных SQL Server.
        - Убедитесь, что выбрано **полное** резервное копирование.
        - Запланируйте периодическое резервное копирование. Дополнительные сведения о запланированном и автоматизированном резервном копировании приведены на сайте Microsoft (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017)
        - Проверьте предложенный путь, при необходимости выберите другой путь.
        - Выберите **проверку резервного копирования по завершении** и **проверку контрольной суммы перед записью на носитель**.
3. Выполните все инструкции.

Аналогичным способом можно создать резервную копию базы данных сервера регистрации. Имя базы данных SQL Server сервера регистрации по умолчанию — **SurveillanceLogServerV2**.

Восстановление конфигурации системы с помощью запланированной резервной копии

Требования
Чтобы исключить изменение настроек системы во время восстановления базы данных конфигурации, остановите работу следующих служб:

- Служба Management Server (см. Управление службами сервера на стр. 383)
- Служба Event Server. Это можно сделать в разделе **Службы** Windows (выполните поиск по **services.msc** на вашем компьютере. В разделе **Службы** найдите **Milestone XProtect Event Server**))
- Служба World Wide Web Publishing Service, также известная как Internet Information Service (IIS). Подробнее о том, как остановить IIS (https://technet.microsoft.com/library/cc732317(WS.10).aspx/)

Откройте Microsoft® SQL Server Management Studio из меню **Пуск** Windows.

В инструменте выполните следующие действия:

1. При подключении укажите имя SQL Server. Используйте учетную запись пользователя, под которой была создана база данных SQL Server.
2. Найдите базу данных SQL Server (имя по умолчанию — **Surveillance**), содержащую полную конфигурацию системы, включая сервер событий, серверы записи, камеры, устройства ввода и вывода, пользователей, правила, профили патрулирования и т.д.
3. Восстановите базу данных SQL Server и выполните следующие действия:
   - Выберите резервное копирование **с** устройства.
   - Выберите тип носителя резервного копирования — **файл**.
   - Найдите и выберите файл резервной копии (**BAK**).
   - Выберите **перезапись существующей базы данных**.
4. Выполните все инструкции.

Аналогичным способом восстановите базу данных SQL Server на сервере регистрации с вашими журналами. Имя базы данных SQL Server сервера регистрации по умолчанию — **SurveillanceLogServerV2**.

Система не будет работать, пока остановлена служба Management Server. После восстановления базы данных не забудьте запустить все службы.

Резервное копирование базы данных сервера регистрации

Для работы с базой данных сервера регистрации используйте такой же метод, как и при работе с конфигурацией системы. База данных сервера регистрации содержит все системные журналы, в том числе ошибки, переданные серверами записи и камерами. Имя базы данных сервера регистрации по умолчанию — **SurveillanceLogServerV2**.

База данных SQL Server находится на сервере регистрации SQL Server. Как правило, сервер регистрации и сервер управления используют один SQL Server для хранения баз данных SQL Server. Резервное копирование базы данных сервера журналов не является критически важным действием, так как база данных не содержит данных о настройках системы. Тем не менее, наличие доступа к системным журналам, сохраненным до резервного копирования/восстановления сервера управления, может оказаться полезным.

Сценарии отказов и неполадок при резервном копировании и восстановлении (объяснение)

- Если после последнего резервного копирования конфигурации системы вы переместили сервер событий или другие зарегистрированные службы, например сервер регистрации, выберите нужную конфигурацию зарегистрированной службы для новой системы. Вы можете сохранить новую конфигурацию после восстановления предыдущей версии системы. Выберите подходящий вариант, ориентируясь на имена хостов служб.
- Если восстановление конфигурации системы не удалось из-за того, что по указанному адресу не обнаружен сервер событий (например, если вы выбрали старую настройку зарегистрированной службы), выполните повторное восстановление.
- Если при восстановлении резервной копии данных конфигурации введен неверный пароль для настройки системы, укажите пароль, который был действителен на момент создания резервной копии.

Перенос сервера управления

На сервере управления системные настройки хранятся в базе данных SQL Server. При переносе сервера управления с одного физического сервера на другой очень важно, чтобы у нового сервера управления тоже был доступ к этой базе данных SQL Server. Существует два различных способа хранения базы данных системных настроек:

- **СетевойSQL Server**: Если системные настройки хранятся в базе данных SQL Server на SQL Server в сети, при установке ПО сервера управления на новом сервере управления можно указать местонахождение базы данных на этом SQL Server. В этом случае применим только следующий параграф об имени хоста и IP-адресе сервера управления, а остальную часть темы следует проигнорировать:

  Имя хоста и IP-адрес сервера управления При переносе сервера управления с одного физического сервера на другой проще всего присвоить новому серверу имя хоста и IP-адрес старого сервера. Это объясняется тем, что для подключения сервер записи использует имя хоста и IP-адрес старого сервера управления. Если присвоить новому серверу управления новое имя хоста и (или) IP-адрес, сервер записи не сможет найти сервер управления, и вам потребуется вручную остановить каждую службу Recording Server в системе, изменить для нее URL-адрес сервера управления, вновь зарегистрировать сервер записи, а затем запустить службу Recording Server.

- **ЛокальныйSQL Server**: При хранении системных настроек в базе данных SQL Server на SQL Server на самом сервере управления важно выполнить резервное копирование системных настроек действующего сервера управления до начала переноса. Резервное копирование базы данных SQL Server с ее последующим восстановлением на SQL Server на новом сервере управления позволяет избежать повторной настройки камер, правил, профилей времени и т. п. после переноса

При переносе сервера управления для восстановления резервной копии потребуется текущий пароль для настройки системы (см. раздел Пароль для настройки системы (объяснение) на стр. 364).

Требования

- **Файл установки ПО для установки на новом сервере управления**
- **Файл лицензии программного обеспечения (.lic)**, полученный при покупке и первоначальной установке системы. Не используйте активированный файл лицензии программного обеспечения, полученный после активации лицензии, выполненной вручную в автономном режиме. Активированный файл лицензии программного обеспечения содержит информацию о конкретном сервере, на котором установлена система. В связи с этим при переносе на новый сервер нельзя использовать активированный файл лицензии программного обеспечения.

Если при переносе также выполняется обновление системного ПО, вы получили новый файл лицензии программного обеспечения. Используйте этот файл.

- Только при использовании **локальногоSQL Server способа: Microsoft® SQL Server Management Studio**
- Что происходит, пока сервер управления недоступен? Недоступность серверов управления (объяснение) на стр. 371
- Скопируйте базу данных сервера регистрации (см. раздел Резервное копирование базы данных сервера регистрации на стр. 369)

Недоступность серверов управления (объяснение)

- **Серверы записи по-прежнему могут вести запись**: Работающие в настоящее время серверы записи получили копию настроек от сервера управления, поэтому могут работать и хранить записи автономно даже после выключения сервера управления. Так, можно выполнять запись по расписанию и по движению, но запись по событию будет работать только в том случае, если она не настроена на события, связанные с сервером управления или другим сервером записи, так как данные этих событий проходят через сервер управления

- **Серверы записи временно хранят данные журналов в локальном режиме**: Они автоматически отправляют данные журналов на сервер управления, когда он вновь становится доступен:
  - **Клиенты не могут войти в систему**: Права доступа пользователей проверяются с помощью сервера управления. Без сервера управления вход клиентов в систему невозможен
  - **Клиенты, уже вошедшие в систему, могут находиться в ней не более четырех часов**: При входе клиентов в систему сервер управления проверяет их права доступа, после чего они могут взаимодействовать с серверами записи не более четырех часов. Если вы сможете настроить и запустить новый сервер управления в течение четырех часов, это не окажет влияния на большинство пользователей
  - **Не удается настроить систему**: Изменить системные настройки нельзя без сервера управления

Milestone рекомендует сообщить пользователям о риске потери связи с системой наблюдения, пока сервер управления выключен.

Перенос системных настроек

Перенос системных настроек осуществляется в три этапа:

1. Создание резервной копии системных настроек. Этот шаг идентичен резервному копированию по расписанию. Также см. Запланированное резервное копирование конфигурации системы на стр. 368.
2. Установка нового сервера управления на новом сервере. См. раздел «Резервное копирование по расписанию», шаг 2.
3. Восстановление системных настроек на новой системе. Также см. Восстановление конфигурации системы с помощью запланированной резервной копии на стр. 368.

Замена сервера записи

Если в работе сервера записи возникли проблемы, и его требуется заменить новым сервером с параметрами старого сервера записи:

1. Получите идентификатор старого сервера записи:
   1. Перейдите в раздел **Серверы записи** и выберите старый сервер записи на панели **Обзор**.
   2. Откройте вкладку **Хранилище**.
   3. Нажмите и удерживайте клавишу CTRL и выберите вкладку **Сведения**.

4. Скопируйте идентификатор сервера записи в нижней части вкладки **Сведения**. Копируйте только сам номер, без слова *ID*.

2. Замените идентификатор сервера записи на новом сервере записи:
    1. Остановите службу Recording Server на старом сервере записи, а затем измените значение параметра **Тип запуска** на **Отключена** в разделе **Службы** Windows.

> **!** Очень важно не допустить одновременного запуска двух серверов записи с одинаковыми идентификаторами.

    2. На новом сервере записи запустите Проводник и перейдите к `C:\ProgramData\Milestone\XProtect Recording Server` или папке, в которой находится сервер записи.
    3. Откройте файл `RecorderConfig.xml`.
    4. Удалите идентификатор (ID), указанный между тегами *<id>* и *</id>*.

    5. Вставьте скопированный идентификатор сервера записи между тегами *<id>* и *</id>*. Сохраните файл *RecorderConfig.xml*.
    6. Откройте реестр: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`.
    7. Откройте раздел **RecorderIDOnMachine** и замените старый идентификатор сервера записи новым идентификатором.
3. Зарегистрируйте новый сервер записи на сервере управления. Для этого нажмите значок Recording Server Manager на панели задач правой кнопкой мыши и выберите **Зарегистрировать**. Дополнительные сведения приведены в разделе Регистрация сервера записи на стр. 213.
4. Перезапустите службу Recording Server. После запуска службы Recording Server к ней будут применены все настройки из старого сервера записи.

Move hardware

Вы можете перемещать оборудование между серверами записи, которые относятся к одному сайту. После перемещения оборудование и связанные с ним устройства будут работать на новом сервере записи. Новые записи также будут храниться на этом сервере. Процесс перемещения оборудования

проходит незаметно для пользователей клиента.

Записи остаются на старом сервере, пока не наступят следующие события:

- Система удалит данные по истечении времени хранения. Записи с защитой доказательств (см. Защита доказательств (объяснение) на стр. 84) не удаляются до истечения времени хранения защиты доказательств. Время хранения защиты доказательств задается в процессе их создания. Теоретически, время хранения не ограничено.
- Записи можно удалить с нового сервера записи каждого устройства на вкладке **Запись**.

При попытке удалить сервер записи, который все еще содержит записи, вы получите соответствующее предупреждение.

> При перемещении оборудования на сервер записи, на котором в настоящее время нет оборудования, пользователи клиента должны выйти из системы и войти в нее снова, чтобы получать данные с устройств.

Функция перемещения оборудования используется в следующих случаях:

- **Балансировка нагрузки**. При перегрузке диска на сервере записи можно добавить новый сервер записи и переместить часть оборудования.
- **Обновление**. При необходимости замены сервера, на котором расположен сервер записи, на новую модель можно установить новый сервер записи и переместить на него оборудование со старого сервера.
- **Замена отказавшего сервера записи**. Если сервер перестал работать в режиме онлайн, вы можете переместить оборудование на другие серверы записи и сохранить работоспособность системы. Вы не сможете получить доступ к старым записям. Дополнительные сведения приведены в разделе Замена сервера записи на стр. 372.

Дистанционные записи

При перемещении оборудования на другой сервер записи система отменяет выполнение текущих или запланированных операций по получению данных со связанных сайтов или с накопителей для хранения данных на камерах. Записи не удаляются, но ожидаемого получения и сохранения данных в базах данных не происходит. В этом случае отображается предупреждение. Получение данных для пользователя XProtect Smart Client, который приступил к получению данных после начала переноса оборудования, завершится сбоем. Пользователь XProtect Smart Client получит уведомление и может повторить попытку позднее.

Если оборудование на удаленном объекте было перенесено, необходимо вручную синхронизировать центральный объект с параметром **Обновить оборудование** для отражения новых настроек на удаленном объекте. Без синхронизации перенесенные камеры на центральном объекте останутся отключенными.

Перенос оборудования (мастер)

Для переноса оборудования с одного сервера записи на другой запустите мастер **Перенос оборудования**. Мастер поможет вам выполнить действия, необходимые для переноса одного или нескольких аппаратных устройств.

Требования
Перед запуском мастера:

- Убедитесь, что у нового сервера записи есть доступ к камере по сети
- Установите сервер записи, на который вы хотите перенести оборудование (см. Установка с помощью Download Manager (объяснение) на стр. 184 или Автоматическая установка сервера записи на стр. 194)
- Установите на новом сервере записи тот же комплект драйверов, который вы используете на действующем сервере (см. раздел Драйверы устройств (объяснение) на стр. 161)

Для запуска мастера:

1. На панели **Навигация по сайту** выберите **Серверы записи**.
2. На панели **Обзор** нажмите правой кнопкой мыши сервер записи, из которого нужно перенести оборудование, или нажмите правой кнопкой мыши конкретное аппаратное устройство.
3. Нажмите **Переместить оборудование**.

   Если сервер записи, из которого вы переносите оборудование, отключен, появится сообщение об ошибке. Переносите оборудование из отключенного сервера записи, только если вы уверены, что он больше никогда не будет подключен к сети. Если вы все равно решите перенести оборудование, а сервер будет вновь подключен к сети, вы рискуете столкнуться с непредвиденным поведением системы, так как одно и то же оборудование будет в течение некоторого времени работать на двух серверах записи. В числе возможных проблем — проблемы с лицензией или с невозможностью отправки событий на правильный сервер записи.

4. При запуске мастера с уровня сервера записи отображается страница **Выберите оборудование, которое хотите перенести**. Выберите аппаратные устройства, которые хотите перенести.
5. На странице **Выберите, на какой сервер записи вы хотите переместить оборудование** выберите необходимый пункт из списка серверов записи, установленных на этом объекте.
6. На странице **Выберите, какое хранилище вы хотите использовать для последующих записей** в панели использования хранилища отображается свободное место в базе данных записи, доступное только для записей в режиме реального времени, а не для архивов. Общее время хранения — это время хранения как для базы данных записи, так и для архивов.

7. Система обработает ваш запрос.
8. Если перенос успешно завершен, нажмите кнопку **Закрыть**. При выборе нового сервера записи в Management Client отображается перенесенное оборудование. Теперь записи хранятся на этом сервере.

   Для устранения неполадок с переносом воспользуйтесь приведенными ниже сведениями.

   > Во взаимосвязанной системе после переноса оборудования на удаленном объекте необходимо вручную синхронизировать центральный объект, чтобы отразить изменения, внесенные на удаленном объекте вами или другим системным администратором.

Устранение неполадок при переносе оборудования

Сбой при переносе оборудования может возникнуть по одной из следующих причин:

Тип ошибки	Способ устранения
Сервер записи не подключен или находится в режиме отработки отказа.	Убедитесь, что сервер записи подключен к сети. Возможно, сервер потребуется зарегистрировать. Если сервер находится в режиме отработки отказа, подождите и повторите операцию.
Сервер записи не соответствует последней версии.	Обновите сервер записи, чтобы его версия не отличалась от версии сервера управления.
Сервер записи не найден в данной конфигурации.	Убедитесь, что сервер записи не удален.
Сбой при обновлении настроек или обмене данными с базой данных конфигурации.	Убедитесь, что ваш SQL Server и база данных подключены и работают.
Сбой остановки оборудования на текущем сервере записи	Возможно, сервер записи заблокирован другим процессом или находится в режиме обработки ошибок. Убедитесь в работоспособности сервера записи и повторите операцию.

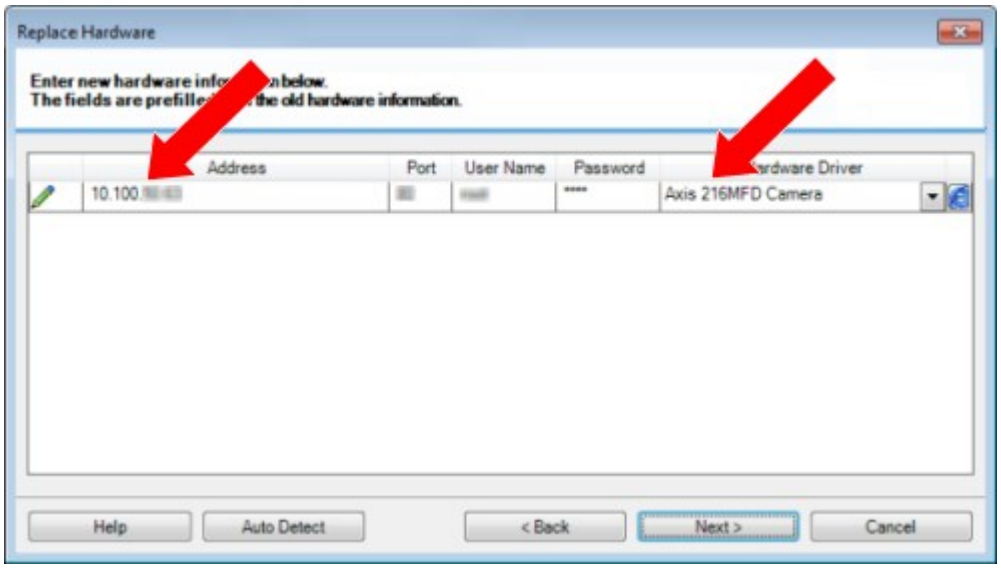
Тип ошибки	Способ устранения
Оборудование не существует.	Убедитесь, что оборудование, которое вы пытаетесь перенести, не было одновременно отключено от системы другим пользователем. Этот сценарий маловероятен.
Сервер записи, из которого перенесено оборудование, вновь подключен к сети, но вы проигнорировали этот сценарий, когда он был отключен от сети.	Вероятнее всего, при запуске мастера **Перенос оборудования** вы предположили, что старый сервер записи никогда не будет подключен к сети, но именно это и произошло во время переноса. Запустите мастер вновь и выберите пункт **Нет** при ответе на вопрос, подтверждаете ли вы, что сервер никогда не будет подключен к сети.
Хранилище записей на источнике недоступно.	Вы пытаетесь перенести оборудование с устройствами, настроенными на использование хранилища записей, которое сейчас отключено от сети. Хранилище записей отключено от сети, если диск отключен от сети либо недоступен по иной причине. Убедитесь, что хранилище записей подключено к сети и повторите операцию.
Обеспечьте доступность всех хранилищ записей на целевом сервере записи.	Вы пытаетесь перенести оборудование на сервер записи, на котором одно или несколько хранилищ записей не подключены к сети. Подключите к сети все хранилища записей на целевом сервере записи. Хранилище записей отключено от сети, если диск отключен от сети либо недоступен по иной причине.

Замена оборудования

При замене аппаратного устройства в сети другим аппаратным устройством необходимо знать IP-адрес, порт, имя пользователя и пароль нового устройства.

Если вы не включили автоматическую активацию лицензии (см. раздел Автоматическая активация лицензии (объяснение) на стр. 132) и внесли изменения в устройства без активации (см. раздел Изменения устройств без активации (объяснение) на стр. 133), **после** замены аппаратных устройств лицензию необходимо активировать вручную. Если новое количество аппаратных устройств превышает общее количество лицензий на устройства, потребуется приобрести новые лицензии на устройства.

1. Откройте раздел требуемого сервера записи и нажмите оборудование, которое требуется заменить, правой кнопкой мыши.
2. Выберите пункт **Заменить оборудование**.
3. Откроется мастер **Замена оборудования**. Нажмите **Далее**.
4. В поле **Адрес** мастера (отмечено красной стрелочкой на изображении) введите IP-адрес нового оборудования. Выберите соответствующий драйвер (если известен) из раскрывающегося списка **Драйвер аппаратного устройства**. В противном случае нажмите **Автоматически определять**. Если для нового оборудования используется другой порт, имя пользователя или пароль, внесите изменения **до запуска автоматического определения (если он необходим)**.



В базу данных мастера уже внесены данные о существующем оборудовании. При замене аппаратного устройства на аналогичное некоторые из этих данных (например, сведения о порте и драйвере) можно использовать повторно.

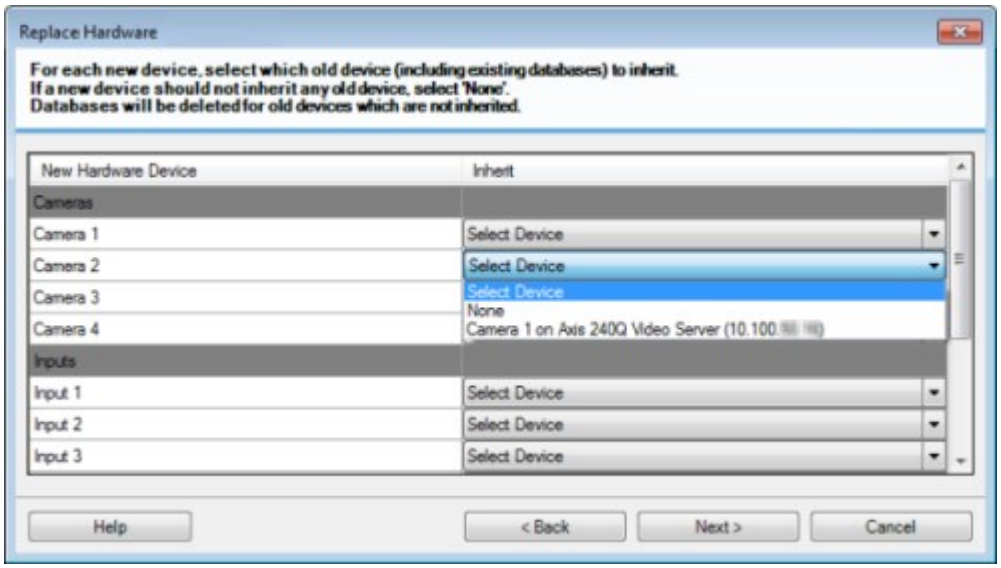
5. Выполните одно из следующих действий:

   - Если вы выбрали необходимый драйвер аппаратного устройства непосредственно из списка, нажмите **Далее**
   - Если в списке вы выбрали **Автоматически определять**, нажмите **Автоматически определять**, дождитесь успешного завершения процесса (при этом с правого края появится символ ✔), а затем нажмите **Далее**.

     Этот шаг выполняется для привязки устройств к своим базам данных в зависимости от количества отдельных камер, микрофонов, вводов, выводов и т. п., присоединенных к старому и новому аппаратному устройству соответственно.

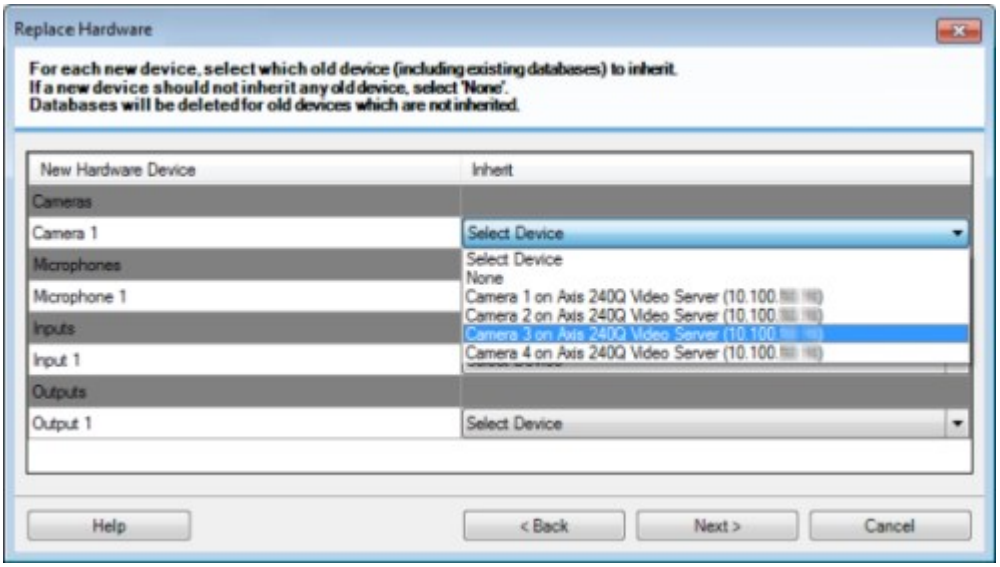
     Важно понимать, **как** выполняется привязка баз данных из старого аппаратного устройства к базам данных нового аппаратного устройства. Привязка отдельных устройств выполняется путем выбора соответствующей камеры, микрофона, ввода, вывода либо пункта **Нет** в правом столбце.

     > ⚠ Обязательно привяжите **все** камеры, микрофоны, вводы, выводы и т. п. Если содержимое привязано к пункту **Нет**, оно будет **утрачено**.

     Пример старого аппаратного устройства, у которого больше отдельных устройств, чем у

нового:



Нажмите **Далее**.

6. Откроется список оборудования, которое нужно добавить, заменить или удалить. Нажмите **Подтвердить**.
7. Последний этап — общие сведения о добавленных, замененных и унаследованных устройствах и об их настройках. Нажмите кнопку **Скопировать в буфер обмена**, чтобы скопировать содержимое в буфер обмена Windows и (или) **Закрыть**, чтобы закрыть мастер.

Обновление данных об оборудовании

Чтобы аппаратное устройство и система использовали одинаковую версию прошивки, необходимо вручную обновить данные об аппаратном устройстве в Management Client. Milestone рекомендует обновлять данные об оборудовании после каждого обновления прошивки аппаратного устройства.

Для получения последних данных об оборудовании:

1. На панели **Навигация по сайту** выберите **Серверы записи**.
2. Откройте раздел требуемого сервера записи и выберите оборудование, для которого необходимо получить последнюю информацию.
3. На панели **Свойства** во вкладке **Сведения** нажмите кнопку **Обновить** в поле **Последнее обновление данных об оборудовании**.

4. Мастер проверит, установлена ли в системе последняя прошивка для оборудования.

   Нажмите кнопку **Подтвердить**, чтобы обновить информацию в Management Client. После завершения обновления текущая версия прошивки аппаратного устройства, обнаруженная системой, отобразится в поле **Версия прошивки** на вкладке **Сведения**.

Изменение местонахождения и имени базы данных SQL Server

Сервер управления, сервер событий, сервер журналов, Identity Provider и XProtect Incident Manager подключаются к различным базам данных SQL Server с помощью строк подключения. Строки подключения хранятся в системном реестре Windows. В случае изменения местонахождения или имени базы данных SQL Server отредактируйте все строки подключения, связанные с базой данных SQL Server.

База данных	Используется
База данных системы наблюдения	• Служба Management Server • Служба Event Server • Пул приложений VideoOS Management Server • Пул приложений VideoOS сервера отчетов
Surveillance_IDP	• Пул приложений VideoOS IDP
Surveilance_IM	• Пул приложений VideoOS IM
Surveillance_LogServerV2	• Служба Log Server

Прежде чем продолжить, выполните следующие действия:

- Создайте резервные копии баз данных SQL Server и системного реестра Windows.
- Убедитесь, что пользователь, запускающий соответствующие службы и пулы приложений, является владельцем базы данных.
- Завершите перенос содержимого из старой базы данных SQL Server в новую.

Чтобы обновить строки подключения с учетом нового местонахождения и имени базы данных SQL Server, выполните следующие действия:

1. Остановите все службы VMX XProtect и пулы приложений, использующие базу данных SQL Server.

   > Службы и пулы приложений могут работать на разных компьютерах в зависимости от архитектуры системы. Остановите все пулы приложений и службы, которые подключаются к одной базе данных SQL Server.

2. В редакторе реестра откройте `HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString`.
3. Обновите строки подключения с учетом нового местонахождения и имени базы данных SQL Server.

   По умолчанию для всех баз данных SQL Server используются следующие строки подключения:

   - **ManagementServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **EventServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ServerService**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ReportServer**: `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IDP**: `Data Source=localhost;Initial Catalog=Surveillance_IDP;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IncidentManager**: `Data Source=localhost;Initial Catalog=Surveillance_IM;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **LogServer**: `Data Source=localhost;Initial Catalog=SurveillanceLogServerV2;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`

4. Запустите все службы XProtect и пулы приложений, которые были остановлены на шаге 1.

Управление службами сервера

На компьютере, где выполняются службы сервера, в области уведомлений на панели задач отображаются значки диспетчера сервера. С помощью этих значков можно получить информацию о службах и выполнить определенные задачи. В частности, можно проверить состояние служб, просмотреть журналы или сообщения о состоянии, а также запустить и остановить службы.

Значки диспетчера сервера на панели задач (объяснение)

В таблице приведены значки на панели задач, которые отражают различные состояния служб, запущенных на сервере управления, сервере записи, отказоустойчивом сервере записи и сервере событий. Значки отображаются в области уведомлений на компьютерах с установленными серверами:

Значок Management Server Manager на панели задач	Значок Recording Server Manager на панели задач	Значок Event Server Manager на панели задач	Значок Failover Recording Server Manager на панели задач	Описание
				**Работа** Отображается при включении и запуске службы сервера. Если служба Failover Recording Server запущена, она может принять на себя функции стандартных серверов записи в случае их сбоя.
				**Остановлено** Отображается при остановке службы сервера.

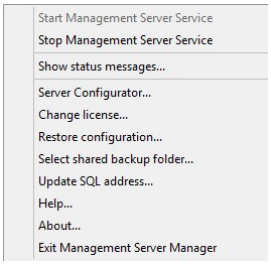
Значок Management Server Manager на панели задач	Значок Recording Server Manager на панели задач	Значок Event Server Manager на панели задач	Значок Failover Recording Server Manager на панели задач	Описание
				Если служба Failover Recording Server приостанавливает работу, она может принять на себя функции стандартных серверов записи в случае их сбоя.
				**Запуск** Отображается, когда служба сервера находится в процессе запуска. Как правило, через некоторое время значок на панели задач меняется на **Работает**.
				**Остановка** Отображается, когда служба сервера находится в процессе остановки. Как правило, через некоторое время значок на панели задач меняется на **Остановлен**.
				**В неизвестном состоянии** Отображается при первоначальной загрузки службы сервера и до получения первых данных, после чего значок на панели задач, как правило, меняется на **Запуск**, а затем на **Работает**.

Значок Management Server Manager на панели задач	Значок Recording Server Manager на панели задач	Значок Event Server Manager на панели задач	Значок Failover Recording Server Manager на панели задач	Описание
				**Работает — автономный режим** Как правило, отображается, когда сервер записи или резервная служба записи выполняется, а служба Management Server — нет.

Запуск или остановка службы Management Server

Значок Management Server Manager на панели задач отражает состояние службы Management Server. Например: **работает**. С помощью этого значка можно запустить или остановить службу Management Server. При остановке службы Management Server вы не сможете использовать Management Client.

1. Нажмите значок Management Server Manager в области уведомлений правой кнопкой мыши. Откроется контекстное меню.



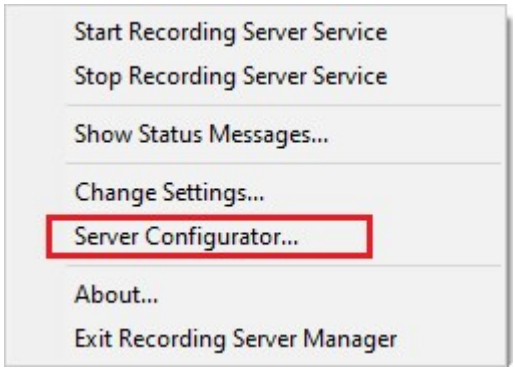
2. Если служба остановлена, нажмите **Запустить службу Management Server**. Значок на панели задач изменится в соответствии с новым состоянием.
3. Чтобы остановить службу, нажмите **Остановить службу Management Server**.

Дополнительные сведения о значках на панели задач приведены в разделе Значки диспетчера сервера на панели задач (объяснение) на стр. 383.

Запуск или остановка службы Recording Server

Значок Recording Server Manager на панели задач отражает состояние службы Recording Server. Например: **работает**. С помощью этого значка можно запустить или остановить службу Recording Server. При остановке службы Recording Server система не сможет взаимодействовать с устройствами, подключенными к серверу. Это означает, что вы не сможете просматривать видео в режиме реального времени или записывать видео.

1. Нажмите значок Recording Server Manager в области уведомлений правой кнопкой мыши. Откроется контекстное меню.

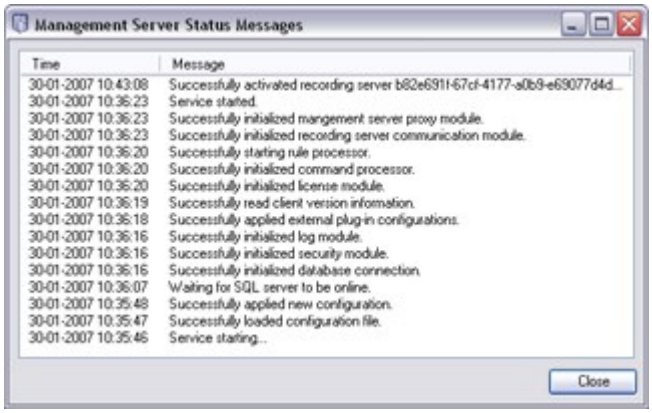


2. Если служба остановлена, нажмите **Запустить службу Recording Server**. Значок на панели задач изменится в соответствии с новым состоянием.
3. Чтобы остановить службу, нажмите **Остановить службу Recording Server**.

Дополнительные сведения о значках на панели задач приведены в разделе Значки диспетчера сервера на панели задач (объяснение) на стр. 383.

Просмотр сообщений о состоянии сервера управления или сервера записи

1. Нажмите соответствующий значок на панели задач в области уведомлений правой кнопкой мыши. Откроется контекстное меню.
2. Выберите **Просмотр сообщений о статусе**. В зависимости от типа сервера появится окно **Сообщения о состоянии сервера управления** или **Сообщения о состоянии сервера записи**. В этом окне отображаются сообщения о состоянии с метками времени:



Управление шифрованием с помощью Server Configurator

Чтобы выбрать сертификаты на локальных серверах для шифрования связи, а также зарегистрировать службы сервера и обеспечить их взаимодействие с серверами, используйте Server Configurator.

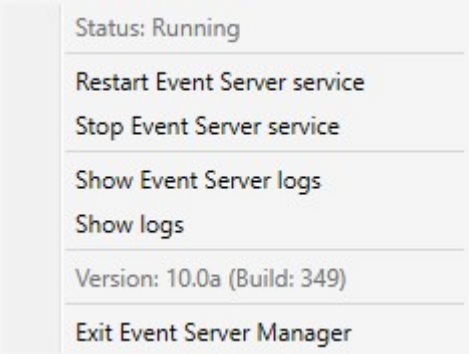
Откройте Server Configurator из меню «Пуск», с помощью значка сервера управления или значка сервера записи на панели задач. См. раздел Server Configurator (служебная программа) на стр. 440.

Дополнительные сведения см. в руководстве по сертификатам, посвященном защите систем XProtect VMS.

Запуск, остановка или перезапуск службы Event Server

Значок Event Server Manager на панели задач отражает состояние службы Event Server. Например: **работает**. С помощью этого значка можно запустить, остановить или перезапустить службу Event Server. При остановке службы некоторые компоненты системы, включая события и сигналы тревоги, не будут работать. Однако вы по-прежнему сможете просматривать и записывать видео. Дополнительные сведения приведены в разделе Остановка службы Event Server на стр. 388.

1. Нажмите значок Event Server Manager в области уведомлений правой кнопкой мыши. Откроется контекстное меню.



2. Если служба остановлена, нажмите **Запустить службу Event Server**. Значок на панели задач изменится в соответствии с новым состоянием.
3. Чтобы перезапустить или остановить службу, нажмите **Перезапустить службу Event Server** или **Остановить службу Event Server**.

Дополнительные сведения о значках на панели задач приведены в разделе Значки диспетчера сервера на панели задач (объяснение) на стр. 383.

Остановка службы Event Server

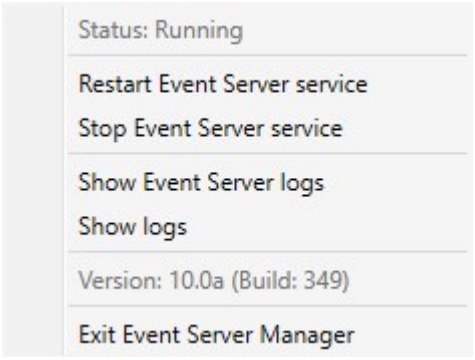
При установке расширений MIP на сервере событий сначала остановите службу Event Server, а затем перезапустите ее. Во время остановки службы некоторые компоненты системы VMS не будут функционировать:

- События и сигналы тревоги не будут сохраняться на сервере событий. Однако события в системе и на устройстве по-прежнему будут активировать действия, например начало записи.
- Расширения XProtect не будут работать в XProtect Smart Client, и их нельзя будет настроить с помощью Management Client.
- Не будут срабатывать события аналитики.
- Не будут срабатывать типичные события.
- Не будут срабатывать сигналы тревоги.
- Не будут работать элементы представления карты, элементы представления списка сигналов и рабочая область диспетчера сигналов в XProtect Smart Client.
- Не будут запускаться расширения MIP на сервере событий.
- Расширения MIP в Management Client и XProtect Smart Client будут работать некорректно.

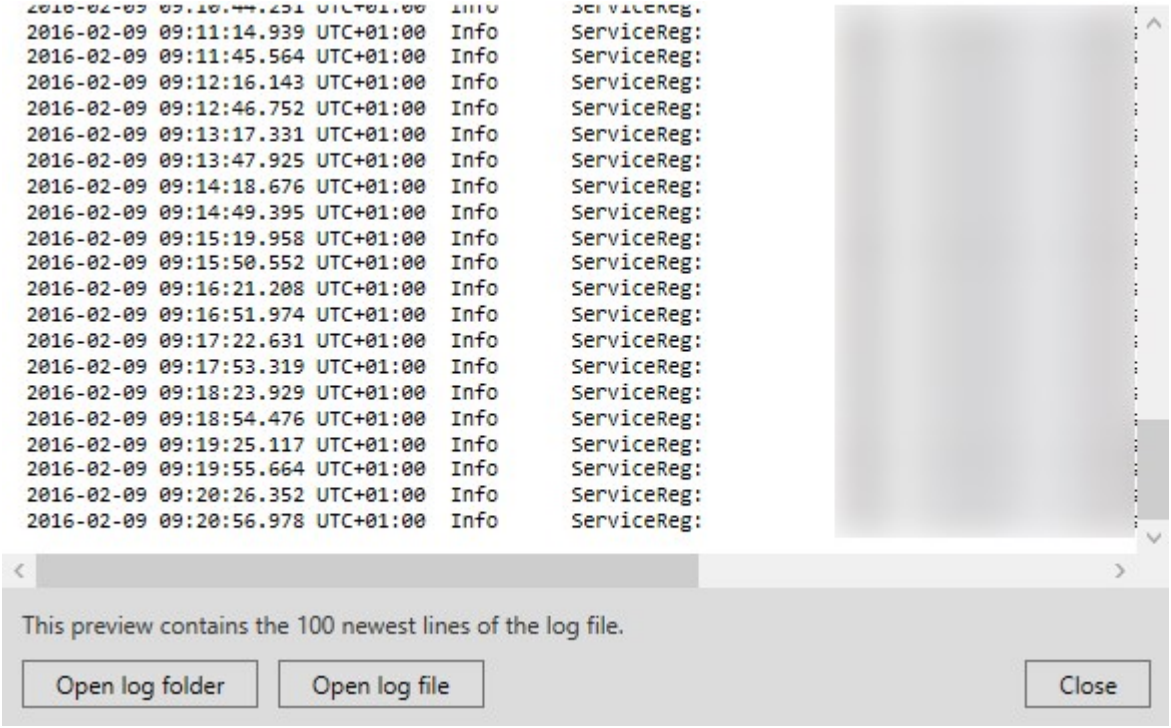
Просмотр журналов сервера событий MIP

В журнале сервера событий можно просмотреть информацию о действиях сервера событий с метками времени. Информация о модулях интеграции сторонних производителей записывается в журнал MIP в подпапке папки **сервера событий**.

1. Нажмите значок Event Server Manager в области уведомлений правой кнопкой мыши. Откроется контекстное меню.



2. Чтобы посмотреть 100 последних строк в журнале Event Server, нажмите **Показать журналы сервера событий**. Откроется средство просмотра журналов.



   1. Нажмите **Открыть файл журнала**, чтобы посмотреть файл журнала.
   2. Нажмите **Открыть папку журнала**, чтобы открыть соответствующую папку.

3. Чтобы просмотреть 100 последних строк в журнале MIP, вернитесь в контекстное меню и нажмите **Показать журналы MIP**. Откроется средство просмотра журналов.

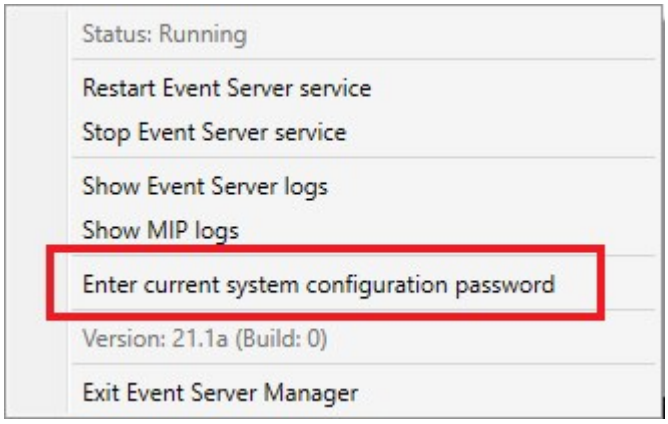
> В случае удаления файла журнала из каталога пункты меню становятся неактивными. Чтобы открыть средство просмотра журналов, сначала нужно скопировать файл журнала и поместить его в соответствующую папку: `C:\ProgramData\Milestone\XProtect Event Server\logs` или `C:\ProgramData\Milestone\XProtect Event Server\logs\MIP Logs`.

Введите текущий пароль конфигурации системы

Если пароль для настройки системы на сервере управления изменен, необходимо ввести текущий пароль для настройки системы на сервере событий.

> Если этого не сделать, то компоненты системы, в том числе управление доступом, прекратят работу.

1. Нажмите значок Event Server Manager в области уведомлений правой кнопкой мыши. Откроется контекстное меню.



2. Для ввода текущего пароля для настройки системы нажмите **Введите текущий пароль конфигурации системы**. Появится новое окно.
3. Введите тот же пароль для настройки системы, который введен на сервере управления.

Управление зарегистрированными службами

В отдельных случаях возникает необходимость взаимодействия серверов и (или) служб с системой, к которой они напрямую не относятся. Отдельные службы могут автоматически регистрироваться в системе. К числу таких служб относятся:

- Служба Event Server
- Служба Log Server

Автоматически зарегистрированные службы отображаются в соответствующем списке.

Серверы/службы можно вручную определить как зарегистрированные службы в Management Client.

Добавление и редактирование зарегистрированных служб

1. В окне **Добавить/удалить зарегистрированные службы** нажмите **Добавить** или **Изменить** в зависимости от задачи.
2. В окне **Добавить зарегистрированную службу** или **Изменить зарегистрированную службу** (в зависимости от выбранного ранее варианта) задайте или измените настройки.
3. Нажмите кнопку **OK**.

Управление конфигурацией сети

В параметрах конфигурации сети можно указать адреса сервера управления в локальной и глобальной сети (LAN и WAN), чтобы обеспечить обмен данными между сервером управления и доверенными серверами.

1. В окне **Добавить/удалить зарегистрированные службы** нажмите **Сеть**.
2. Укажите IP-адрес сервера управления в локальной или глобальной сети.

   Если все задействованные серверы (сервер управления и доверенные серверы) находятся в локальной сети, достаточно указать адрес локальной сети. Если доступ одного или нескольких задействованных серверов к системе осуществляется через интернет-соединение, укажите также адрес в глобальной сети.

3. Нажмите кнопку **OK**.

Свойства зарегистрированных служб

В окне **Добавить зарегистрированную службу** или **Изменить зарегистрированную службу** укажите следующее:

Компонент	Требование
Тип	Предварительно заполненное поле.
Имя	Имя зарегистрированной службы. Имя используется только для отображения в Management Client.
URL-адреса	Нажмите **Добавить**, чтобы добавить IP-адрес или имя хоста зарегистрированной службы. При указании имени хоста в качестве части URL-адреса необходимо использовать существующий хост, который доступен в сети. URL-адреса должны начинаться с *http://* или *https://* и не должны содержать ни один из следующих символов: < > & ' " * ? | [ ] ". **Пример** стандартного формата URL-адреса: *http://ipaddress:port/directory* (где port (порт) и directory (каталог) являются необязательными). При необходимости можно добавить несколько URL-адресов.
Доверенные	Установите этот флажок, чтобы настроить доверие для зарегистрированной службы (это актуально в большинстве случаев, однако этот параметр обеспечивает возможность добавить зарегистрированную службу, а затем отметить ее как доверенную при последующем редактировании). Изменение статуса доверия влияет и на статус других зарегистрированных служб, использующих один или несколько URL-адресов, заданных для соответствующей зарегистрированной службы.
Описание	Описание зарегистрированной службы. Описание используется только для отображения в Management Client.
Advanced	Если используется расширенная версия службы, она включает определенные схемы URI (например, HTTP, HTTPS, TCP или UDP), которые необходимо настроить для каждого заданного адреса хоста. Таким образом, адрес хоста имеет несколько конечных точек, каждая из которых имеет свою схему, а также соответствующий адрес хоста и IP-порт.

Удаление драйверов устройств (объяснение)

Если на компьютере больше не нужны драйверы устройств, комплекты драйверов можно удалить из системы. Для этого выполните стандартную процедуру удаления программ из Windows.

Если установлено несколько пакетов драйверов, и при удалении файлов возникли проблемы, для их полного удаления можно воспользоваться сценарием из установочной папки пакета драйверов.

В случае удаления пакетов драйверов связь между сервером записи и камерами станет невозможной. Не удаляйте пакеты драйверов при обновлении компонентов: новую версию можно установить поверх старой. Удаление пакета драйверов допускается только при удалении всей системы.

Удаление сервера записи

При удалении сервера записи удаляются его настройки, указанные в Management Client, включая **все** связанное с ним оборудование (камеры, устройства ввода и т. п.).

1. На панели **Обзор** нажмите сервер записи, который необходимо удалить, правой кнопкой мыши.
2. Выберите **Удалить сервер записи**.
3. Если вы уверены, нажмите кнопку **Да**.
4. Сервер записи и все связанное с ним оборудование удалены.

Удаление всего оборудования с сервера записи

При удалении оборудования все связанные с ним данные удаляются безвозвратно.

1. Нажмите правой кнопкой мыши сервер записи, на котором нужно удалить оборудование.
2. Выберите **Удалить все устройства**.
3. Подтвердите удаление.

Изменение имени хоста на компьютере сервера управления

Если адрес сервера управления соответствует полному доменному имени (FQDN) или имени хоста, изменение имени хоста на этом компьютере повлечет за собой изменения в XProtect, которые необходимо принять во внимание и устранить.

К изменению имени хоста сервера управления следует подходить с особой тщательностью, так как впоследствии может возникнуть необходимость в очистке данных.

В следующих разделах описываются возможные осложнения в работе, связанные с изменением имени хоста.

Срок действия сертификатов

Сертификаты используются для шифрования обмена данными между службами. Сертификаты устанавливаются на всех компьютерах, на которых работает одна или несколько служб XProtect.

В зависимости от способа создания сертификатов они могут быть привязаны к компьютеру, на котором установлены. Тогда они будут действительны только при условии, что имя компьютера остается неизменным.

Дополнительные сведения о создании сертификатов см. в разделе, посвященном основным сведениям о сертификатах.

При изменении имени компьютера используемые сертификаты могут стать недействительными, а VMS XProtect не удастся запустить. Чтобы возобновить работу системы, выполните следующие действия:

- Создайте новые сертификаты и переустановите их на всех компьютерах.
- С помощью Server Configurator примените новые сертификаты на всех компьютерах, чтобы включить шифрование данных.

В результате новые сертификаты будут зарегистрированы, а система снова начнет работать.

Потеря свойств данных клиентов зарегистрированных служб

Если вы завершаете регистрацию с помощью Server Configurator после изменения, например, адреса сервера управления, то все изменения данных зарегистрированных служб будут перезаписаны. Соответственно, если вы изменили данные зарегистрированных служб, изменения должны быть применены для всех служб, зарегистрированных на сервере управления, на компьютере с измененным именем.

Данные зарегистрированных служб, которые можно редактировать, доступны в разделе **Инструменты** > **Зарегистрированные службы** > **Изменить**:

- Доверенные
- Advanced
- Флаг «Внешняя»
- Любой URL-адрес, добавленный вручную

В Milestone Customer Dashboard имя хоста будет отображаться без изменений.

Milestone Customer Dashboard — это бесплатный онлайн-инструмент для партнеров, реселлеров Milestone и пользователей XProtect, предназначенный для управления и мониторинга программного обеспечения и лицензий Milestone.

Изменение имени сервера управления в системе, которая подключена к Milestone Customer Dashboard, не будет автоматически отображаться в Milestone Customer Dashboard.

Старое имя хоста будет отображаться в Milestone Customer Dashboard до завершения активации новой лицензии. Изменение имени не нарушает работу Milestone Customer Dashboard. После новой активации запись в базе данных обновится и будет содержать новое имя хоста. Дополнительные сведения о Milestone Customer Dashboard приведены в разделе Milestone Customer Dashboard (описание)

Изменение имени хоста может привести к изменению адреса SQL Server.

Если SQL Server располагается на том же компьютере, что и сервер управления, то при изменении имени этого компьютера изменится и адрес SQL Server. Таким образом адрес SQL Server потребуется обновить для компонентов, расположенных на разных компьютерах, а также для компонентов на локальном компьютере, которые для подключения к SQL Server используют имя компьютера вместо localhost. В частности, это касается компонента Event Server, который использует ту же базу данных, что и Management Server. Кроме того, это может быть применимо к компоненту Log Server, который использует другую базу данных, если она находится на том же SQL Server.

См. раздел Изменение местонахождения и имени базы данных SQL Server на стр. 381.

Изменение имени хоста в Milestone Federated Architecture

Изменение имени компьютера, подключенного к системе Milestone Federated Architecture, приведет к определенным последствиям. Это касается я не только сайтов, подключенных внутри рабочих групп, но доменов.

Хост сайта — корневой узел архитектуры

Если изменить имя компьютера, на котором работает центральный объект архитектуры, то все дочерние узлы автоматически переподключатся к новому адресу. В этом случае переименование не предполагает никаких дополнительных действий.

Хост сайта — дочерний узел архитектуры

Чтобы избежать проблем с подключением при изменении имени компьютера, на котором работает один или несколько федеративных сайтов, добавьте альтернативный адрес на задействованный сайт перед переименованием компьютера. Задействованный сайт — это узел, хост-компьютер которого будет переименован. Дополнительные сведения о проблемах с подключением, вызванных незапланированными или непредусмотренными изменениями имен хостов, и о способах их устранения приведены в разделе Проблема: главный узел в схеме Milestone Federated Architecture не может подключиться к дочернему узлу.

Альтернативный адрес добавляется в области **Свойства** на панели **Навигация по сайту** или на панели **Иерархия федеративных сайтов**. Должны быть соблюдены следующие предварительные условия:

- Альтернативный адрес добавлен и доступен до переименования хост-компьютера.
- Альтернативный адрес соответствует новому имени хост-компьютера (используемому при переименовании).

Дополнительные сведения о получении доступа к панели **Свойства** приведены в разделе Настройка свойств сайта.

Чтобы обновление прошло без осложнений, остановите работу Management Client на узле, который является родительским по отношению к узлу, на котором будет изменено имя хоста. В противном случае остановите и перезапустите клиент после переименования компьютера. Дополнительные сведения см. в разделе Запуск или остановка службы Management Server.

Кроме того, убедитесь, что указанный альтернативный адрес отражается на панели **Иерархия федеративных сайтов** на центральном объекте. В противном случае остановите и перезапустите Management Client.

После переименования хоста и перезагрузки компьютера федеративный сайт автоматически изменит адрес на новый.

Управление журналами серверов

Существуют журналы серверов следующих типов:

- Журнал системы
- Контрольный журнал
- Журналы на основе правил

Они используются для фиксации сведений об использовании системы. Эти журналы доступны в Management Client в разделе **Журналы серверов**.

Сведения о журналах, применяемых для устранения и анализа программных ошибок, приведены в разделе Журналы отладки (объяснение) на стр. 401.

Получение сведений об активности пользователей, событиях, действиях и ошибках

Используйте журналы для получения подробных сведений об активности пользователей, событиях, действиях и ошибках в системе.

Для просмотра журналов в Management Client перейдите на панель **Навигация по сайту** и выберите пункт **Журналы серверов**.

Тип журнала	Что фиксируется в журнале?
Системные журналы	Информация, относящаяся к системе
Контрольные журналы	Активность пользователей
Журналы на основе правил	Правила, в которых пользователи задали действие **Создать новую <запись журнала>**. Дополнительные сведения о действии с <записью журнала> см. в разделе Действия и завершающие действия.

Для отображения журналов на другом языке см. Вкладка «Общая информация» (параметры) на стр. 418 в разделе **Параметры**.

Сведения об экспорте журналов в виде файлов значений, разделенных запятыми (.csv), см. в разделе Экспорт журналов.

Сведения об изменении настроек журналов приведены в разделе Вкладка «Журналы серверов» (параметры) на стр. 421.

Применение фильтров в журналах

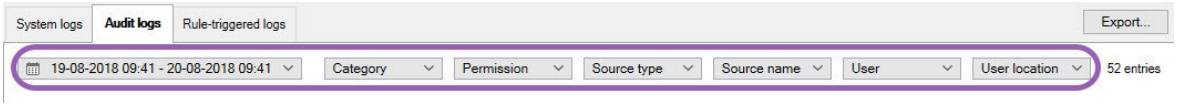
В каждом окне журнала можно применить фильтры, чтобы просмотреть, например, записи журнала за конкретный интервал времени, по конкретному устройству или пользователю.

> Фильтры создаются на основе записей журнала, в настоящий момент отображающихся в пользовательском интерфейсе.

1. На панели **Навигация по сайту** выберите пункт **Журналы серверов** По умолчанию отображается вкладка **Системные журналы**.

   Для просмотра другого типа журнала перейдите на другую вкладку.

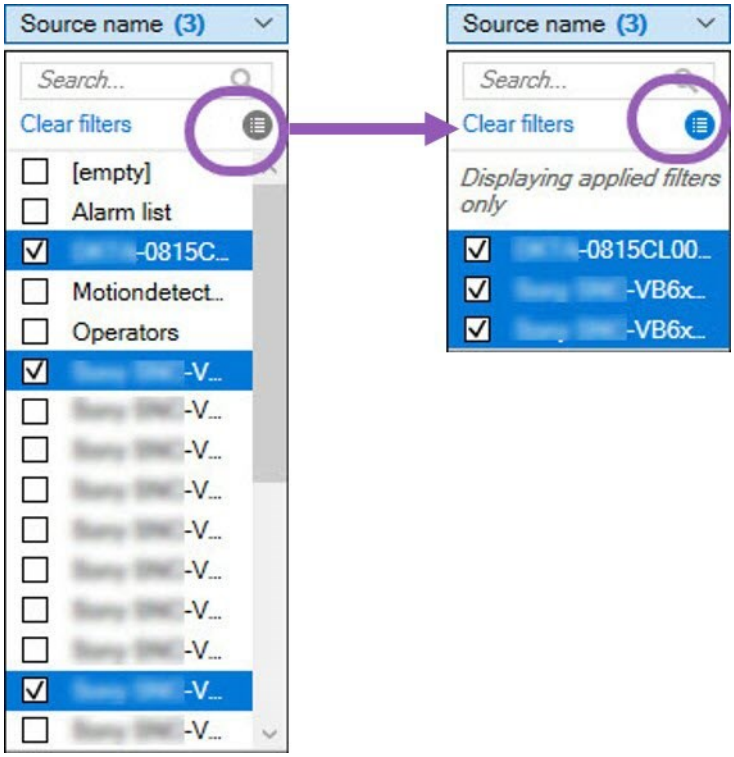
2. На соответствующей вкладке выберите группу фильтров, например **Категория**, **Тип источника** или **Пользователь**.



   Появится список фильтров. В списке фильтров отображается не более 1 000 фильтров.

3. Выберите фильтр, чтобы применить его. Выберите фильтр еще раз, чтобы снять его.

   Дополнительно: В списке фильтров выберите пункт **Отображать только примененные фильтры**, чтобы видеть только те фильтры, которые вы применили.



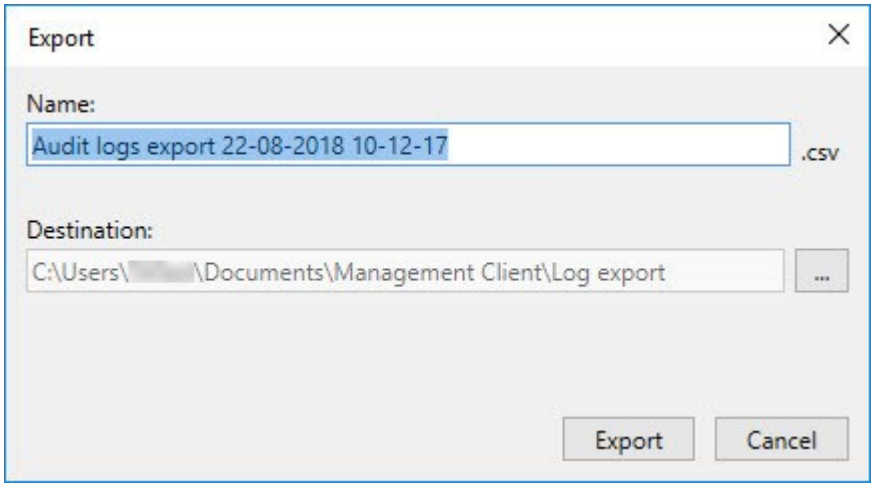
При экспорте журналов экспортируемое содержимое зависит от примененных вами фильтров. Сведения об экспорте приведены в разделе Экспорт журналов.

Экспорт журналов

Экспорт журналов помогает, например, сохранить записи журнала по истечении срока их хранения журналов. Журналы можно экспортировать в виде файлов значений, разделенных запятыми (.csv).

Для экспорта журнала:

1. Выберите пункт **Экспортировать** в правом верхнем углу. Откроется окно **Экспорт**.



2. В поле **Имя** окна **Экспорт** введите имя файла журнала.
3. По умолчанию экспортированные файлы журналов сохраняются в папке **Экспорт журналов**.

   Чтобы задать другое местонахождение, выберите пункт ... в правой части поля **Место назначения**.
4. Для экспорта журнала нажмите кнопку **Экспортировать**.

Экспортируемое содержимое зависит от примененных вами фильтров. Сведения об экспорте приведены в разделе Применение фильтров к журналам.

Поиск по журналам

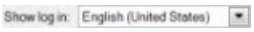
Для поиска по журналу воспользуйтесь пунктом **Критерии поиска** в верхней части панели журналов:

1. Выберите критерии поиска из списков.
2. Нажмите кнопку **Обновить**, чтобы на панели журналов отразились ваши критерии поиска. Для очистки критериев поиска и возврата к просмотру всего содержимого журнала нажмите кнопку **Очистить**.

Если дважды нажать любую строку, в окне **Сведения о журнале** будут показаны полные сведения. Таким же образом можно прочитать записи журнала, содержащие больше текста, чем помещается в одной строке.

Изменение языка журналов

1. В нижней части панели журналов, в списке **Язык отображения журнала**, выберите требуемый язык.



2. Журнал будет отображаться на выбранном языке. При последующем открытии журнала будет использован язык по умолчанию.

Разрешить компонентам 2018 R2 и более ранних версий записывать информацию в журналы

Версия 2018 R3 сервера регистрации включает новую функцию аутентификации для обеспечения дополнительной безопасности. В результате этого компоненты версии 2018 R2 и более ранних не могут записывать журналы на сервер регистрации.

Затронутые компоненты:

- XProtect Smart Client
- Встраиваемое расширение XProtect LPR
- LPR Server
- Встраиваемое расширение управления доступом
- Сервер событий
- Встраиваемое расширение сигналов тревоги

Если вы используете версию 2018 R2 или более раннюю версию любого из вышеуказанных компонентов, необходимо решить, разрешать ли компоненту записывать журналы на сервер регистрации:

1. Выберите пункт **Инструменты** > **Опции**.
2. В диалоговом окне **Параметры**, в нижней части вкладки **Журналы серверов**, найдите поле **Разрешить запись журналов компонентам версии 2018 R2 и более ранних**.
    - Чтобы разрешить запись журналов компонентам версии 2018 R2 и более ранних, поставьте отметку в этом поле
    - Чтобы запретить запись журналов компонентам версии 2018 R2 и более ранних, снимите отметку в этом поле

Диагностика и устранение неполадок

Журналы отладки (объяснение)

Журналы отладки применяются для выявления недостатков и неисправностей системы.

Информация о журналах использования системы приведена в разделе Управление журналами серверов на стр. 396.

Журналы отладки в схеме XProtect находятся в следующем месте:

- `C:\ProgramData\Milestone\IDP\Logs`

  > Доступ к нему имеется только у пользователя IIS или администратора. При изменении пользователя IIS эти разрешения необходимо обновить.

- `C:\ProgramData\Milestone\MIPSDK`
- `C:\ProgramData\Milestone\XProtect Data Collector Server\Logs`
- `C:\ProgramData\Milestone\XProtect Event Server\Logs`
- `C:\ProgramData\Milestone\XProtect Log Server`
- `C:\ProgramData\Milestone\XProtect Management Server\Logs`
- `C:\ProgramData\Milestone\XProtect Mobile Server\Logs`
- `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
- `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`

Проблема: Изменение SQL Server и местонахождения базы данных препятствует получению доступа к базе данных

Если местонахождение SQL Server и баз данных ПО для управления видео изменилось (например, в результате изменения имени хоста компьютера, на котором работает SQL Server), сервер записи не сможет получить доступ к базе данных.

Решение: Измените строки подключения, чтобы они соответствовали изменениям, внесенным в SQL Server и базу данных. См. раздел Изменение местонахождения и имени базы данных SQL Server на стр. 381.

Проблема: Сбой запуска сервера записи из-за конфликта портов

Эта проблема может возникать только в том случае, если работает служба простого протокола передачи электронной почты (SMTP), которая использует порт 25. Если порт 25 уже используется, запуск службы Recording Server невозможен. Важно, чтобы порт 25 был доступен для службы SMTP сервера записи.

Служба SMTP: Проверка и варианты решения проблемы

Чтобы проверить, установлена ли служба SMTP:

1. В меню **Пуск** Windows выберите **Панель управления**.
2. В **Панели управления** дважды нажмите **Установка и удаление программ**.
3. В левой части окна **Установка и удаление программ** нажмите **Установка и удаление компонентов Windows**.
4. В мастере **Компоненты Windows** выберите пункт **Internet Information Services (IIS)** и нажмите **Сведения**.
5. В окне **Internet Information Services (IIS)** убедитесь в наличии отметки в поле **Служба SMTP**. Если отметка поставлена, служба SMTP установлена.

Если служба SMTP установлена, выберите одно из следующих решений:

Решение 1: Отключение службы SMTP или настройка ее ручного запуска

Это решение позволяет вам запускать сервер записи без остановки службы SMTP:

1. В меню **Пуск** Windows выберите **Панель управления**.
2. В **Панели управления** дважды нажмите **Администрирование**.
3. В окне **Администрирование** дважды нажмите **Службы**.
4. В окне **Службы** дважды нажмите **Простой протокол передачи почты (SMTP)**.
5. В окне **Свойства SMTP** нажмите **Остановить**, затем установите **Тип запуска**: **Вручную** или**Отключена**.

   Если установлено значение **Вручную**, службу SMTP можно запустить вручную из окна **Службы** или из командной строки с помощью команды *net start SMTPSVC*.
6. Нажмите кнопку **OK**.

Решение 2: Удаление службы SMTP

Удаление службы SMTP может повлиять на другие приложения, использующие ее.

1. В меню **Пуск** Windows выберите **Панель управления**.
2. В окне **Панель управления** дважды нажмите **Установка и удаление программ**.
3. В левой части окна **Установка и удаление программ** нажмите **Установка и удаление компонентов Windows**.
4. В мастере **Компоненты Windows** выберите пункт **Internet Information Services (IIS)** и нажмите

Сведения.

5. В окне **Internet Information Services (IIS)** снимите отметку в поле **Служба SMTP**.
6. Нажмите кнопки **ОК**, **Далее** и **Готово**.

Проблема: Recording Server отключается от сети при переключении на кластерный узел Management Server

Если в целях резервирования Management Server настроен кластер Microsoft, Recording Server или Recording Server могут отключиться от сети при переключении Management Server между кластерными узлами.

Для устранения неполадки сделайте следующее:

> При внесении изменений в конфигурацию в диспетчере отказоустойчивости кластеров Microsoft приостановите управление и мониторинг службы, чтобы Server Configurator удалось внести изменения и запустить и/или остановить службу Management Server. Если вы меняете тип запуска службы отказоустойчивого кластера на «вручную», это не должно приводить к конфликтам с Server Configurator.

На компьютерах Management Server:

1. Запустите Server Configurator на всех компьютерах, где установлен сервер управления.
2. Перейдите на страницу **Регистрация**.
3. Нажмите значок карандаша ( ), чтобы разблокировать редактирование адреса сервера управления.
4. Измените адрес сервера управления на имя роли кластера, на котором размещено Management Server, например `http://MyCluster`.
5. Нажмите **Регистрация**.

На компьютерах, где установлены компоненты, использующие Management Server (например, Recording Server, Mobile Server, Event Server, API Gateway):

1. Запустите Server Configurator на каждом компьютере.
2. Перейдите на страницу **Регистрация**.
3. Измените адрес сервера управления на имя роли кластера, на котором размещено Management Server, например `http://MyCluster`.
4. Нажмите **Регистрация**.

Проблема: Главный узел в схеме Milestone Federated Architecture не может подключиться к подчиненному узлу

Если на объекте переименован компьютер-хост, действующий в качестве подчиненного узла в Milestone Federated Architecture, к нему не сможет подключиться главный узел.

Для восстановления подключения между главным узлом и объектом

- Отключите затронутый объект от главного узла Дополнительные сведения см. в разделе Отключение объекта от иерархии.
- Повторно подключите объект с использованием нового имени его хоста. Дополнительные сведения см. в разделе Добавление объекта к иерархии.

> Чтобы убедиться, что изменения вступили в силу, можно остановить и перезапустить Management Client на узле, который действует в качестве главного узла того узла, для которого изменено имя хоста. Дополнительные сведения см. в разделе Запуск или остановка службы Management Server.

Дополнительные сведения о последствиях изменения имени хоста в схеме Milestone Federated Architecture приведены в разделе Изменение имени хоста в Milestone Federated Architecture.

Проблема: Служба базы данных SQL Azure недоступна

Если при использовании базы данных SQL Azure в процессе установки либо обычной работы возникает проблема с подключением, ее причиной может быть временная недоступность службы базы данных SQL Azure.

Служба базы данных SQL Azure — это служба, в которой за большинство традиционных функций сопровождения базы данных отвечает Microsoft. Эта служба может быть недоступна в течение непродолжительных периодов времени и способна в определенной степени восстанавливаться без участия пользователя.

Ошибки базы данных фиксируются в файлах журналов VMS XProtect вместе с соответствующим идентификатором инцидента, который можно предоставить в службу поддержки Microsoft, если база данных SQL Azure недоступна в течение долгого времени.

Дополнительные сведения см. в разделе Устранение распространенных неполадок с подключением к базе данных SQL Azure.

Проблема: Проблемы с использованием внешнего IDP

Не удается войти в систему

Идентификаторы URI перенаправления

Вход в систему может завершиться неудачно, если, например, URI перенаправления является неверным. Дополнительные сведения приведены в разделе Добавление URI перенаправления для веб-клиентов на стр. 429.

Нет заявок или заявки не добавлены к ролям

Если для пользователей внешнего IDP не определены заявки, которые могут использоваться VMS XProtect, или если заявки не были добавлены к ролям в VMS XProtect, вход в систему одним из клиентов не удастся, даже если пользователь внешнего IDP был успешно аутентифицирован внешним IDP.

Однако пользователи внешнего IDP по-прежнему могут получить доступ к VMS XProtect, даже если для пользователей внешнего IDP не определены заявки. В этом случае администратор VMS XProtect должен вручную добавить пользователей внешнего IDP к одной или нескольким ролям после первоначального входа в систему пользователей внешнего IDP.

Параметр аутентификации недоступен в диалоговом окне входа в систему.

Если вы введете неверный адрес компьютера в диалоговом окне входа в клиенте, клиент не получит ответ на вызов API. Вызов API выполняется при запуске клиента и при каждом изменении адреса, и он запрашивает, какие параметры аутентификации поддерживает установка VMS XProtect.

Если клиент не получает ответа на вызов API при запуске клиента, клиент по умолчанию возвращается к отображению стандартных параметров аутентификации.

Заявки нельзя выбрать в ролях

Заявки, которые вы хотите использовать в ролях, необходимо добавить в конфигурацию IDP, прежде чем их можно будет выбрать в ролях. Заявки можно добавить на вкладке **Внешний IDP** диалогового окна **Параметры**: Вкладка «Внешний IDP» (параметры) на стр. 425. Если заявка не добавлена в конфигурацию IDP, вы не сможете выбрать ее в ролях.

Обновление

Обновление (объяснение)

Обновление проводится для всех компонентов, установленных на компьютере. Во время обновления нельзя удалить установленные компоненты. Чтобы удалить установленные компоненты, используйте функцию Windows **Добавление и удаление программ** до или после обновления. Во время обновления все компоненты, кроме базы данных сервера управления, автоматически удаляются и заменяются. В том числе драйверы из комплекта драйверов.

База данных сервера записи содержит все настройки системы (настройки сервера записи, настройки камеры, правила и т.д.). Пока база данных сервера управления не удалена, повторная настройка вашей системы не требуется, даже если вам нужно настроить новые функции в новой версии.

Обратная совместимость с серверами записи версий XProtect, предшествующих текущей версии, ограничена. У вас будет доступ к записям на более старых серверах записи, но для изменения их конфигурации потребуется текущая версия. Milestone рекомендует обновить все серверы записи в вашей системе.

При выполнении обновления, в том числе серверов записи, вам будет предложено обновить драйверы видеоустройств или оставить их в текущей версии. Если вы обновляете драйверы, после повторного запуска вашей системы аппаратным устройствам может потребоваться несколько минут для подключения к новым драйверам видеоустройств. Это связано с рядом внутренних проверок новых установленных драйверов.

При обновлении с версии 2017 R3 или старше до версии 2018 R1 или более поздней версии, или если в вашей системе установлены камеры более старой версии, вам потребуется вручную загрузить комплект драйверов со страницы загрузки на нашем веб-сайте (https://www.milestonesys.com/downloads/). Чтобы проверить, есть ли у вас камеры, которые используют драйверы из комплекта для старых устройств, посетите эту страницу на нашем веб-сайте (https://www.milestonesys.com/community/business-partner-tools/device-packs/).

При обновлении с версии 2018 R1 или старше до версии 2018 R2 или более поздней версии важно обновить все серверы записи в вашей системе, установив исправление безопасности перед переходом на новую версию. Переход на новую версию без исправления безопасности приведет к сбою серверов записи.

Инструкции по установке исправления безопасности на серверы записи есть на нашем веб-сайте https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/.

Если требуется шифрование подключений между сервером управления и серверами записи, все серверы записи нужно обновить до версии не ниже 2019 R2.

Рекомендованная последовательность обновления описана в Рекомендации по обновлению на стр. 410.

Требования к обновлению

- Приготовьте файл лицензии программного обеспечения (LIC) (см. Лицензии (объяснение) на стр. 129):
  - **Установка пакета обновления**: При установке сервера управления мастер может попросить указать местонахождение файла лицензии программного обеспечения. Можно использовать как файл лицензии программного обеспечения, который вы получили после покупки вашей системы (или в ходе последнего обновления), так и активированный файл лицензии программного обеспечения, который вы получили в ходе последней активации лицензии.
  - **Обновление версии**: При покупке новой версии вы получаете новый файл лицензии программного обеспечения. При установке сервера управления мастер может попросить указать местонахождение нового файла лицензии программного обеспечения.

  Перед продолжением система проверит файл лицензии программного обеспечения. Для добавленных ранее аппаратных устройств и других устройств, которым требуется лицензия, начнется льготный период. Если вы не включили автоматическую активацию лицензии (см. Включить автоматическую активацию лицензии на стр. 137), не забудьте активировать лицензии вручную до истечения льготного периода. Если у вас нет файла лицензии программного обеспечения, обратитесь к реселлеру XProtect.
- Подготовьте программное обеспечение **новой версии продукта**. Вы можете загрузить его со страницы загрузки на веб-сайте Milestone.

- Обязательно создайте резервную копию конфигурации системы (см. Резервное копирование и восстановление конфигурации системы (объяснение) на стр. 361).

  На сервере управления конфигурация системы хранится в базе данных SQL Server. База данных SQL Server может находиться в экземпляре SQL Server на самом компьютере сервера управления или в экземпляре SQL Server в сети.

  Если вы используете базу данных SQL Server в экземпляре SQL Server в сети, сервер управления должен иметь разрешения администратора в экземпляре SQL Server для создания, перемещения или обновления базы данных SQL Server. Для обычного использования и ведения базы данных SQL Server серверу управления требуется только быть владельцем базы данных.

- Если вы планируете включать шифрование во время установки, у вас должны быть установлены надлежащие сертификаты, которым доверяют соответствующие компьютеры. Дополнительные сведения приведены в разделе Защищенное соединение (объяснение) на стр. 162.

Когда вы будете готовы приступить к обновлению, выполните процедуры, описанные в разделе Рекомендации по обновлению на стр. 410.

Обновите VMS XProtect для работы в режиме совместимости со стандартом FIPS 140-2

Начиная с версии 2020 R3, настройки VMS XProtect предусматривают работу с использованием только экземпляров алгоритмов, сертифицированных по FIPS 140-2.

Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

> Для систем, соответствующих требованиям FIPS 140-2, с операциями экспорта и базами данных архивирования мультимедиа из версий VMS XProtect, предшествующих 2017 R1, шифрование которых выполнятся с помощью шифров, не соответствующих FIPS, данные необходимо архивировать там, где к ним можно будет получить доступ после включения FIPS.

Далее описано, как настроить VMS XProtect для работы в режиме, совместимом со стандартом FIPS 140-2:

1. Отключите политику безопасности FIPS для Windows на всех компьютерах, входящих в состав VMS, включая компьютер с SQL Server.

   Во время обновления нельзя установить VMS XProtect, если поддержка FIPS включена в операционной системе Windows.

2. Автономные модули интеграции сторонних производителей должны выполняться в ОС Windows с поддержкой FIPS.

   Если автономный модуль интеграции несовместим с FIPS 140-2, его нельзя будет запустить после включения режима FIPS в операционной системе Windows.

   Чтобы этого не случилось:

   - Сохраните все автономные модули интеграции в VMS XProtect;
   - свяжитесь с поставщиками этих модулей интеграции и уточните, совместимы ли они с FIPS 140-2;
   - разверните автономные модули интеграции, совместимые с FIPS 140-2;

3. убедитесь, что драйверы и, следовательно, подключение к устройствам, подходят для режима совместимости с FIPS 140-2.

   VMS XProtect гарантирует и может организовать работу в режиме совместимости с FIPS 140-2 при соблюдении следующих критериев:

   - Устройства используют только совместимые драйверы для подключения к VMS XProtect

     В разделе Соответствие стандарту FIPS 140-2 руководства по укреплению безопасности приведены дополнительные сведения о драйверах для обеспечения соответствия.
     .

   - Устройства используют комплект драйверов версии 11.1 или выше.

     Драйверы из комплекта драйверов для старых устройств не могут гарантировать подключение в режиме совместимости с FIPS 140-2.

   - Устройства подключаются по HTTPS с использованием протокола SRTP или протокола RTSP по HTTPS для видеопотока.

     > Модули драйверов не могут гарантировать совместимость подключения по HTTP со стандартом FIPS 140-2. Подключение может работать как совместимое, но нет гарантий, что оно действительно является совместимым.

   - Компьютер, на котором выполняется сервер записи, использует ОС Windows с включенным режимом FIPS.

4. Данные в базе данных мультимедиа должны шифроваться с помощью шифров, соответствующих требованиям FIPS 140-2.

   Это требование можно обеспечить, запустив инструмент обновления базы данных мультимедиа. Подробные сведения о настройке VMS XProtect для запуска в режиме совместимости с FIPS 140-2 см. в разделе Соответствие стандарту FIPS 140-2 руководства по укреплению.

5. Перед включением FIPS в операционной системе Windows выполните настройку вашей системы VMS XProtect и убедитесь, что все компоненты и устройства могут работать в среде с включенной поддержкой FIPS, а затем обновите пароли оборудования в XProtect Management Client.

   Для этого в Management Client нажмите правой кнопкой мыши сервер записи, выбранный в узле **Серверы записи**, и выберите **Добавить оборудование**. Перейдите в мастер **добавления оборудования**. При этом все учетные данные обновятся и зашифруются в режиме совместимости с FIPS.

FIPS можно включить только после обновления всей системы VMS, включая клиенты.

Рекомендации по обновлению

Прежде чем приступить к обновлению, ознакомьтесь с требованиями к обновлению (см. Требования к обновлению на стр. 407), в том числе к созданию резервных копий баз данных SQL Server.

Драйверы устройств теперь разделяются на два комплекта драйверов: стандартный комплект драйверов с драйверами более новых версий и комплект драйверов для старых устройств с драйверами старых версий. Стандартный комплект драйверов всегда автоматически устанавливается при обновлении. Если у вас старые камеры, которые используют драйверы из комплекта для старых устройств, и у вас не установлен комплект драйверов для старых устройств, система не установит комплект драйверов для старых устройств автоматически.

Если в вашей системе есть старые камеры, Milestone рекомендует проверить, используют ли камеры драйверы из комплекта для старых устройств на этой странице (https://www.milestonesys.com/community/business-partner-tools/device-packs/). Проверить, установлен ли у вас комплект драйверов для старых устройств, можно в системных папках XProtect. Для загрузки комплекта драйверов для старых устройств перейдите на страницу загрузки (https://www.milestonesys.com/downloads/).

Если ваша система работает в конфигурации **Один компьютер**, то новое программное обеспечение можно устанавливать поверх существующего.

В системе Milestone Interconnect или Milestone Federated Architecture сначала обновляют центральный объект, а затем удаленные объекты.

В распределенной системе обновление проводится в следующем порядке:

1. Обновите сервер управления, выбрав вариант **Пользовательская установка** в программе установки (см. Установка системы — вариант «Пользовательская» на стр. 176).
    1. На странице мастера, где выбирают компоненты, предварительно выбраны все компоненты сервера управления.
    2. Укажите SQL Server и базу данных. Решите, следует ли оставить базу данных SQL Server, которая уже используется, и сохранять имеющиеся данные в базе данных.

    > Когда начнется установка, функции сервера записи обработки отказа будут недоступны (см. Сервер записи обработки отказа (объяснение) на стр. 43).

    > Если включено шифрование сервера управления, серверы записи будут работать автономно до завершения обновления и включения шифрования сервера управления (см. Защищенное соединение (объяснение) на стр. 162).

2. Обновите серверы записи обработки отказа. С веб-страницы загрузки сервера управления (управляется Download Manager) установите Recording Server.

    > Если вы планируете включить шифрование на серверах записи обработки отказа и хотите сохранить функции обработки отказа, обновляйте сервер записи обработки отказа без шифрования и включайте его после завершения обновления серверов записи.

    На этом этапе функции сервера отказоустойчивости снова доступны.

3. Если вы планируете использовать шифрование данных, которые передаются с серверов записи или серверов записи обработки отказа на клиенты, и вам важно, чтобы клиенты могли получать данные во время обновления, выполните обновление всех клиентов и служб, которые получают потоки данных с серверов записи, и только после этого обновляйте серверы записи. Это следующие клиенты и службы:
    - XProtect Smart Client
    - Management Client
    - Management Server
    - Сервер XProtect Mobile
    - XProtect Event Server
    - DLNA Server Manager

- Milestone Open Network Bridge
- Объекты, которые получают потоки данных с сервера записи через Milestone Interconnect
- Некоторые модули интеграции сторонних производителей MIP SDK

4. Обновите серверы записи. Серверы записи можно установить с помощью мастера установки (см. Установка сервера записи с помощью Download Manager на стр. 185) или автоматически (см. Автоматическая установка сервера записи на стр. 194). Преимущество автоматической установки в том, что ее можно выполнять дистанционно.

   > Если включено шифрование, а сертификат аутентификации выбранного сервера не является доверенным на всех соответствующих работающих компьютерах, они будут отключены. Дополнительные сведения приведены в разделе Защищенное соединение (объяснение) на стр. 162.

Выполните эти действия на других объектах в вашей системе.

Сведения о пользовательском интерфейсе

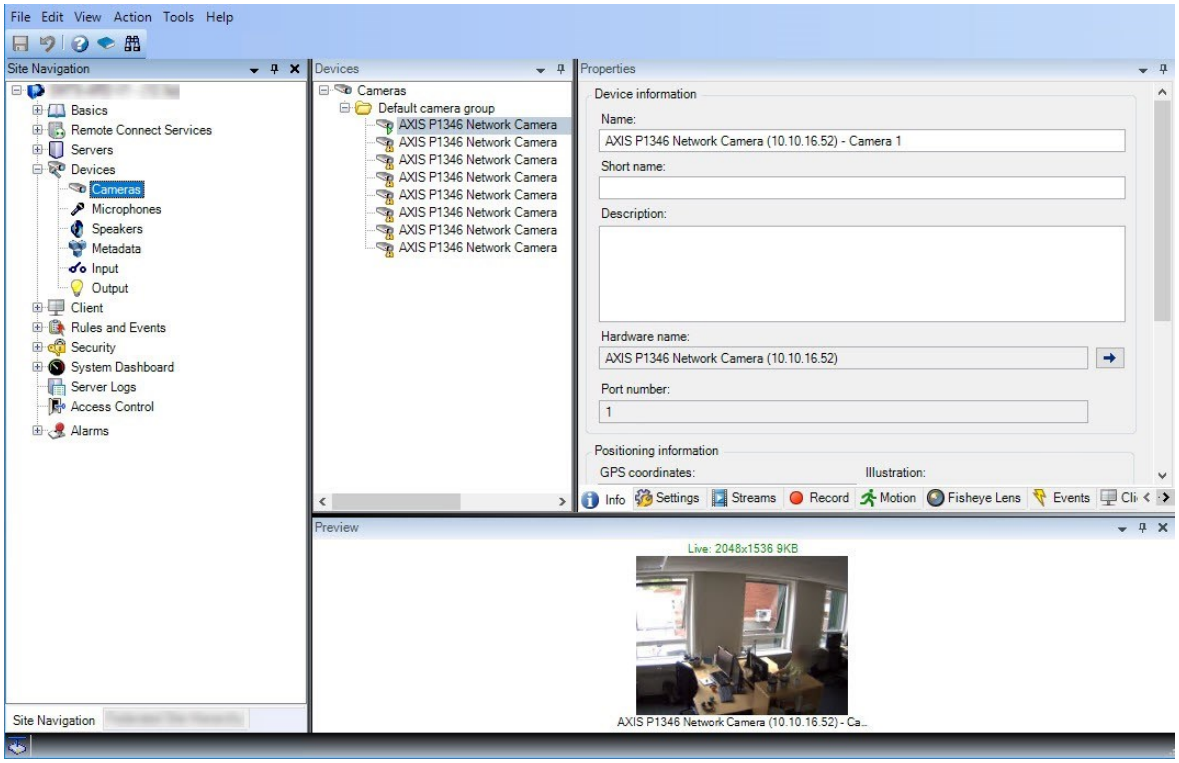
Главное окно и панели

Окно Management Client делится на панели. Вы можете задать количество и расположение панелей самостоятельно:

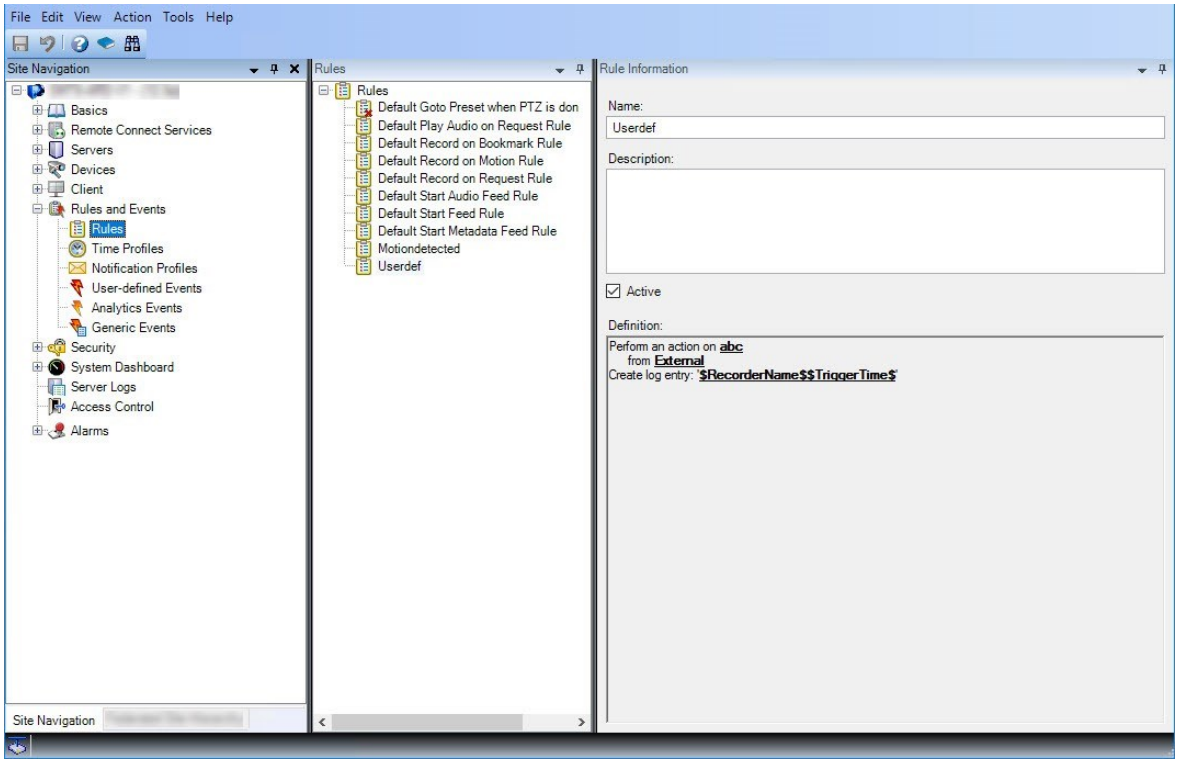
- Настройка системы
- Задача
- Доступные функции

Ниже показаны примеры типичных макетов окна:

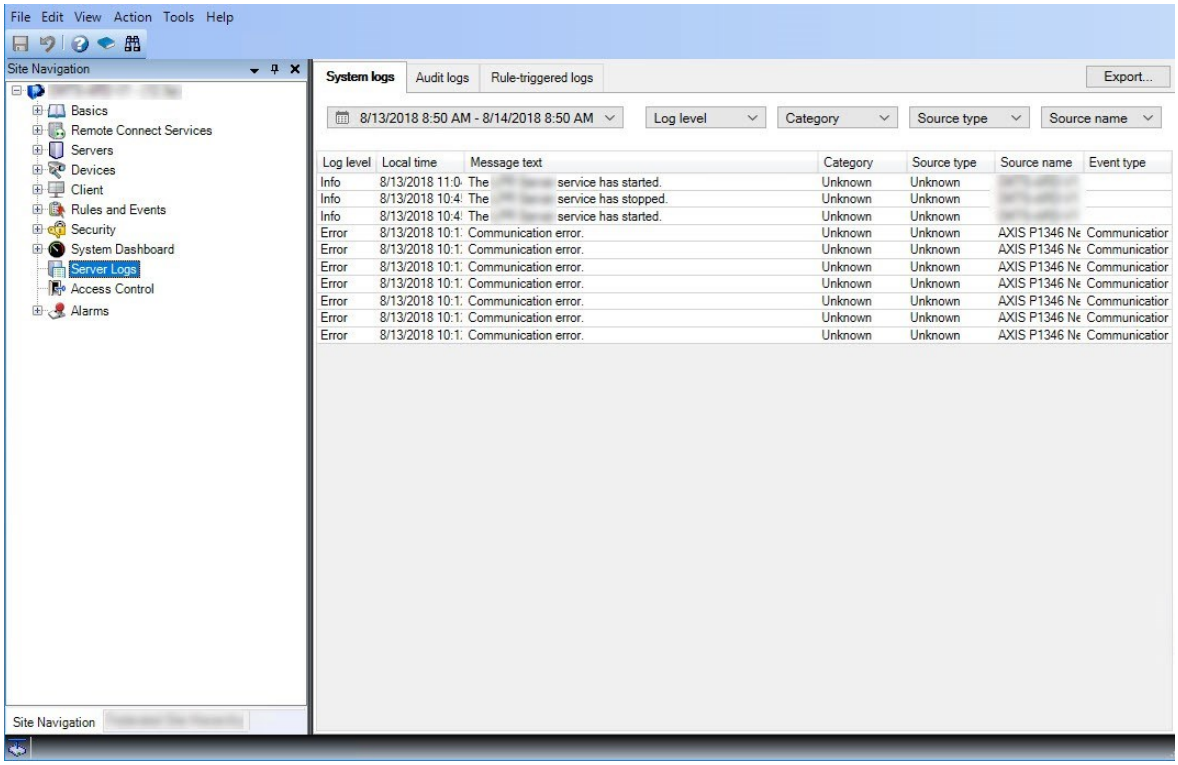
- При работе с серверами записи и устройствами:



- При работе с правилами, профилями времени и уведомлений, пользователями, ролями:

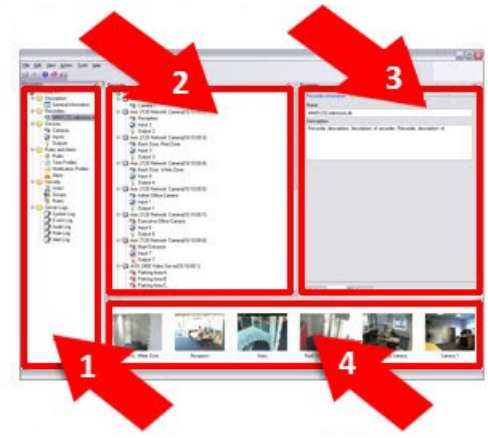


- При просмотре журналов:



Расположение панелей

На изображении показан типичный макет окна. Вы можете менять расположение, и на вашем компьютере оно может быть другим.



1. Панель «Навигация по сайту» и панель «Иерархия федеративных сайтов»
2. Панель «Обзор»
3. Панель свойств
4. Панель предварительного просмотра

Панель «Навигация по сайту»

Это главный элемент навигации в Management Client. Здесь отображаются имя, параметры и конфигурации сайта, на который вы вошли. Имя сайта отображается в верхней части панели. Функции сгруппированы по категориям, которые отражают возможности программного обеспечения.

На панели **Навигация по сайту** можно настроить систему и управлять ей в соответствии с потребностями. Если ваша система состоит не из одного сайта, а включает также федеративные сайты, то для управления этими сайтами служит панель **Иерархия федеративных сайтов**.

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Панель «Иерархия федеративных сайтов»

В этом элементе навигации отображаются все родительские и дочерние сайты Milestone Federated Architecture в иерархии.

Вы выбираете любой сайт, выполняете вход, и для этого сайта запускается Management Client. Сайт, на котором вы находитесь, всегда будет в самом верху иерархии.

Панель «Обзор»

Служит для обзора элемента, выбранного на панели **Навигация по сайту**, например, здесь может отображаться подробный список. При выборе элемента на панели **Обзор** его свойства обычно отображаются на панели **Свойства**. Нажав элемент на панели **Обзор** правой кнопкой мыши, можно перейти к функциям управления.

Панель свойств

Содержит свойства элемента, выбранного на панели **Обзор**. Свойства отображаются на нескольких отдельных вкладках:

Панель предварительного просмотра

Панель **Предварительный просмотр** появляется при работе с серверами записи и устройствами. Здесь отображаются кадры предварительного просмотра с выбранных камер или информация о состоянии устройства. В примере показан кадр предварительного просмотра с камеры с информацией о разрешении и скорости передачи данных в потоке трансляции с камеры:

По умолчанию информация на кадрах предварительного просмотра с камеры относится к потокам трансляции. Она отображается зеленым шрифтом над кадром предварительного просмотра. Если вы хотите, чтобы отображалась информация потока записи (красный шрифт), выберите в меню пункты **Вид** > **Показать потоки записи**.

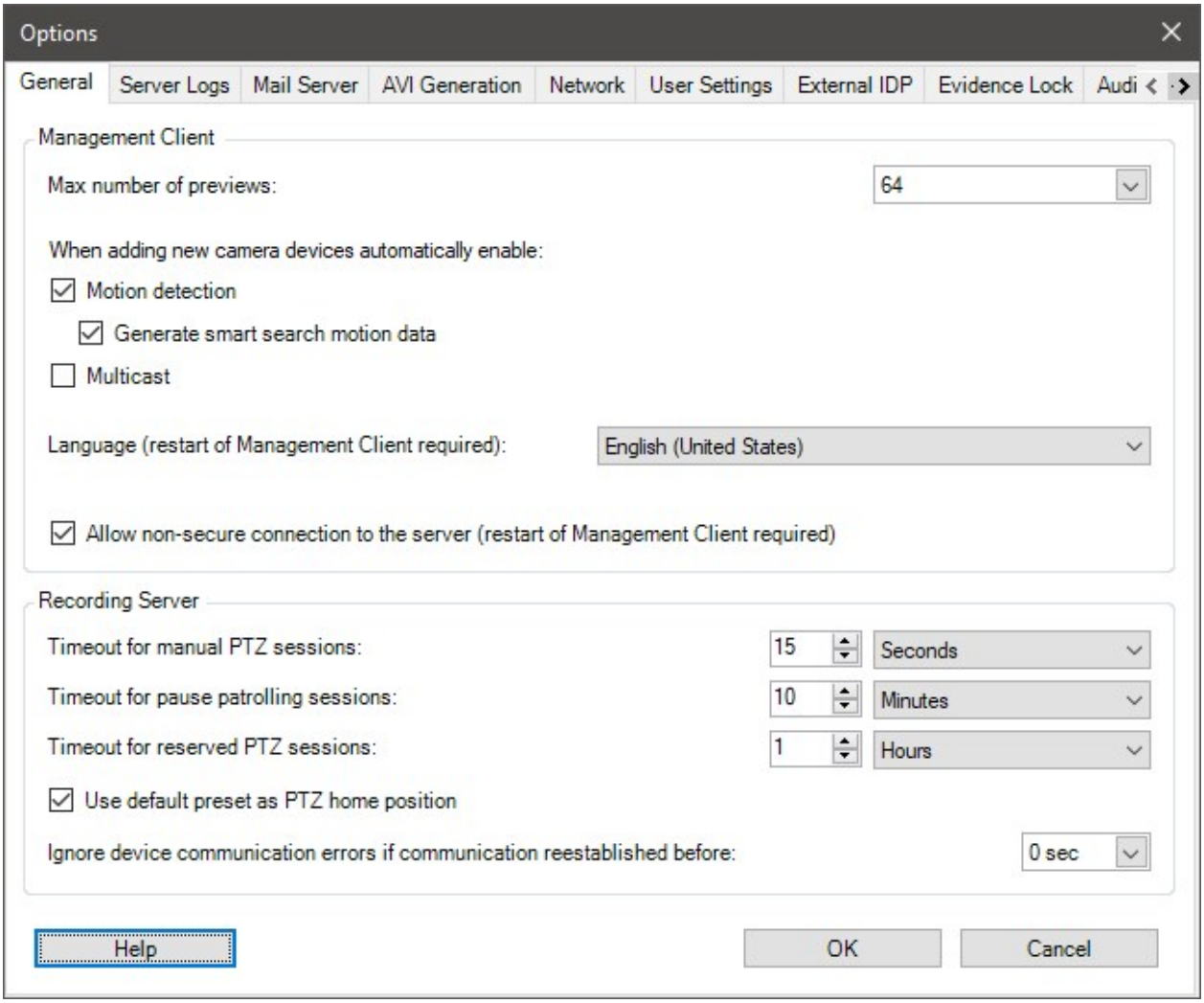
Если на панели **Предварительный просмотр** отображаются кадры с нескольких камер с высокой частотой кадров, это может повлиять на производительность. Для управления количеством кадров предварительного просмотра и их частотой выберите в меню пункты **Опции** > **Общее**.

Параметры системы (диалоговое окно «Опции»)

В диалоговом окне **Опции** можно указать количество параметров, связанных с общим видом и функциями системы.

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Чтобы открыть это диалоговое окно, выберите **Инструменты** > **Опции**.



Вкладка «Общая информация» (параметры)

На вкладке «Общая информация» можно указать общие параметры для Management Client и сервера записи.

Management Client

Имя	Описание
Максимальное количество изображений для предварительного	Выберите максимальное количество эскизов для отображения на панели **Предварительный просмотр**.

Имя	Описание
просмотра	По умолчанию отображаются 64 эскиза. Выберите в меню пункт **Действие** > **Обновить**, чтобы применить изменение. Система может замедляться из-за большого количества эскизов при высокой частоте кадров.
При добавлении новых камер автоматически включаются следующие функции: Обнаружение движений	Установите флажок, чтобы включить обнаружение движений на новых камерах при их добавлении в систему в мастере **добавления оборудования**. Этот параметр не влияет на настройки обнаружения движений на уже имеющихся камерах. Обнаружение движений на камере включается и отключается на вкладке **Движение** этой камеры.
При добавлении новых камер автоматически включаются следующие функции: Сгенерировать данные движения для интеллектуального поиска	Для формирования данных движения для интеллектуального поиска на камере должно быть включено обнаружение движений. Установите этот флажок, чтобы включить создание данных движения для интеллектуального поиска на новых камерах при их добавлении в систему в мастере **добавления оборудования**. Этот параметр не влияет на настройки обнаружения движений на уже имеющихся камерах. Формирование данных движения для интеллектуального поиска для камеры включается и отключается на вкладке **Движение** этой камеры.
При добавлении новых камер автоматически включаются следующие функции: Многоадресная передача	Установите этот флажок, чтобы включить обнаружение движений на новых камерах при их добавлении в систему в мастере **добавления оборудования**. Этот параметр не влияет на настройки многоадресной передачи на уже имеющихся камерах. Многоадресная передача для камеры включается и отключается на вкладке **Клиент** этой камеры.

Имя	Описание
Язык	Выберите язык Management Client. Для использования нового языка перезапустите Management Client.
Разрешить незащищенные соединения с сервером	Установите этот флажок, чтобы разрешить незащищенное соединение с сервером по протоколу HTTP. (Пользователям не направляется запрос на создание незащищенного соединения с сервером.) Чтобы применить параметр, перезапустите Management Client.

Сервер записи

Имя	Описание
Тайм-аут для ручных сессий PTZ	Пользователи клиентов с необходимыми разрешениями могут вручную прерывать патрулирование камер PTZ. Выберите, сколько времени должно пройти до восстановления обычного патрулирования после прерывания вручную. Этот параметр применяется ко всем камерам PTZ в вашей системе. По умолчанию установлено значение 15 секунд. Конкретное время ожидания для камер можно указать на вкладке **Предустановки** камеры.
Тайм-аут паузы сессий патрулирования	Пользователи клиентов с достаточным PTZ-приоритетом могут приостанавливать патрулирование камер PTZ. Выберите, сколько времени должно пройти до восстановления обычного патрулирования после приостановки. Этот параметр применяется ко всем камерам PTZ в вашей системе. По умолчанию установлено значение 10 минут. Конкретное время ожидания для камер можно указать на вкладке **Предустановки** камеры.
Тайм-аут для зарезервированных	Задайте период ожидания по умолчанию для зарезервированных сеансов PTZ. Когда пользователь запускает зарезервированный сеанс PTZ, другие

Имя	Описание
сессий PTZ	пользователи не могут использовать камеру PTZ до тех пор, пока ее не отключат от сеанса вручную или пока не истечет время сеанса. По умолчанию установлено значение 1 час. Конкретное время ожидания для камер можно указать на вкладке **Предустановки** камеры.
Использовать предустановку по умолчанию как исходное положение PTZ	Установите этот флажок, чтобы использовать исходную предустановку по умолчанию вместо исходного положения камер PTZ при нажатии кнопки **Исходное положение** в клиенте. Для камеры необходимо задать исходную предустановку по умолчанию. Если исходная предустановка по умолчанию не задана, при нажатии кнопки **Исходное положение** в клиенте ничего не произойдет. По умолчанию этот флажок не установлен. Сведения о задании исходной предустановки см. в разделе Назначение исходной предустановки камеры по умолчанию на стр. 268
Игнорировать ошибки связи устройства, если связь восстановлена до	Система регистрирует все ошибки связи оборудования и устройств, но в этом разделе можно выбрать, как долго должна присутствовать ошибка связи, чтобы обработчик правил активировал событие **Ошибка связи**.

Вкладка «Журналы серверов» (параметры)

На вкладке **Журналы серверов** можно задать параметры журналов серверов управления системы.

Дополнительные сведения см. в разделе Получение сведений об активности пользователей, событиях, действиях и ошибках.

Имя	Описание
Журналы	Выберите тип журнала, который нужно настроить: • Системные журналы

Имя	Описание
	• Контрольные журналы • Журналы на основе правил
Параметры	Отключите или включите журналы и укажите период хранения. Разрешите компонентам 2018 R2 и более ранних версий записывать информацию в журналы. Дополнительные сведения приведены в разделе Разрешить компонентам 2018 R2 и более ранних версий записывать информацию в журналы. Для **системных** журналов укажите уровень сообщений, которые нужно регистрировать: • Все (включает неопределенные сообщения) • Информация, предупреждения и ошибки • Предупреждения и ошибки • Ошибки (параметр по умолчанию) Для **контрольных** журналов включите регистрацию доступа пользователей, чтобы система регистрировала все действия пользователей в XProtect Smart Client. К ним относятся, например, экспорт, включение выводов и просмотр камер в режиме реального времени и в режиме воспроизведения. Укажите следующие параметры: • Длина очереди воспроизведения Если пользователь воспроизводит видео в течение этого периода, система создает только одну запись в журнале. Если воспроизведение выходит за пределы этого периода, система создает новую запись в журнале. • Количество записей (кадров), которое пользователь может просмотреть до создания системой записи в журнале

Вкладка «Почтовый сервер» (параметры)

На вкладке **Почтовый сервер** можно задать параметры почтового сервера системы. Дополнительные сведения приведены в разделе Профили уведомлений (объяснение).

Имя	Описание
Адрес электронной почты отправителя	Введите электронный адрес, который должен указываться в качестве отправителя уведомлений по электронной почте для всех профилей уведомлений. Пример: **sender@organization.org**.
Адрес почтового сервера	Введите адрес почтового сервера SMTP, с которого будут отправляться уведомления по электронной почте. Пример: **mailserver.organization.org**.
Порт почтового сервера	Порт TCP, который используется для подключения к почтовому серверу. По умолчанию для незашифрованных подключений используется порт 25, для зашифрованных подключений обычно используется порт 465 или 587.
Шифровать соединение с сервером	Установите этот флажок, если нужно защитить подключение между сервером управления и почтовым сервером SMTP. Подключение защищается с помощью команды протокола электронной почты STARTTLS. В этом режиме сеанс начинается с незашифрованного подключения, затем почтовый сервер SMTP отправляет команду STARTTLS на сервер управления для перехода на защищенное соединение с использованием SSL.
Сервер требует входа в систему	Если этот флажок установлен, пользователи должны указать имя пользователя и пароль, чтобы войти в почтовый сервер.

Вкладка «Генерирование AVI» (параметры)

На вкладке **Генерирование AVI** можно указать параметры сжатия для создания видеороликов в формате AVI. Эти параметры необходимо настроить, если вы хотите включать AVI-файлы в уведомления по электронной почте, которые отправляются профилями уведомлений на основе правил.

Также см. Активация уведомлений по электронной почте на основе правил.

Имя	Описание
Устройство сжатия данных	Выберите кодек (технологию сжатия/распаковки), который хотите использовать. Чтобы в списке было доступно больше кодеков, установите их на сервере управления. Не все камеры поддерживают все кодеки.
Качество сжатия	(доступно не для всех кодеков). С помощью ползунка выберите степень сжатия (**0**–**100**), выполняемого кодеком. **0** означает отсутствие сжатия, что обычно дает высокое качество изображений и большой размер файлов. **100** означает максимальное сжатие, что обычно дает низкое качество изображений и небольшой размер файлов. Если ползунок неактивен, значит качество сжатия полностью зависит от выбранного кодека.
Ключевой кадр каждые	(доступно не для всех кодеков). Если нужно использовать ключевые кадры, установите этот флажок и укажите необходимое количество кадров между ключевыми кадрами. Ключевой кадр — это отдельный кадр, который сохраняется с указанными интервалами. Ключевой кадр содержит всё представление камеры, в то время как в остальных кадрах записываются только те пикселы, которые изменяются. Это позволяет значительно уменьшить размер файлов. Если флажок недоступен или не установлен, каждый кадр будет содержать всё представление камеры.
Скорость передачи данных	(доступно не для всех кодеков). Если нужно использовать определенную скорость передачи данных, установите этот флажок и укажите скорость (килобайт в секунду). Скорость передачи данных представляет размер прикрепленного AVI-файла. Если флажок недоступен или не установлен, скорость передачи данных будет определяться выбранным кодеком.

Вкладка «Сеть» (параметры)

На вкладке **Сеть** можно указать IP-адреса локальных клиентов, если клиенты подключаются к серверу записи через Интернет. Так система наблюдения будет распознавать их как подключающихся из локальной сети.

Можно также указать версию IP системы: IPv4 или IPv6. Значение по умолчанию — IPv4.

Вкладка «Отметки» (параметры)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

На вкладке **Отметки** можно указать параметры отметок, их идентификаторы и функцию в XProtect Smart Client.

Имя	Описание
Префикс номера отметки	Укажите префикс для всех отметок, сделанных пользователями XProtect Smart Client.
Время отметки по умолчанию	Укажите время начала и окончания отметки по умолчанию, заданной в XProtect Smart Client. Этот параметр должен соответствовать: • правилу отметки по умолчанию, см. Правила (узел «Правила и события»); • Подробнее о буферизации перед событием для каждой камеры см. в разделе Управление буферизацией перед событием.

Задание разрешений роли в отношении отметок описано в разделе Вкладка «Устройство» (роли) на стр. 600.

Вкладка «Параметры пользователя» (параметры)

На вкладке **Параметры пользователя** можно указать предпочтительные параметры пользователя, например, отображать ли сообщение при включенной дистанционной записи.

Вкладка «Внешний IDP» (параметры)

На вкладке **Внешний IDP** в Management Client можно добавить и настроить внешний IDP и регистрировать заявки от внешнего IDP.

Имя	Описание
Включено	Внешний IDP включен по умолчанию.
Имя	Имя внешнего IDP. Имя отображается в поле **Аутентификация** в окне входа клиента.
Центр аутентификации	URL-адрес внешнего IDP.
Добавить	Добавление и настройка внешнего IDP. При выборе пункта **Добавить** открывается диалоговое окно **Внешний IDP**, где можно ввести информацию для конфигурации (см. **Настройка внешнего IDP** после таблицы).
Редактировать	Редактирование конфигурации внешнего IDP.
Удалить	Удаление конфигурации внешнего IDP.  При удалении внешнего IDP пользователи, которые проходят аутентификацию через этот внешний IDP, не смогут войти в VMS XProtect. Если вы снова добавите внешний IDP, при входе будут созданы новые пользователи, т.к. идентификатор внешнего IDP изменится.

Настройка внешнего IDP

- Чтобы добавить внешний IDP, выберите **Добавить** в разделе **Внешний IDP** и введите информацию в таблицу ниже. Вы можете добавить только один внешний IDP:

Имя	Описание
Имя	Введенное здесь имя внешнего IDP появится в поле **Аутентификация** в окне журнала клиента.
Идентификатор клиента и	Их получают из внешнего IDP. Идентификатор клиента и секретный код клиента передаются из внешнего IDP по защищенному подключению.

Имя	Описание
Секретный код клиента	
Путь обратного вызова	Часть URL-адреса для потока перенаправления аутентификации для входа пользователей. Процесс входа пользователя инициируется в XProtect VMS. Браузер запускается со страницей входа, размещенной во внешнем IDP. Когда процесс аутентификации завершен, вызывается путь обратного вызова (адрес входа XProtect + /idp/ + путь обратного вызова), и пользователь перенаправляется в VMS XProtect. По умолчанию используется значение /signin-oidc. Формат перенаправления Путь обратного вызова состоит из адреса входа, введенного в клиенте + /idp/ + пути обратного вызова, настроенного на внешнем IDP. URI зависит от клиента, поэтому URI, например Smart Client и XProtect Web Client, будут разными. Адрес сервера управления — это адрес, который вы вводите в диалоговом окне входа в формате Smart Client или XProtect Management Client. Для XProtect Web Client и XProtect Mobile адрес перенаправления — это введенный адрес + порт + /idp/ + путь обратного вызова.
Запросить вход	Укажите внешнему IDP, должен ли пользователь оставаться в системе или требуется его верификация. В зависимости от внешнего IDP для верификации может требоваться пароль или полные данные для входа.
Заявка, которая используется для создания имени пользователя	При необходимости укажите, какая заявка внешнего IDP используется для создания уникального имени пользователя при автоматической подготовке пользователя в VMS. Дополнительные сведения о создании уникальных имен пользователей с помощью заявок приведены в разделе Уникальные пользовательские имена для пользователей внешнего IDP.
Области	При необходимости используйте области, чтобы ограничить количество заявок от внешнего IDP. Если вам известно, что заявки, относящиеся к вашей системе VMS, находятся в определенной области, можно использовать эту область, чтобы ограничить количество заявок от внешнего IDP.

Регистрация заявок

После регистрации заявок от внешнего IDP можно связать заявки с ролями в VMS для определения прав доступа пользователей в VMS. Дополнительные сведения приведены в разделе Привязка заявок от внешнего IDP.

- Чтобы зарегистрировать заявки от внешнего IDP, выберите **Добавить** в разделе **Зарегистрированные заявки** и введите информацию в таблицу ниже:

Имя	Описание
Внешний поставщик удостоверений	Название внешнего IDP.
Название заявки	Название заявки, определенное во внешнем IDP. В этом поле название заявки должно быть введено точно так, как оно установлено во внешнем IDP. Название заявки больше нигде не встречается в Management Client.
Отображаемое имя	Отображаемое название заявки. Это название, которое вы увидите при настройке ролей в Management Client.
С учетом регистра	Указывает, учитывается ли регистр в значении заявки. Примеры значений, в которых обычно учитывается регистр: — текстовое представление идентификаторов, например, GUID: F951B1F0-2FED-48F7-88D3-49EB5999C923 или OadFgrDesdFesff= Примеры значений, в которых обычно не учитывается регистр: — адреса электронной почты — имена ролей — имена групп .
Добавить, **Изменить**, **Удалить**	Регистрация и ведение заявок.

Имя	Описание
	При изменении заявки на веб-сайте внешнего IDP пользователям потребуется заново войти в клиент XProtect. Допустим, пользователю Бобу нужно назначить роль оператора. В этом случае на веб-сайте внешнего IDP добавляется заявка на имя Боба, но если Боб уже выполнил вход в XProtect, ему потребуется войти заново, чтобы изменения вступили в силу.

Добавление URI перенаправления для веб-клиентов

URI перенаправления — это местонахождение, в которое перенаправляется пользователь после успешного входа. URI перенаправления должны точно совпадать с адресами веб-клиентов. Например, вы не сможете войти через внешний IDP, если откроете XProtect Web Client из **https://localhost:8082/index.html** и если добавленный URI перенаправления для веб-клиентов — **https://127.0.0.1:8082/index.html**.

Имя	Описание
URI	URI XProtect Web Client в формате **https://[mobile server]:[port]/index.html**. В URI перенаправления регистр не учитывается. Введите URI перенаправления для каждого адреса, который можно использовать для доступа к серверу XProtect Mobile / XProtect Web Client. Например, URI перенаправления могут использоваться как со сведениями о домене, так и без них. • https://[имя устройства]:8082/index.html • https://[полное имя устройства, включая домен]:8082/index.html • https://localhost:8082/index.html • https://127.0.0.1:8082/index.html • https://[server_IP]:8082/index.html • https://[общедоступний IP для сервера XProtect Mobile]:[public port]/index.html

Имя	Описание
	• https://[общедоступний DNS для сервера XProtect Mobile]:[public port]/index.html
Добавить, **Изменить**, **Удалить**	Регистрация и ведение URI перенаправления.  При удалении URI для работы системы нужно сохранить хотя бы один URI перенаправления.

Вкладка «Панель мониторинга клиента» (параметры)

На вкладке **Панель мониторинга клиента** можно включать и отключать Milestone Customer Dashboard.

Панель мониторинга клиента — это служба онлайн-мониторинга, в которой графически отображается текущее состояние вашей системы, в том числе возможные технические проблемы, такие как сбои камер. Эти данные могут просматривать системные администраторы или другие лица, имеющие доступ к информации о вашей системе.

В любой момент можно установить или снять флажок, чтобы изменить параметры панели мониторинга клиента.

Вкладка «Защита доказательств» (параметры)

 Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

На вкладке **Защита доказательств** можно определять и редактировать профили защиты доказательств и продолжительность хранения защищенных данных по желанию пользователей клиента.

Имя	Описание
Профили защиты	Список заданных профилей защиты доказательств.

Имя	Описание
доказательств	Существующие профили защиты доказательств можно добавлять и удалять. Профиль защиты доказательств, созданный по умолчанию удалить нельзя, но можно изменить его настройки времени и имя.
Настройки времени блокировки	Продолжительность защиты доказательств, которую могут выбрать пользователи клиента. Время можно задать в часах, днях, неделях, месяцах, годах. Также оно может быть неопределенным или настраиваться пользователем.

Информацию о том, как задать разрешения роли для доступа к защите доказательств, см. в настройках роли в Вкладка «Устройство» (роли) на стр. 600.

Вкладка «Аудиосообщения» (параметры)

На вкладке **Аудиосообщения** можно загружать файлы с аудиосообщениями, которые используются для трансляции сообщений, активируемой правилами.

Загружать можно не более 50 файлов, а размер отдельного файла должен быть не больше 1 МБ.

Имя	Описание
Имя	Содержит имя сообщения. Имя вводится при добавлении сообщения. Чтобы отправить сообщение в систему, нажмите **Добавить**.
Описание	Содержит описание сообщения. Описание вводится при добавлении сообщения. В поле описания можно ввести цель сообщения или само сообщение.
Добавить	Используется для загрузки аудиосообщений в систему. Поддерживаются стандартные форматы аудиофайлов Windows: • WAV, • WMA, • FLAC.

Имя	Описание
Редактировать	Используется для изменения имени и описания или замены самого файла.
Удалить	Удаление аудиосообщения из списка.
Воспроизвести	Нажмите эту кнопку, чтобы прослушать аудиосообщение с компьютера, на котором выполняется Management Client.

Создание правил, которые активируют воспроизведение аудиосообщений, описано в разделе, посвященном добавлению правил.

Подробные сведения обо всех действиях, которые можно использовать в правилах, см. в разделе Действия и действия завершения.

Вкладка «Параметры конфиденциальности»

На вкладке **Параметры конфиденциальности** можно включать и отключать сбор данных об использовании в XProtect Mobile Server, клиенте XProtect Mobile, XProtect Web Client и XProtect Smart Client. Затем нажмите **OK**.

Включая сбор данных об использовании, вы соглашаетесь, что Milestone Systems будет использовать технологию Google в качестве стороннего поставщика, что не исключает обработки данных в США. Дополнительные сведения о защите данных и сборе данных по использованию см. в руководстве по конфиденциальности GDPR.

Вкладка «Настройки управления доступом» (параметры)

Для использования XProtect Access необходимо приобрести базовую лицензию, дающую доступ к этой функции.

Имя	Описание
Показать панель	При установке этого флажка в разделах **Управление доступом** > **Общие**

Имя	Описание
разработки свойств	**настройки** появляется дополнительная информация для разработчика. Этот параметр предназначен только для разработчиков модулей интеграции системы управления доступом.

Вкладка «События аналитики» (параметры)

На вкладке **События аналитики** можно включить события аналитики и настроить их функции.

Имя	Описание
Включить	Укажите, нужно ли использовать события аналитики. По умолчанию эта функция отключена.
Порт	Укажите порт, который используется этой функцией. По умолчанию используется порт 9090. Убедитесь, что соответствующие поставщики инструментов VCA используют тот же номер порта. При изменении номера порта не забудьте изменить номер порта поставщиков.
Все сетевые адреса или **Заданные сетевые адреса**	Задайте разрешение для всех событий со всех IP-адресов/имен хостов или только для событий с IP-адресов/имен хостов, указанных в **Списке адресов** (см. ниже).
Список адресов	Задайте список доверенных IP-адресов/имен хостов. Список применяет фильтр к входящим данным таким образом, чтобы принимались только события от определенных IP-адресов/имен хостов. Можно использовать систему доменных имен (DNS), форматы адресов IPv4 и IPv6. Адреса в список можно добавлять вручную, путем ввода каждого IP-адреса или имени хоста. Кроме того, можно импортировать внешний список адресов.

Имя	Описание
	• **Ручной ввод**: Введите IP-адрес/имя хоста в список адресов. Повторите для каждого адреса, который нужно ввести. • **Импорт**: Нажмите **Импорт** для поиска внешнего списка адресов. Внешний список должен быть в формате TXT, в каждой строке должно быть по одному IP-адресу/имени хоста.

Вкладка «Сигналы тревоги и события» (параметры)

На вкладке **Сигналы тревоги и события** можно задать параметры сигналов тревоги, событий и журналов. Более подробно об этих параметрах см. также в разделе Ограничение размера базы данных на стр. 146.

Имя	Описание
Срок хранения закрытых тревог	Укажите количество дней хранения сигналов тревоги с состоянием **Закрыт** в базе данных. Если установить значение **0**, сигнал тревоги удаляется после закрытия.  У сигналов тревоги всегда есть метки времени. Если сигнал тревоги активирован камерой, эта метка будет сопровождаться изображением со временем срабатывания сигнала тревоги. Сама информация о сигнале тревоги хранится на сервере событий, а видеозаписи, связанные с прилагаемым изображением, хранятся на соответствующем сервере системы наблюдения. Чтобы иметь возможность просматривать изображения, связанные с вашими сигналами тревоги, храните видеозаписи по крайней мере столько же времени, сколько планируете хранить сигналы тревоги на сервере событий.

Имя	Описание
Срок хранения всех остальных тревог	Укажите количество дней хранения сигналов тревоги с состоянием **Новый**, **Выполняется** или **Отложено**. Если задать значение 0, сигнал тревоги отображается в системе, но не сохраняется. У сигналов тревоги всегда есть метки времени. Если сигнал тревоги активирован камерой, эта метка будет сопровождаться изображением со временем срабатывания сигнала тревоги. Сама информация о сигнале тревоги хранится на сервере событий, а видеозаписи, связанные с прилагаемым изображением, хранятся на соответствующем сервере системы наблюдения. Чтобы иметь возможность просматривать изображения, связанные с вашими сигналами тревоги, храните видеозаписи по крайней мере столько же времени, сколько планируете хранить сигналы тревоги на сервере событий.
Включить словесную регистрацию	Установите этот флажок, чтобы вести более подробный журнал взаимодействия с сервером событий. Он будет храниться столько дней, сколько указано в поле **Срок хранения журналов**.
Типы события	Укажите количество дней хранения событий в базе данных. Существует два способа это исправить: • Можно указать время хранения для целой группы событий. Типам событий со значением **Следовать за группой** будет присваиваться значение группы событий. • Время хранения можно указать для отдельных типов событий, даже если значение задано группе событий. Если задано значение **0**, события не сохраняются в базе данных.

Имя	Описание
	Внешние события (заданные пользователем события, типичные события и события входного сигнала аппаратного устройства) имеют значение **0** по умолчанию, и это значение нельзя изменить. Эти типы событий возникают настолько часто, что их хранение в базе данных может сказаться на производительности.

Вкладка «Типичные события» (параметры)

На вкладке **Типичные события** можно указать типичные события и параметры, связанные с источником данных.

Дополнительные сведения о том, как настроить фактические типичные события, приведены в разделе Типичные события (объяснение).

Имя	Описание
Источник данных	Можно выбрать один из двух источников данных по умолчанию и задать пользовательский источник данных. Выбор зависит от сторонней программы и (или) оборудования и программного обеспечения, с которым требуется взаимодействовать: **Совместимый**: Включены заводские параметры, отображает все байты, TCP и UDP, только IPv4, порт 1234, без разделителя, только локальный хост, кодировка текущей кодовой страницы (ANSI). **Международный**: Включены заводские параметры, отображает только статистику, только TCP, IPv4+6, порт 1235, разделитель <CR><LF>, только локальный хост, кодировка UTF-8. (<CR><LF> = 13,10). [Источник данных A] [Источник данных Б] и так далее.

Имя	Описание
Новые	Нажмите, чтобы задать новый источник данных.
Имя	Имя источника данных.
Включено	Источники данных по умолчанию отключены. Установите этот флажок, чтобы включить источник данных.
Сброс	Нажмите эту кнопку, чтобы сбросить все параметры выбранного источника данных. Имя, введенное в поле **Имя**, сохраняется.
Порт	Номер порта источника данных.
Выбор типа протокола	Протоколы, которые система должна прослушивать и анализировать для обнаружения типичных событий: **Любой**: TCP и UDP. **TCP**: Только TCP. **UDP**: Только UDP. Пакеты TCP и UDP, которые используются для типичных событий, могут содержать специальные символы, например, @, #, +, ~ и другие.
Выбор типа IP	Возможные типы IP-адреса: IPv4, IPv6 или оба.
Разделитель байтов	Выберите разделитель байтов для разделения записей типичных событий. По умолчанию для источника данных типа **Международный** (см. **Источники данных** выше) принято значение **13,10**. (13,10 = <CR><IF>).
Echo type selector	Доступные форматы получения отображения: • **Статистика отображения**: Отображение в формате: **[X],[Y],[Z],[Имя типичного события]** **[X]** = номер запроса. **[Y]** = количество символов. **[Z]** = количество совпадений с типичным событием. **[Имя типичного события]** = имя, введенное в поле **Имя**.

Имя	Описание
	• **Отображать все байты**: Отображение всех байтов. • **Без отображения**: Отключает отображение любых данных.
Выбор типа кодирования	По умолчанию в списке отображаются только наиболее актуальные варианты. Установите флажок **Показать все**, чтобы отобразить все доступные тип кодирования.
Allowed external IPv4 addresses	Укажите IP-адреса, с которыми сервер управления должен иметь возможность взаимодействовать для управления внешними событиями. Здесь также можно исключить IP-адреса, с которых вы не хотите получать данные.
Allowed external IPv6 addresses	Укажите IP-адреса, с которыми сервер управления должен иметь возможность взаимодействовать для управления внешними событиями. Здесь также можно исключить IP-адреса, с которых вы не хотите получать данные.

Меню компонентов

Меню Management Client

Меню «Файл»

Вы можете сохранить изменения в конфигурации и выйти из приложения. Также можно создать резервную копию конфигурации; подробнее об этом см. раздел Резервное копирование и восстановление конфигурации системы (объяснение) на стр. 361.

Меню «Правка»

Здесь можно отменить изменения.

Меню «Вид»

Имя	Описание
Сброс разметки приложения	Сброс положения и размера панелей в Management Client к настройкам по умолчанию.

Имя	Описание
Окно предварительного просмотра	Здесь можно включить и отключить панель **Предварительный просмотр** при работе с серверами записи и устройствами.
Показать потоки записи	По умолчанию информация, которая отображается вместе с изображениями на панели **Предварительный просмотр**, относится к потокам в режиме реального времени с камер. Если вместо этого вам нужна информация о потоках записи, выберите **Показать потоки записи**.
Иерархия федеративных сайтов	По умолчанию панель **Иерархия федеративных сайтов** включена.
Навигация по сайту	По умолчанию панель **Навигация по сайту** включена.

Меню «Действие»

Содержимое меню **Действие** различается в зависимости от элемента, выбранного на панели **Навигация по сайту**. Действия, которые можно выбрать здесь — такие же, как в контекстном меню (при нажатии на элемент правой кнопкой мыши).

Подробнее о буферизации перед событием для каждой камеры см. в разделе Управление буферизацией перед событием.

Имя	Описание
Обновить	Функция всегда доступна и позволяет повторно загрузить запрошенную информацию с сервера управления.

Меню «Инструменты»

Имя	Описание
Зарегистрированные службы	Управление зарегистрированными службами. См. раздел Управление зарегистрированными службами на стр. 390.
Эффективные роли	Просмотр всех ролей выбранного пользователя или группы.
Опции	Открывает диалоговое окно «Опции», которое позволяет настраивать и редактировать глобальные параметры системы. Дополнительные сведения приведены в разделе Параметры системы (диалоговое окно «Опции») на стр. 417.

Меню «Справка»

Позволяет получить доступ к справочной системе и информации о версии Management Client.

Server Configurator (служебная программа)

Свойства вкладки «Шифрование»

На этой вкладке можно задать следующие свойства:

Прежде чем создавать сертификаты для всех компьютеров, необходимо настроить кластер в кластерной среде и убедиться, что он работает. После этого можно установить сертификаты и выполнить регистрацию с помощью Server Configurator для всех узлов кластера. Дополнительные сведения см. в руководстве по сертификатам, посвященном защите систем XProtect VMS.

Имя	Описание	Задача
Сертификат сервера	Здесь выбирается сертификат, который будет использоваться для шифрования двустороннего подключения между сервером управления, службами сбора данных и серверами записи.	Включить шифрование при передаче на сервер управления и из

Имя	Описание	Задача
		него Включить шифрование сервера для серверов записи или удаленных серверов
Сервер событий и расширения	Выберите сертификат, который будет использоваться для шифрования двусторонних подключений между сервером событий и компонентами, обменивающимися данными с сервером событий, включая LPR Server.	Включить шифрование сервера событий на стр. 333
Сертификат потоковых мультимедиа	Выберите сертификат, который будет использоваться для шифрования связи между серверами записи и всеми клиентами, серверами и интеграциями, которые получают потоки данных от серверов записи.	Включить шифрование для клиентов и серверов
Сертификат мобильных потоковых мультимедиа	Здесь выбирается сертификат, который будет использоваться для шифрования связи между мобильным сервером и мобильными и веб-клиентами, получающими потоки данных с мобильного сервера.	Включить шифрование на мобильном сервере

Регистрация серверов

Имя	Описание	Задача
Адрес сервера управления	Адрес сервера управления обычно включает имя хоста или полное доменное имя компьютера. По умолчанию этот адрес активен только с компьютера в VMS XProtect без установленного сервера управления. Как правило, адрес сервера управления не следует изменять с компьютера, на котором	Дополнительную информацию о последствиях изменения адреса сервера управления на компьютере с установленным сервером управления можно получить в следующих разделах:

Имя	Описание	Задача
	установлен сервер управления. Однако если, например, вы используете Server Configurator в схеме обработки отказа, вам может потребоваться изменить адрес с помощью компьютера сервера управления. Это может произойти в среде отказоустойчивого кластера или в другом сценарии схемы обработки отказа. • Чтобы активировать поле **Адрес сервера управления** на компьютере с установленным сервером управления, нажмите на значок ручки ( ). **Внимание:** При обновлении адреса сервера управления вам необходимо получить доступ к каждому компьютеру, на котором установлены компоненты, и изменить на нем адрес сервера управления.	Изменение имени хоста на компьютере сервера управления
Регистрация	Зарегистрируйте серверы, работающие на компьютере, с помощью назначенного сервера управления.	Регистрация сервера записи

Выбор языка

Используйте эту вкладку, чтобы выбрать язык для Server Configurator. Набор языков для Server Configurator соответствует набору языков для Management Client.

Имя	Описание
Выберите язык	Выберите язык пользовательского интерфейса.

При работе в среде отказоустойчивого кластера рекомендуется приостанавливать кластер перед запуском задач в Server Configurator. Это необходимо, потому что Server Configurator может потребоваться остановить службы при применении изменений, а среда отказоустойчивого кластера может мешать этой операции.

Значки состояния служб на панели задач

Значки в таблице показывают различные состояния служб, выполняемых на серверах в VMS XProtect. Значки доступны на компьютерах с установленными серверами:

Значок Management Server Manager на панели задач	Значок Recording Server Manager на панели задач	Значок Event Server Manager на панели задач	Значок Failover Recording Server Manager на панели задач	Описание
				**Работа** Отображается при включении и запуске службы сервера. Если служба Failover Recording Server запущена, она может принять на себя функции стандартных серверов записи в случае их сбоя.
				**Остановлено** Отображается при остановке службы сервера.

Значок Management Server Manager на панели задач	Значок Recording Server Manager на панели задач	Значок Event Server Manager на панели задач	Значок Failover Recording Server Manager на панели задач	Описание
				Если служба Failover Recording Server приостанавливает работу, она может принять на себя функции стандартных серверов записи в случае их сбоя.
				**Запуск** Отображается, когда служба сервера находится в процессе запуска. Как правило, через некоторое время значок на панели задач меняется на **Работает**.
				**Остановка** Отображается, когда служба сервера находится в процессе остановки. Как правило, через некоторое время значок на панели задач меняется на **Остановлен**.
				**В неизвестном состоянии** Отображается при первоначальной загрузки службы сервера и до получения первых данных, после чего значок на панели задач, как правило, меняется на

Значок Management Server Manager на панели задач	Значок Recording Server Manager на панели задач	Значок Event Server Manager на панели задач	Значок Failover Recording Server Manager на панели задач	Описание
				Запуск, а затем на **Работает**.
				**Работает — автономный режим** Как правило, отображается, когда сервер записи или резервная служба записи выполняется, а служба Management Server — нет.

Запуск и остановка служб с помощью значков на панели задач

Нажав правой кнопкой мыши значок в области уведомлений, можно открыть значки на панели задач для запуска и остановки служб.

- Запуск или остановка службы Management Server
- Запуск или остановка службы Recording Server

Management Server Manager (значок на панели задач)

Используйте пункты меню значка Management Server Manager для выполнения задач Management Server Manager.

Имя	Описание
ПускManagement Server и **СтопManagement Server**	Запуск и остановка службы Management Server. При остановке службы Management Server вы не сможете использовать Management Client. Значок на панели задач отображает состояние службы. Дополнительные сведения о состоянии значков на панели задач см. в разделе Значки на панели задач диспетчера сервера (объяснение).

Имя	Описание
Просмотр сообщений о статусе	Просмотр списка сообщений о статусе с временными отметками.
Изменить параметры пароля для настройки системы	Назначение или изменение пароля для настройки системы. Также можно отказаться от использования пароля для настройки системы, удалив все назначенные ранее пароли. Изменить параметры пароля для настройки системы
Ввести пароль для настройки системы	Введите пароль. Это функция применяется, например, если файл, содержащий настройки пароля, удален или поврежден. Дополнительные сведения приведены в разделе Вход в параметры пароля для настройки системы.
Настройка сервера управления для обработки отказа	Запустите мастер настройки сервера управления для обработки отказа или откройте страницу **Управление конфигурацией**, чтобы управлять существующей конфигурацией. Дополнительные сведения об отказоустойчивом кластере приведены в разделе XProtect Management Server Failover на стр. 57.
Server Configurator	Откройте **Server Configurator** для регистрации серверов и управления шифрованием. Дополнительные сведения об управлении шифрованием приведены в разделе Управление шифрованием с помощью Server Configurator.
Изменить лицензию	На компьютере сервера управления измените код лицензии на программное обеспечение. Новый код лицензии может потребоваться, например, для обновления системы XProtect. Дополнительные сведения приведены в разделе Изменение кода лицензии на программное обеспечение.
Восстановить конфигурацию	Открывает диалоговое окно, из которого можно восстановить конфигурацию системы. Прежде чем нажать **Восстановить**, внимательно прочитайте информацию в диалоговом окне. Дополнительные сведения приведены в разделе Восстановление конфигурации системы из резервной копии, созданной вручную.
Выбрать общую	Прежде чем создавать резервную копию конфигурации системы, укажите

Имя	Описание
папку резервного копирования	папку резервного копирования, где будет храниться копия. Дополнительные сведения приведены в разделе Выбор общей папки резервного копирования.
Обновить адрес SQL	Откройте мастер, чтобы изменить адрес SQL Server. В редких случаях, когда меняется имя хоста, может потребоваться привести адрес SQL Server в соответствие с изменениями. Дополнительные сведения приведены в разделе Изменение имени хоста может вызвать изменение адреса сервера SQL.

Узел «Основы»

Информация о лицензии (узел «Базовые сведения»)

В окне **Сведения о лицензии** можно отслеживать все лицензии с одним файлом лицензии программного обеспечения на этом и на всех других объектах, ваши подписки Milestone Care, а также выбрать способ активации лицензий.

Дополнительную информацию о различных сведениях и функциях, доступных в окне **Сведения о лицензии**, см. в разделе Окно «Сведения о лицензии» на стр. 141.

Информация об объекте (узел «Основы»)

В крупной среде Milestone Federated Architecture с большим количеством дочерних сайтов общий обзор и поиск контактных данных администраторов каждого дочернего сайта может представлять трудности.

Вы можете добавить дополнительные сведения в каждый дочерний сайт, и эта информация затем будет доступна администраторам центрального объекта.

Можно добавить следующую информацию:

- название объекта
- адрес/расположение
- администратор(ы)
- Дополнительная информация

Узел «Службы удаленного подключения»

Подключение к камере Axis нажатием одной кнопки (узел «Службы удаленного подключения»)

Ниже представлены свойства подключения к камере Axis нажатием одной кнопки.

Имя	Описание
Пароль для камеры	Ввести/изменить. Предоставляется вместе с камерой при покупке. Для получения дополнительной информации см. руководство к вашей камере или веб-сайт Axis (https://www.axis.com/).
Пользователь камеры	Для получения подробной информации см. **Пароль для камеры**.
Описание	Ввести/изменить описание камеры.
Внешний адрес	Ввести/изменить веб-адрес сервера ST, к которому подключается камера.
Внутренний адрес	Ввести/изменить веб-адрес сервера ST, к которому подключается сервер записи.
Имя	При необходимости измените имя элемента.
Ключ аутентификации владельца	См. **Пароль для камеры**.
Пароли (для сервера контроля)	Введите пароль. Пароль должен быть идентичен полученному от поставщика вашей системы.
Пароли (для сервера ST)	Введите пароль. Пароль быть идентичен введенному при установке компонента «Подключение к Axis нажатием одной кнопки».
Зарегистрировать/отменить регистрацию в службе контроля Axis	Укажите, хотите ли вы зарегистрировать камеру Axis в службе контроля Axis. Это можно сделать во время настройки или позже.

Имя	Описание
Серийный номер	Серийный номер оборудования, указанный производителем. Серийный номер часто (но не всегда) идентичен MAC-адресу.
Использовать учетные данные	Установите флажок, если вы хотите использовать учетные данные во время установки сервера ST.
Имя пользователя (для сервера контроля)	Введите имя пользователя. Имя пользователя должно быть идентичным полученному от поставщика вашей системы.
Имя пользователя (для сервера ST)	Введите имя пользователя. Должно быть идентично введенному при установке **компонента «Подключение к Axis нажатием одной кнопки»**.

Узел «Серверы»

Серверы (узел)

В этом разделе описано, как установить и настроить серверы записи и серверы записи обработки отказа. Вы также узнаете, как добавить в систему новое оборудование и выполнить взаимное подключение других объектов.

- Серверы записи (узел «Серверы») на стр. 449
- Серверы отказоустойчивости (узел «Серверы») на стр. 464

Серверы записи (узел «Серверы»)

Система использует серверы записи для записи потоков видеоданных и обмена данными с камерами и другими устройствами. Система наблюдения, как правило, состоит из нескольких серверов записи.

Серверы записи — это компьютеры, на которых установлено ПО Recording Server, настроенные для взаимодействия с сервером управления. Серверы записи отображаются на панели **Обзор**: откройте папку **Серверы** и выберите **Серверы записи**.

Обратная совместимость с версиями сервера записи, предшествующими этой версии сервера управления, ограничена. Вы можете получать доступ к записям на серверах записи со старыми версиями, однако для изменения их конфигурации их версия должна соответствовать этой версии сервера управления. Milestone рекомендует обновить все серверы записи в системе до версии сервера управления.

Окно «Настройки сервера записи»

Нажав правой кнопкой мыши значок Recording Server Manager на панели задач и выбрав **Изменить настройки**, можно указать следующее:

Имя	Описание
Адрес	IP-адрес (пример: 123.123.123.123) или имя хоста (пример: ourserver) сервера управления, к которому должен быть подключен сервер записи. Эта информация необходима для связи сервера записи с сервером управления.
Порт	Номер порта, который должен использоваться для связи с сервером управления. По умолчанию используется порт 9000. Если необходимо, эти сведения можно изменить.
Порт веб-сервера	Номер порта, который будет использоваться для обработки запросов веб-сервера, например, для обработки команд управления PTZ-камерой, а также для просмотра и запросов в реальном времени от XProtect Smart Client. По умолчанию используется порт 7563. Если необходимо, эти сведения можно изменить.
Порт сервера оповещения	Номер порта, который будет использоваться, когда сервер записи получает информацию TCP (некоторые устройства используют TCP для отправки сообщений о событиях). По умолчанию используется порт 5432 (по умолчанию он отключен). Если необходимо, эти сведения можно изменить.
Порт сервера SMTP	Номер порта, который будет использоваться, когда сервер записи получает информацию SMTP (простой протокол передачи электронной почты). SMTP — это стандарт отправки сообщений электронной почты между серверами. Некоторые устройства используют SMTP для отправки сообщений о событиях или изображений на сервер системы наблюдения по электронной почте. По умолчанию используется порт 25, который можно включать и отключать. Если необходимо, номер порта можно изменить.
Шифровать	Прежде чем включить шифрование и выбрать из списка сертификат

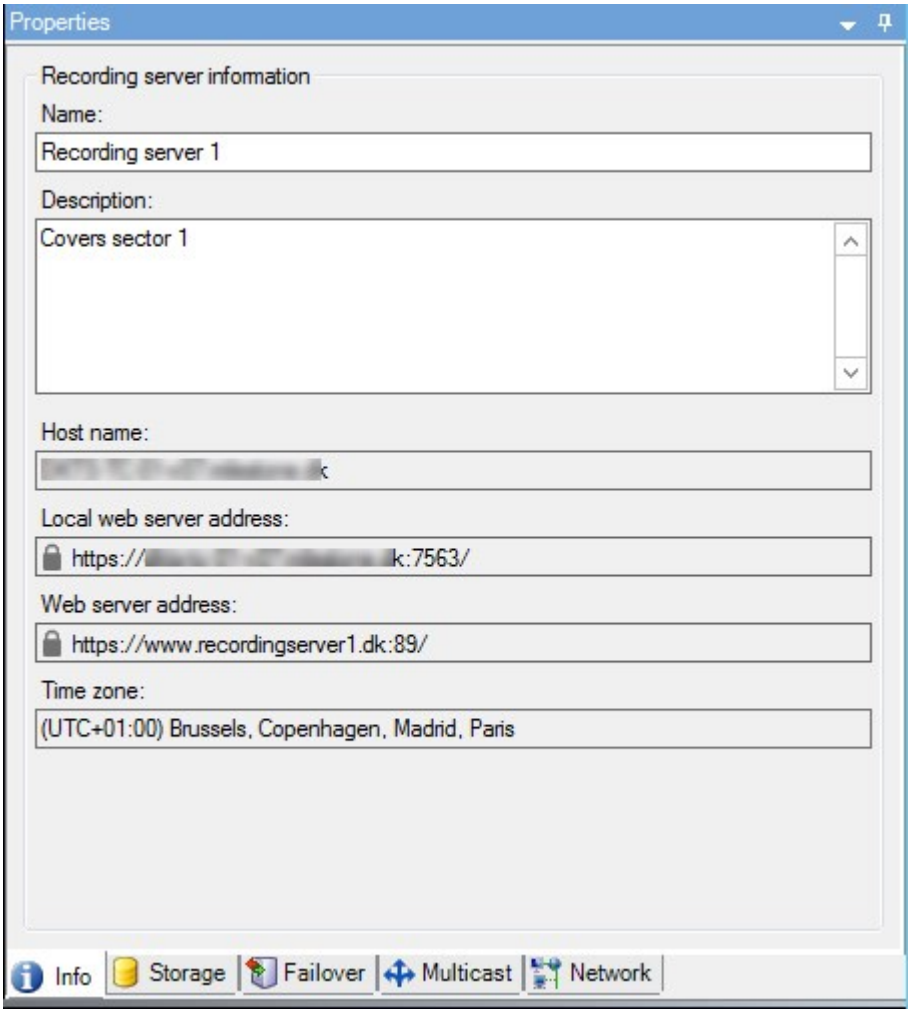
Имя	Описание
соединения между сервером управления и сервером записи	аутентификации сервера, убедитесь, что вы сначала включили шифрование на сервере управления и что сертификат сервера управления является доверенным на сервере записи. Дополнительные сведения приведены в разделе Защищенное соединение (объяснение) на стр. 162.
Шифровать подключение к клиентам и службам, передающим потоки данных	Прежде чем включить шифрование и выбрать из списка сертификат аутентификации сервера, убедитесь, что сертификат является доверенным на всех компьютерах, где запущены службы, получающие потоки данных с сервера записи. XProtect Smart Client и все службы, получающие потоки данных с сервера записи, должны быть обновлены до 2019 R1 или более новой версии. Может потребоваться обновить некоторые решения сторонних производителей, созданные с помощью версий MIP SDK, предшествующих 2019 R1. Дополнительные сведения приведены в разделе Защищенное соединение (объяснение) на стр. 162. Чтобы проверить, использует ли ваш сервис записи шифрование, см Просмотр состояния шифрования при подключении к клиентам на стр. 317.
Подробно	Просмотр информации о выбранном сертификате из хранилища сертификатов Windows.

Свойства серверов записи

Вкладка «Информация» (сервер записи)

На вкладке **Информация** можно проверить или изменить имя и описание сервера записи.

Здесь можно просмотреть имя и адреса хоста. Значок замка перед адресом веб-сервера указывает на зашифрованную связь с клиентами и службами, которые получают потоки данных с этого сервера записи.



Имя	Описание
Имя	Здесь можно ввести имя сервера записи. Это имя используется в системе и клиентах, когда сервер записи отображается в списке. Имя не обязательно должно быть уникальным. При переименовании сервера записи имя меняется глобально в Management Client.
Описание	Здесь можно ввести описание, которое будет отображаться в некоторых списках системы. Описание не является обязательным.
Имя узла	Отображает имя хоста сервера записи.

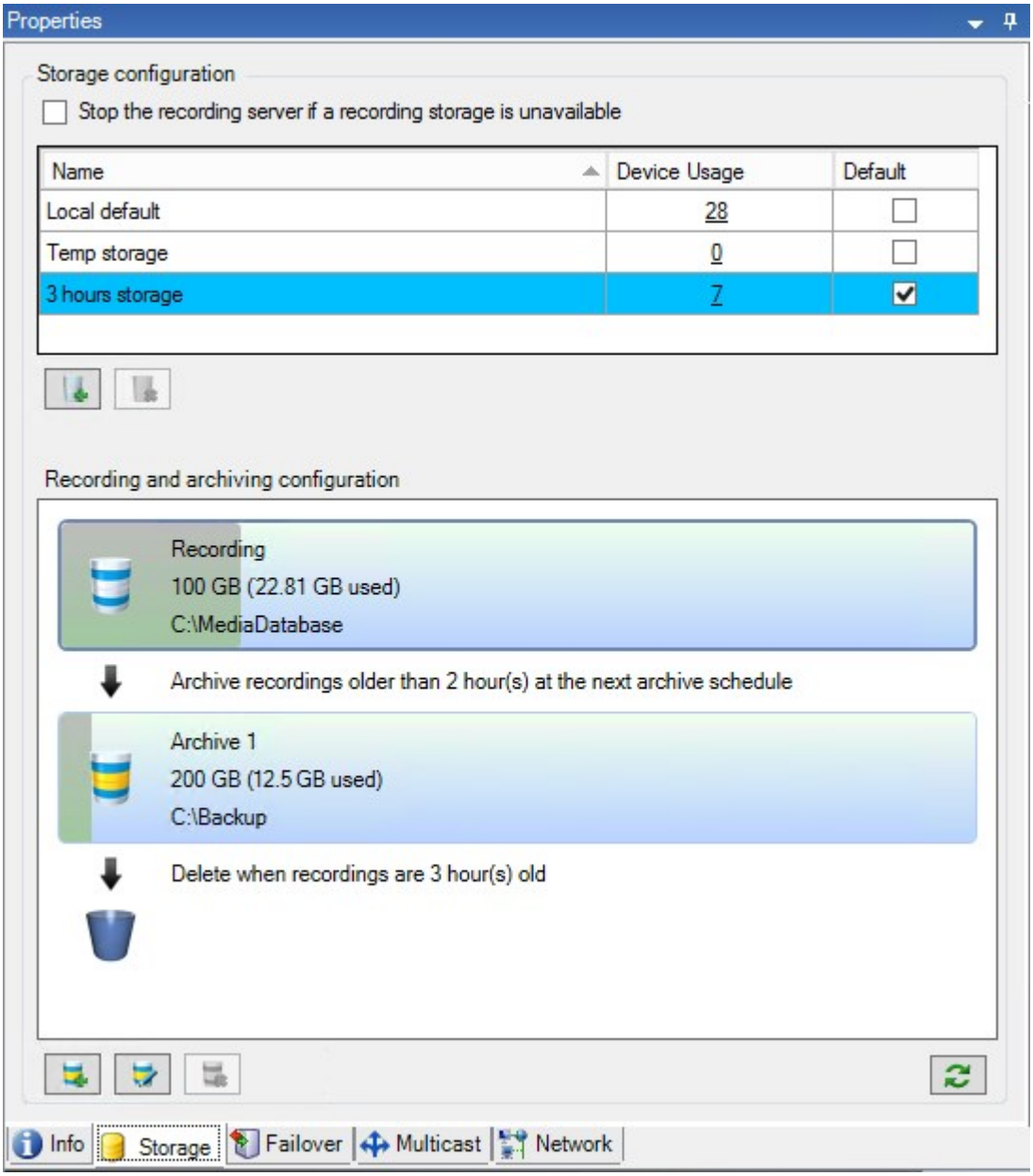
Имя	Описание
Адрес локального веб-сервера	Отображает локальный адрес веб-сервера записи. Локальный адрес используется, например, для обработки команд управления PTZ-камерой, а также для обработки запросов на просмотр и прямую передачу в режиме реального времени из XProtect Smart Client. В адрес включается номер порта, который используется для обмена данными с веб-сервером (как правило, порт 7563). При включении шифрования для связи с клиентами и серверами, получающими потоки данных от сервера записи, отображается значок замка, а адрес включает **https** вместо **http**.
Адрес веб-сервера	Здесь отображается общедоступный адрес веб-сервера записи в Интернете. Если в системе используется брандмауэр или NAT-маршрутизатор, введите адрес брандмауэра или NAT-маршрутизатора, чтобы клиенты, получающие доступ к системе наблюдения через Интернет, могли подключаться к серверу записи. Общедоступный адрес и номер порта указываются на вкладке **Свойства**. При включении шифрования для связи с клиентами и серверами, получающими потоки данных от сервера записи, отображается значок замка, а адрес включает **https** вместо **http**.
Часовой пояс	Отображает часовой пояс, в котором расположен сервер записи.

Вкладка «Хранилище» (сервер записи)

На вкладке **Хранение** можно просматривать и настраивать хранилища для выбранного сервера записи и управлять ими.

Текущий объем свободного места в архивах и хранилищах записей отмечается горизонтальной чертой. Вы можете задать поведение сервера записи в ситуациях, когда хранилища записей становятся недоступными. Это особенно актуально, если система включает серверы отказоустойчивости.

Если вы используете функцию **Защита доказательств**, место, занятое материалами защиты доказательств, обозначается вертикальной красной чертой.



Свойства окна «Параметры хранения и записи»

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

В диалоговом окне **Параметры хранения и записи** укажите следующее сведения:

Имя	Описание
Имя	Измените имя хранилища, если необходимо. Имена должны быть уникальными.
Путь	Укажите путь к каталогу, в котором будут сохраняться записи этого хранилища. Хранилище не обязательно должно находиться на компьютере сервера записи. Если каталога не существует, его можно создать. Сетевые диски следует указывать в формате UNC (универсальное соглашение об именовании), например: `\\server\volume\directory\`.
Время хранения	Укажите, в течение какого времени записи должны оставаться в архиве, прежде чем они будут удалены или перемещены в следующий архив (зависит от настроек архива). Время хранения всегда должно превышать время хранения предыдущего архива или базы данных записей по умолчанию. Это связано с тем, что количество дней хранения архива включает все периоды хранения, ранее указанные в процессе.
Максимальный размер	Выберите максимальное количество гигабайт данных записи для сохранения в базе данных записей. Данные записей свыше указанного количества гигабайт автоматически перемещаются в первый архив в списке (если таковой указан) или удаляются. ⚠ Если остается менее 5 ГБ свободного места, система всегда автоматически архивирует (или удаляет, если следующий архив не определен) наиболее старые данные в базе данных. Если остается менее 1 ГБ свободного места, данные удаляются. Базе данных всегда требуется 250 МБ свободного пространства. По достижении этого предела (если данные не удаляются достаточно быстро) данные больше не будут записываться в базу данных, пока вы не освободите достаточно места. Фактический максимальный размер базы данных — это указанное вами количество гигабайт минус 5 ГБ.
Подписывание	Включает функцию цифровой подписи для записей. Таким образом система, например, подтверждает, что экспортированное видео не было изменено или искажено при воспроизведении.

Имя	Описание
	Система использует алгоритм цифровой подписи SHA-2.
Шифрование	Выберите уровень шифрования записей: • Нет • Облегченный (меньшая загрузка ЦП) • Интенсивный (большая загрузка ЦП) Система использует алгоритм шифрования AES-256. При выборе **облегченного** уровня будет зашифрована часть записи. При выборе **интенсивного** уровня будет зашифрована вся запись. При включении шифрования потребуется указать пароль.
Пароль	Введите пароль для пользователей, которым разрешено просматривать зашифрованные данные. Milestone рекомендует использовать надежные пароли. Надежные пароли не содержат общеупотребительных слов и не являются частью имени пользователя. Они содержат восемь или более алфавитно-цифровых символов, прописные и строчные буквы, а также специальные символы.

Свойства окна «Настройки архива»

В диалоговом окне **Настройки архива** введите следующие сведения:

Имя	Описание
Имя	Измените имя хранилища, если необходимо. Имена должны быть уникальными.
Путь	Укажите путь к каталогу, в котором будут сохраняться записи этого хранилища. Хранилище не обязательно должно находиться на компьютере сервера записи. Если каталога не существует, его можно создать. Сетевые диски следует указывать в формате UNC (универсальное соглашение об именовании),

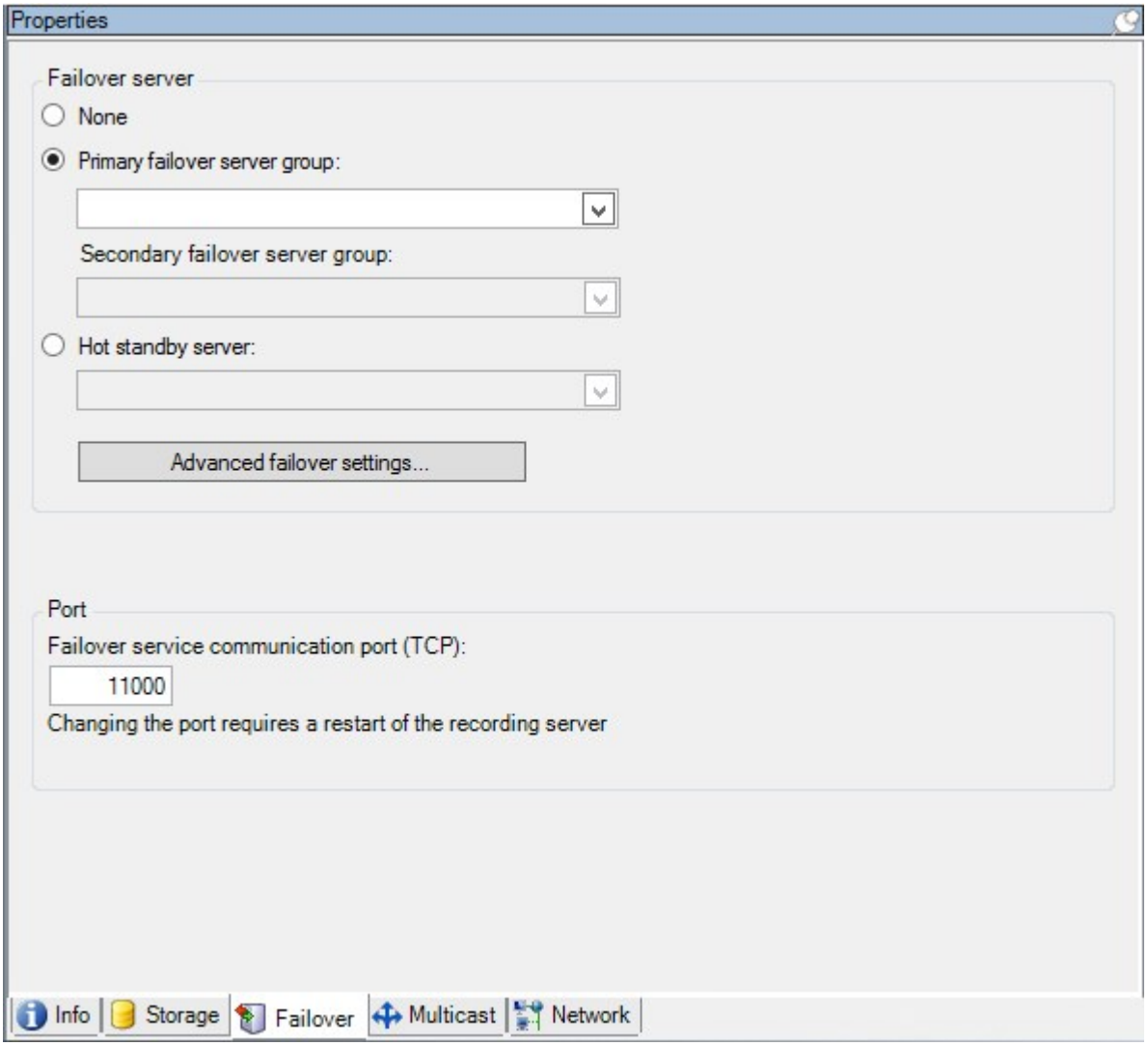
Имя	Описание
	например: `\\server\volume\directory\`.
Время хранения	Укажите, в течение какого времени записи должны оставаться в архиве, прежде чем они будут удалены или перемещены в следующий архив (зависит от настроек архива). Время хранения всегда должно превышать время хранения предыдущего архива или базы данных записей по умолчанию. Это связано с тем, что количество дней хранения архива включает все периоды хранения, ранее указанные в процессе.
Максимальный размер	Выберите максимальное количество гигабайт данных записи для сохранения в базе данных записей. Данные записей свыше указанного количества гигабайт автоматически перемещаются в первый архив в списке (если таковой указан) или удаляются. Если остается менее 5 ГБ свободного места, система всегда автоматически архивирует (или удаляет, если следующий архив не определен) наиболее старые данные в базе данных. Если остается менее 1 ГБ свободного места, данные удаляются. Базе данных всегда требуется 250 МБ свободного пространства. По достижении этого предела (если данные не удаляются достаточно быстро) данные больше не будут записываться в базу данных, пока вы не освободите достаточно места. Фактический максимальный размер базы данных — это указанное вами количество гигабайт минус 5 ГБ.
Расписание	Настройте расписание архивирования, где указаны интервалы, с которыми должен выполняться процесс архивирования. Архивирование можно выполнять очень часто (теоретически — каждый час в течение всего года) или очень редко (например, каждый первый понедельник или раз в 36 месяцев).
Уменьшить частоту кадров	Чтобы уменьшить частоту кадров при архивировании, установите флажок **Уменьшить частоту кадров** и настройте количество кадров в секунду (FPS). Уменьшение частоты кадров на выбранное количество кадров в секунду позволяет записям занимать меньше места в архиве, но также снижает их

Имя	Описание
	качество. MPEG-4/H.264/H.265 автоматически сокращается как минимум до ключевых кадров. 0,1 = 1 кадр за 10 секунд.

Вкладка «Обработка отказа» (сервер записи)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Если в организации используются серверы записи обработки отказа, перейдите на вкладку **Резерв**, чтобы назначить резервные серверы для серверов записи (см. раздел Свойства вкладки «Резерв»).



Подробные сведения о серверах записи обработки отказа, установке и параметрах, группах отказоустойчивых серверов и их параметрах см. в разделе Сервер записи обработки отказа (объяснение) на стр. 43.

Свойства вкладки «Обработка отказа»

Имя	Описание
Нет	Выберите настройку без серверов записи обработки отказа.

Имя	Описание
Основная группа серверов отказоустойчивости / Вспомогательная группа серверов отказоустойчивости	Выберите обычную настройку обработки отказа с одной основной и, по возможности, одной вспомогательной группой серверов отказоустойчивости.
Сервер горячей замены	Выберите схему горячей замены с одним выделенным сервером записи в качестве сервера горячей замены.
Доп. параметры отработки отказа	Открывает окно **Доп. параметры отработки отказа**: • **Полная поддержка**: Включает полную поддержку обработки отказа для устройства • **Только для режима «Прямая передача в режиме реального времени»**: Включает только поддержку обработки отказа для потоков в режиме реального времени на устройстве • **Отключено**: Отключает поддержку обработки отказа для устройства
Резервный порт служебной связи (TCP)	Номер порта по умолчанию — 11000. Этот порт используется для связи между серверами записи и серверами записи обработки отказа. При изменении порта сервер записи **должен** быть запущен и **должен** быть подключен к серверу управления.

Вкладка «Многоадресная передача» (сервер записи)

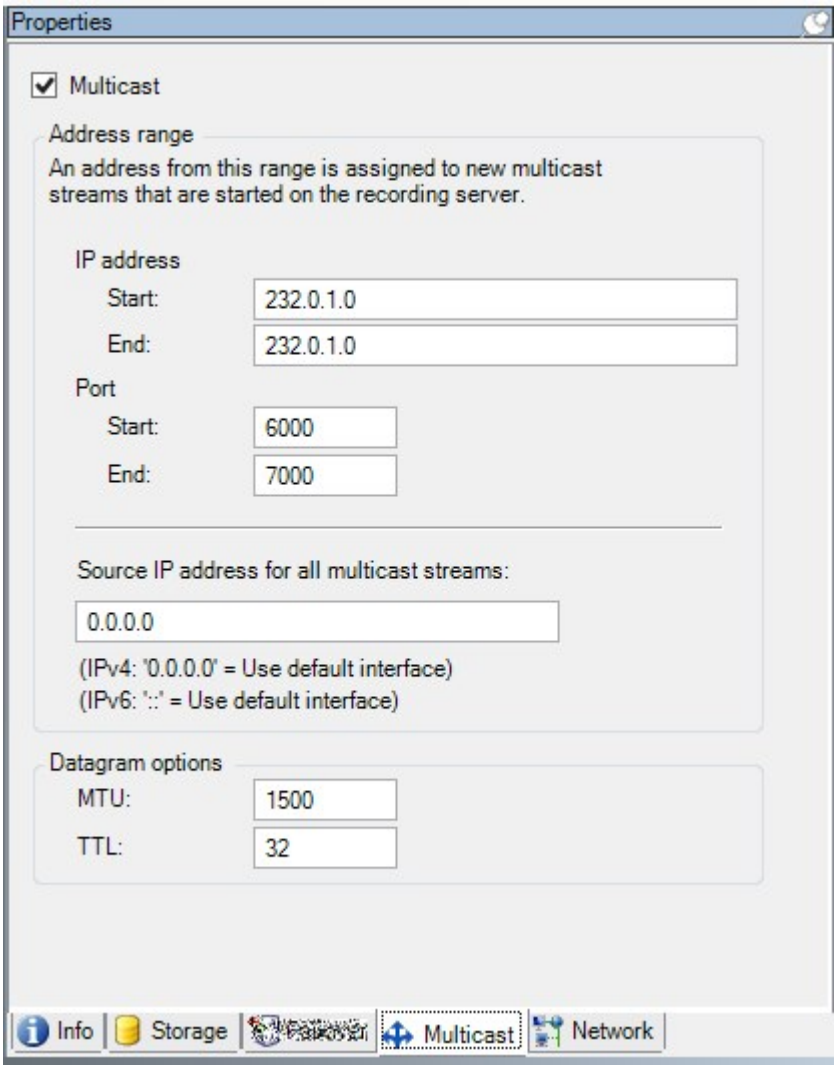
Система поддерживает многоадресную передачу видеопотоков в реальном времени с серверов записи. Если несколько пользователей XProtect Smart Client захотят просмотреть прямую передачу с одной и той же камеры, многоадресная передача поможет сэкономить значительное количество системных ресурсов. Многоадресная передача может оказаться полезной, если вы используете функцию Matrix, где несколько клиентов должны просматривать видео в реальном времени с одной и той же камеры.

Многоадресная передача возможна только для видеопотоков в реальном времени, а не для записанного видео/аудио.

Если сервер записи оснащен несколькими сетевыми адаптерами, использовать многоадресную передачу можно только по одному из них. Указать нужный адаптер можно в Management Client.

При использовании серверов отказоустойчивости необходимо также указать IP-адреса сетевых адаптеров на таких серверах (см. раздел Вкладка «Многоадресная передача» (сервер отказоустойчивости) на стр. 467).

Кроме того, для успешной реализации многоадресной передачи необходимо настроить сетевое оборудование для пересылки пакетов данных многоадресной передачи только требуемой группе получателей. В противном случае многоадресная передача может не отличаться от трансляции, что может существенно снизить производительность сети.



Назначение диапазона IP-адресов

Укажите диапазон адресов для потоков многоадресной передачи с выбранного сервера записи. Когда пользователи просматривают видео многоадресной передачи с сервера записи, клиенты подключаются к этим адресам.

Для каждого потока с камеры для многоадресной передачи IP-адрес и комбинация портов должны быть уникальными (пример: IPv4: 232.0.1.0:6000). Вы можете использовать либо один IP-адрес и множество портов, либо множество IP-адресов и меньшее количество портов. По умолчанию система предлагает один IP-адрес и диапазон из 1000 портов, но эти параметры можно изменить по мере необходимости.

IP-адреса для многоадресной передачи должны находиться в диапазоне, определенном IANA для динамического распределения хостов. IANA — это служба, контролирующая глобальное распределение IP-адресов.

Имя	Описание
IP-адрес	В поле **Начало** укажите первый IP-адрес в требуемом диапазоне. Затем в поле **Окончание** укажите последний IP-адрес в диапазоне.
Порт	В поле **Начало** укажите первый номер порта в требуемом диапазоне. Затем в поле **Окончание** укажите последний номер порта в диапазоне.
Исходный IP-адрес всех потоков многоадресной передачи	Вы можете осуществлять многоадресную передачу только с одного сетевого интерфейса, поэтому это поле актуально, если на вашем сервере записи есть несколько сетевых интерфейсов или сетевой интерфейс с несколькими IP-адресами. Чтобы использовать интерфейс сервера записи по умолчанию, оставьте в поле значение 0.0.0.0 (IPv4) или :: (IPv6). Если вы хотите использовать другой сетевой интерфейс или другой IP-адрес на том же сетевом интерфейсе, укажите IP-адрес требуемого интерфейса. • IPv4: от 224.0.0.0 до 239.255.255.255. • IPv6: диапазон приведен на сайте IANA (https://www.iana.org/).

Указание параметров дейтаграммы

Здесь указываются параметры пакетов данных (дейтаграмм), отправляемых посредством многоадресной передачи.

Имя	Описание
MTU	Максимальный размер пакета — наибольший разрешенный физический размер пакета данных (в байтах). Сообщения, размер которых превышает указанный размер, перед отправкой разделяются на более мелкие пакеты. Значение по умолчанию — 1500; также является значением по умолчанию для большинства компьютеров Windows и сетей Ethernet.
TTL	Время жизни — максимальное разрешенное количество пролетов (hop), которое может пройти пакет данных, прежде. Пролетом считается точка между двумя сетевыми устройствами, как правило маршрутизатор. Значение по умолчанию — 128.

Вкладка «Сеть» (сервер записи)

Если вам требуется получать доступ к VMS с помощью XProtect Smart Client через общедоступную или ненадежную сеть, Milestone рекомендует использовать защищенное VPN-подключение. Это позволит обеспечить защиту обмена данными между XProtect Smart Client и VMS.

Общедоступный IP-адрес сервера записи задается на вкладке **Сеть**.

В чем преимущества общедоступного адреса?

Клиенты могут подключаться из локальной сети или из Интернета, и в любом случае система наблюдения должна предоставлять подходящие адреса, чтобы клиенты могли получить доступ к записанному или транслируемому видео с серверов записи:

- Если клиенты подключаются локально, система наблюдения должна предоставить локальные адреса и номера портов.
- Если клиенты подключаются из Интернета, система наблюдения должна предоставлять общедоступный адрес сервера записи. Это адрес брандмауэра или маршрутизатора NAT (Network Address Translation — преобразование сетевых адресов), кроме того, номер порта также часто отличается. Затем адрес и номер порта могут передаваться на локальный адрес и порт сервера.

Серверы отказоустойчивости (узел «Серверы»)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Сервер записи обработки отказа — это дополнительный сервер записи, который берет на себя функции стандартного сервера записи, если тот становится недоступным. Для сервера записи обработки отказа можно настроить два режима: **сервер холодного резерва** или **сервер горячей замены**.

Серверы записи обработки отказа устанавливаются так же, как и стандартные серверы записи (см. Установка сервера записи обработки отказа с помощью Download Manager на стр. 189). После установки серверов записи обработки отказа они отображаются в Management Client. Milestone рекомендует устанавливать серверы записи обработки отказа на отдельных компьютерах. Убедитесь, что для серверов записи обработки отказа настроен правильный IP-адрес/имя хоста сервера управления. Разрешения пользователя для учетной записи пользователя, от имени которой выполняется служба сервера отказоустойчивости, предоставляются в процессе установки. Они включают:

- разрешения на запуск/останов для сервера записи обработки отказа;
- разрешения доступа на чтение и запись для файла RecorderConfig.xml.

Если для шифрование выбран сертификат, администратор должен предоставить пользователю резервного сервера разрешение на доступ для чтения для выбранного закрытого ключа сертификата.

Если сервер записи обработки отказа берет на себя функции сервера записи, в котором применяется шифрование, Milestone рекомендует также подготовить сервер записи обработки отказа для использования шифрования. Дополнительные сведения приведены в разделах Защищенное соединение (объяснение) на стр. 162 и Установка сервера записи обработки отказа с помощью Download Manager на стр. 189.

Вы можете указать, какой тип обработки отказа требуется на уровне устройства. Для каждого устройства на сервере записи выберите тип поддержки: «полная», «только при прямой передаче» или «без обработки отказа». Это поможет определить приоритетность ресурсов обработки отказа и, например, настроить обработку отказа только для видео, но не для звуковой информации, или обработку отказа только для самых важных, а не для всех, камер.

Когда система работает в режиме обработки отказа, нельзя заменять или перемещать оборудование, обновлять сервер записи или вносить изменения в конфигурации устройств, включая параметры хранения или видеопотоков.

Сервер записи обработки отказа в режиме холодной замены

В конфигурации холодной замены сервера записи обработки отказа можно объединять несколько серверов записи обработки отказа в группу отказоустойчивых серверов. Вся группа отказоустойчивых серверов будет принимать на себя функции любого из нескольких предварительно выбранных серверов записи, если один их них станет недоступен. Количество создаваемых групп не ограничено (см. Объединение серверов записи обработки отказа в группу холодной замены на стр. 230).

Группирование имеет четкое преимущество: когда вам впоследствии потребуется указать, какие серверы записи обработки отказа должны принимать на себя функции сервера записи, можно выбрать группу таких серверов. Если в выбранной группе несколько серверов записи обработки отказа, у вас будет несколько таких серверов, готовых принять на себя функции сервера записи, если он станет недоступным. Можно указать дополнительную группу серверов обработки отказа, которая будет принимать на себя функции основной группы, если все серверы записи в основной группе заняты. Сервер записи обработки отказа может одновременно принадлежать только одной группе.

Серверы записи обработки отказа в группе отказоустойчивых серверов упорядочиваются в последовательность. Последовательность определяет порядок, в котором серверы записи обработки отказа будут принимать на себя функции сервера записи. По умолчанию последовательность отражает порядок добавления серверов записи обработки отказа в группу отказоустойчивых серверов: первый добавленный сервер является первым в последовательности. Если необходимо, эти сведения можно изменить.

Серверы записи обработки отказа в режиме горячей замены

В конфигурации сервера записи обработки отказа горячей замены вы назначаете один сервер записи обработки отказа для резервирования только **одного** сервера записи. По этой причине система может поддерживать режим «ожидания» для этого сервера записи обработки отказа, то есть он синхронизируется с правильной/текущей конфигурацией сервера записи, для которого он выделен, и резервирование выполняется гораздо быстрее, чем в конфигурации сервера записи обработки отказа холодной замены. Как упоминалось выше, серверы горячей замены назначаются только одному серверу записи и их нельзя группировать. Серверы обработки отказа, уже входящие в группу отказоустойчивых серверов, нельзя назначить в качестве серверов записи горячей замены.

Проверка сервера записи обработки отказа

Чтобы проверить объединение видеоданных с сервера отказоустойчивости с сервером записи, необходимо сделать сервер записи недоступным, остановив службу сервера записи или завершив работу компьютера этого сервера.

Ручное вмешательство в сеть, такое как отсоединение сетевого кабеля или блокировка сети с помощью инструмента тестирования, недопустимо.

Свойства вкладки «Сведения» (сервер отказоустойчивости)

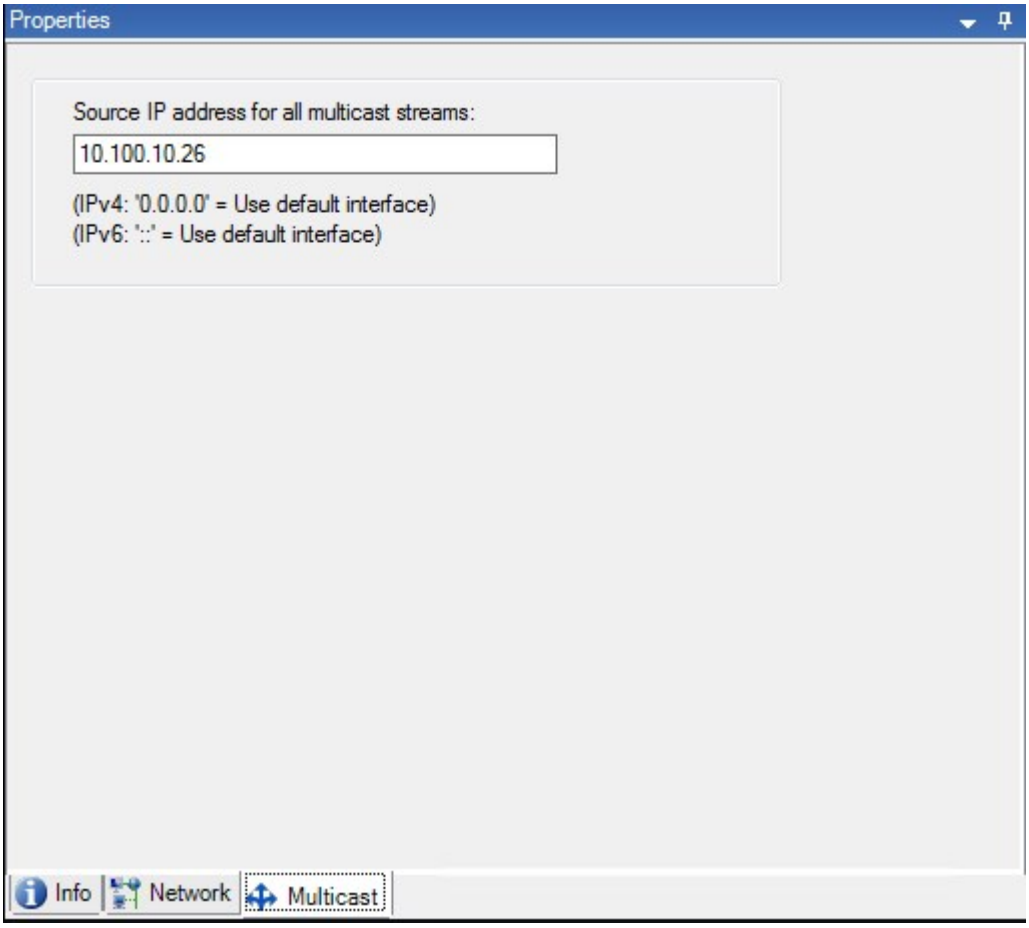
Укажите следующие свойства сервера записи обработки отказа:

Имя	Описание
Имя	Имя сервера записи обработки отказа в том виде, в котором оно отображается в Management Client, журналах и т. д.
Описание	Необязательное поле, который можно использовать для описания сервера записи обработки отказа (например, вместо какого сервера записи он действует).
Имя узла	Отображает имя хоста сервера записи обработки отказа. Этот параметр нельзя изменить.
Адрес локального веб-сервера	Отображает локальный адрес веб-сервера сервера записи обработки отказа. Локальный адрес используется, например, для обработки команд управления PTZ-камерой, а также для обработки запросов на просмотр и прямую передачу в режиме реального времени из XProtect Smart Client. В адрес включается номер порта, который используется для обмена данными с веб-сервером (как правило, порт 7563). Если сервер записи обработки отказа берет на себя функции сервера записи, в котором применяется шифрование, сервер записи обработки отказа также необходимо подготовить для использования шифрования. При включении шифрования для связи с клиентами и серверами, получающими потоки данных от сервера записи, отображается значок замка, а адрес включает **https** вместо **http**.
Адрес веб-сервера	Отображает общедоступный адрес веб-сервера сервера записи обработки отказа в Интернете. Если в системе используется брандмауэр или NAT-маршрутизатор, введите адрес брандмауэра или NAT-маршрутизатора, чтобы клиенты, получающие доступ к системе наблюдения через Интернет, могли подключаться к серверу записи обработки отказа.

Имя	Описание
	Общедоступный адрес и номер порта указываются на вкладке **Свойства**. При включении шифрования для связи с клиентами и серверами, получающими потоки данных от сервера записи, отображается значок замка, а адрес включает **https** вместо **http**.
UDP-порт	Номер порта, используемый для связи между серверами записи обработки отказа. По умолчанию используется порт 8844.
Database location	Укажите путь к базе данных, используемой сервером записи обработки отказа для хранения записей. Вы не можете изменить путь к базе данных в процессе переключения с сервера записи на сервер записи обработки отказа. Вы не можете изменить путь к базе данных, пока сервер записи обработки отказа заменяет сервер записи.

Вкладка «Многоадресная передача» (сервер отказоустойчивости)

Если вы используете серверы отказоустойчивости и включили многоадресную передачу потока в режиме реального времени, необходимо указать IP-адрес используемого сетевого адаптера как на серверах записи, так и на серверах отказоустойчивости.



Дополнительные сведения о многоадресной передаче приведены в разделе Включение многоадресной передачи для сервера записи на стр. 225.

Свойства вкладки «Сведения» (группа отказоустойчивых серверов)

Поле	Описание
Имя	Имя группы отказоустойчивых серверов в том виде, в котором оно отображается в Management Client, в журналах и т. д.
Описание	Дополнительное описание, например физическое местонахождение сервера.

Свойства вкладки «Последовательность» (группа отказоустойчивых серверов)

Поле	Описание
Укажите последовательность аварийного переключения	Используйте кнопки **Вверх** и **Вниз**, чтобы установить желаемую последовательность регулярных серверов записи обработки отказа в группе.

Удаленный сервер для Milestone Interconnect

Milestone Interconnect™ дает возможность подключить несколько небольших, физически разнесенных систем XProtect к центральному объекту XProtect Corporate. Такие небольшие объекты (так называемые удаленные объекты) можно создавать для мобильных систем (например, катеров, автобусов и поездов). Такие объекты не требуют постоянного сетевого подключения.

Вкладка «Информация» (удаленный сервер)

Имя	Описание
Имя	Имя, под которым удаленный сервер отображается в списках системы или клиентов. Имя не обязательно должно быть уникальным. При переименовании сервера имя меняется глобально в Management Client.
Описание	Описание удаленного сервера (необязательно). Описание отображается во многих списках системы. Например, при наведении указателя мыши на имя оборудования на панели **Обзор**:
Модель	Продукт XProtect, установленный на удаленном объекте.
Версия	Версия удаленной системы.
Код лицензии на программное обеспечение	Код лицензии на ПО удаленной системы.

Имя	Описание
Драйвер	Определяет драйвер, который обеспечивает подключение к удаленному серверу.
Адрес	Имя хоста и IP-адрес оборудования.
IE	Открывает домашнюю страницу поставщика оборудования, настроенную по умолчанию. Эта страница используется для управления оборудованием.
Идентификатор удаленной системы	Уникальный идентификатор системы удаленного объекта, используемый XProtect для таких целей, как управление лицензиями.

Вкладка «Параметры» (удаленный сервер)

На вкладке **Параметры** можно просмотреть имя удаленной системы.

Вкладка «События» (удаленный сервер)

Вы можете добавлять события из удаленной системы на центральный объект, чтобы создавать правила и таким образом немедленно реагировать на события из удаленной системы. Количество событий зависит от их количества в удаленной системе. События по умолчанию нельзя удалить.

Если список неполный:

1. Нажмите правой кнопкой мыши соответствующий удаленный сервер на панели **Обзор** и выберите **Обновить оборудование**.
2. В диалоговом окне отображаются все изменения (удаленные, обновленные и добавленные устройства) в удаленной системе с момента установки или последнего обновления настройки Milestone Interconnect. Нажмите **Подтвердить**, чтобы обновить центральный объект с учетом внесенных изменений.

Вкладка «Дистанционное получение»

На вкладке **Дистанционное получение** можно управлять настройками получения дистанционной записи для удаленного объекта в установке Milestone Interconnect:

Укажите следующие свойства:

Имя	Описание
Получать записи на макс.	Определяет максимальную полосу пропускания в Кбит/с, которая будет использоваться для получения записей с удаленного объекта. Установите флажок, чтобы включить ограничение на получение.
Получать записи между	Указывает, что получение записей с удаленного объекта ограничено определенным интервалом времени. Задания, не завершенные ко времени окончания, продолжаются до их полного выполнения. Поэтому, если время окончания имеет решающее значение, необходимо установить более раннее время, чтобы незавершенные задания могли быть выполнены. Если система принимает автоматическое получение или запрос на получение от XProtect Smart Client за пределами интервала времени, такой запрос будет принят, однако задача не будет запущена до наступления установленного интервала времени. Вы можете посмотреть отложенные задачи на получение дистанционной записи, инициированные пользователями, в разделе **Информационная панель системы** -> **Текущие задачи**.
Получать на устройства параллельно	Определяет максимальное количество устройств, с которых происходит одновременное получение записей. Измените значение по умолчанию, если вам необходим больший или меньший объем (в зависимости от возможностей системы).

После изменения настроек может пройти несколько минут, прежде чем изменения отразятся в системе.

Вышеперечисленное не относится к прямому воспроизведению дистанционных записей.
Все камеры, настроенные на прямое воспроизведение, доступны для прямого воспроизведения и используют необходимую полосу пропускания.

Узел «Устройства»

Устройства (раздел «Устройства»)

Устройства отображаются в Management Client при добавлении оборудования с помощью мастера **Добавить оборудование**. См. раздел Добавление оборудования на стр. 232.

Если у устройств имеются одинаковые свойства, ими можно управлять при помощи групп устройств; см. раздел Группы устройств (объяснение) на стр. 63.

Также устройствами также можно управлять по отдельности.

Включение/отключение и переименование отдельных устройств осуществляется с помощью оборудования сервера записи. См. раздел Включение/отключение устройств с помощью групп устройств.

Для выполнения других действий по настройке камер и управлению ими откройте раздел **Устройства** на панели «Навигация по сайту» и выберите устройство:

- **Камеры**
- **Микрофоны**
- **Динамики**
- **Метаданные**
- **Вводы**
- **Выводы**

На панели «Обзор» камеры можно объединить в группы. Благодаря этому можно быстро получить общее представление об используемых камерах. Первоначальное объединение в группы осуществляется в процессе работы с мастером **Добавить оборудование**.

> Сведения о поддерживаемом оборудовании см. на странице «Поддерживаемое оборудование» на веб-сайте Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/)

Значки состояния устройств

При выборе устройства информация о его текущем состоянии отображается на панели **Обзор**. Следующие значки обозначают состояние устройств:

Камера	Микрофон	Динамик	Метаданные	Вход	Вывод	Описание
						**Устройство включено и получает данные**: Устройство включено и передает поток в режиме реального времени.
						**Устройство ведет запись**: Устройство ведет запись данных в системе.
						**Устройство временно остановлено, или у него отсутствует поток данных**: При остановке устройства информация в систему не передается. Если это камера, просмотр видео в режиме реального времени невозможен. Остановленное устройство может по-прежнему взаимодействовать с сервером записи для получения событий, установки параметров и т. п., в отличие от ситуации, когда устройство отключено.
						**Устройства отключены**: Устройство не может быть запущено автоматически при помощи правила и не способно взаимодействовать с сервером записи. Если камера отключена,

Камера	Микрофон	Динамик	Метаданные	Вход	Вывод	Описание
						просмотр видео в режиме реального времени или в записи невозможен.
						**Идет восстановление базы данных устройства**:
						**Устройство требует внимания**: Устройство работает неправильно. Наведите курсор мыши на значок устройства, чтобы просмотреть описание проблемы во всплывающей подсказке.
						**Состояние неизвестно**: Состояние устройства неизвестно, если, например, сервер записи отключен от сети.
						Некоторые значки могут объединяться как в показанном примере: в нем значок **Устройство включено и получает данные** объединен со значком **Устройство ведет запись**.

Камеры (узел «Устройства»)

Камеры добавляются автоматически при добавлении оборудования в систему и по умолчанию включены.

По умолчанию в системе задано правило запуска передачи данных, которое обеспечивает автоматическую передачу в систему видеопотоков со всех подключенных камер. При необходимости правило по умолчанию можно отключить и (или) изменить.

Выполните настройку в указанном порядке, чтобы решить наиболее распространенные задачи настройки камеры:

1. Настройте параметры камер; см. вкладку «Настройки» (устройства).
2. Настройте потоки; см. вкладку «Потоки» (устройства).
3. Настройте движение; см. вкладку «Движение» (устройства).
4. Настройте запись; см. вкладку «Запись» (устройства) и раздел Мониторинг баз данных устройств.
5. При необходимости задайте остальные параметры.

Микрофоны (узел «Устройства»)

Микрофоны добавляются автоматически при добавлении оборудования к системе. По умолчанию они отключены, поэтому перед использованием их нужно включить либо в мастере **Добавление оборудования**, либо позже. Отдельные лицензии на микрофоны не требуются. Можно использовать столько микрофонов, сколько требуется в вашей системе.

Микрофоны можно использовать совершенно независимо от камер.

Установленное в системе по умолчанию правило начала передачи звуковой информации гарантирует, что потоки звуковой информации со всех подключенных микрофонов автоматически передаются в систему. При необходимости правило по умолчанию можно отключить и (или) изменить.

Для настройки микрофонов используйте следующие вкладки:

- Вкладка «Информация», см. раздел Вкладка «Информация» (устройства)
- Вкладка «Настройки», см. раздел Вкладка «Настройки» (устройства)
- Вкладка «Запись», см. раздел Вкладка «Запись» (устройства)
- Вкладка «События», см. раздел Вкладка «События» (устройства)

Динамики (узел «Устройства»)

Динамики добавляются автоматически при добавлении оборудования в систему. По умолчанию они отключены, поэтому перед использованием их нужно включить либо в мастере **Добавление оборудования**, либо позже. Отдельная лицензия на динамики не требуется. Можно использовать столько динамиков, сколько требуется в вашей системе.

Динамики можно использовать совершенно независимо от камер.

В системе есть правило начала передачи звуковой информации по умолчанию при запуске устройства, таким образом, устройство готово отправлять включенную пользователем звуковую информацию в динамики. При необходимости правило по умолчанию можно отключить и (или) изменить.

Для настройки динамиков используйте следующие вкладки:

- Вкладка «Информация», см. раздел Вкладка «Информация» (устройства)
- Вкладка «Настройки», см. раздел Вкладка «Настройки» (устройства)
- Вкладка «Запись», см. раздел Вкладка «Запись» (устройства)

Метаданные (узел «Устройства»)

Установленное в системе по умолчанию правило начала передачи гарантирует, что потоки метаданных со всего подключенного оборудования, поддерживающего метаданные, автоматически передаются в систему. При необходимости правило по умолчанию можно отключить и (или) изменить.

Для настройки устройств метаданных используйте следующие вкладки:

- Вкладка «Информация», см. раздел Вкладка «Информация» (устройства)
- Вкладка «Настройки», см. раздел Вкладка «Настройки» (устройства)
- Вкладка «Запись», см. раздел Вкладка «Запись» (устройства)

Устройства ввода (узел «Устройства»)

Устройства ввода можно использовать совершенно независимо от камер.

Прежде чем выбрать использование внешних модулей ввода на устройстве, убедитесь, что само устройство распознает работу датчика. На большинстве устройств эту информацию можно найти в интерфейсах конфигурации или с помощью команд сценария CGI (Общий интерфейс шлюза).

Устройства ввода добавляются автоматически при добавлении оборудования к системе. По умолчанию они отключены, поэтому перед использованием их нужно включить либо в мастере **Добавление оборудования**, либо позже. Отдельная лицензия на устройства ввода не требуется. Можно использовать столько устройств ввода, сколько необходимо в системе.

Для настройки устройств ввода используйте следующие вкладки:

- Вкладка «Информация», см. раздел Вкладка «Информация» (устройства)
- Вкладка «Настройки», см. раздел Вкладка «Настройки» (устройства)
- Вкладка «События», см. раздел Вкладка «События» (устройства)

Устройства вывода (узел «Устройства»)

Устройства вывода можно активировать вручную с помощью Management Client и XProtect Smart Client.

Прежде чем указать использование внешних модулей вывода на устройстве, убедитесь, что оно может управлять устройством, подключенным к выводу. На большинстве устройств эту информацию можно найти в интерфейсах конфигурации или с помощью команд сценария CGI (Общий интерфейс шлюза).

Устройства вывода добавляются автоматически при добавлении оборудования к системе. По умолчанию они отключены, поэтому перед использованием их нужно включить либо в мастере **Добавление оборудования**, либо позже. Отдельная лицензия на устройства вывода не требуется. Можно использовать столько устройств вывода, сколько необходимо в системе.

Для настройки устройств вывода используйте следующие вкладки:

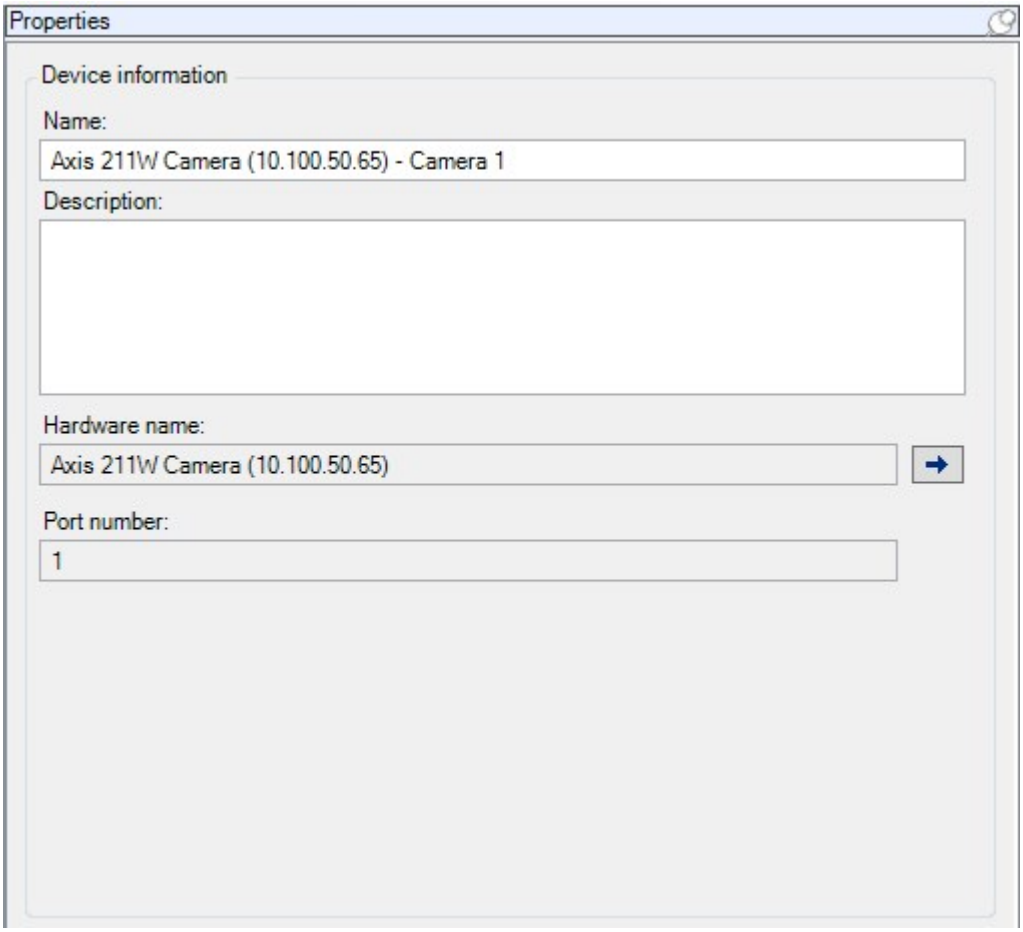
Вкладка «Информация», см.

- Вкладка «Информация», см. раздел Вкладка «Информация» (устройства)
- Вкладка «Настройки», см. раздел Вкладка «Настройки» (устройства)

Вкладки «Устройства»

Вкладка «Сведения» (устройства)

На вкладке **Сведения** можно просматривать и изменять основную информацию об устройстве, приведенную в нескольких полях.
Вкладка **Сведения** есть у всех устройств.



Свойства вкладки «Сведения»

Имя	Описание
Имя	Имя используется во всех случаях, когда устройство упоминается в системе и клиентах. При переименовании устройства его имя изменяется глобально в Management Client.
Описание	Введите описание устройства (необязательно). Описание отображается во многих списках системы. Например, это происходит при наведении курсора мыши на имя на панели **Обзор**.

Имя	Описание
Имя оборудования	Отображает имя оборудования, к которому подключено устройство. В этом месте изменить поле нельзя, но это можно сделать, если нажать на расположенную рядом с ним кнопку **Перейти**. Вы перейдете в раздел информации об оборудовании, где сможете изменить имя.
Номер порта	Отображает порт, через который устройство подключено к оборудованию. Как правило, номер порта оборудования с одним устройством — **1**. Применительно к оборудованию с несколькими устройствами, например, видеосерверам с несколькими каналами, номер порта, как правило, обозначает канал, через который подключено устройство (например, **3**).
Короткое имя	Введите сюда сокращенное имя камеры. Максимальное количество символов — 128. При использовании интеллектуальной карты короткое имя автоматически отображается на такой карте вместе с камерой. В противном случае отображается полное имя.
Координаты	Введите географические координаты камеры в формате **latitude, longitude**. Введенное вами значение определяет положение значка камеры на интеллектуальной карте в XProtect Smart Client и клиентом XProtect Mobile.. Это поле предназначено преимущественно для интеграции с интеллектуальными картами и модулями сторонних производителей.
Направление	Введите направление наблюдения камеры, измеренное относительно точки, находящейся строго в северном направлении по вертикальной оси. Введенное вами значение определяет направление значка камеры на интеллектуальной карте в XProtect Smart Client и клиентом XProtect Mobile.. Значение по умолчанию — 0,0. Это поле предназначено преимущественно для интеграции с интеллектуальными картами и модулями сторонних производителей.

Имя	Описание
Поле обзора	Введите ширину поля обзора в градусах. Введенное вами значение определяет угол поля обзора значка камеры на интеллектуальной карте в XProtect Smart Client и клиентом XProtect Mobile.. Значение по умолчанию — 0,0.  Это поле предназначено преимущественно для интеграции с интеллектуальными картами и модулями сторонних производителей.
Глубина	Введите глубину поля обзора в метрах или футах. Введенное вами значение определяет протяженность поля обзора значка камеры на интеллектуальной карте в XProtect Smart Client и клиентом XProtect Mobile.. Значение по умолчанию — 0,0.  Это поле предназначено преимущественно для интеграции с интеллектуальными картами и модулями сторонних производителей.
Просмотреть положение в браузере	Нажмите кнопку, чтобы проверить правильность введенных географических координат. Ваш стандартный Интернет-браузер откроет карты Google на указанном вами положении.  Это поле предназначено преимущественно для интеграции с интеллектуальными картами и модулями сторонних производителей.

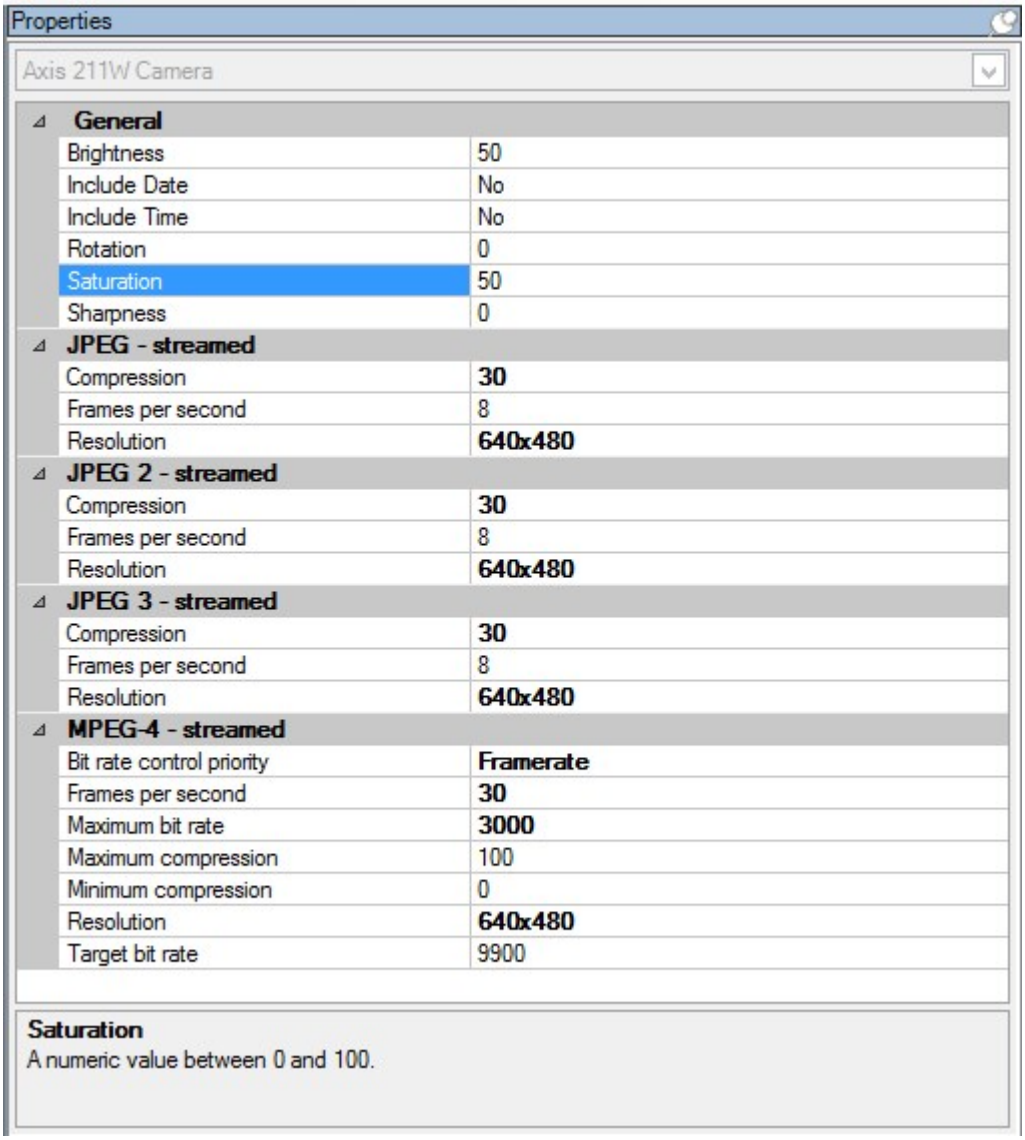
Вкладка «Настройки» (устройства)

На вкладке **Настройки** можно просматривать и изменять настройки устройства, приведенные в нескольких полях.
Вкладка **Настройки** есть у всех устройств.

В таблице отображаются как изменяемые значения, так и значения только для чтения. Значение, отличное от заданного по умолчанию, выделено жирным шрифтом.

Содержимое таблицы зависит от драйвера устройства.

Допустимые диапазоны отображаются в информационном поле под таблицей настроек:



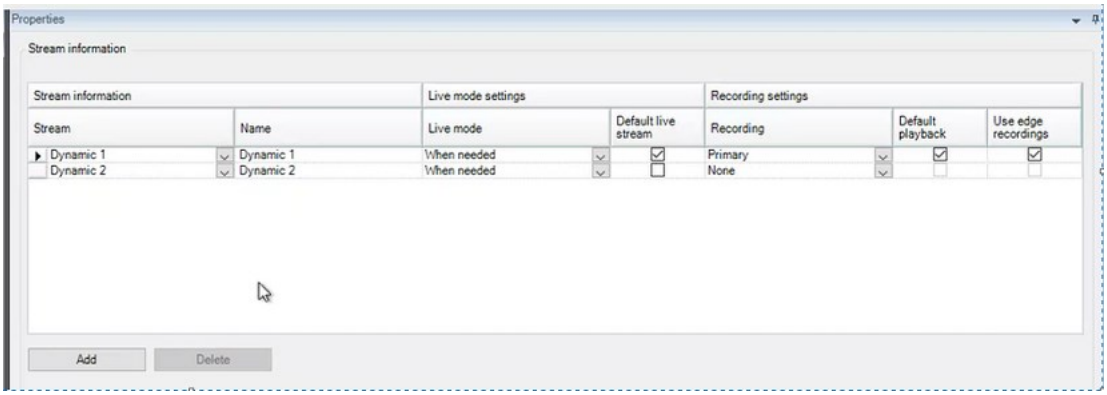
Дополнительные сведения о настройках камеры приведены в разделе Просмотр или изменение настроек камеры.

Вкладка «Потоки» (устройства)

Вкладка **Потоки** есть у следующих устройств:

- Камеры

На вкладке **Потоки** по умолчанию отображается один поток. Это — заданный по умолчанию для выбранной камеры поток, используемый для прямой передачи видеоданных и записанного видео. При использовании адаптивного воспроизведения необходимо создать два потока.



Задачи на вкладке «Потоки»

Имя	Описание
Добавить	Нажмите, чтобы добавить поток в список. Добавление потока

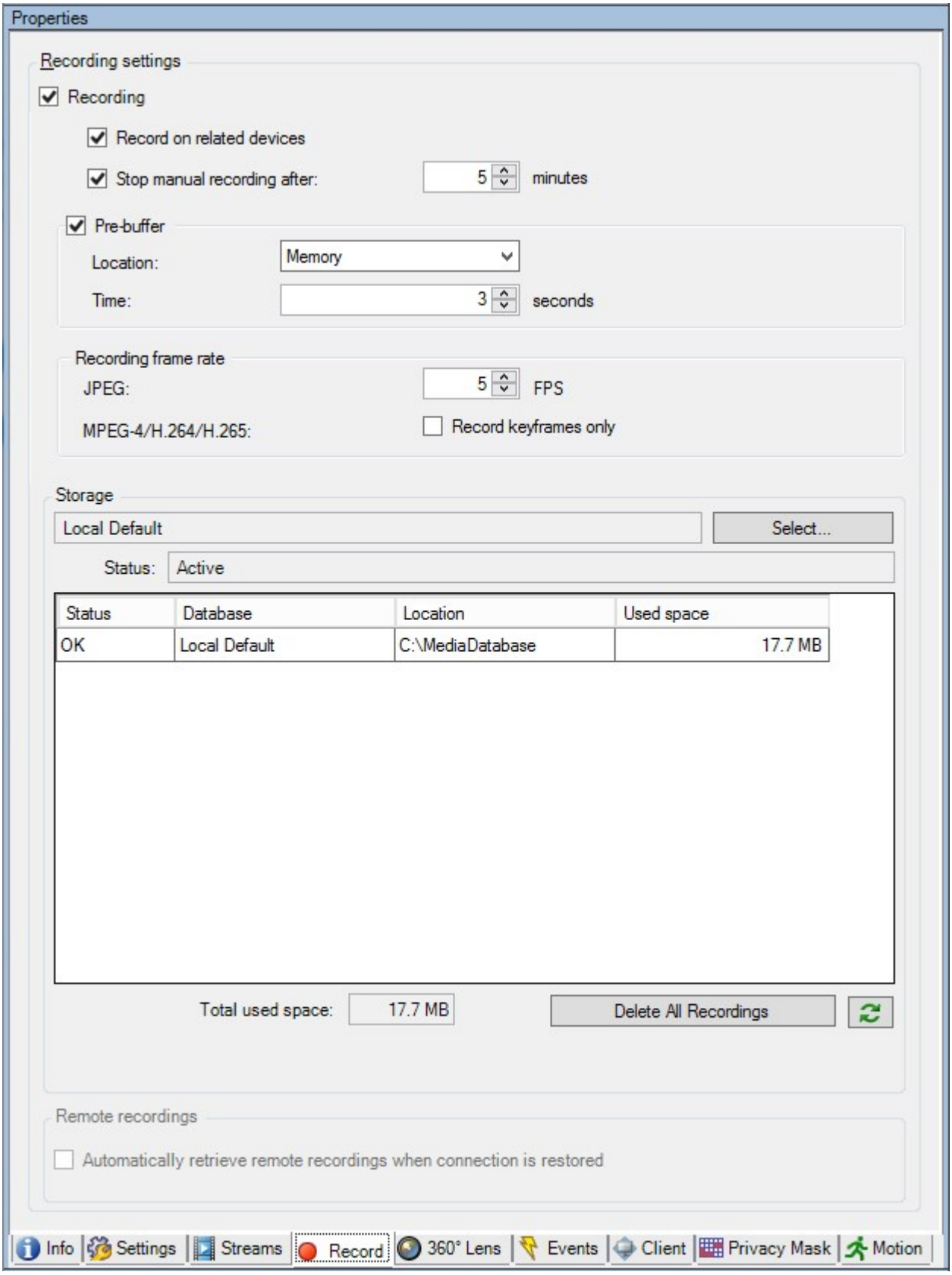
Вкладка «Запись» (устройства)

Вкладка **Запись** есть у следующих устройств:

- Камеры
- Микрофоны
- Динамики
- Метаданные

Записи с устройства сохраняются в базе данных, только если включена запись и соблюдены критерии связанного с записью правила.

Выделить параметры, значения которых нельзя изменить, нельзя.


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

Задачи на вкладке «Запись»

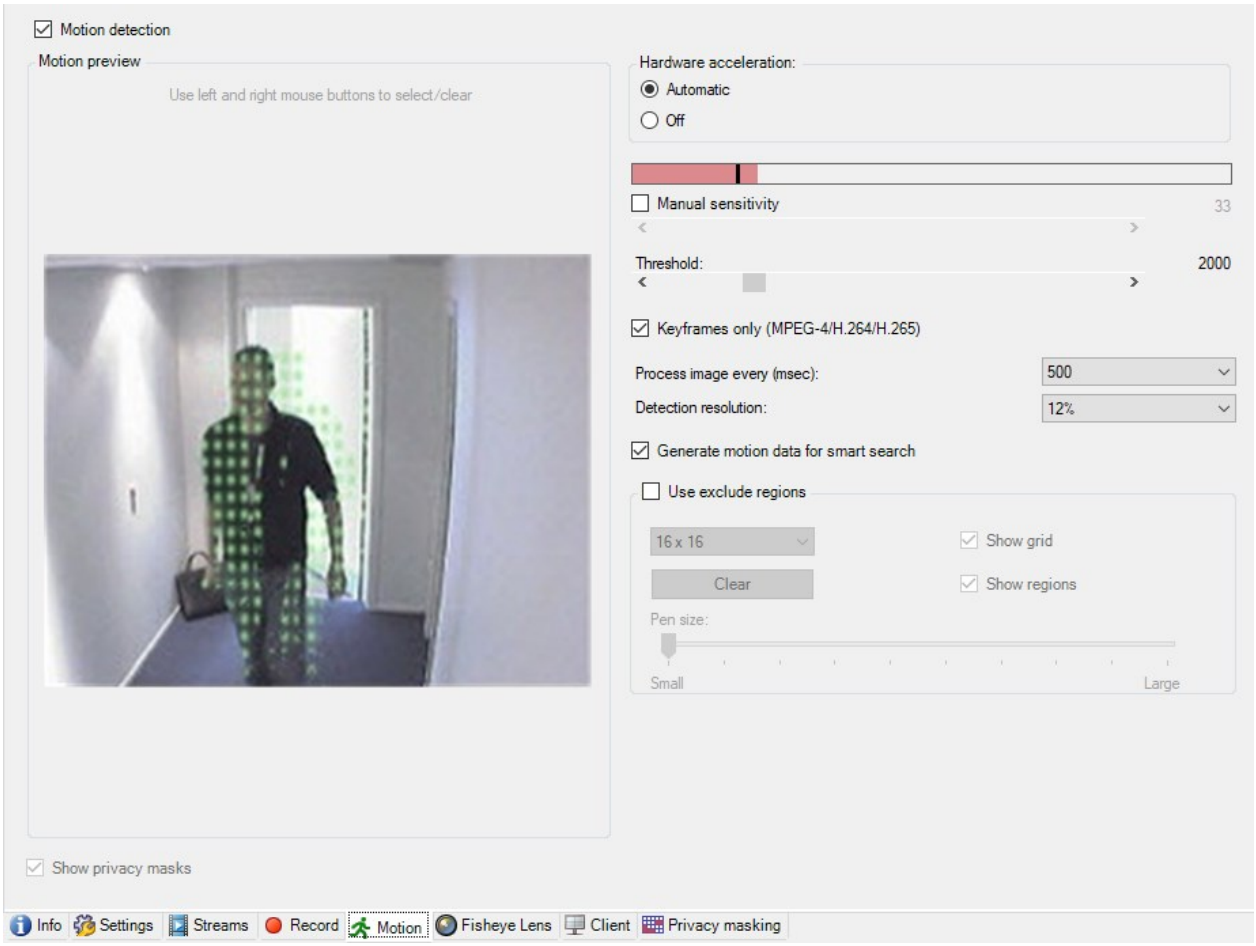
Имя	Описание
Запись	Включение/отключение записи Включение записи на связанных устройствах
Буферизация перед событием	Буферизация перед событием и хранение записей, сделанных с ее помощью (объяснение) Управление буферизацией перед событием Ручное управление записью
Частота кадров при записи	Указание частоты кадров при записи Включение записи ключевых кадров
Хранилище	Мониторинг состояния баз данных устройств
Выбрать	Перенос устройств из одного хранилища в другое
Удаление всех записей	Если вы добавили все устройства из состава группы к одному и тому же серверу, используйте эту кнопку: Удалить записи
Автоматическое получение дистанционных записей при восстановлении подключения	Сохранение и получение дистанционной записи

Вкладка «Движение» (устройства)

Вкладка **Движение** есть у следующих устройств:

- Камеры

На вкладке **Движение** можно включить и настроить обнаружение движений для выбранной камеры.



Задачи на вкладке «Движение»

Имя	Описание
Обнаружение движений	Включение и отключение обнаружения движений
Аппаратное ускорение	Выберите пункт **Автоматически**, чтобы включить аппаратное ускорение, или **Отключено**, чтобы отключить эту настройку. Дополнительные сведения см. в разделе Включение или отключение аппаратного ускорения.

Имя	Описание
Маски конфиденциальности	Если заданы области с постоянными масками конфиденциальности, можно поставить отметку в поле **Маски конфиденциальности**, чтобы отобразить маски конфиденциальности на вкладке **Движение**. Задать области с масками конфиденциальности можно в Вкладка «Конфиденциальная маскировка» (устройства) на стр. 501. В областях, закрытых постоянными масками конфиденциальности, обнаружение движений не работает.
Ручная настройка чувствительности	Определите, **насколько должен измениться каждый пиксель** на изображении, чтобы оно рассматривалось как движение: Включение ручной регулировки чувствительности при анализе движений
Пороговое значение	Определите, **сколько пикселей** в изображении должно измениться, чтобы оно рассматривалось как движение: Указание порогового значения при анализе движений
Только ключевые кадры (MPEG-4/H.264/H.265)	Поставьте отметку в этом поле, чтобы включить обнаружение движений только в ключевых кадрах, а не во всем видеопотоке. Применимо только к форматам MPEG-4/H.264/H.265. Обнаружение движений в ключевых кадрах позволяет уменьшить объем вычислительной мощности, используемой для анализа.
Обработка изображения каждые (мс)	Выберите из списка интервал обработки изображения: он задает частоту анализа при обнаружении движений. Например, каждые 1 000 миллисекунд — это один раз в секунду. Значение по умолчанию — 500 миллисекунд. Этот интервал применяется, если фактическая частота кадров выше интервала, заданного в этом пункте.
Разрешение при обнаружении движений	Выберите в этом списке разрешение, чтобы оптимизировать производительность системы при обнаружении движений. Анализируется только выбранный процент изображения, например, 25 %. При анализе 25 % выполняется анализ только каждого четвертого пикселя

Имя	Описание
	изображения, а не всех пикселей. Оптимизация функции обнаружения движений позволяет снизить объем вычислительной мощности, используемой для анализа, но делает обнаружение движений менее точным.
Сгенерировать данные движения для интеллектуального поиска	Когда поставлена отметка в этом поле, система создает данные движения для изображений, используемых для обнаружения движений. Например, если выбрано обнаружение движений только в ключевых кадрах, данные движения формируются только для ключевых кадров. Дополнительные данные движения позволяют пользователю клиента при помощи функции интеллектуального поиска быстро искать нужные записи по движению в выбранной области изображения. Система не создает данные движения для областей, закрытых постоянными масками конфиденциальности, но делает это для областей со съемными масками конфиденциальности (см. раздел Обнаружение движений (объяснение)). Пороговое значение при обнаружении движений и исключенные области не влияют на генерируемые данные движения. • Задайте значение по умолчанию для создаваемых данных интеллектуального поиска для камер в разделе **Инструменты** > **Параметры** > **Общие**.
Использовать исключенные области	Отключите обнаружение движений в конкретных областях поля обзора камеры: Указание областей, исключаемых при обнаружении движений

Вкладка «Предустановки» (устройства)

У следующих устройств есть вкладка **Предустановки**:

- PTZ-камеры, поддерживающие исходные предустановки

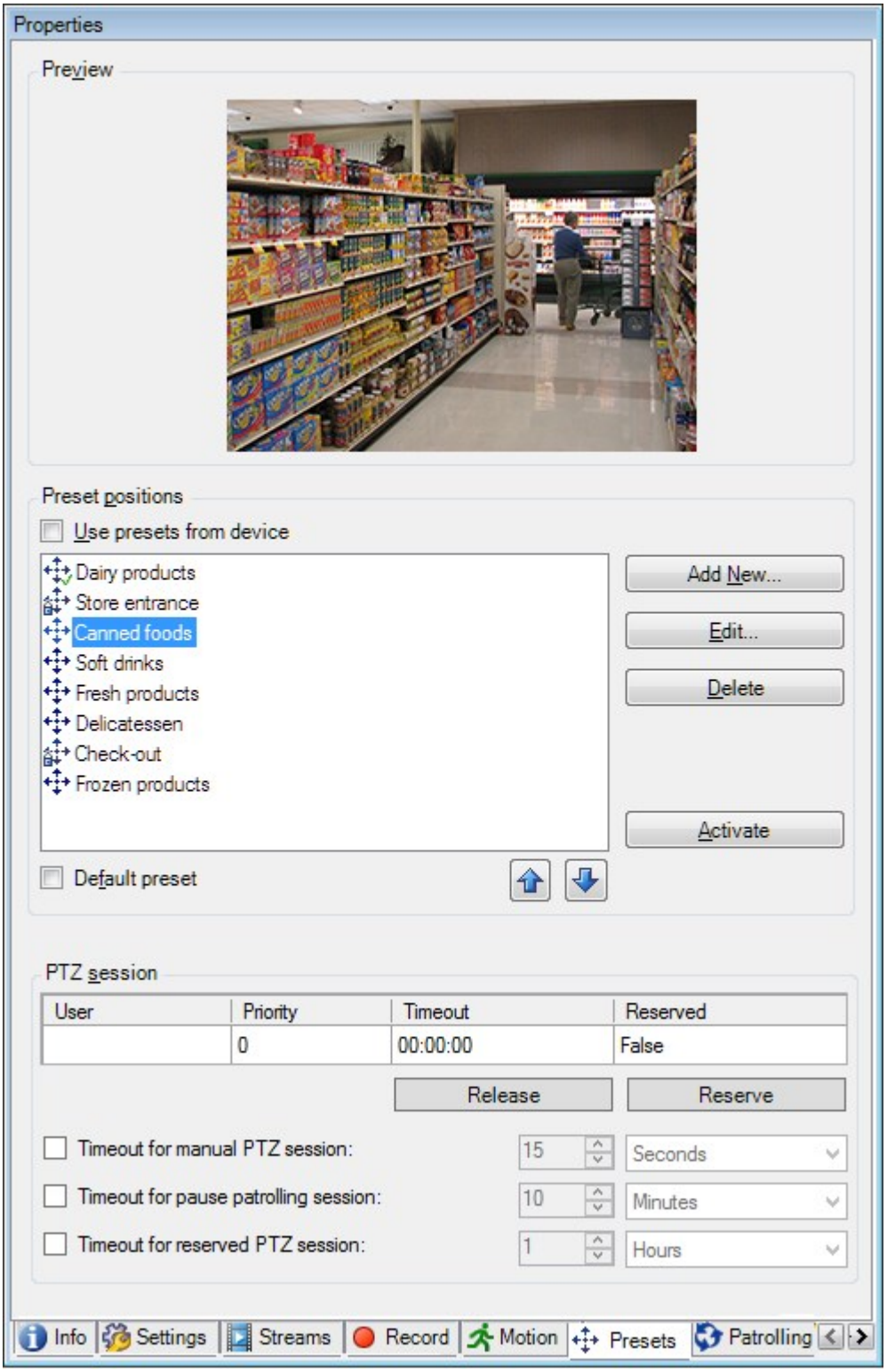
На вкладке **Предустановки** можно создать или импортировать исходные предустановки, например:

- В правилах — для задания движения PTZ-камеры (поворотной камеры с трансфокатором) в определенную исходную предустановку, когда происходит событие
- В патрулировании — для автоматического перемещения PTZ-камеры между несколькими

исходными предустановками

- Для ручной активации пользователями XProtect Smart Client

Назначение PTZ-разрешений ролям осуществляется на вкладке «Общая безопасность» (см. раздел Вкладка «Общая безопасность» (роли) на стр. 563) или на вкладке «PTZ» (см. раздел Вкладка PTZ (роли) на стр. 616).


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

Задачи на вкладке «Предустановки»

Имя	Описание
Новые	Добавляет в систему исходную предустановку для камеры: Добавить исходную предустановку (тип 1)
Использовать предустановку с устройства	Добавляет исходную предустановку для PTZ-камер на самой камере: Использовать исходную предустановку из камеры (тип 2)
Предустановка по умолчанию	Задает одну из исходных предустановок PTZ-камеры в качестве ее исходной предустановки по умолчанию: Задать исходную предустановку камеры по умолчанию в качестве предустановки по умолчанию
Редактировать	Изменяет существующую исходную предустановку, заданную в системе: Изменить исходную предустановку камеры (только тип 1) Изменяет имя исходной предустановки, заданное в камере: Переименовать исходную предустановку камеры (только тип 2)
Заблокировано	Поставьте отметку в этом поле, чтобы заблокировать исходную предустановку. Заблокировать исходную предустановку можно для того, чтобы у пользователей в XProtect Smart Client или пользователей с ограниченными разрешениями в системе безопасности не было возможности изменить или удалить предустановку. Заблокированные предустановки обозначены следующим значком:  . Предустановки блокируются в рамках добавления

Имя	Описание
	исходной предустановки (см. раздел Добавление исходной предустановки (тип 1)) и ее изменения (см. раздел Изменение исходной предустановки (только тип 1)).
Активировать	Нажмите эту кнопку, чтобы протестировать исходную предустановку камеры: Протестировать исходную предустановку (только тип 1).
Зарезервировать и **Освободить**	Не разрешает другим пользователям взять на себя управление камерой и освободить ее в случае резервирования. Администраторы с достаточными разрешениями в системе безопасности для запуска зарезервированного сеанса PTZ могут запустить PTZ-камеру в этом режиме. Это не позволяет другим пользователям взять на себя управление камерой. При наличии достаточных разрешений можно освободить зарезервированные сеансы PTZ других пользователей: Зарезервировать и освободить сеансы PTZ-управления.
Сеанс PTZ	Проверяет, выполняет ли система патрулирование или находится под контролем пользователя: Свойства сеанса PTZ на стр. 491. Позволяет просматривать состояние PTZ-камер и управлять временем ожидания камер: Задать время ожидания для сеансов PTZ.

Свойства сеанса PTZ

В таблице **Сеанс PTZ** показано текущее состояние PTZ-камеры.

Имя	Описание
Пользователь	Показывает пользователя, который нажал кнопку **Зарезервировано** и в настоящее время управляет PTZ-камерой. Если система активировала сеанс патрулирования, отображается надпись **Идет патрулирование**
Приоритет	Отображает PTZ-приоритет пользователя. Переключить сеансы PTZ на себя можно только с пользователей с меньшим приоритетом, чем ваш.
Время ожидания	Отображает время ожидания для текущего сеанса PTZ.
Зарезервировано	Указывает, является ли текущий сеанс зарезервированным сеансом PTZ: • **Да**: Зарезервирован • **Нет**: Не зарезервирован

Переключатели в разделе **Сеанс PTZ** позволяют изменить следующее время ожидания каждой PTZ-камеры.

Имя	Описание
Время ожидания для ручного сеанса PTZ	Задайте время ожидания для ручных сеансов PTZ на этой камере, если оно должно отличаться от времени ожидания, заданного по умолчанию. Задать время ожидания по умолчанию можно в меню **Инструменты** в разделе **Параметры**.
Время ожидания для приостановленного сеанса PTZ при патрулировании	Задайте время ожидания для приостановленных сеансов PTZ при патрулировании на этой камере, если оно должно отличаться от времени ожидания, заданного по умолчанию. Задать время ожидания по умолчанию можно в меню **Инструменты** в разделе **Параметры**.
Время ожидания для зарезервированного сеанса PTZ	Задайте время ожидания для зарезервированных сеансов PTZ на этой камере, если оно должно отличаться от времени ожидания, заданного по умолчанию. Задать время ожидания по умолчанию можно в меню **Инструменты** в разделе **Параметры**.

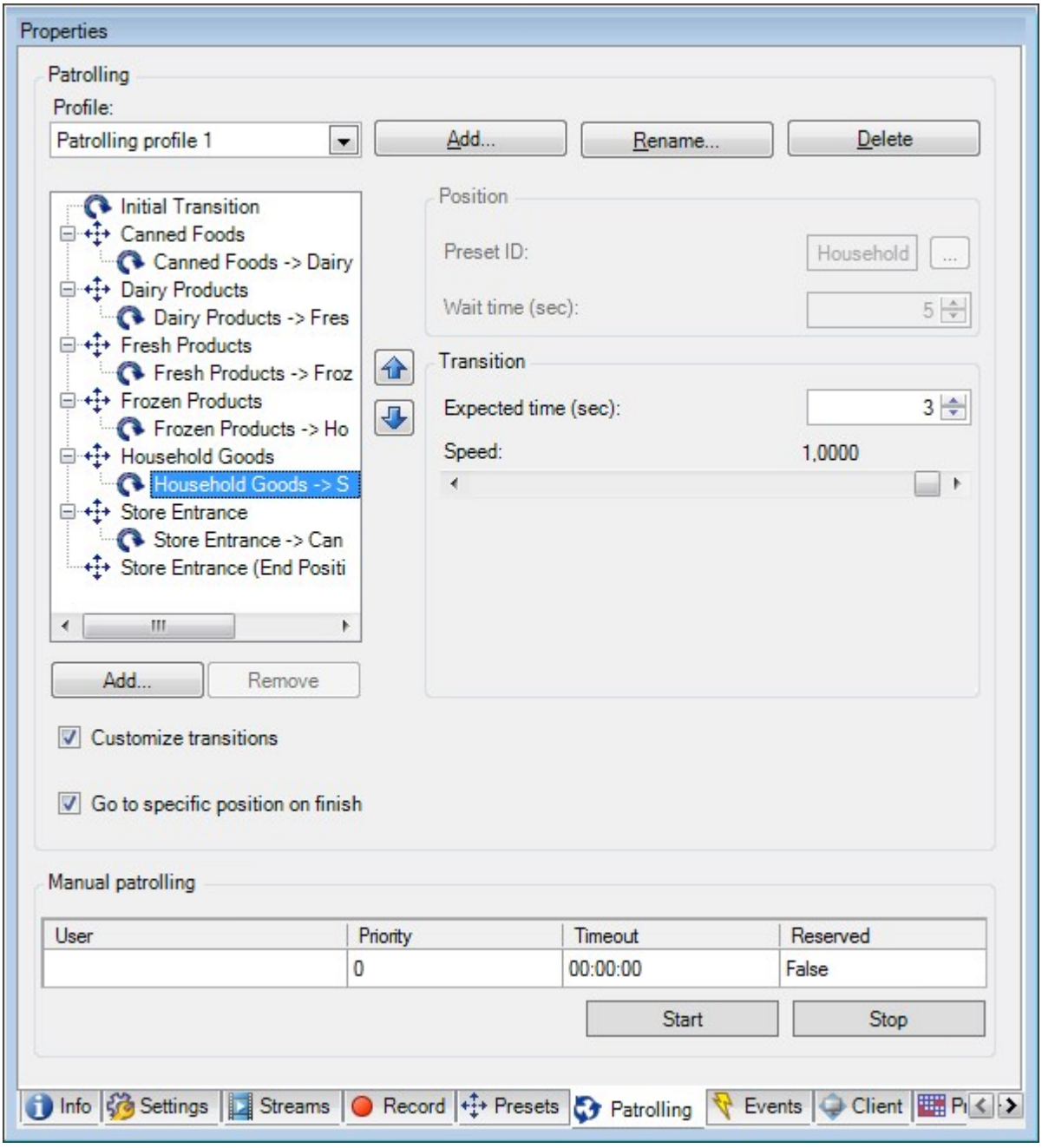
Вкладка «Патрулирование» (устройства)

Вкладка **Патрулирование** есть у следующих устройств:

- PTZ-камеры

На вкладке **Патрулирование** можно создать профили патрулирования, определяющие автоматическое перемещение PTZ-камер (поворотных камер с трансфокатором) между несколькими исходными предустановками.
До начала работы с патрулированием необходимо задать не менее двух исходных предустановок камеры на вкладке **Предустановки**; см. раздел Добавление исходной предустановки (тип 1).

Вкладка **Патрулирование**, на которой отображается профиль патрулирования с пользовательскими переходами:


Properties
Patrolling
Profile:
Patrolling profile 1
Add...
Rename...
Delete
Initial Transition
Canned Foods
Canned Foods -> Dairy
Dairy Products
Dairy Products -> Fres
Fresh Products
Fresh Products -> Froz
Frozen Products
Frozen Products -> Ho
Household Goods
Household Goods -> S
Store Entrance
Store Entrance -> Can
Store Entrance (End Positi
Position
Preset ID:
Household
Wait time (sec):
5
Transition
Expected time (sec):
3
Speed:
1,0000
Add...
Remove
Customize transitions
Go to specific position on finish
Manual patrolling
User
Priority
Timeout
Reserved
0
00:00:00
False
Start
Stop
Info
Settings
Streams
Record
Presets
Patrolling
Events
Client

Задачи на вкладке «Патрулирование»

Имя	Описание
Добавить	Добавление профиля патрулирования
Идентификатор предустановки	Указание исходных предустановок в профиле патрулирования
Время ожидания (с)	Указание времени нахождения в каждой исходной предустановке
Настроить переходы	Пользовательская настройка переходов (PTZ-камера)
Перейти к определенному положению по завершению	Указание конечного положения при патрулировании
Патрулирование вручную	Проверьте, выполняется ли патрулирование системой или под контролем пользователя.
Кнопки **Пуск** и **Стоп**	Используйте кнопки **Пуск** и **Стоп** для запуска и остановки патрулирования вручную. Сведения о том, как задать время, которое должно пройти до возобновления обычного патрулирования для всех или некоторых PTZ-камер, см. в разделе Указание времени ожидания для сеанса PTZ.

Свойства патрулирования вручную

В таблице **Патрулирование вручную** показано текущее состояние PTZ-камеры.

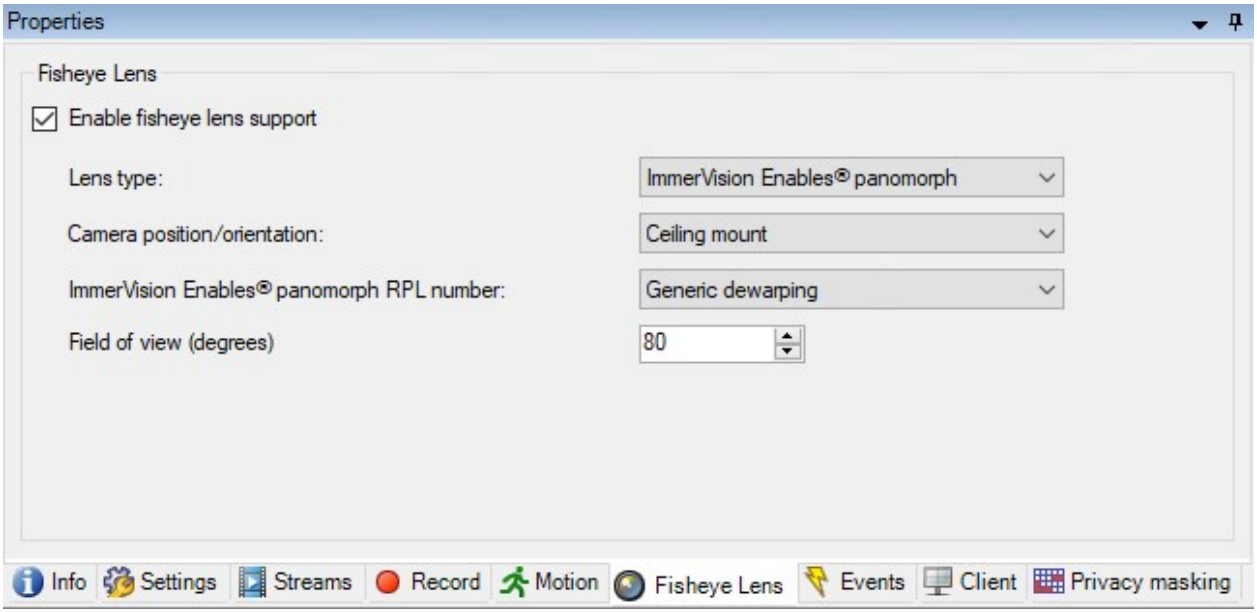
Имя	Описание
Пользователь	Обозначает пользователя, который зарезервировал сеанс PTZ или начал патрулирование вручную и в настоящее время управляет камерой. Если система активировала сеанс патрулирования, отображается надпись **Идет патрулирование**
Приоритет	Отображает PTZ-приоритет пользователя. Переключить сеансы PTZ на себя можно только с пользователей или профилей патрулирования с меньшим приоритетом, чем ваш.
Время ожидания	Обозначает оставшееся время текущих зарезервированных сеансов PTZ или сеансов PTZ, осуществляемых вручную.
Зарезервировано	Указывает, является ли текущий сеанс зарезервированным сеансом PTZ. • **Да**: Зарезервирован • **Нет**: Не зарезервирован

Объектив типа «рыбий глаз» (устройства)

Вкладка **Объектив типа «рыбий глаз»** есть у следующих устройств:

- Стационарные камеры с объективом типа «рыбий глаз»

На вкладке **Объектив типа «рыбий глаз»** можно включить и настроить поддержку объектива типа «рыбий глаз» для выбранной камеры.



Задача на вкладке «Объектив типа "рыбий глаз"»

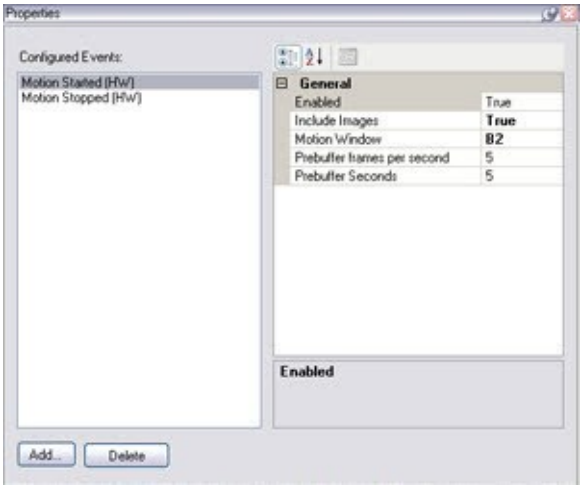
Имя	Описание
Включить поддержку "рыбьего глаза"	Включение и отключение поддержки объектива типа «рыбий глаз»

Вкладка «События» (устройства)

Вкладка **События** есть у следующих устройств:

- Камеры
- Микрофоны
- Вводы

Помимо системных событий, некоторые устройства можно настроить на инициирующие события. Эти события можно использовать при создании в системе правил на основе событий. С технической точки зрения, они возникают не в системе наблюдения, а в физическом оборудовании/устройстве.



Задачи на вкладке «События»

Имя	Описание
Кнопки **Добавить** и **Удалить**	Добавление или удаление события для устройства

Вкладка «Событие» (свойства)

Имя	Описание
Настроенные события	То, какие события можно выбирать и добавлять в списке **Настроенные события**, определяется исключительно событием и его конфигурацией. Для некоторых типов устройств этот список пуст.
Общая информация	Список свойств зависит от устройства и события. Чтобы событие сработало надлежащим образом, некоторые (или все) свойства должны быть заданы одинаково на устройстве и на этой вкладке.

Вкладка «Клиент» (устройства)

Вкладка **Клиент** есть у следующих устройств:

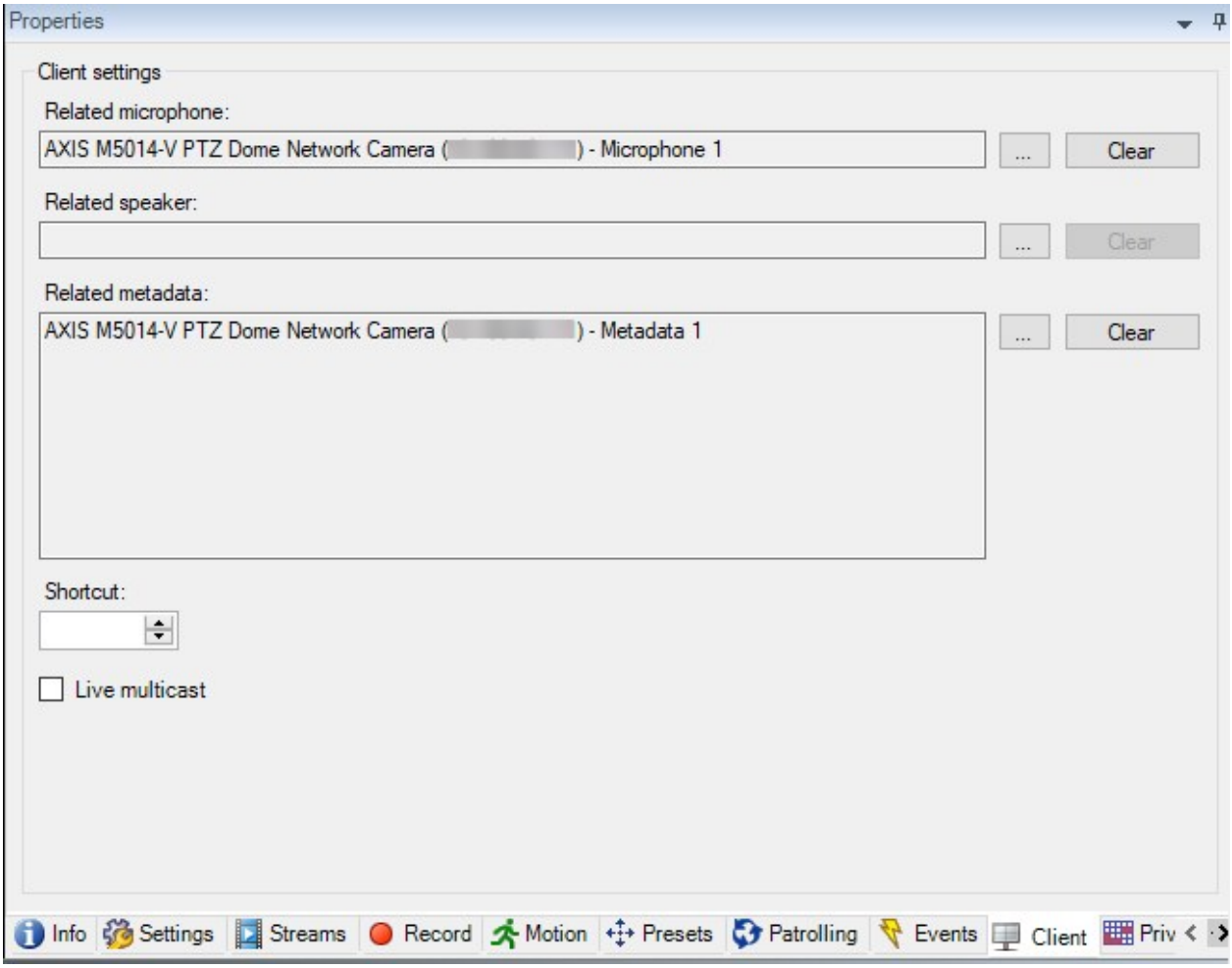
- Камеры

На вкладке **Клиент** можно указать, какие другие устройства просматриваются и прослушиваются при использовании камеры в XProtect Smart Client.

Связанные устройства ведут запись тогда же, когда запись ведется камерой; см. раздел Включение записи на связанных устройствах на стр. 251.

Также на камере можно включить **Многоадресную прямую передачу**. Означает, что камера осуществляет многоадресную передачу потоков трансляции клиентам через сервер записи в режиме реального времени.

Потоки многоадресной передачи не шифруются, даже если на сервере записи используется шифрование.



Свойства вкладки «Клиент»

Имя	Описание
Связанный микрофон	Укажите микрофон на камере, который пользователи XProtect Smart Client по умолчанию используют для прослушивания звуковой информации. При необходимости пользователь XProtect Smart Client может задать другой микрофон. Укажите микрофон, который связан с video push камерой для потоковой передачи видео со звуковой информацией. Связанные микрофоны ведут запись, когда камера ведет запись.
Связанный динамик	Укажите, через какие динамики на камере говорят пользователи XProtect Smart Client по умолчанию. При необходимости пользователь XProtect Smart Client может выбрать другой динамик. Связанные динамики ведут запись, когда камера ведет запись.
Связанные метаданные	Укажите одно или несколько устройств хранения метаданных на камере, из которых пользователи XProtect Smart Client получают данные. Связанные устройства хранения метаданных ведут запись, когда камера ведет запись.
Сочетания клавиш	Чтобы пользователям XProtect Smart Client было проще выбирать камеры, задайте сочетания клавиш для камеры. • Сочетание клавиш должно однозначно идентифицировать камеру • Номер быстрого доступа к камере должен содержать не более четырех цифр
Многоадресная прямая передача	Система поддерживает многоадресную передачу потоков трансляции с сервера записи на XProtect Smart Client. Для включения многоадресной передачи потоков трансляции с камеры поставьте отметку в поле.  Многоадресная прямая передача работает только с потоком, указанным в качестве потока камеры по умолчанию на вкладке **Потоки**.

Имя	Описание
	Также необходимо настроить многоадресную передачу для сервера записи. См. раздел Включение многоадресной передачи для сервера записи на стр. 225. Потоки многоадресной передачи не шифруются, даже если на сервере записи используется шифрование.

Вкладка «Конфиденциальная маскировка» (устройства)

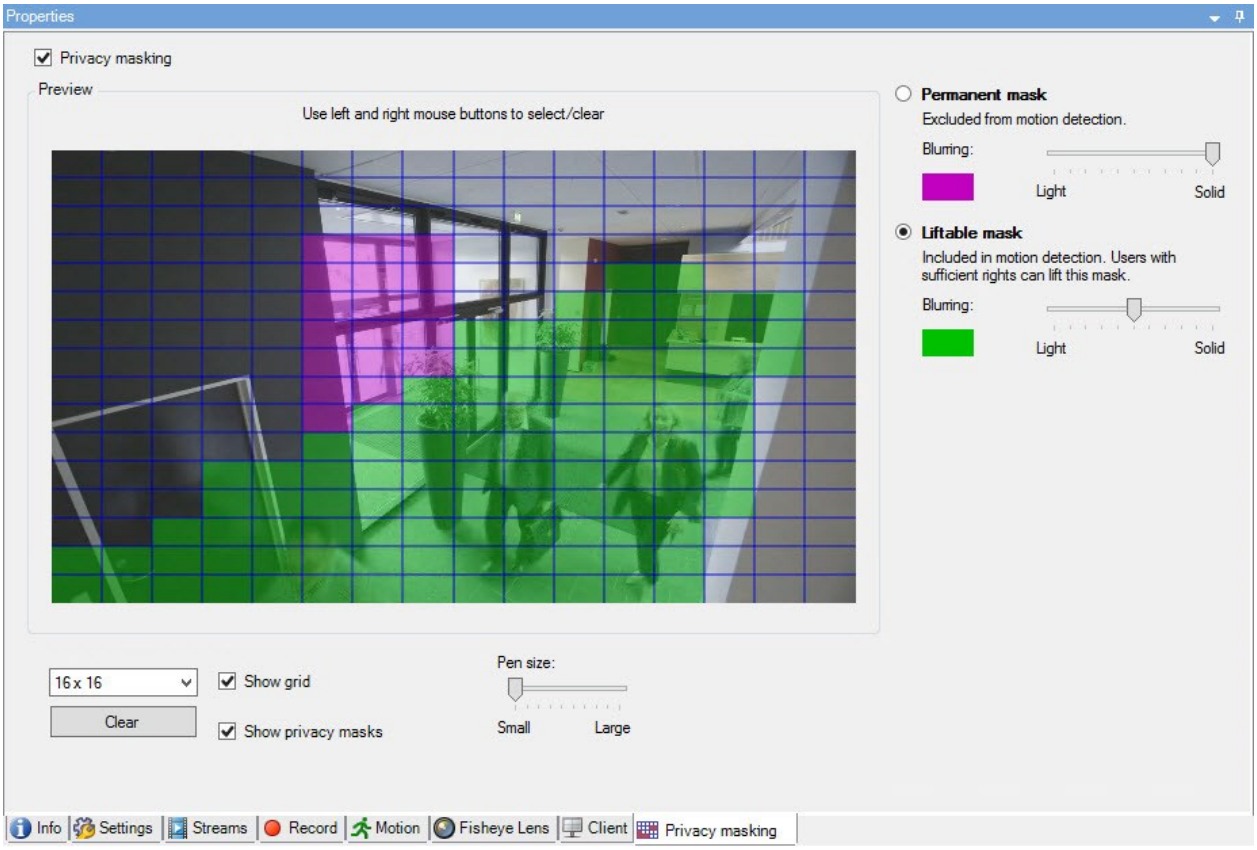
Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

XProtect Essential+ 2018 R1 и более поздних версий не поддерживает конфиденциальную маскировку, поэтому при переходе с систем, где применялись маски конфиденциальности, маски будут удалены.

Вкладка **Конфиденциальная маскировка** есть у следующих устройств:

- Камеры

На вкладке **Конфиденциальная маскировка** можно включить и настроить защиту конфиденциальности выбранной камеры.



Задачи на вкладке «Конфиденциальная маскировка»

Имя	Описание
Маски конфиденциальности	Включение/отключение конфиденциальной маскировки Маски конфиденциальности (объяснение)
Постоянная маска и **Съемная маска**	Решите, какая маска конфиденциальности вам необходима, постоянная или съемная: Настройка масок конфиденциальности

Задачи, связанные с конфиденциальной маскировкой

Задача	Описание
Измените время ожидания съемных масок конфиденциальности для профиля Smart Client, связанного с ролью с разрешением снимать маски конфиденциальности.	Изменение времени ожидания для съемных масок конфиденциальности
Включите или отключите для роли разрешение снимать маски конфиденциальности.	Предоставление пользователям разрешения снимать маски конфиденциальности
Создайте отчет об устройствах с информацией о текущих настройках конфиденциальной маскировки для камер.	Создайте отчет о настройках конфиденциальной маскировки

Вкладка «Конфиденциальная маскировка» (свойства)

Имя	Описание
Grid size	Выбранный шаг сетки определяет плотность сетки независимо от того, видна ли сетка при предварительном просмотре. Можно выбрать одно из следующих значений: 8×8, 16×16, 32×32 или 64×64.
Пусто	Очищает **все** заданные маски конфиденциальности.
Показывать сетку	Чтобы сетка стала видимой, поставьте отметку в поле **Показывать сетку**.
Показать маски	Когда в поле **Показать маски конфиденциальности** поставлена отметка

Имя	Описание
конфиденциальности	(по умолчанию), при предварительном просмотре постоянные маски конфиденциальности отображаются фиолетовым цветом, а съемные маски конфиденциальности — зеленым. Milestone рекомендует поставить отметку в поле **Показать маски конфиденциальности**, чтобы вы и ваши коллеги могли видеть текущие настройки конфиденциальности.
Размер пера	Используйте ползунок **Размер пера**, чтобы задать размер выделения при нажатии кнопки мыши и перемещении сетки для выбора областей. По умолчанию задан маленький размер, эквивалентный одной клетке сетки.
Постоянная маска	Отображается фиолетовым цветом при предварительном просмотре на этой вкладке и на вкладке **Движение**. Постоянные маски конфиденциальности всегда видны в XProtect Smart Client, и снять их невозможно. Ее можно использовать для охвата областей видеоданных, которые не требуют наблюдения, (например, мест общего пользования, где наблюдение запрещено). Из постоянных масок исключаются области обнаружения движений. Область маски конфиденциальности можно настроить так, что она будет сплошной либо в некоторой степени размытой. Настройки области применяются как к видео в режиме реального времени, так и к записанному видео.
Съемная маска	Отображается зеленым цветом при предварительном просмотре на этой вкладке. В XProtect Smart Client пользователи с достаточным уровнем пользовательских разрешений могут снимать съемные маски конфиденциальности. По умолчанию маски конфиденциальности снимаются на 30 минут либо до тех пор, пока пользователь не применит их вновь. Помните о том, что маски конфиденциальности снимаются на видео со всех камер, к которым у пользователя есть доступ. Если у пользователя XProtect Smart Client нет разрешения на снятие масок конфиденциальности, система запросит выполнение операции пользователем с достаточными правами. Область маски конфиденциальности можно настроить так, что она будет сплошной либо в некоторой степени размытой. Настройки области

Имя	Описание
	применяются как к видео в режиме реального времени, так и к записанному видео.
Размытая	Используйте ползунок, чтобы выбрать степень размытости масок конфиденциальности в клиентах, или оставьте область сплошной. По умолчанию в постоянных масках конфиденциальности применяется сплошная (непрозрачная) область. По умолчанию в съемных масках конфиденциальности применяется область средней степени размытости. Можно сообщить пользователям клиентов о том, как выглядят постоянные и съемные маски конфиденциальности, чтобы они отличали одну от другой.

Окно «Свойства оборудования»

В системе предусмотрено несколько способов добавления оборудования на серверы записи.

Если оборудование находится за маршрутизатором с поддержкой NAT или брандмауэром, может потребоваться указать другой номер порта и настроить на маршрутизаторе/брандамауэре сопоставление порта и IP-адреса, используемого оборудованием.

Мастер **добавления оборудования** обнаруживает оборудование, такое как камеры и видеокодеры, в сети и добавляет его на серверы записи в системе. Этот мастер также помогает добавлять серверы дистанционной записи для конфигураций Milestone Interconnect. Добавлять оборудование можно только на **один сервер записи** за раз.

Вкладка «Информация» (оборудование)

Подробные сведения о вкладке **Информация** для удаленных серверов см. в документе Вкладка «Информация» (удаленный сервер) на стр. 469.

Имя	Описание
Имя	Укажите имя. Имя, под которым оборудование отображается в списках системы

Имя	Описание
	или клиентов. Имя не обязательно должно быть уникальным. При переименовании оборудования имя меняется глобально в Management Client.
Описание	Введите описание оборудования (необязательно). Описание отображается во многих списках системы. Например, при наведении указателя мыши на имя оборудования на панели **Обзор**: 
Модель	Определяет модель оборудования.
Серийный номер	Серийный номер оборудования, указанный производителем. Серийный номер часто (но не всегда) идентичен MAC-адресу.
Драйвер	Определяет драйвер, который обеспечивает подключение к оборудованию.
IE	Открывает домашнюю страницу поставщика оборудования, настроенную по умолчанию. Вы можете использовать эту страницу для управления оборудованием.
Адрес	Имя хоста и IP-адрес оборудования.
MAC-адрес	Указывает адрес управления доступом к среде (MAC-адрес) системного оборудования. MAC-адрес — это уникальное 12-значное шестнадцатеричное число, которое позволяет идентифицировать каждое оборудование в сети.
Версия прошивки:	Версия прошивки аппаратного устройства. Чтобы в системе всегда отображалась текущая версия прошивки, запускайте мастер **Обновление данных оборудования** после каждого ее обновления.
Последнее изменение пароля	В поле **Последнее изменение пароля** отображается метка времени последней смены пароля в соответствии с локальными параметрами времени компьютера, с которого выполнялась смена пароля.

Имя	Описание
Последнее обновление данных оборудования:	Время и дата последнего обновления данных оборудования.

Вкладка «Настройки» (оборудование)

На вкладке **Настройки** можно проверить или изменить настройки оборудования.

Содержимое вкладки **Настройки** определяется выбранным оборудованием и может варьироваться в зависимости от его типа. Для некоторого оборудования содержимое вкладки **Настройки** либо не отображается вообще, либо доступно только для чтения.

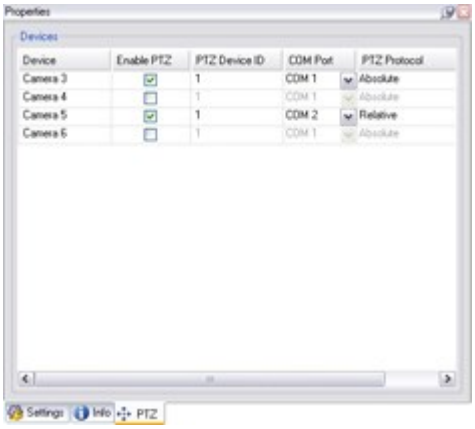
Подробнее о вкладке **Настройки** для удаленных серверов см. в Вкладка «Параметры» (удаленный сервер) на стр. 470.

Вкладка PTZ (видеокодеры)

На вкладке **PTZ** вы можете разрешить PTZ (поворотную камеру с трансфокатором) для видеокодеров. Вкладка доступна, если выбранное устройство является видеокодером или если драйвер поддерживает как камеры без PTZ, так и PTZ-камеры.

Прежде чем использовать функции PTZ-камер, подключенных к видеокодеру, на вкладке **PTZ** необходимо включить использование PTZ отдельно для каждого канала видеокодера.

Не все видеокодеры поддерживают использование PTZ-камер. При этом даже видеокодерам, поддерживающим использование PTZ-камер, может потребоваться дополнительная настройка. Обычно для этого необходимо установить дополнительные драйверы через браузерный интерфейс конфигурации, доступный по IP-адресу устройства.



Вкладка **PTZ**, на которой функция PTZ включена для двух каналов видеокодера.

Узел «Клиент»

Клиенты (узел)

В этой статье описана персонализация пользовательского интерфейса для операторов в XProtect Smart Client и для системных администраторов в Management Client.

Smart Wall (узел «Клиент»)

Свойства Smart Wall

Вкладка "Инфо"

На вкладке **Информация** определения Smart Wall можно добавить и изменить свойства Smart Wall.

Имя	Описание
Имя	Имя определения Smart Wall. Отображается в XProtect Smart Client в качестве имени группы вида Smart Wall.
Описание	Описание определения Smart Wall. Описание используется только внутренне в XProtect Management Client.
Текст статуса	Отображение статуса камеры и системы в элементах вида камеры.

Имя	Описание
Без строки заголовка	Сокрытие панели заголовка на всех элементах макета видеостены.
Строка заголовка	Отображение панели заголовка на всех элементах макета видеостены.

Вкладка "Препозиции"

На вкладке **Предустановки** определения Smart Wall можно добавить и изменить Smart Wall предустановки[1].

Имя	Описание
Добавить новый	Добавьте препозицию в ваше определение Smart Wall. Введите имя и описание препозиции.
Редактировать	Измените имя или описание препозиции.
Удалить	Удалите препозицию.
Активация	Применение препозиции к мониторам Smart Wall, которые настроены для использования препозиции. Чтобы использовать препозицию автоматически, необходимо использовать правило, которое использует препозицию.

Вкладка "Макет"

На вкладке **Макет** определения Smart Wall можно расположить мониторы в соответствии со схемой расположения физических мониторов на видеостене. Макет также используется в XProtect Smart Client.

[1]Предварительно заданный макет для одного или нескольких мониторов Smart Wall в XProtect Smart Client. Препозиции определяют, какие камеры будут показаны и какой будет структура содержимого на каждом мониторе видеостены.

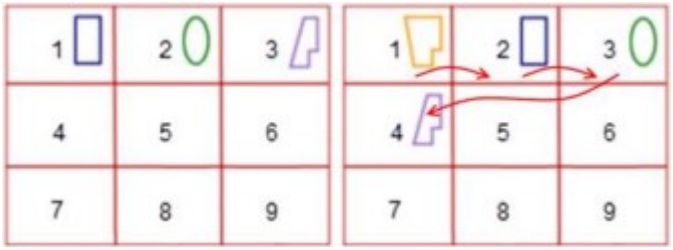
Имя	Описание
Редактировать	Регулировка положения мониторов.
Перемещение	Чтобы переместить монитор в новую позицию, выберите его и перетащите в нужное место или нажимайте одну из кнопок со стрелками, чтобы двигать монитор в выбранном направлении.
Кнопки масштабирования	Увеличивайте или уменьшайте предварительный просмотр макета Smart Wall, чтобы правильно позиционировать мониторы.
Имя	Имя монитора. Имя отображается в XProtect Smart Client.
Размер	Размер физического монитора на видеостене.
Соотношение сторон	Отношение высоты/ширины физического монитора на видеостене.

Свойства монитора

Вкладка "Инфо"

На вкладке **Информация** монитора в предустановке Smart Wall можно добавить мониторы и изменить параметры мониторов.

Имя	Описание
Имя	Имя монитора. Имя отображается в XProtect Smart Client.
Описание	Описание монитора. Описание используется только внутренне в XProtect Management Client.
Размер	Размер физического монитора на видеостене.
Соотношение сторон	Отношение высоты/ширины физического монитора на видеостене.

Имя	Описание
Пустая препозиция	Определяет, что должно отображаться на мониторе с макетом пустой препозиции, когда новая препозиция Smart Wall активируется или выбирается в XProtect Smart Client: • Выберите **Сохранить**, чтобы сохранить текущее содержимое монитора. • Выберите **Очистить**, чтобы убрать все содержимое с монитора.
Элемент пустой препозиции	Определяет, что должно отображаться в элементе пустой препозиции, когда новая Smart Wall препозиция активируется или выбирается в XProtect Smart Client: • Выберите **Сохранить**, чтобы сохранить текущее содержимое в элементе макета. • Выберите **Очистить**, чтобы убрать все содержимое из элемента макета.
Вставка элемента	Определяет, как камеры вставляются в макет мониторов при просмотре в XProtect Smart Client: • **Независимо** — меняется только содержимое связанного элемента макета, остальное содержимое макета остается неизменным. • **Связано** — содержимое элементов макета перемещается слева направо. Если, к примеру, камера вставлена в позицию 1, предыдущая камера из позиции 1 перемещается в позицию 2, предыдущая камера из позиции 2 перемещается в позицию 3 и т. д. В этом примере показаны следующие параметры: 

Вкладка "Препозиции"

На вкладке **Предустановки** для монитора в предустановке Smart Wall можно изменить макет представления и содержимое монитора в выбранной предустановке Smart Wall.

Имя	Описание
Препозиция	Список препозиций Smart Wall для выбранного определения Smart Wall.
Редактировать	Нажмите **Изменить**, чтобы изменить макет и содержимое выбранного монитора. Дважды нажмите камеру, чтобы удалить отдельную камеру. Нажмите **Очистить**, чтобы определить новый макет или исключить монитор в предустановке Smart Wall так, чтобы монитор стал доступен для другого содержимого, не управляемого предустановкой Smart Wall. Нажмите  , чтобы выбрать макет для использования с монитором, затем нажмите кнопку **OK**.

Профили Smart Client (узел «Клиент»)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

На следующих вкладках вы можете указать свойства каждого профиля Smart Client. При необходимости вы можете заблокировать настройки в Management Client, чтобы пользователи XProtect Smart Client не могли их изменить.

Чтобы создать или изменить профили Smart Client, разверните узел **Клиент** и выберите **Профили Smart Client**.

Вкладка «Информация» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Сведения	Имя и описание, приоритет существующих профилей, а также обзор ролей, которые использует профиль.

Вкладка	Описание
	Если пользователю назначено несколько ролей, каждая из которых имеет отдельный профиль Smart Client, пользователь получает профиль Smart Client с наивысшим приоритетом.

Вкладка «Общая информация» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Общая информация	Такие параметры, как отображение/скрытие, сворачивание и разворачивание настроек меню, вход/выход, запуск, время ожидания, информация и отправка сообщений, а также включение или отключение определенных вкладок в XProtect Smart Client. Параметры **Сообщения об ошибках камеры**, **Сообщения об ошибках сервера** и **Сообщения об ошибках видео в режиме реального времени** позволяют определить, будут ли эти сообщения об ошибках отображаться в виде наложения, в виде черного изображения с наложением или они будут скрыты. **Сообщение об остановке видео в режиме реального времени** отображается в XProtect Smart Client, когда поток в режиме реального времени с камеры останавливается. Например, если камера перестала отправлять изображения, хотя она остается подключенной. ⚠ Если вы **скроете** сообщения об ошибках камер, существует риск того, что оператор не заметит информацию о потери связи с камерой. Параметр **Камеры, разрешенные во время поиска** позволяет контролировать, какое количество камер операторы могут добавить в операции поиска в XProtect Smart Client. Настройка максимального числа камер позволяет предотвратить перегрузку системы. Параметр **Онлайн-справка** позволяет отключить справочную систему в XProtect

Вкладка	Описание
	Smart Client. Параметр **Видеоруководства** позволяет отключить кнопку **Видеоруководства** в XProtect Smart Client. Эта кнопка перенаправляет операторов на страницу видеоруководств: https://www.milestonesys.com/support/help-yourself/video-tutorials/

Вкладка Advanced (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Advanced	Расширенные (Advanced) параметры, такие как максимальное количество потоков декодирования, устранение чересстрочности и параметры часового пояса. **Максимальное число потоков декодирования** устанавливает количество потоков декодирования, используемых для видеопотоков. Это помогает повысить производительность компьютеров с многоядерными процессорами в режиме реального времени и в режиме воспроизведения. Точный прирост производительности зависит от видеопотока. Этот параметр главным образом подходит для закодированных видеопотоков с высокой разрешающей способностью: например, для формата H.264/H.265 повышение производительности может оказаться значительным, а для JPEG или MPEG-4 — нет. Используя устранение **чересстрочности**, можно преобразовать видео в формат с прогрессивной разверткой. Чересстрочность определяет обновление изображения на экране. При использовании чересстрочной развертки изображение обновляется таким образом: сначала сканируется каждая нечетная строка изображения, а затем каждая четная. Это позволяет повысить частоту обновления, так как при каждом сканировании обрабатывается меньше информации. Однако чересстрочная развертка может привести к появлению мерцания, или могут быть заметны изменения только половины строк изображения. **Адаптивное потоковое воспроизведение** позволяет XProtect Smart Client автоматически выбирать видеопотоки с оптимальным разрешением для элемента просмотра. Это снижает нагрузку на CPU и GPU и повышает производительность декодирования и общую производительность компьютера. Для этого необходимо

Вкладка	Описание
	настроить многопоточную передачу видеопотоков в режиме реального времени с разными разрешениями, см. Управление многопоточной передачей. Адаптивное потоковое воспроизведение можно применять в режиме реального времени и в режиме воспроизведения. В режиме воспроизведения адаптивное потоковое воспроизведение называется адаптивным воспроизведением. Для адаптивного воспроизведения необходимо, чтобы два потока были настроены на запись. Подробнее о том, как добавлять потоки для адаптивного потокового воспроизведения в режиме реального времени и для адаптивного воспроизведения, см. в разделе Добавление потока на стр. 254.

Вкладка «Наблюдение» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Наблюдение	Доступность режима наблюдения и других функций в режиме реального времени, воспроизведения с камер, кнопок наложения камеры и рамок, а также встраиваемых расширений MIP, связанных с режимом наблюдения.

Вкладка «Воспроизведение» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Воспроизведение	Доступность режима воспроизведения и других функций воспроизведения, макета печати отчета, независимого воспроизведения, отметок и рамок, а также встраиваемых расширений MIP, связанных с режимом воспроизведения.

Вкладка «Настройка» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Настройка	Доступность общих настроек/панелей/кнопок, встраиваемого расширения MIP, связанного с настройкой, а также разрешений на редактирование карты и редактирование буферизации видео в режиме реального времени.

Вкладка «Экспорт» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Экспорт	Пути, маски конфиденциальности, форматы видео и кадров, данные, которые необходимо включить при их экспорте, форматы экспорта для XProtect Smart Client – Player и многое другое.

Вкладка «Временная шкала» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Временная шкала	Необходимо ли включать звуковую информацию, видимость индикации времени и движения, а также способ обработки промежутков в воспроизведении. Также здесь можно выбрать, необходимо ли показывать дополнительные данные или дополнительные маркеры из других источников.

Вкладка «Управление доступом» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Управление доступом	Выберите, должны ли уведомления запроса доступа всплывать на экране XProtect Smart Client при их активации событиями.

Вкладка «Диспетчер сигналов тревоги» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Диспетчер тревог	Укажите следующее: • Уведомления о сигналах тревоги на рабочем столе должны отображаться на компьютерах с установленным XProtect Smart Client. Уведомления появляются только в том случае, если запущен XProtect Smart Client (даже если свернут) Уведомления о сигналах тревоги на рабочем столе появляются только в том случае, если сигналы тревоги имеют определенный приоритет, например **Средний** или **Высокий**. Чтобы настроить приоритеты сигналов тревоги, которые активируют уведомления, перейдите в раздел **Сигналы тревоги** > **Настройки данных сигналов тревоги** > **Уровни данных сигналов тревоги**. Для каждого необходимого приоритета сигнала тревоги установите флажок **Включить уведомления на рабочем столе**. См. Настройки данных сигналов тревоги (узел «Сигналы тревоги»)

Вкладка	Описание
	• Сигналы тревоги должны воспроизводить звуковые уведомления на компьютерах с установленным XProtect Smart Client. Звуковые уведомления воспроизводятся только в том случае, если запущен XProtect Smart Client (даже если свернут) Звуковые уведомления для сигналов тревоги воспроизводятся только в том случае, если с сигналом тревоги связан звук. Чтобы связать звуки с сигналами тревоги, перейдите в раздел **Сигналы тревоги** > **Настройки данных сигналов тревоги** > **Уровни данных сигналов тревоги**. Для каждого необходимого приоритета сигнала тревоги выберите звук, который будет связан с сигналом тревоги. См. Настройки данных сигналов тревоги (узел «Сигналы тревоги»)

Вкладка «Интеллектуальная карта» (профили Smart Client)

На этой вкладке можно задать следующие свойства:

Вкладка	Описание
Интеллектуальная карта	Здесь указываются настройки функции интеллектуальной карты. Вы можете указать следующие параметры: • Milestone Map Service доступен для использования в качестве картографического фона • OpenStreetMaps доступен для использования в качестве картографического фона • XProtect Smart Client автоматически создает местонахождение, когда пользователь добавляет пользовательский оверлей на интеллектуальную карту.

Вкладка	Описание
	Вы также можете указать, как часто система должна удалять данные, связанные с интеллектуальными картами, с вашего компьютера. Чтобы XProtect Smart Client быстрее отображал интеллектуальную карту, клиент сохраняет данные карты в кэше на вашем компьютере. Со временем это может замедлить работу компьютера. Кэширование не применяется к Google Maps. Если в качестве картографического фона вы хотите использовать Bing Maps или Google Maps, введите ключ Bing Maps API или ключ Maps Static API от Google.

Профили Management Client (узел «Клиент»)

Данные функции доступны только в XProtect Corporate.

Вкладка «Информация» (профили Management Client)

На вкладке **Информация** можно установить для профилей Management Client следующие параметры:

Компонент	Требование
Имя	Введите имя профиля Management Client.
Приоритет	Используйте стрелки «Вверх» и «Вниз», чтобы установить приоритет профиля Management Client.
Описание	Введите описание профиля. Не обязательно.
Роли, использующие профиль Management Client	В этом поле отображаются роли, связанные с профилем Management Client. Недоступно для редактирования.

Вкладка «Профиль» (профили Management Client)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

На вкладке **Профиль** можно включить или отключить видимость следующих элементов пользовательского интерфейса Management Client:

Навигация

В этом разделе можно настроить, будет ли администратор, связанный с профилем Management Client, видеть различные функции и возможности, расположенные на панели **Навигация**.

Элемент навигации	Описание
Основы	Позволяет администратору, связанному с профилем Management Client, видеть **Информацию о лицензии** и **Информацию о сайте**.
Службы удаленного подключения	Позволяет администратору, связанному с профилем Management Client, видеть **Подключение к камере Axis нажатием одной кнопки**.
Серверы	Позволяет администратору, связанному с профилем Management Client, видеть **Серверы записи** и **Серверы отказоустойчивости**.
Устройства	Позволяет администратору, связанному с профилем Management Client, видеть **Камеры**, **Микрофоны**, **Динамики**, **Метаданные**, **Устройства ввода** и **Устройства вывода**.
Клиент	Позволяет администратору, связанному с профилем Management Client, видеть **Smart Wall**, **Группы отображений**, **Профили Smart Client**, **Профили Management Client** и **Matrix**.
Правила и события	Позволяет администратору, связанному с профилем Management Client, видеть **Правила**, **Профили времени**, **Профили уведомлений**, **Пользовательские событий**, **События аналитики** и **Типичные события**.

Элемент навигации	Описание
Безопасность	Позволяет администратору, связанному с профилем Management Client, видеть **Роли** и **Базовых пользователей**.
Информационная панель системы	Позволяет администратору, связанному с профилем Management Client, видеть **Системный монитор**, **Пороговые значения системного монитора**, **Защиту доказательств**, **Текущие задачи** и **Отчеты о конфигурации**.
Журналы серверов	Позволяет администратору, связанному с профилем Management Client, просматривать системные и контрольные журналы, а также журналы, активируемые правилами.
Управление доступом	Позволяет администратору, связанному с профилем Management Client, видеть функции **управления доступом**, если вы добавили в систему какие-либо интеграции или встраиваемые расширения управления доступом.

Подробно

В этом разделе можно настроить, будет ли администратор, связанный с профилем Management Client, видеть различные вкладки для определенного канала устройства, например вкладку **Настройки** или вкладку **Запись** для камер.

Канал устройства	Описание
Камеры	Позволяет администратору, связанному с профилем Management Client, частично или полностью видеть настройки и вкладки, связанные с камерой.
Микрофоны	Позволяет администратору, связанному с профилем Management Client, частично или полностью видеть настройки и вкладки, связанные с микрофоном.
Динамики	Позволяет администратору, связанному с профилем Management Client, частично или полностью видеть настройки и вкладки, связанные с динамиком.
Метаданные	Позволяет администратору, связанному с профилем Management Client, частично или полностью видеть настройки и вкладки, связанные с метаданными.

Канал устройства	Описание
Вход	Позволяет администратору, связанному с профилем Management Client, частично или полностью видеть настройки и вкладки, связанные с устройствами ввода.
Вывод	Позволяет администратору, связанному с профилем Management Client, частично или полностью видеть настройки и вкладки, связанные с устройствами вывода.

Меню «Инструменты»

В этом разделе можно настроить, будет ли администратор, связанный с профилем Management Client, видеть элементы, являющиеся частью меню **Инструменты**.

Параметры меню «Инструменты»	Описание
Зарегистрированные службы	Позволяет администратору, связанному с профилем Management Client, видеть **Зарегистрированные службы**.
Эффективные роли	Позволяет администратору, связанному с профилем Management Client, видеть **Эффективные роли**.
Опции	Позволяет администратору, связанному с профилем Management Client, видеть **Опции**.

Федеративные сайты

В этом разделе можно настроить, будет ли администратор, связанный с профилем Management Client, видеть панель **Иерархия федеративных сайтов**.

Узел «Правила и события»

Правила (узел «Правила и события»)

Система содержит ряд правил по умолчанию, которые можно использовать для основных функций без предварительной настройки. Правила по умолчанию можно отключать и изменять по своему усмотрению. Если вы измените или отключите правила по умолчанию, система может не работать

должным образом и не гарантировать автоматическую подачу потоков видеоданных и звуковой информации в систему.

Правило по умолчанию	Описание
Перейти к предустановке, когда PTZ будет готова	Гарантирует, что по завершении ручного управления PTZ-камеры переходят в соответствующие исходные предустановки. По умолчанию это правило отключено. Даже если правило включено, для его работы сначала нужно определить исходные предустановки по умолчанию для соответствующих PTZ-камер. Это можно сделать на вкладке **Предустановки**.
Воспроизведение звуковой информации по запросу	Обеспечивает автоматическую запись видео при возникновении внешнего запроса. Запрос всегда активируется системой, имеющей внешнюю интеграцию с вашей системой, а правило в основном используется интеграторами внешних систем или встраиваемыми расширениями.
Запись по отметке	Обеспечивает автоматическую запись видео, когда оператор устанавливает отметку в XProtect Smart Client. Правило работает при условии, что запись для соответствующих камер включена. По умолчанию запись включена. Время записи по умолчанию для этого правила составляет три секунды до установки отметки и 30 секунд после установки отметки. Правило позволяет изменить время записи по умолчанию. Буферизация перед событием, которую можно настроить на вкладке «Запись», должна соответствовать времени записи перед событием или превышать его.
Запись при движении	Обеспечивает, что запись начинается при обнаружении движения на видео с камер (при условии, что функция записи для соответствующих камер включена). По умолчанию запись включена. Правило по умолчанию определяет запись на основе обнаруженного движения, но оно не гарантирует запись видео, поскольку вы можете отключить функцию записи для одной или нескольких камер. Даже если вы включили функцию записи, помните, что на качество записи могут влиять настройки отдельной камеры.
Запись по	Обеспечивает автоматическую запись видео по внешнему запросу (при

Правило по умолчанию	Описание
запросу	условии, что функция записи для соответствующих камер включена). По умолчанию запись включена. Запрос всегда активируется системой, имеющей внешнюю интеграцию с вашей системой, а правило в основном используется интеграторами внешних систем или встраиваемыми расширениями.
Запуск потока звуковой информации	Обеспечивает автоматическую передачу в систему потоков звуковой информации со всех подключенных микрофонов и динамиков. Хотя правило по умолчанию предоставляет доступ к потокам звуковой информации от подключенных микрофонов и динамиков сразу после установки системы, оно не гарантирует запись звука, поскольку параметры записи необходимо настраивать отдельно.
Запуск потока	Обеспечивает автоматическую передачу в систему потоков видеоданных со всех подключенных камер. Хотя правило по умолчанию предоставляет доступ к потокам видеоданных с подключенных камер сразу после установки системы, оно не гарантирует запись видео, поскольку параметры записи камер необходимо настраивать отдельно.
Запуск потока метаданных	Обеспечивает автоматическую передачу в систему потоков данных со всех подключенных камер. Хотя правило по умолчанию предоставляет доступ к потокам данных с подключенных камер сразу после установки системы, оно не гарантирует запись данных, поскольку параметры записи камер необходимо настраивать отдельно.
Показать уведомление запроса доступа	Обеспечивает, чтобы все события контроля доступа, отнесенные к категории «Запрос доступа», вызывали всплывающее уведомления о запросе доступа в XProtect Smart Client (при условии, что функция уведомлений не отключена в профиле Smart Client).

Восстановление правил по умолчанию

Если вы случайно удалили одно из правил по умолчанию, его можно восстановить, используя описанные ниже действия:

Правило по умолчанию	Вводимый текст
Перейти к предустановке, когда PTZ будет готова	Выполните действие «Ручной сеанс PTZ остановлен» со всех камер Сразу перейдите к предустановке по умолчанию на устройстве, на котором произошло событие
Воспроизведение звуковой информации по запросу	Выполните действие «Запросить воспроизведение аудиосообщения» из внешнего устройства Воспроизведите аудиосообщение из метаданных на устройствах из метаданных с приоритетом 1
Запись по отметке	Выполните действие «Получен запрос на ссылку на отметку» из всех камер, всех микрофонов, всех динамиков, начните запись на три секунды раньше на устройстве, на котором произошло событие Выполняйте действие 30 секунд, затем сразу остановите запись
Запись при движении	Выполните действие «Перемещение начато» из всех камер, начните запись на три секунды раньше на устройстве, на котором произошло событие Выполните действие «Перемещение начато» из всех камер, остановите запись через три секунды
Запись по запросу	Выполните действие «Получен запрос на начало записи» из внешнего устройства, сразу начните запись на всех устройствах из метаданных Выполните действие «Получен запрос на начало записи» из внешнего устройства, сразу остановите запись
Запуск потока звуковой информации	Выполните действие в интервале времени, всегда запускайте поток на всех микрофонах, всех динамиках Выполните действие по истечении интервала времени, сразу остановите поток
Запуск потока	Выполните действие в интервале времени, всегда запускайте поток на всех камерах Выполните действие по истечении интервала времени, сразу остановите поток

Правило по умолчанию	Вводимый текст
Запуск потока метаданных	Выполните действие в интервале времени, всегда запускайте поток на всех метаданных Выполните действие по истечении интервала времени, сразу остановите поток
Показать уведомление запроса доступа	Выполните действие «Запрос доступа» (категории «Управление доступом») из Системы [+ устройства] Отобразите встроенное уведомление запроса доступа

Профили уведомлений (узел «Правила и события»)

Здесь можно указать следующие свойства для профилей уведомлений:

Компонент	Требование
Имя	Введите информативное имя для профиля уведомлений. В дальнейшем имя будет появляться всякий раз при выборе профиля уведомлений в процессе создания правила.
Описание (необязательно)	Введите описание профиля уведомлений. Описание появляется при наведении указателя мыши на профиль уведомлений в списке **Профили уведомлений** на панели «Обзор».
Получатели	Введите адреса электронной почты, на которые должны отправляться уведомления профиля уведомлений. При вводе нескольких адресов разделяйте их точкой с запятой. Пример: aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
Тема	Введите текст, который будет отображаться в качестве темы уведомления по электронной почте. В поле темы и текста сообщения можно вставить системные переменные, такие как **Имя устройства**. Чтобы вставить переменные, нажмите на соответствующие ссылки под текстовым полем.

Компонент	Требование
Текст сообщения	Введите текст, который будет отображаться в текстовом поле уведомления по электронной почте. Помимо текста сообщения, каждое уведомление по электронной почте автоматически включает следующую информацию: • Событие, которое активировало отправку уведомления • Источник прикрепленных кадров или видеороликов в формате AVI
Интервал между уведомлениями	Укажите минимальное время (в секундах), которое должно пройти между отправкой каждого уведомления по электронной почте. Примеры: • Если указать значение **120**, перед отправкой следующего уведомления по электронной почте пройдет минимум две минуты, даже если профиль уведомлений вновь активируется правилом до истечения этих двух минут • Если указано значение **0**, уведомления по электронной почте будут отправляться каждый раз, когда профиль уведомлений активируется правилом. Это может привести к отправке очень большого количества уведомлений по электронной почте. При использовании значения **0** следует тщательно оценить, стоит ли использовать профиль уведомлений в правилах, которые могут часто активироваться.
Количество изображений	Укажите максимальное количество кадров, которое можно включить в каждое электронное письмо профиля уведомлений. Количество по умолчанию: пять изображений.
Интервал между изображениями (мс)	Укажите количество миллисекунд между записями, представленными на включенных изображениях. Пример: При значении по умолчанию 500 миллисекунд включенные изображения отображают записи с интервалом в полсекунды между ними.
Время до события (с)	Этот параметр используется для указания времени начала файла AVI. По умолчанию файл AVI включает записи за 2 секунды до активации профиля уведомлений. Можно изменить этот параметр, указав необходимое количество секунд.
Время после события (с)	Этот параметр используется для указания времени окончания файла AVI. По умолчанию файл AVI заканчивается через 4 секунды после активации профиля уведомлений. Можно изменить этот параметр, указав необходимое количество секунд.

Компонент	Требование
Частота кадров	Укажите количество кадров в секунду, которое должен содержать файл AVI. Частота по умолчанию: пять кадров в секунду. Чем выше частота кадров, тем лучше качество изображения и больше размер файла AVI.
Вложить изображения в сообщение электронной почты	Если выбран этот параметр (по умолчанию он выбран), изображения вставляются в текст уведомлений по электронной почте. В противном случае изображения включаются в письмо как прикрепленные файлы.

Обзор событий

При добавлении основанного на событии правила в мастере **Управление правилом** можно выбрать один из нескольких типов события. Для удобства выбираемые события разделены на следующие группы:

Оборудование:

Определенное оборудование может самостоятельно создавать события, например обнаруживать движение. Их можно использовать в качестве событий, но перед этим необходимо настроить их на оборудовании. Можно использовать только события из отдельных типов оборудования, так как не все типы камер способны обнаруживать несанкционированные действия или изменения температуры.

Аппаратные — настраиваемые события:

Настраиваемые события из оборудования автоматически импортируются из драйверов устройств. Это означает, что они зависят от конкретного оборудования и не описаны в этом документе. Настраиваемые события выполняются только после их добавления в систему и настройки на вкладке **Событие** для соответствующего оборудования. Некоторые настраиваемые события также требуют настройки самой камеры (оборудования).

Аппаратные — заранее определенные события:

Событие	Описание
Ошибка связи (аппаратная)	Возникает, когда подключение к оборудованию прервано.

Событие	Описание
Связь начата (аппаратная)	Возникает, когда связь с оборудованием успешно установлена.
Связь прекращена (аппаратная)	Возникает, когда связь с оборудованием успешно прекращена.

Устройства — настраиваемые события:

Настраиваемые события из устройств автоматически импортируются из драйверов устройств. Это означает, что они зависят от конкретного устройства и не описаны в этом документе. Настраиваемые события выполняются только после их добавления в систему и настройки на вкладке **Событие** для соответствующего устройства.

Устройства — предварительно заданные события:

Событие	Описание
Получен запрос на ссылку на отметку	Возникает, когда в клиентах сделана отметка в режиме трансляции. Кроме того, это одно из требований для использования записи по умолчанию в правиле обработки отметок.
Ошибка связи (устройство)	Возникает, когда подключение к устройству прервано, или когда предпринята безуспешная попытка установить связь с устройством.
Связь начата (устройство)	Возникает, когда связь с устройством успешно установлена.
Связь остановлена (устройство)	Возникает, когда связь с устройством успешно прекращена.
Защита доказательств изменена	Возникает, когда пользователем клиента или посредством MIP SDK изменена защита доказательств для устройств.
Доказательство заблокировано	Возникает, когда для устройств пользователем клиента или посредством MIP SDK создана защита доказательств.

Событие	Описание
Доказательство разблокировано	Возникает, когда пользователем клиента или посредством MIP SDK удалена защита доказательств для устройств.
Переполнение рассылки начато	Переполнение канала (переполнение хранилища медиаданных) возникает, когда сервер записи не в состоянии получать данные со скоростью, заданной в настройках, и поэтому вынужден отклонить определенные записи. Если сервер работает надлежащим образом, основной причиной переполнения канала является недостаточная скорость записи на диск Проблему можно устранить путем уменьшения объема записываемых данных или повышения производительности системы хранения информации. Объем записываемых данных можно уменьшить путем снижения частоты кадров, разрешения или качества изображения камер, но это может привести к ухудшению качества записи. Если такой сценарий не подходит, можно повысить производительность системы хранения информации: установить дополнительные диски для распределения нагрузки либо установить диски или контролеры с повышенными скоростными характеристиками. Это событие можно использовать для активации действий, помогающих устранить проблему, например для уменьшения частоты кадров при записи.
Переполнение рассылки остановлено	Возникает при завершении переполнения канала (см. раздел Переполнение рассылки начато на стр. 530).
Получен запрос на клиентскую рассылку в реальном времени	Возникает, когда пользователи клиента запрашивают с устройства поток трансляции. Это событие возникает по факту запроса, даже если запрос пользователя клиента позднее окажется безуспешным, например, потому что у пользователя клиента нет разрешений, необходимых для просмотра запрошенного сигнала в режиме реального времени, или потому что сигнал по какой-либо причине прерван.
Передача данных клиенту в реальном времени прекращена	Возникает, когда пользователи клиента больше не запрашивают с устройства поток трансляции.

Событие	Описание
Ручная запись начата	Возникает, когда пользователь клиента начинает сеанс записи с камеры. Это событие активируется, даже если устройство уже ведет запись по событиям, основанным на правилах.
Ручная запись остановлена	Возникает, когда пользователь клиента останавливает сеанс записи с камеры. Если система обработки правил также начала сеанс записи, она продолжает вести запись даже после ручного прекращения записи.
Получен запрос на отмеченные данные	Возникает, когда в клиентах или посредством MIP SDK в режиме воспроизведения активирована защита доказательств. Создание события, которое можно использовать в правилах.
Перемещение начато	Возникает, когда система обнаруживает движение в видео, полученном с камер. Этот тип событий требует, чтобы для камер, к которым привязано событие, была включена функция обнаружения движений. В дополнение к системной функции обнаружения движений, некоторые камеры способны обнаруживать движения самостоятельно и активировать событие **Начало движения (аппаратное)**, но это зависит от настройки оборудования камеры и самой системы. Также см. Аппаратные — настраиваемые события: на стр. 528.
Движение остановлено	Возникает, когда на полученном видео больше не обнаруживается движение. Также см. Перемещение начато на стр. 531. Этот тип событий требует, чтобы для камер, к которым привязано событие, была включена функция обнаружения движений. В дополнение к системной функции обнаружения движений, некоторые камеры способны обнаруживать движения самостоятельно и активировать событие «Окончание движения (аппаратное)», но это зависит от настройки оборудования камеры и самой системы. Также см. Аппаратные — настраиваемые события: на стр. 528.
Вывод включен	Возникает, когда включен внешний выходной порт на устройстве. Этот тип событий требует, чтобы хотя бы одно устройство в системе поддерживало выходные порты.

Событие	Описание
Вывод изменен	Возникает, когда на устройстве изменено состояние внешнего выходного порта. Этот тип событий требует, чтобы хотя бы одно устройство в системе поддерживало выходные порты.
Вывод выключен	Возникает, когда на устройстве отключен внешний выходной порт. Этот тип событий требует, чтобы хотя бы одно устройство в системе поддерживало выходные порты.
Начат ручной сеанс PTZ	Возникает, когда на камере начинается сеанс PTZ с ручным контролем (в отличие от сеанса PTZ, основанного на плановом патрулировании или автоматической активации по событию). Этот тип событий требует, чтобы камеры, к которым привязано событие, были PTZ-камерами.
Ручной сеанс PTZ остановлен	Возникает, когда на камере останавливается сеанс ручного управления PTZ (в отличие от сеанса PTZ, основанного на плановом патрулировании или автоматической активации по событию). Этот тип событий требует, чтобы камеры, к которым привязано событие, были PTZ-камерами.
Запись начата	Возникает при начале записи. Это отдельное событие для ручного начала записи.
Запись остановлена	Возникает при остановке записи. Это отдельное событие для ручной остановки записи.
Настройка изменены	Возникает при успешном изменении настроек на устройстве.
Ошибка изменения настроек	Возникает при безуспешной попытке изменить настройки на устройстве.

Внешние события — заранее определенные события:

Событие	Описание
Запросить воспроизведение аудиосообщения	Возникает при запросе воспроизведения аудиосообщения через MIP SDK. С помощью MIP SDK сторонние разработчики могут подключать к вашей системе собственные встраиваемые расширения, например для интеграции внешних систем управления доступом и т. п.
Получен запрос на начало записи	Возникает при запросе начала записи через MIP SDK. С помощью MIP SDK сторонние разработчики могут подключать к вашей системе собственные встраиваемые расширения, например для интеграции внешних систем управления доступом и т. п.
Получен запрос на остановку записи	Возникает при запросе останова записи через MIP SDK. С помощью MIP SDK сторонние разработчики могут подключать к вашей системе собственные встраиваемые расширения, например для интеграции внешних систем управления доступом и т. п.

Внешние события — типичные события:

Типичные события позволяют выполнять операции путем отправки простых команд в систему по IP-сети. Цель типичных событий — позволить максимально возможному количеству внешних источников взаимодействовать с системой.

Внешние события — пользовательские события:

Также можно выбрать из ряда пользовательских событий, созданных специально для системы. Такие пользовательские события можно использовать для:

- Предоставления пользователям клиентов возможности вручную запускать события при просмотре в клиентах видео в режиме реального времени
- Решения множества других задач. Например, можно создать пользовательские события, которые возникают при получении от устройства данных определенного типа.

  Также см. Пользовательские события (объяснение) на стр. 92.

Серверы записи:

Событие	Описание
Архив доступен	Возникает, когда архив сервера записи становится доступен после периода недоступности. Также см. Архив недоступен на стр. 534.
Архив недоступен	Возникает, когда архив сервера записи становится недоступным, например, если прервано подключение к архиву, расположенному на сетевом диске. В таких случаях архивация записей невозможна. Это событие можно использовать, например, для активации сигнала тревоги или профиля уведомлений, чтобы соответствующим работникам организации автоматически отправлялось уведомление по электронной почте.
Архивирование не завершено	Возникает, когда во время последнего сеанса архивирования не завершено создание архива для сервера записи, но запланировано начало нового сеанса.
База данных удаляет записи перед указанием размера хранения	Возникает, когда лимит времени хранения достигнут до момента достижения лимита размера базы данных.
База данных удаляет записи перед указанием времени хранения	Возникает, когда лимит размера базы данных достигнут до момента достижения лимита времени хранения.
База данных заполнена – автоматическая архивация	Возникает, когда диск базы данных заполнен. Диск базы данных заполнен, когда на диске осталось менее 5 ГБ свободного пространства. Самые старые данные в базе данных всегда автоматически архивируются (или удаляются, если не задан следующий архив), когда остается менее 5 ГБ свободного пространства.
Диск с базой данных заполнен - удаление	Возникает, когда диск базы данных заполнен, и осталось менее 1 ГБ свободного пространства. Если следующий архив не задан, данные удаляются. Базе данных всегда требуется 250 МБ свободного пространства.

Событие	Описание
	При достижении этого лимита (если данные не удаляются достаточно быстро) новые данные не записываются в базу данных до тех пор, пока не будет освобождено достаточно пространства. Фактический максимальный размер базы данных — это указанное вами количество гигабайт минус 5 ГБ.
База данных заполнена - автоматическая архивация	Возникает, когда архив сервера записи заполнен и должен быть автоматически помещен в автоматически созданный архив в хранилище.
Восстановление базы данных	Возникает при повреждении базы данных. В этом случае система автоматически пытается применить два различных метода восстановления базы данных: быстрый и тщательный.
Хранилище базы данных доступно	Возникает, когда хранилище сервера записи становится доступно после периода недоступности. Также см. Хранилище базы данных недоступно на стр. 535. Это событие можно использовать, например, для начала записи, если она была остановлена событием **Хранилище базы данных недоступно**.
Хранилище базы данных недоступно	Возникает, когда хранилище сервера записи становится недоступно, например, если прервано подключение к хранилищу, расположенному на сетевом диске. В таких случаях архивация записей невозможна. Это событие можно использовать, например, для остановки записи, активации сигнала тревоги или профиля уведомлений, чтобы соответствующим работникам организации автоматически отправлялось уведомление по электронной почте.
Сбой зашифрованной связи с резервным сервером	Возникает, когда происходит ошибка взаимодействия по протоколу SSL между сервером отказоустойчивости и контролируемыми серверами записи.
Переключение начато	Возникает, когда сервер записи обработки отказа берет на себя функции сервера записи. Также см. раздел Серверы отказоустойчивости (раздел).
Переключение остановлено	Возникает, когда сервер записи вновь становится доступен и может взять на себя функции сервера записи обработки отказа

События системного монитора

События системного монитора активируются при превышении пороговых значений, заданных в разделе **Пороговые значения системного монитора**. Также см. Просмотрите текущее состояние оборудования и при необходимости устраните неполадки. на стр. 321.

Для выполнения данной функции требуется, чтобы работала служба Data Collector.

Системный монитор — сервер:

Событие	Описание
Использование ЦП - критическое значение	Возникает, когда уровень использования центрального процессора превышает критическое пороговое значение.
Использование ЦП - нормальное значение	Возникает, когда уровень использования центрального процессора становится ниже порогового значения, на котором выдается предупреждение.
Использование ЦП — предупреждение	Возникает, когда уровень использования центрального процессора превышает пороговое значение, на котором выдается предупреждение, или становится ниже критического порогового значения.
Использование памяти - критическое значение	Возникает, когда уровень использования памяти превышает критическое пороговое значение.
Использование памяти — нормальное значение	Возникает, когда уровень использования памяти становится ниже порогового значения, на котором выдается предупреждение.
Использование памяти — предупреждение	Возникает, когда уровень использования памяти превышает пороговое значение, на котором выдается предупреждение, или становится ниже критического порогового значения.

Событие	Описание
Декодирование NVIDIA — критическое значение	Возникает, когда уровень декодирования NVIDIA превышает критическое пороговое значение.
Декодирование NVIDIA - нормальное значение	Возникает, когда уровень использования декодирования NVIDIA становится ниже порогового значения, на котором выдается предупреждение.
Декодирование NVIDIA - предупреждение	Возникает, когда уровень использования декодирования NVIDIA превышает пороговое значение или становится ниже критического порогового значения.
Память NVIDIA — критическое значение	Возникает, когда уровень использования памяти NVIDIA превышает критическое пороговое значение.
Память NVIDIA — нормальное значение	Возникает, когда уровень использования памяти NVIDIA становится ниже порогового значения, на котором выдается предупреждение.
Память NVIDIA - предупреждение	Возникает, когда уровень использования памяти NVIDIA превышает пороговое значение или становится ниже критического порогового значения.
Визуализация NVIDIA — критическое значение	Возникает, когда уровень визуализации NVIDIA превышает критическое пороговое значение.
Визуализация NVIDIA — нормальное значение	Возникает, когда уровень визуализации NVIDIA становится ниже порогового значения, на котором выдается предупреждение.
Визуализация NVIDIA - предупреждение	Возникает, когда уровень использования визуализации NVIDIA превышает пороговое значение, на котором выдается предупреждение, или становится ниже критического порогового значения.
Доступный сервис -	Возникает, когда служба сервера перестает работать.

Событие	Описание
критическое значение	Для этого события пороговые значения отсутствуют.
Доступный сервис - нормальное значение	Возникает, когда служба сервера возвращается в рабочее состояние. Для этого события пороговые значения отсутствуют.

Системный монитор — камера:

Событие	Описание
Прямая передача FPS - критическое значение	Возникает, когда количество кадров в секунду при прямой передаче становится ниже критического порогового значения.
Прямая передача FPS — нормальное значение	Возникает, когда количество кадров в секунду при прямой передаче превышает пороговое значение, на котором выдается предупреждение.
Прямая передача FPS - предупреждение	Возникает, когда количество кадров в секунду при прямой передаче становится ниже порогового значения, на котором выдается предупреждение, или превышает критическое пороговое значение.
Запись FPS - критическое значение	Возникает, когда количество кадров в секунду при записи становится ниже критического порогового значения.
Запись FPS — нормальное значение	Возникает, когда количество кадров в секунду при записи превышает критическое пороговое значение, на котором выдается предупреждение.
Запись FPS - предупреждение	Возникает, когда количество кадров в секунду при записи становится ниже порогового значения, на котором выдается предупреждение, или превышает критическое пороговое значение.

Событие	Описание
Используемое место — критическое значение	Возникает, когда объем хранилища, используемого для записей конкретной камеры, превышает критическое пороговое значение.
Используемое место - нормальное значение	Возникает, когда объем хранилища, используемого для записей конкретной камеры, становится ниже порогового значения, на котором выдается предупреждение.
Используемое место — предупреждение	Возникает, когда объем хранилища, используемого для записей конкретной камеры, превышает пороговое значение, на котором выдается предупреждение, или становится ниже критического порогового значения.

Системный монитор — диск:

Событие	Описание
Свободное место - критическое значение	Возникает, когда уровень использования дискового пространства превышает критическое пороговое значение.
Свободное место - нормальное значение	Возникает, когда уровень использования дискового пространства становится ниже порогового значения, на котором выдается предупреждение.
Свободное место — предупреждение	Возникает, когда уровень использования дискового пространства превышает пороговое значение, на котором выдается предупреждение, или становится ниже критического порогового значения.

Системный монитор — хранилище:

Событие	Описание
Время хранения - критическое значение	Возникает, когда система прогнозирует, что хранилище будет заполняться быстрее, чем предусмотрено критическим пороговым значением времени хранения. Например, когда данные видеопотоков заполняют хранилище быстрее, чем ожидалось.
Время хранения — нормальное значение	Возникает, когда система прогнозирует, что хранилище будет заполняться медленнее, чем предусмотрено пороговым значением времени хранения, на котором выдается предупреждение. Например, когда данные видеопотоков заполняют хранилище с ожидаемой скоростью.
Время хранения — предупреждение	Возникает, когда система прогнозирует, что хранилище будет заполняться быстрее, чем предусмотрено критическим пороговым значением времени хранения, на котором выдается предупреждение, или медленнее, чем предусмотрено критическим пороговым значением времени хранения. Например, когда данные видеопотоков заполняют хранилище быстрее, чем предполагалось, из-за большего объема движений с камер, настроенных на запись при движении.

Прочее:

Событие	Описание
Сбой автоматической активации лицензии	Возникает при сбое автоматической активации лицензии. Для этого события пороговые значения отсутствуют.
Плановое изменение пароля началось	Возникает при начале планового изменения пароля.
Плановое изменение пароля успешно выполнено	Возникает, когда плановое изменение пароля выполнено без ошибок.
Плановое изменение пароля выполнено с ошибками	Возникает, когда плановое изменение пароля выполнено с ошибками.

События из расширений и интеграций XProtect:

События из расширений и интеграций XProtect можно использовать в системе правил, например:

- События аналитики также можно использовать в системе правил

Действия и завершающие действия

Набор действий и завершающих действий может использоваться для создания правил в мастере **Управление правилом**. У вас могут быть и другие доступные действия, если в вашей системе используются расширения XProtect или специфичные для поставщика встраиваемые расширения. Для каждого типа действий при необходимости указываются сведения о завершающем действии.

Мастер «Управление правилом»

Действие	Описание
Начать запись на <устройствах>	Начало записи на выбранных устройствах и сохранение этих данных в базе данных. При выборе этого типа действий мастер **Управление правилом** просит указать: Когда должна начинаться запись. Это происходит немедленно или за несколько секунд до активирующего события/начала активирующего интервала времени. Также указывается, на каких устройствах должно выполняться действие. Этот тип действий требует, чтобы на устройствах, с которыми связано действие, была включена запись. Сохранение данных, предшествующих событию или интервалу времени, возможно только в том случае, если для соответствующих устройств включена буферизация перед событием. Включение записи и настройка параметров буферизации перед событием для устройства осуществляются на вкладке **Запись**. **Требуется завершающее действие**: Этот тип действий требует наличия одного или нескольких завершающих действий. На одном из следующих этапов мастер автоматически просит вас указать завершающее действие: **Остановить запись**. Без этого завершающего действия запись может теоретически продолжаться бесконечно. При желании также можно задать дополнительные завершающие действия.

Действие	Описание
Запустить поток на <устройствах>	Запустить поток данных с устройств в систему. Когда запущен поток данных с устройства, данные передаются с устройства в систему, и в зависимости от типа данных их можно просматривать и записывать. При выборе этого типа действий мастер **Управление правилом** просит указать, на каких устройствах должны быть запущены потоки. Система добавляет правило по умолчанию, которое гарантирует, что потоки всегда будут запущены на всех камерах. **Требуется завершающее действие**: Этот тип действий требует наличия одного или нескольких завершающих действий. На одном из следующих этапов мастер автоматически просит вас указать завершающее действие: **Остановить поток**. Также можно указать дополнительные завершающие действия. Применение обязательного завершающего действия **Остановить поток** для остановки потока с устройства означает, что данные с устройства перестают передаваться в систему. В этом случае просмотр видео в режиме реального времени и его запись станут невозможны. Тем не менее устройство, на котором вы остановили поток, по-прежнему способно взаимодействовать с сервером записи, и вы можете автоматически запустить поток вновь при помощи правила, в отличие от ситуации, когда устройство отключено вручную. Несмотря на то, что этот тип действий предоставляет доступ к потокам данных с выбранных устройств, он не гарантирует запись данных, и параметры записи необходимо настроить отдельно.
Задать <предустановку> для <Smart Wall>	Задает выбранную предустановку для XProtect Smart Wall. Укажите предустановку на вкладке **Smart WallПредустановки**. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.

Действие	Описание
Задать <монитор> <Smart Wall> для отображения <камер>	Задает конкретный монитор XProtect Smart Wall для отображения видео в режиме реального времени с выбранных камер на этом объекте или на подчиненном объекте, настроенном в Milestone Federated Architecture. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Задать <монитор> <Smart Wall> для отображения <сообщений>	Задает конкретный монитор XProtect Smart Wall для отображения заданного пользователем текстового сообщения размером до 200 символов. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Удалить <камеры> из <Smart Wall> <монитора>	Прекращение воспроизведения видео с конкретной камеры. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Задать частоту кадров прямой передачи на <устройствах>	Задает конкретную частоту кадров, которая будет использоваться в системе при отображении видео в режиме реального времени с выбранных камер. Этот параметр заменяет настроенную для камер частоту кадров по умолчанию. Это указывается на вкладке **Настройки**. При выборе этого типа действий мастер **Управление правилом** просит указать, какую частоту кадров необходимо задать, а также на каких устройствах. Всегда проверяйте, поддерживают ли соответствующие камеры выбранную частоту кадров. **Требуется завершающее действие**: Этот тип действий требует наличия одного или нескольких завершающих действий. На одном из следующих этапов мастер автоматически просит вас указать завершающее действие: **Восстановить частоту кадров**

Действие	Описание
	при прямой передаче по умолчанию Без этого завершающего действия частота кадров по умолчанию теоретически никогда не будет восстановлена. При желании также можно задать дополнительные завершающие действия.
Задать частоту кадров записи на <устройствах>	Задает конкретную частоту кадров, которая будет использоваться в системе при сохранении записанного видео с выбранных камер в базе данных. Этот параметр заменяет настроенную для камер частоту кадров при записи по умолчанию. При выборе этого типа действий мастер **Управление правилом** просит указать, какую частоту кадров при записи необходимо задать, а также на каких камерах. Задать частоту кадров при записи можно задать только для видеокодека формата JPEG, в котором каждый кадр по отдельности сжимается в JPEG-изображение. Также этот тип действий требует, чтобы на камерах, с которыми связано действие, была включена запись. Включение записи для камеры осуществляется на вкладке **Запись**. Максимальная доступная частота кадров зависит от типа соответствующих камер и от выбранного для них разрешения изображения. **Требуется завершающее действие**: Этот тип действий требует наличия одного или нескольких завершающих действий. На одном из следующих этапов мастер автоматически просит вас указать завершающее действие: **Восстановить частоту кадров при записи по умолчанию**. Без этого завершающего действия частота кадров при записи по умолчанию теоретически никогда не будет восстановлена. При желании также можно задать дополнительные завершающие действия.
Задать частоту кадров для всех кадров MPEG-4/H.264/H.265 при записи на <устройствах>	Задает частоту кадров для записи всех кадров, когда система сохраняет в базе данных записанное видео с выбранных камер, а не только ключевые кадры. Включение записи ключевых кадров работает только на вкладке **Запись**. При выборе этого типа действий мастер **Управление правилом** просит выбрать устройства, к которым должно применяться

Действие	Описание
	действие. Включить запись ключевых кадров можно только для форматов MPEG-4/H.264/H.265. Также этот тип действий требует, чтобы на камерах, с которыми связано действие, была включена запись. Включение записи для камеры осуществляется на вкладке **Запись**. **Требуется завершающее действие**: Этот тип действий требует наличия одного или нескольких завершающих действий. На одном из следующих этапов мастер автоматически просит вас указать завершающее действие: **Восстановить частоту кадров при записи по умолчанию для ключевых кадров MPEG-4/H.264/H.265** Без этого завершающего действия настройка по умолчанию теоретически никогда не будет восстановлена. При желании также можно задать дополнительные завершающие действия.
Начать патрулирование на <устройстве> при помощи <профиля> с PTZ-приоритетом <приоритет>	В соответствии с определенным профилем патрулирования запускает PTZ-патрулирование на определенной камере с определенным приоритетом. Именно так должно осуществляться патрулирование, включая последовательность исходных предустановок, настроек времени и другие параметры. Если вы выполнили обновление со старой версии системы, старые значения приоритета (**Очень низкий**, **Низкий**, **Средний**, **Высокий** и**Очень высокий**) теперь имеют следующий вид: • Очень низкий = 1 000 • Низкий = 2 000 • Средний = 3 000 • Высокий = 4 000 • Очень высокий = 5 000 При выборе этого типа действий мастер **Управление правилом** просит выбрать профиль патрулирования. Можно выбрать только один профиль патрулирования на одном устройстве. Выбрать несколько профилей патрулирования нельзя.

Действие	Описание
	 Этот тип действий требует, чтобы устройства, к которым привязано действие, были PTZ-устройствами.  Для устройств необходимо задать не менее одного профиля патрулирования. Указание профилей патрулирования для PTZ-камеры осуществляется на вкладке **Патрулирование**. **Требуется завершающее действие**: Этот тип действий требует наличия одного или нескольких завершающих действий. На одном из следующих этапов мастер автоматически просит вас указать завершающее действие: **Остановить патрулирование** Теоретически без этого завершающего действия патрулирование никогда не остановится. Также можно указать дополнительные завершающие действия.
Приостановить патрулирование на <устройствах>	Приостанавливает PTZ-патрулирование. При выборе этого типа действий мастер **Управление правилом** просит указать, на каких устройствах должно быть приостановлено патрулирование.  Этот тип действий требует, чтобы устройства, к которым привязано действие, были PTZ-устройствами.  Для устройств необходимо задать не менее одного профиля патрулирования. Указание профилей патрулирования для PTZ-камеры осуществляется на вкладке **Патрулирование**.

Действие	Описание
	Требуется завершающее действие: Этот тип действий требует наличия одного или нескольких завершающих действий. На одном из следующих этапов мастер автоматически просит вас указать завершающее действие: **Возобновить патрулирование** Теоретически без этого завершающего действия патрулирование будет приостановлено на неограниченное время. При желании можно задать дополнительные завершающие действия.
Переместить <устройство> на <исходную> предустановку с PTZ-приоритетом <priority>	Перемещает конкретную камеру на определенную исходную предустановку, всегда — в соответствии с приоритетом. При выборе этого типа действий мастер **Управление правилом** просит выбрать исходную предустановку. Можно выбрать только одну исходную предустановку на одной камере. Выбрать несколько исходных предустановок нельзя. Этот тип действий требует, чтобы устройства, к которым привязано действие, были PTZ-устройствами. Это действие требует, чтобы ранее для этих устройств была задана, как минимум, одна исходная предустановка. Указание исходных предустановок для PTZ-камеры осуществляется на вкладке **Предустановки**. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Переместить на предустановку по умолчанию на <устройствах> с PTZ-приоритетом	Перемещает одну или несколько конкретных камер на их соответствующие исходные предустановки по умолчанию, но всегда в соответствии с приоритетом. При выборе этого типа действий мастер **Управление правилом** просит выбрать устройства, к которым должно применяться действие.

Действие	Описание
<приоритет>	Этот тип действий требует, чтобы устройства, к которым привязано действие, были PTZ-устройствами. Это действие требует, чтобы ранее для этих устройств была задана, как минимум, одна исходная предустановка. Указание исходных предустановок для PTZ-камеры осуществляется на вкладке **Предустановки**. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Задать <состояние> для устройства вывода	Задает конкретное состояние (активированное или неактивированное) для вывода на определенном устройстве. При выборе этого типа действий мастер **Управление правилом** просит указать, какое состояние необходимо задать, а также на каких устройствах. Этот тип действий требует, чтобы на каждом из устройств, с которыми связано действие, к порту вывода был подключен хотя бы один внешний модуль вывода. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Создать отметку на <устройстве>	Создает отметку в потоке трансляции или записях с выбранного устройства. С помощью отметки можно легко отследить определенное событие или период времени. Настройка отметок осуществляется в диалоговом окне **Параметры**. При выборе этого типа действий мастер **Управление правилом** просит указать сведения об отметках и выбрать устройства. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении

Действие	Описание
	события или через определенный период времени.
Воспроизвести звуковое <сообщение> на <устройствах> с <приоритетом>	Воспроизводит звуковое сообщение на выбранных устройствах, активированных событием. Этими устройствами являются преимущественно динамики или камеры. Этот тип действий требует предварительной выгрузки сообщения в систему в разделе **Инструменты** > **Параметры** > вкладка **Звуковые сообщения**. Вы можете создавать дополнительные правила для одного и того же события и отправлять разные сообщения на каждое устройство, но всегда — в соответствии с приоритетом. Последовательность контролируется приоритетами, задаваемыми в правиле и на устройстве для роли на вкладке **Речь**: • Если воспроизводится одно сообщение, и на тот же динамик отправляется другое сообщение с тем же приоритетом, второе сообщение будет воспроизведено по окончании первого • Если воспроизводится одно сообщение, и на тот же динамик отправляется другое сообщение с более высоким приоритетом, первое сообщение будет прервано, и немедленно будет воспроизведено второе
Отправить уведомление на <профиль>	Отправляет уведомление с помощью определенного профиля уведомлений. При выборе этого типа действий мастер **Управление правилом** просит выбрать профиль уведомлений, а также с каких устройств следует отправлять изображения до сигнала тревоги. Можно выбрать только один профиль уведомления. Выбрать несколько профилей уведомления нельзя. Один профиль уведомлений может содержать несколько получателей. Также можно создавать дополнительные правила для одного и того же события и отправлять разные уведомления на каждый из профилей уведомлений. Содержимое правил можно скопировать для его повторного использования, нажав правило правой кнопкой мыши в списке **Правила**.

Действие	Описание
	Этот тип действий требует, чтобы был задан по меньшей мере один профиль уведомлений. Изображения до сигнала тревоги будут включены только в том случае, если для соответствующего профиля уведомлений включен параметр **Включать изображения**. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Создать новую <запись журнала>	Создает запись в журнале правил. При выборе этого типа действий мастер **Управление правилом** просит задать текст для записи журнала. При вводе текста журнала в сообщении можно использовать такие переменные как **$DeviceName$**, **$EventName$**. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Запустить встраиваемое расширение на <устройствах>	Запускает одно или несколько встраиваемых расширений. При выборе этого типа действий мастер **Управление правилом** просит указать требуемые встраиваемые расширения, а также на каких устройствах они должны быть запущены. Этот тип действий требует, чтобы в системе было установлено, как минимум, одно встраиваемое расширение. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Остановить встраиваемое расширение на <устройствах>	Останавливает одно или несколько встраиваемых расширений. При выборе этого типа действий мастер **Управление правилом** просит указать требуемые встраиваемые расширения, а также на каких устройствах они должны быть остановлены. Этот тип действий требует, чтобы в системе было установлено,

Действие	Описание
	как минимум, одно встраиваемое расширение. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Применить новые настройки на <устройствах>	Изменяет настройки на одном или нескольких устройствах. При выборе этого типа действий мастер **Управление правилом** просит выбрать соответствующие устройства. Также можно задать необходимые настройки на указанных вами устройствах.  Если вы задаете настройки для нескольких устройств, можно изменить только настройки, доступные для всех указанных устройств. **Пример**: Вы указываете, что действие должно быть связано с устройством 1 и устройством 2. На устройстве 1 имеются настройки A, B и C, а на устройстве 2 имеются настройки B, C и D. В этом случае вы сможете изменить только настройки, доступные для обоих устройств, а именно — настройки B и C. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Задать Matrix для просмотра <устройств>	Показывает видео с выбранных камер на компьютере, способном отображать видео, активированное при помощи Matrix (например, на компьютере, на котором установлен XProtect Smart Client). При выборе этого типа действий мастер **Управление правилом** просит выбрать получателя Matrix, а также одно или несколько устройств, с которых следует показать видео на выбранном получателе Matrix. Этот тип действий позволяет одновременно выбрать только

Действие	Описание
	одного получателя Matrix. Если вы хотите, чтобы видео с выбранных устройств отображалось на нескольких получателях Matrix, необходимо создать правило для каждого требуемого получателя Matrix либо воспользоваться функцией XProtect Smart Wall. Нажатием правой кнопкой мыши правила из списка **Правила** можно скопировать содержимое правила для его повторного использования. Таким образом, вам не требуется создавать почти одинаковые правила «с нуля». В рамках настройки самих получателей Matrix пользователи должны указать номер порта и пароль, необходимые для взаимодействия с Matrix. Убедитесь, что у пользователей есть доступ к этой информации. Также, как правило, пользователи должны задать IP-адреса или допустимые хосты, с которых принимаются команды отображения видео, активированного Matrix. В этом случае пользователям также требуется знать IP-адрес сервера управления либо используемого маршрутизатора или брандмауэра.
Отправить прерывание SNMP	Создает небольшое сообщение, фиксирующее события на выбранных устройствах. Текст ловушки SNMP создается автоматически и не может быть изменен. Оно может содержать тип источника и имя устройства, на котором произошло событие. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Получить и сохранить дистанционные записи с	Получает и сохраняет с выбранных устройств (которые поддерживают дистанционную запись) дистанционные записи за определенный период до и после активирующего события. Это правило не зависит от настройки **Автоматически получить**

Действие	Описание
<устройств>	**дистанционные записи при восстановлении подключения**. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Получить и сохранить дистанционные записи между <время начала и окончания> с <устройств>	Получает и сохраняет с выбранных устройств (которые поддерживают дистанционную запись) дистанционные записи за определенный период. Это правило не зависит от настройки **Автоматически получить дистанционные записи при восстановлении подключения**. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Сохранить прикрепленное изображение	Сохраняет для последующего использования изображение, полученное при помощи события «Изображения получены» и отправленное с камеры в электронном письме по протоколу SMTP. В будущем это действие может быть активировано и другими событиями. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Активировать архивирование в <архивах>	Запускает процесс архивирования в одном или нескольких архивах. При выборе этого типа действий мастер **Управление правилом** просит выбрать соответствующие архивы. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
На <объекте> активировать	Актуально преимущественно для Milestone Federated Architecture, но также может использоваться в рамках схемы с одним

Действие	Описание
<пользовательское событие>	объектом. Используйте это правило для активации пользовательского события на объекте, как правило — на удаленном объекте с федеративной иерархией. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Показать <уведомление о запросе доступа>	Позволяет отображать на экране XProtect Smart Client всплывающее уведомление о запросе доступа, когда соблюдены критерии для активирующих событий. Milestone рекомендует использовать для этого действия события контроля доступа в качестве активирующих событий, так как уведомления о запросе доступа обычно настраиваются для работы со связанным командами контроля доступа и камерами. Этот тип действий требует, чтобы в системе было установлено по меньшей мере одно встраиваемое расширение для управления доступом. **Необязательное действие останова**: для этого типа действия действие останова не требуется.Можно указать дополнительные завершающие действия, которые выполняются при наступлении события или через определенный период времени.
Изменить пароль на аппаратных устройствах	Заменяет пароль на выбранных аппаратных устройствах случайным образом сгенерированным паролем, основанным на требованиях к паролям для конкретного аппаратного устройства. Список поддерживаемых аппаратных устройств см. в разделе Поиск оборудования. Это действие доступно, только если вы настраиваете правило с помощью типа правил **Выполнять повторяющееся действие через <интервалы>** Для этого действия доступны следующие события: • Плановое изменение пароля началось на стр. 540

Действие	Описание
	• Плановое изменение пароля успешно выполнено на стр. 540 • Плановое изменение пароля выполнено с ошибками на стр. 540 Для этого типа действий завершающее действие отсутствует. Вы можете просмотреть ход выполнения действия в разделе **Текущие задачи**. Дополнительные сведения приведены в разделе Просмотр задач, выполняющихся на серверах записи на стр. 318. Для просмотра результатов действия откройте раздел **Журналы серверов** на вкладке **Системные журналы**. Дополнительные сведения приведены в разделе Вкладка «Журналы серверов» (параметры) на стр. 421. Дополнительные сведения см. в разделе Системные журналы.

Тестирование события аналитики (свойств)

При тестировании требований события аналитики открывается окно, в котором выполняется проверка четырех условий и описываются возможные ошибки и способы их устранения.

Условие	Описание	Сообщения об ошибках и способы их устранения
Изменения сохранены	Если это новое событие, сохранено ли оно? Или, если в имя события внесены изменения, сохранены ли эти изменения?	**Сохраните изменения перед тестированием события аналитики**. Решение/пояснение: Сохраните изменения.
События аналитики включены	Включена ли функция событий аналитики?	**События аналитики не включены**. Решение/пояснение: Включите функцию событий аналитики. Для этого откройте раздел **Инструменты** > **Параметры** > **События аналитики**

Условие	Описание	Сообщения об ошибках и способы их устранения
		и выберите кнопку-переключатель **Включено**.
Допустимый адрес	Является ли допустимым IP-адрес/имя хоста компьютера, отправляющего событие (включен ли он в список адресов для событий аналитики)?	**Локальное имя хоста должно быть задано в качестве допустимого адреса для службы событий аналитики**. Решение/пояснение: Добавьте компьютер в список адресов для событий аналитики, включающий допустимые IP-адреса или имена хоста. **Ошибка при разрешении локального имени хоста**. Решение/пояснение: IP-адрес или имя хоста компьютера не найдено или недействительно.
Отправка события аналитики	Удалось ли отправить тестовое событие на сервер событий?	См. таблицу ниже.

Каждый этап помечен как неудачный: ❌ или успешный: ✓.

Сообщения об ошибках и способы решения для условия **Отправка события аналитики**:

Сообщение об ошибке	Решение
Сервер событий не найден	Не удалось найти сервер событий в списке зарегистрированных служб.
Ошибка при подключении к серверу событий	Не удается подключиться к серверу событий через указанный порт. Вероятнее всего, эта ошибка возникает из-за проблем с сетью либо остановки службы Event Server.
Ошибка при отправке события аналитики	Подключение к серверу событий установлено, но отправить событие не удается. Вероятнее всего, эта ошибка возникает из-за проблем с сетью (например, если истекло время ожидания).
Ошибка при получении ответа с	Событие было отправлено на сервер событий, но ответ не получен. Вероятнее всего, эта ошибка возникает из-за проблем с сетью или

Сообщение об ошибке	Решение
сервера событий	занятым портом. См. журнал сервера событий, как правило, находящийся в `ProgramData\Milestone\XProtect Event Server\Logs\`.
Неизвестное серверу событий событие аналитики	Событие неизвестно службе Event Server. Вероятнее всего, эта ошибка возникает из-за того, что событие или внесенные в событие изменения не сохранены.
Сервер событий получил недопустимое событие аналитики	Формат события является неверным.
Недопустимый отправитель для сервера событий	Вероятнее всего, компьютер не внесен в список допустимых IP-адресов или имен хостов.
Внутренняя ошибка сервера событий	Ошибка на сервере событий. См. журнал сервера событий, как правило, находящийся в `ProgramData\Milestone\XProtect Event Server\Logs\`.
С сервера событий получен недопустимый ответ	Недопустимый ответ. Возможно, порт занят, или возникли проблемы с сетью. См. журнал сервера событий, как правило, находящийся в `ProgramData\Milestone\XProtect Event Server\Logs\`.
Неизвестный ответ сервера событий	Ответ является действительным, но не распознан. Вероятно, эта ошибка возникает из-за проблем с сетью или занятого порта. См. журнал сервера событий, как правило, находящийся в `ProgramData\Milestone\XProtect Event Server\Logs\`.
Непредвиденная ошибка	Для получения помощи обратитесь в службу поддержки Milestone.

Типичные события и источники данных (свойства)

Эта функция доступна только в случае, если установлен сервер событий XProtect.

Типичное событие (свойства)

Компонент	Требование
Имя	Уникальное имя для типичного события. Имя должно быть уникальным среди событий всех типов, таких как пользовательские события, события аналитики и т. д.
Включено	Типичные события по умолчанию включены. Снимите флажок, чтобы отключить событие.
Выражение	Выражение, которое система должна учитывать при анализе пакетов данных. Можно использовать следующие операторы: • `( )`: обеспечивают обработку связанных параметров как одной логической единицы. При анализе их можно использовать для соблюдения определенного порядка обработки. **Пример**: Критерий поиска `(User001 OR Door053) AND Sunday` сначала обрабатывает два выражения внутри скобок, а затем комбинирует этот результат с последней частью строки. Таким образом, сначала система ищет все пакеты, содержащие параметры `User001` или `Door053`, после чего просматривает результаты на наличие в них параметра `Sunday`. • `AND`: оператор `AND` указывает на то, что должны присутствовать параметры, расположенные по обе стороны оператора `AND`. **Пример**: Критерий поиска `User001 AND Door053 AND Sunday` возвращает результат только в том случае, если все параметры `User001`, `Door053` и `Sunday` включены в выражение. Присутствия только одного или двух параметров недостаточно. Чем больше параметров вы комбинируете с помощью AND, тем меньше получаете результатов. • `OR`: с помощью оператора `OR` указывается, что должен присутствовать один из параметров **Пример**: Критерий поиска `"User001" OR "Door053" OR "Sunday"` возвращает результаты, содержащие `User001`, `Door053` или `Sunday`. Чем больше параметров вы комбинируете с помощью `OR`, тем больше получаете результатов.

Компонент	Требование
Тип выражения	Указывает, насколько точно система должна анализировать полученные пакеты данных. Возможны следующие варианты: • **Поиск**. Чтобы событие произошло, полученный пакет данных должен содержать текст, указанный в поле **Выражение**, но также может включать прочий контент **Пример**: Если вы указали, что полученный пакет должен содержать параметры `User001` и `Door053`, то событие активируется в случае, если полученный пакет содержит параметры `User001`, `Door053` и `Sunday`, поскольку в полученном пакете содержатся два обязательных параметра • **Соответствие**. Чтобы событие произошло, полученный пакет данных должен содержать именно тот текст, который указан в поле **Выражение**, и ничего больше • **Регулярное выражение**. Чтобы событие произошло, текст, указанный в поле **Выражение**, должен определять шаблоны в полученных пакетах данных Если переключиться с вариантов **Поиск** или **Соответствие** на **Регулярное выражение**, текст в поле **Выражение** автоматически преобразуется в регулярное выражение.
Приоритет	Приоритет указывается в виде числа от 0 (самый высокий приоритет) до 999999 (самый низкий приоритет). Один и тот же пакет данных может анализироваться на присутствие различных событий. Возможность назначать приоритет каждому событию позволяет определить событие, которое будет активировано, если полученный пакет соответствует критериям нескольких событий. Когда система получает пакет TCP и/или UDP, анализ пакета начинается с анализа события, имеющего самый высокий приоритет. Таким образом, когда пакет соответствует критериям нескольких событий, активируется только событие с самым высоким приоритетом. Если пакет соответствует критериям нескольких событий с одинаковым приоритетом, например двух событий с приоритетом 999, активируются все события с этим приоритетом.
Проверить соответствие выражения строке события	Строка события, которая будет проверена на соответствие выражению, введенному в поле **Выражение**.

Веб-перехватчики (узел «Правила и события»)

В узле **Веб-перехватчики** можно создавать, редактировать и удалять конечные точки веб-перехватчиков.

При создании и редактировании веб-перехватчиков можно использовать следующие поля:

Поле	Описание
Имя	Введите уникальное имя конечной точки веб-перехватчика. Имя веб-перехватчика не может быть пустым.
Адрес	URL-адрес веб-сервера или приложения, в который требуется отправлять данные событий. При обновлении URL-адреса веб-сервера нужно обновить URL-адрес веб-перехватчика в узле «Веб-перехватчики». При использовании протокола HTTP в незащищенных сетях (например, открытый Интернет) все события отображаются в виде простого текста.
Токен	Введите токен, который служит для защиты взаимодействия с другими приложениями путем проверки источника HTTP POST. Использование токена для защиты взаимодействий необязательно, но рекомендуется.
Версия API	Версия встраиваемого расширения веб-перехватчика и API, используемых для реализации функций веб-перехватчика.

Узел «Безопасность»

Роли (узел «Безопасность»)

Вкладка «Информация» (роли)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

На вкладке **Информация** вы можете установить следующие параметры роли:

Имя	Описание
Имя	Введите имя роли.
Описание	Введите описание роли.
Профиль **Management Client**	Выберите профиль Management Client, который необходимо связать с ролью. Нельзя применить это к роли **администраторов** по умолчанию. Требуются разрешения для управления безопасностью на сервере управления.
Профиль **Smart Client**	Выберите профиль Smart Client, который необходимо связать с ролью. Требуются разрешения для управления безопасностью на сервере управления.
Профиль времени по умолчанию	Выберите профиль времени по умолчанию, который необходимо связать с ролью. Нельзя применить это к роли **администраторов** по умолчанию.

Имя	Описание
Профиль защиты доказательств	Выберите профиль защиты доказательств, который необходимо связать с ролью.
Вход в Smart Client в профиле времени	Выберите профиль времени, для которого пользователю XProtect Smart Client, связанному с этой ролью, разрешен вход в систему. Если пользователь XProtect Smart Client входит в систему по истечении этого периода, будет автоматически осуществлен выход. Нельзя применить это к роли **администраторов** по умолчанию.
Разрешить вход в Smart Client	Установите флажок, чтобы разрешить пользователям, связанным с этой ролью, вход в XProtect Smart Client. Доступ к Smart Client по умолчанию запрещен. Снимите флажок, чтобы запретить доступ к XProtect Smart Client.
Разрешить вход в клиент XProtect Mobile	Установите флажок, чтобы разрешить пользователям, связанным с этой ролью, вход в клиент XProtect Mobile. Доступ к клиенту XProtect Mobile по умолчанию запрещен. Снимите флажок, чтобы запретить доступ к клиенту XProtect Mobile.
Разрешить вход в XProtect Web Client	Установите флажок, чтобы разрешить пользователям, связанным с этой ролью, вход в XProtect Web Client. Доступ к XProtect Web Client по умолчанию запрещен. Снимите флажок, чтобы запретить доступ к XProtect Web Client.
Требуется авторизация	Установите флажок, чтобы связать авторизацию входа в систему с ролью. Это означает, что при входе пользователя в систему XProtect Smart Client или Management Client запрашивает вторую авторизацию, обычно со стороны привилегированного пользователя или менеджера. Чтобы администраторы имели возможность авторизовать пользователей, настройте разрешение сервера управления **Авторизация пользователей** на вкладке **Общая безопасность**. Нельзя применить это к роли **администраторов** по умолчанию.
Сделать пользователей анонимными во время сессий PTZ	Установите флажок, чтобы скрыть имена пользователей, связанных с этой ролью, когда они управляют сеансами PTZ.

Вкладка «Пользователи и группы» (роли)

На вкладке **Пользователи и группы** назначаются роли пользователям и группам (см. Назначение ролям пользователей и групп и их удаление из ролей на стр. 313). Можно назначить пользователей и группы Windows или базовых пользователей (см. Пользователи (объяснение) на стр. 72).

Внешний IDP (роли)

На вкладке **Внешний IDP** вы можете просмотреть существующие заявки и добавить новые заявки к ролям.

Имя	Описание
Внешний поставщик удостоверений	Название внешнего IDP.
Название заявки	Переменная, определенная во внешнем IDP.
Стоимость заявки	Стоимость заявки, например имя группы, которую можно использовать для назначения пользователю соответствующей роли.

Вкладка «Общая безопасность» (роли)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

На вкладке **Общая безопасность** можно настроить общие разрешения для ролей. Для каждого компонента, доступного в вашей системе, укажите разрешения доступа для ролей, установив **Разрешить** или **Запретить**. Если доступ к компоненту запрещен, этот компонент не отображается на вкладке **Общая безопасность** для пользователя в данной роли.

Вкладка **Общая безопасность** недоступна в бесплатной версии XProtect Essential+.

Для XProtect Corporate вы можете определить больше разрешений доступа, чем для других продуктов XProtect VMS. Это связано с тем, что вы можете настроить дифференцированные разрешения администратора только в XProtect Corporate, в то время как общие разрешения для роли, которая использует XProtect Smart Client, XProtect Web Client или XProtect Mobile, можно настроить во всех продуктах.

Общие настройки безопасности применяются только к текущему объекту.

Если вы связываете пользователя с несколькими ролями и в настройках безопасности выбираете **Запретить** для одной роли и **Разрешить** для другой, выбор значения **Запретить** отменяет значение **Разрешить**.

Ниже показано, что происходит с каждым отдельным разрешением для различных компонентов системы, если вы выберете **Разрешить** для соответствующей роли. При использовании XProtect Corporate вы можете под каждым компонентом системы увидеть, какие настройки доступны **только** для вашей системы.

Чтобы настроить разрешения безопасности для роли, системный администратор может использовать флажки **Разрешить** или **Запретить** для каждого компонента или функции системы. Любые разрешения безопасности, которые вы настраиваете, применяются для компонента или функции всей системы. Например, если вы установите флажок **Запретить** в поле **Камеры**, все камеры, добавленные в систему, будут недоступны для данной роли. Напротив, если вы установите флажок **Разрешить**, пользователь с данной ролью сможет видеть все камеры, добавленные в систему. Результатом выбора **Разрешить** или **Запретить** для ваших камерах станет то, что настройки камеры на вкладке **Устройство** унаследуют настройки, выполненные на вкладке **Общая безопасность**, так что все камеры будут либо доступны, либо недоступны для определенной роли.

При настройке разрешений безопасности для **отдельных** камер или других элементов можно установить такие отдельные разрешения на вкладке соответствующего компонента или функции системы только в том случае, если вы **не установили никаких общих разрешений** для компонента или функции системы на вкладке **Общая безопасность**.

Информация ниже также относится к разрешениям, которые можно настроить с помощью MIP SDK.

Если вы хотите переключить базовую лицензию с XProtect Corporate на один из других продуктов, убедитесь, что удалены все разрешения безопасности, доступные только для XProtect Corporate. Если вы не удалите эти разрешения, выполнить переключение не удастся.

Сервер управления

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Подключение	Позволяет пользователям подключаться к Management Server. Это разрешение включено по умолчанию. Вы можете временно отклонить разрешение на подключение для той или иной роли для обслуживания, а затем повторно предоставить доступ к системе. ⚠ Для предоставления доступа к системе это разрешение должно быть выбрано.
Прочитать	⚠ Является административным разрешением высокого уровня, которое предоставляет значительные права доступа к VMS XProtect, включая доступ к конфиденциальным данным, таким как учетные данные, настроенные в системе. Предоставляет разрешение на доступ к широкому диапазону функций, включая: • Вход в систему с помощью Management Client • Список текущих задач • Журналы серверов Также предоставляет доступ к следующим компонентам: • Службы удаленного подключения • Профили Smart Client • Профили Management Client • Matrix • Профили времени • Зарегистрированные серверы и API регистрации службы

Разрешение безопасности	Описание
	Данное разрешение также отображает некоторую конфиденциальную информацию для клиента: • Учетные данные для любого настроенного внешнего IDP • Учетные данные, IP-адреса и прочая информация для всех камер в VMS XProtect • Учетные данные для настроенного почтового сервера • Учетные данные для любого настроенного Matrix • Учетные данные, настроенные для функции взаимной связи • Учетные данные, настроенные для активации лицензии Данное разрешение не отображает учетные данные пользователей VMS XProtect. Сюда входят базовые пользователи, пользователи Windows и пользователи из внешних IDP.
Редактировать	Предоставляет разрешение на изменение данных в широком диапазоне функций, включая: • Опции • Управление лицензиями Разрешение также позволяет пользователям создавать, удалять и изменять следующие компоненты: • Службы удаленного подключения • Группы устройств • Matrix • Профили времени • Профили уведомлений • Зарегистрированные серверы Предоставляет разрешение на настройку диапазонов локальных IP-адресов при настройке сети на сервере записи.

Разрешение безопасности	Описание
Системный монитор	Предоставляет разрешение на просмотр данных системного монитора.
API статуса	Предоставляет разрешение на выполнение запросов к API статуса, расположенному на сервере записи. Это означает, что роль с данным разрешением имеет доступ для чтения статуса элементов, расположенных на сервере записи.
Управление иерархией федеративных сайтов	Предоставляет разрешение на подключение и отключение текущего сайта к другим сайтам в рамках иерархии федеративных сайтов. Если вы включите данное разрешение только на дочернем сайте, пользователь все равно сможет отсоединить сайт от родительского сайта.
Резервная копия конфигурации	Предоставляет разрешение на создание резервных копий конфигурации системы с помощью функций резервного копирования и восстановления системы.
Авторизация пользователей	Предоставляет разрешение на авторизацию пользователей в случае, когда им предложено выполнить второй вход в XProtect Smart Client или Management Client. На вкладке **Информация** вы определяете, требуется ли авторизация входа в систему для той или иной роли.
Управление безопасностью	Предоставляет разрешение на управление разрешениями для сервера управления. Также позволяет пользователям создавать, удалять и изменять следующие функции: • Роли • Базовые пользователи • Профили Smart Client • Профили Management Client

Серверы записи

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Редактировать	Предоставляет разрешение на редактирование свойств на серверах записи, за исключением параметров конфигурации сети, требующих разрешение на редактирование на сервере управления.
Удалить	Предоставляет разрешение на удаление серверов записи. Для этого необходимо также предоставить пользователю разрешения на удаление: • Группы безопасности оборудования, если оборудование было добавлено на сервер записи. Если какое-либо устройство на сервере записи содержит защиты доказательств, сервер записи можно удалить только когда он находится в автономном режиме (офлайн).
Управление оборудованием	Предоставляет разрешение на добавление оборудования на серверах записи.
Управление хранилищем	Предоставляет разрешение на управление контейнерами хранения на сервере записи, а именно на создание, удаление, перемещение и очистку контейнеров хранения.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для серверов записи.

Резервные серверы

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр серверов отказоустойчивости в Management Client и доступ к ним.
Редактировать	Предоставляет разрешение на создание, обновление, удаление, перемещение, а также включение или отключение серверов отказоустойчивости в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для серверов отказоустойчивости.

Серверы Mobile

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на управление всеми записями системы

Разрешение безопасности	Описание
	безопасности для этой части системы Management Client.
Редактировать	Предоставляет разрешение на изменение и удаление мобильных серверов в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для мобильных серверов.
Создать	Предоставляет разрешение на добавление мобильных серверов в систему.

Оборудование

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Редактировать	Предоставляет разрешение на изменение свойств оборудования.
Удалить	Предоставляет разрешение на удаление оборудования. Если какое-либо аппаратное устройство содержит защиты доказательств, оборудование можно удалить только когда сервер записи находится в автономном режиме (офлайн).
Команды	Предоставляет разрешение на отправку драйверам специальных команд и тем

Разрешение безопасности	Описание
драйвера	самым позволяет управлять функциями и конфигурацией самого устройства. Разрешение **Команды драйвера** предназначено только для специально разработанных встраиваемых расширений MIP в клиентах. Это разрешение не позволяет управлять задачами стандартной конфигурации.
Просмотр паролей	Предоставляет разрешение на просмотр паролей на аппаратных устройствах в диалоговом окне **Редактировать оборудование**.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для оборудования.

Камеры

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр камер в клиентах и Management Client.
Редактировать	Предоставляет разрешение на изменение свойств камер в Management Client. Также разрешение позволяет пользователям включать или отключать

Разрешение безопасности	Описание
	камеру.
Просмотр прямой трансляции	Предоставляет разрешение на просмотр видео с камер в режиме реального времени в клиентах и Management Client.
Просмотр видео в режиме реального времени с ограниченным доступом	Предоставляет разрешение на просмотр видео с камер в режиме реального времени и с ограниченным доступом в клиентах и Management Client.
Воспроизведение	Предоставляет разрешение на воспроизведение во всех клиентах записанного видео с камер.
Воспроизводить записи с ограничением	Предоставляет разрешение на воспроизведение во всех клиентах записанного видео с ограниченным доступом с камер.
Получить дистанционные записи	Предоставляет разрешение на получение в клиентах записей с камер на удаленных объектах или из накопителей для хранения данных на камерах.
Прочитать эпизоды	Предоставляет разрешение на чтение информации об эпизоде, связанной, например, с воспроизведением записанного видео в клиентах.
Интеллектуальный поиск	Предоставляет разрешение на использование функции интеллектуального поиска в клиентах.
Экспорт	Предоставляет разрешение на экспорт записей из клиентов.
Создать отметки	Предоставляет разрешение на создание отметок в записанном видео и видео в режиме реального времени в клиентах.
Прочитать отметки	Предоставляет разрешение на поиск и чтение сведений об отметках в клиентах.

Разрешение безопасности	Описание
Редактировать отметки	Предоставляет разрешение на редактирование отметок в клиентах.
Удаление закладок	Предоставляет разрешение на удаление отметок в клиентах.
Создать и расширить защиту доказательств	Предоставляет разрешение на создание и расширение защиты доказательств в клиентах.
Прочитать защиты доказательств	Предоставляет разрешение на поиск и чтение защиты доказательств в клиентах.
Удалить и снизить защиту доказательств	Предоставляет разрешение на удаление или снижение защиты доказательств в клиентах.
Создать и расширить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на создание и расширение ограничений в клиентах.
Считать ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на просмотр списка существующих ограничений в клиентах.
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на удаление и уменьшение ограничений в клиентах.
Начать запись вручную	Предоставляет разрешение на запуск записи видео вручную в клиентах.
Остановить запись вручную	Предоставляет разрешение на остановку записи видео вручную в клиентах.

Разрешение безопасности	Описание
Команды AUX	Предоставляет разрешение на использование вспомогательных (AUX) команд на камере из клиентов. **Команды AUX** позволяют пользователям, например, управлять стеклоочистителями на камере, подключенной с помощью видеокодера. Управление устройствами, связанными с камерой и подключенными через вспомогательные соединения, осуществляется из клиента.
Ручная сессия PTZ	Предоставляет разрешение на использование функций PTZ на PTZ-камерах в клиентах и Management Client.
Активировать исходную предустановку PTZ или профиль патрулирования	Предоставляет разрешение на перемещение PTZ-камер на исходные предустановки, запуск и остановку профилей патрулирования, а также приостановку патрулирование в клиентах и Management Client. Чтобы разрешить пользователю с этой ролью использовать на камере другие функции PTZ, включите разрешение **Ручная сессия PTZ**.
Управление исходными предустановками PTZ или профилями патрулирования	Предоставляет разрешение на добавление, изменение и удаление исходных предустановок и профилей патрулирования на PTZ-камерах в клиентах и Management Client. Чтобы разрешить пользователю с этой ролью использовать на камере другие функции PTZ, включите разрешение **Ручная сессия PTZ**.
Заблокировать/разблокировать исходные предустановки PTZ	Предоставляет разрешение на блокировку и разблокировку исходных предустановок в Management Client. Это запрещает или разрешает другим пользователям изменять исходные предустановки в клиентах и Management Client.

Разрешение безопасности	Описание
Зарезервировать сессии PTZ	Предоставляет разрешение на настройку PTZ-камер в режиме зарезервированной сессии PTZ в клиентах и Management Client. В зарезервированной сессии PTZ другие пользователи с более высоким PTZ-приоритетом не смогут осуществлять функции управления. Чтобы разрешить пользователю с этой ролью использовать на камере другие функции PTZ, включите разрешение **Ручная сессия PTZ**.
Освободить сеансы PTZ	Предоставляет разрешение на освобождение сессий PTZ других пользователей из Management Client. Вы всегда можете освобождать собственные сеансы PTZ — данное разрешение не требуется.
Удалить записи	Предоставляет разрешение на удаление сохраненных видеозаписей из системы с помощью Management Client.
Снять маски конфиденциальности	Предоставляет разрешение на временное снятие масок конфиденциальности в XProtect Smart Client. Это разрешение также позволяет другим пользователям XProtect Smart Client снимать маски конфиденциальности.  Снятие масок конфиденциальности применяется только к маскам конфиденциальности, снятие которых настроено в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для камеры.

Микрофоны

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр микрофонов в клиентах и Management Client.
Редактировать	Предоставляет разрешение на изменение свойств микрофона в Management Client. Также разрешение позволяет пользователям включать или отключать микрофоны.
Прослушать прямую трансляцию	Предоставляет разрешение на прослушивание из динамиков звука в реальном времени в клиентах и Management Client.
Прослушать звук в реальном времени с ограниченным доступом	Предоставляет разрешение на прослушивание из динамиков звука в реальном времени с ограниченным доступом в клиентах и Management Client.
Воспроизведение	Предоставляет разрешение на воспроизведение в клиентах записанной звуковой информации из микрофонов.
Воспроизводить записи с ограничением	Предоставляет разрешение на воспроизведение в клиентах записанной запрещенной звуковой информации из микрофонов.

Разрешение безопасности	Описание
Получить дистанционные записи	Предоставляет разрешение на получение записей в клиентах из микрофонов на удаленных объектах или из накопителей для хранения данных на камерах.
Прочитать эпизоды	Предоставляет разрешение на чтение информации об эпизоде, связанной, например, с вкладкой **Воспроизведение** в клиентах.
Экспорт	Предоставляет разрешение на экспорт записей из клиентов.
Создать отметки	Предоставляет разрешение на создание отметок в клиентах.
Прочитать отметки	Предоставляет разрешение на поиск и чтение сведений об отметках в клиентах.
Редактировать отметки	Предоставляет разрешение на редактирование отметок в клиентах.
Удаление закладок	Предоставляет разрешение на удаление отметок в клиентах.
Создать и расширить защиту доказательств	Предоставляет разрешение на создание или расширение защиты доказательств в клиентах.
Прочитать защиты доказательств	Предоставляет разрешение на поиск и чтение сведений о защите доказательств в клиентах.
Удалить и снизить защиту доказательств	Предоставляет разрешение на удаление или снижение защиты доказательств в клиентах.
Создать и расширить	Предоставляет разрешение на создание и

Разрешение безопасности	Описание
ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	расширение ограничений на микрофоны в клиентах.
Считать ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на просмотр списка существующих ограничений на микрофоны в клиентах.
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на удаление и уменьшение ограничений на микрофоны в клиентах.
Начать запись вручную	Предоставляет разрешение на запуск записи звука вручную в клиентах.
Остановить запись вручную	Предоставляет разрешение на остановку записи звука вручную в клиентах.
Удалить записи	Предоставляет разрешение на удаление сохраненных записей из системы.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для микрофонов.

Динамики

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр динамиков в клиентах и Management Client.
Редактировать	Предоставляет разрешение на изменение свойств динамиков в Management Client. Также разрешение позволяет пользователям включать или отключать динамики.
Прослушать прямую трансляцию	Предоставляет разрешение на прослушивание из динамиков звука в реальном времени в клиентах и Management Client.
Прослушать звук в реальном времени с ограниченным доступом	Предоставляет разрешение на прослушивание из динамиков звука в реальном времени с ограниченным доступом в клиентах и Management Client.
Говорить	Предоставляет разрешение говорить через динамики в клиентах.
Воспроизведение	Предоставляет разрешение на воспроизведение в клиентах записанной звуковой информации из динамиков.
Воспроизводить записи с ограничением	Предоставляет разрешение на воспроизведение в клиентах записанной

Разрешение безопасности	Описание
	звуковой информации из динамиков.
Получить дистанционные записи	Предоставляет разрешение на получение записей в клиентах из динамиков на удаленных объектах или из накопителей для хранения данных на камерах.
Прочитать эпизоды	Предоставляет разрешение на использование функции «Эпизоды» при просмотре записанной звуковой информации из динамиков в клиентах.
Экспорт	Предоставляет разрешение на экспорт записанной звуковой информации из динамиков в клиентах.
Создать отметки	Предоставляет разрешение на создание отметок в клиентах.
Прочитать отметки	Предоставляет разрешение на поиск и чтение сведений об отметках в клиентах.
Редактировать отметки	Предоставляет разрешение на редактирование отметок в клиентах.
Удаление закладок	Предоставляет разрешение на удаление отметок в клиентах.
Создать и расширить защиту доказательств	Предоставляет разрешение на создание или расширение защиты доказательств для защиты записанной звуковой информации в клиентах.
Прочитать защиты доказательств	Предоставляет разрешение на просмотр записанной звуковой информации, защищенной с помощью защиты доказательств в клиентах.

Разрешение безопасности	Описание
Удалить и снизить защиту доказательств	Предоставляет разрешение на удаление или снижение уровня защиты доказательств для защищенной звуковой информации в клиентах.
Создать и расширить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на создание и расширение ограничений на динамики в клиентах.
Считать ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на просмотр списка существующих ограничений на динамики в клиентах.
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на удаление и уменьшение ограничений на динамики в клиентах.
Начать запись вручную	Предоставляет разрешение на запуск записи звука вручную в клиентах.
Остановить запись вручную	Предоставляет разрешение на остановку записи звука вручную в клиентах.
Удалить записи	Предоставляет разрешение на удаление сохраненных записей из системы.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для динамиков.

Метаданные

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на получение метаданных в клиентах.
Редактировать	Предоставляет разрешение на изменение свойств метаданных в Management Client. Также разрешение позволяет пользователям включать или отключать устройства метаданных.
Наблюдение	Предоставляет разрешение на получение метаданных в режиме реального времени с устройств метаданных в клиентах.
Просмотр видео в режиме реального времени с ограниченным доступом	Предоставляет разрешение на получение метаданных в режиме реального времени с ограниченным доступом с устройств метаданных в клиентах.
Воспроизведение	Предоставляет разрешение на воспроизведение в клиентах записанных данных из устройств метаданных.
Воспроизводить записи с ограничением	Предоставляет разрешение на воспроизведение в клиентах записанных данных с ограниченным доступом из устройств метаданных.
Получить дистанционные	Предоставляет разрешение на получение

Разрешение безопасности	Описание
записи	записей в клиентах из устройств метаданных на удаленных объектах или из накопителей для хранения данных на камерах.
Прочитать эпизоды	Предоставляет разрешение на чтение информации об эпизоде, связанной, например, с вкладкой **Воспроизведение** в клиентах.
Экспорт	Предоставляет разрешение на экспорт записей в клиентах.
Создать и расширить защиту доказательств	Предоставляет разрешение на создание защиты доказательств в клиентах.
Прочитать защиты доказательств	Предоставляет разрешение на просмотр защиты доказательств в клиентах.
Удалить и снизить защиту доказательств	Предоставляет разрешение на удаление или снижение защиты доказательств в клиентах.
Создать и расширить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на создание и расширение ограничений на метаданные в клиентах.
Считать ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Предоставляет разрешение на просмотр списка существующих ограничений на метаданные в клиентах.
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального	Предоставляет разрешение на удаление и уменьшение ограничений на метаданные в клиентах.

Разрешение безопасности	Описание
времени и воспроизведение	
Начать запись вручную	Предоставляет разрешение на запуск записи метаданных вручную в клиентах.
Остановить запись вручную	Предоставляет разрешение на остановку записи метаданных вручную в клиентах.
Удалить записи	Предоставляет разрешение на удаление сохраненных записей из системы.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для метаданных.

Вход

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр устройств ввода в клиентах и Management Client.
Редактировать	Предоставляет разрешение на изменение свойств устройств ввода в Management Client. Также разрешение позволяет пользователям включать или

Разрешение безопасности	Описание
	отключать устройство ввода.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для устройств ввода.

Вывод

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр устройств вывода в клиентах.
Редактировать	Предоставляет разрешение на изменение свойств устройств вывода в Management Client. Также разрешение позволяет пользователям включать или отключать устройство вывода.
Активация	Предоставляет разрешение на активацию устройств вывода в клиентах.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для устройств вывода.

Smart Wall

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение для управления всеми разрешениями безопасности в XProtect Management Client.
Прочитать	Включает разрешение для просмотра видеостены в XProtect Smart Client.
Редактировать	Включает разрешение на изменение свойств определения Smart Wall в XProtect Management Client.
Удалить	Предоставляет разрешение удалять существующие определения Smart Wall в XProtect Management Client.
Управление	Предоставляет разрешение активировать и изменять определения Smart Wall, например изменять и активировать препозиции или применять камеры к видам в XProtect Smart Client и XProtect Management Client. Вы можете сопоставить команду **Управлять** с профилями времени, которые определяют, когда применяются пользовательские разрешения.
Создать Smart Wall	Предоставляет разрешение создавать новые определения Smart Wall в XProtect Management Client.
Управление безопасностью	Включает разрешение для управления всеми разрешениями безопасности в XProtect Management Client для определения Smart Wall.
Воспроизведение	Предоставляет разрешение на воспроизведение записанных

Разрешение безопасности	Описание
	данных с видеостены в XProtect Smart Client. Вы можете сопоставить команду **Воспроизвести** с профилями времени, которые определяют, когда применяются разрешения пользователя.

Группы отображений

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр групп отображений в клиентах и Management Client. Группы отображений создаются в Management Client.
Редактировать	Предоставляет разрешение на изменение свойств групп отображений в Management Client.
Удалить	Предоставляет разрешение на удаление групп отображений в Management Client.
Управление	Предоставляет разрешение на использование групп отображений в XProtect Smart Client, то есть на создание и удаление подгрупп и отображений.

Разрешение безопасности	Описание
Создать группу видов	Предоставляет разрешение на создание групп отображений в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для групп отображений.

Пользовательские события

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр пользовательских событий в клиентах.
Редактировать	Предоставляет разрешение на изменение свойств пользовательских событий в Management Client.
Удалить	Предоставляет разрешение на удаление пользовательских событий в Management Client.
Активировать	Предоставляет разрешение на активацию пользовательских событий в клиентах.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для пользовательских

Разрешение безопасности	Описание
	событий.
Создать пользовательское событие	Предоставляет разрешение на создание новых пользовательских событий в Management Client.

События аналитики

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр событий аналитики в Management Client.
Редактировать	Предоставляет разрешение на изменение свойств событий аналитики в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для событий аналитики.

Типичные события

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр типичных событий в клиентах и Management Client.
Редактировать	Предоставляет разрешение на изменение свойств типичных событий в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для типичных событий.

Matrix

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на выбор и отправку видео получателю Matrix из клиентов.
Редактировать	Предоставляет разрешение на изменение свойств Matrix в Management Client.
Удалить	Предоставляет разрешение на удаление Matrix в Management Client.

Разрешение безопасности	Описание
СоздатьMatrix	Предоставляет разрешение на создание нового Matrix в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для всех Matrix.

Правила

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр существующих правил в Management Client.
Редактировать	Предоставляет разрешение на изменение свойств правил и определение алгоритма правил в Management Client. Для этого разрешения необходимо, чтобы у пользователя были разрешения на чтение на всех устройствах, на которые распространяется правило.
Удалить	Предоставляет разрешение на удаление правил из Management Client. Для этого разрешения необходимо, чтобы у пользователя были разрешения на чтение на всех устройствах, на которые распространяется правило.
Создать правило	Предоставляет разрешение на создание новых правил в Management Client. Для этого разрешения необходимо, чтобы у пользователя были разрешения на

Разрешение безопасности	Описание
	чтение на всех устройствах, на которые распространяется правило.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для всех правил.

Объекты

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр других объектов в Management Client. Подключенные объекты соединяются с помощью Milestone Federated Architecture. Чтобы редактировать свойства, вам необходимы разрешения «Редактирование» на сервере управления на каждом объекте.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности на всех объектах.

Системный монитор

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр системных мониторов в XProtect Smart Client.
Редактировать	Предоставляет разрешение на изменение свойств системных мониторов в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для всех системных мониторов.

Поиск метаданных

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр функции **Использование метаданных** в Management Client и связанных настройках, однако не позволяет изменять настройки.
Редактирование конфигурации поиска метаданных	Предоставляет разрешение на включение или отключение категорий поиска метаданных, например метаданных о людях или транспортных средствах, в Management Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для поиска метаданных.

Поиск

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Читать общие операции поиска	Предоставляет разрешение на просмотр и открытие сохраненных общих операций поиска в XProtect Smart Client.
Создать общие операции поиска	Предоставляет разрешение на сохранение только что настроенных операций поиска как общих операций поиска XProtect Smart Client.
Изменить общие операции поиска	Предоставляет разрешение на изменение сведений или конфигурации сохраненных общих операций поиска в XProtect Smart Client, например имени, описания, камер и категорий поиска.
Удалить общие операции поиска	Предоставляет разрешение на удаление сохраненных общих операций поиска.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности в Management Client для поиска.

Сигналы тревоги

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Управление	Предоставляет разрешение на управление сигналами тревоги в Smart Client. Например, изменение приоритетов сигналов тревоги, повторное назначение сигналов тревоги другим пользователям, подтверждение сигналов тревоги, изменение состояния нескольких сигналов тревоги (например, с **Новый** на **Назначено**). Чтобы изменить настройки сигнала тревоги, вам также потребуется разрешение **Изменение настроек сигнала тревоги**. Вкладка **Сигналы тревоги и события** появляется в диалоговом окне **Опции** только если данное разрешение предоставлено.
Представление	Предоставляет разрешение на просмотр вкладки **Диспетчер сигналов тревоги** в XProtect Smart Client и получение сигналов тревоги и их настроек через API. Чтобы просмотреть сигналы тревоги в XProtect Smart Client, необходимо предоставить разрешение **Просмотр** хотя бы для одного определения тревоги. По умолчанию вы просматриваете сигналы тревоги из решений сторонних производителей.
Отключить оповещения	Предоставляет разрешение на отключение сигналов тревоги.
Получать уведомления	Предоставляет разрешение на получение уведомлений о сигналах тревоги в клиентах XProtect Mobile и XProtect Web Client.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для сигналов тревоги.
Изменение настроек сигнала тревоги	Предоставляет разрешение на изменение определений тревоги, состояний сигналов тревоги, категорий сигналов тревоги, звуков сигналов тревоги, хранения сигналов тревоги и хранения событий. Чтобы изменить настройки сигнала тревоги, также потребуется разрешение **Управление**.

Определения тревог

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Представление	Предоставляет разрешение на просмотр определений тревоги, состояний сигналов тревоги, категорий сигналов тревоги, звуков сигналов тревоги, хранения сигналов тревоги и хранения событий.
Запись	Включает разрешение **Просмотр**.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для определений тревоги.

Журналы серверов

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Чтение записей системного журнала	Предоставляет разрешение на просмотр записей системного журнала.
Чтение записей контрольного журнала	Предоставляет разрешение на просмотр записей контрольного журнала.
Чтение записей триггерного журнала	Предоставляет разрешение на просмотр записей журнала срабатываний по правилам.

Разрешение безопасности	Описание
Чтение конфигурации журнала	Предоставляет разрешение на чтение настроек журнала в меню **Инструменты** > **Опции** > **Журналы серверов**.
Обновление конфигурации журнала	Предоставляет разрешение на изменение настроек журнала в меню **Инструменты** > **Опции** > **Журналы серверов**.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для сигналов тревоги.

Управление доступом

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Редактировать	Предоставляет разрешение на изменение свойств систем управления доступом в Management Client.
Использовать контроль доступа	Предоставляет пользователю разрешение на использование любых функций, связанных с управлением доступом, в клиентах.
Просмотреть список владельцев карт	Позволяет пользователю просматривать список владельцев карт на вкладке **Управление доступом** в клиентах.
Получать уведомления	Позволяет пользователю получать уведомления о запросах доступа в клиентах.
Управление безопасностью	Предоставляет разрешение на управление разрешениями безопасности для всех систем управления доступом.

Распознавание номерного знака

Если ваша система выполняется с XProtect LPR, укажите следующие разрешения для пользователя:

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Использовать LPR	Предоставляет разрешение на использование всех функций распознавания номерного знака (LPR) в клиентах.
Управление списками соответствия номерных знаков	Предоставляет разрешение на добавление, импорт, изменение, экспорт и удаление списков соответствия номерных знаков в Management Client
Считать списки соответствия номерных знаков	Предоставляет разрешение на просмотр списков соответствия номерных знаков.
Управление безопасностью	Предоставляет разрешение на управление всеми разрешениями безопасности в Management Client для всех определений транзакций.

Источники транзакций

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр свойств для источников транзакций в Management Client.
Редактировать	Предоставляет разрешение на изменение свойств источников транзакций в Management Client.

Разрешение безопасности	Описание
Удалить	Предоставляет разрешение на удаление источников транзакций в Management Client.
Создать	Предоставляет разрешение на создание источников транзакций в Management Client.
Управление безопасностью	Предоставляет разрешение для управления всеми разрешениями безопасности в Management Client для всех источников транзакций.

Определение транзакции

Разрешение безопасности	Описание
Полный контроль	Включает разрешение на управление всеми записями системы безопасности для этой части системы.
Прочитать	Предоставляет разрешение на просмотр свойств для определений транзакций в Management Client.
Редактировать	Предоставляет разрешение на изменение свойств определений транзакций в Management Client.
Удалить	Предоставляет разрешение на удаление определений транзакций в Management Client.
Создать	Предоставляет разрешение на создание определений транзакций в Management Client.
Управление безопасностью	Предоставляет разрешение на управление всеми разрешениями безопасности в Management Client для всех определений транзакций.

Встраиваемые расширения MIP

С помощью MIP SDK сторонние разработчики могут подключать к вашей системе собственные встраиваемые расширения, например, для интеграции внешних систем управления доступом и других подобных задач.

Вкладка «Устройство» (роли)

Доступные функции зависят от используемой системы. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Вкладка **Устройство** позволяет указать, какие функции устройства (например, камеры) или группы устройств в XProtect Smart Client могут использовать пользователи/группы с выбранной ролью.

Действие необходимо повторить для каждого устройства. Вы также можете выбрать группу устройств и настроить разрешения ролей для всех устройств в группе в одно действие.

Вы можете устанавливать или снимать флажки, как было описано выше. Однако имейте в виду, что в этом случае настройка применяется ко **всем** устройствам в группе. Также можно выбрать отдельные устройства в группе и точно указать, к каким из них следует применить соответствующее разрешение.

Разрешения, связанные с камерой

Здесь настраиваются следующие разрешения для камер:

Имя	Описание
Прочитать	Выбранные камеры будут отображаться в клиентах.
Просмотр прямой трансляции	Позволяет в режиме реального времени просматривать видео с выбранных камер в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение предоставляется как часть разрешений приложения. Укажите профиль времени или оставьте значение по умолчанию.
Просмотр видео в режиме	Позволяет в режиме реального времени

Имя	Описание
реального времени с ограниченным доступом	просматривать видео с ограниченным доступом с выбранных камер в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение предоставляется как часть разрешений приложения. Укажите профиль времени или оставьте значение по умолчанию.
Воспроизведение > На временной шкале	Позволяет воспроизводить записанное видео с выбранных камер в клиентах. Укажите профиль времени или оставьте значение по умолчанию.
Воспроизведение > Воспроизвести до	Позволяет воспроизводить записанное видео с выбранных камер в клиентах. Если необходимо, укажите ограничение воспроизведения.
Воспроизводить записи с ограничением	Позволяет воспроизводить записанное видео с ограниченным доступом с выбранных камер в клиентах. Укажите профиль времени или оставьте значение по умолчанию.
Прочитать эпизоды	Позволяет читать информацию об эпизодах, например, связанную с обозревателем эпизодов, в клиентах.
Интеллектуальный поиск	Позволяет использовать функцию интеллектуального поиска в клиентах.
Экспорт	Позволяет пользователю экспортировать записи из клиентов.
Начать запись вручную	Позволяет запускать запись видео вручную с выбранных камер в клиентах.
Остановить запись вручную	Позволяет останавливать запись видео вручную с выбранных камер в клиентах.

Имя	Описание
Прочитать отметки	Позволяет выполнять поиск и чтение сведений об отметках в клиентах.
Редактировать отметки	Позволяет редактировать отметки в клиентах.
Создать отметки	Позволяет добавлять отметки в клиентах.
Удаление закладок	Позволяет удалять отметки в клиентах.
Команды AUX	Позволяет использовать вспомогательные команды из клиентов.
Создать и расширить защиту доказательств	Позволяет пользователю клиента: • Добавлять камеру к новым или существующим защитам доказательств. • Увеличивать срок действия существующей защиты доказательств • Увеличивать защищенный интервал существующей защиты доказательств. Требуются разрешения пользователя на все устройства, включенные в защиту доказательств.
Удалить и снизить защиту доказательств	Позволяет пользователю клиента: • Удалять камеру из существующей защиты доказательств • Удалять существующие защиты доказательств • Уменьшать срок действия существующей защиты доказательств

Имя	Описание
	• Уменьшать защищенный интервал существующей защиты доказательств. Требуются разрешения пользователя на все устройства, включенные в защиту доказательств.
Прочитать защиты доказательств	Позволяет пользователю клиента выполнять поиск и чтение сведений о защите доказательств.
Создать и расширить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Создавать ограничение на прямую трансляцию на камере • Создавать ограничение на воспроизведение для записей с камеры • Добавлять новую камеру в ограничение на прямую трансляцию или воспроизведение • Увеличивать период ограничения для записей с камеры Требуются разрешения пользователя на все устройства, включенные в ограничение.
Считать ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Просматривать список существующих ограничений на прямую трансляцию и воспроизведение на камере • Настраивать фильтры и выполнять поиск в списке ограничений на прямую трансляцию и воспроизведение на камере

Имя	Описание
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Удалять ограничение на прямую трансляцию на камере • Удалять ограничение на воспроизведение для записей с камеры • Уменьшать период ограничения для записей с камеры • Изменять настройки ограничения на прямую трансляцию или воспроизведение Требуются разрешения пользователя на все устройства, включенные в ограничение.

Разрешения, связанные с микрофоном

Здесь настраиваются следующие разрешения для микрофонов:

Имя	Описание
Прочитать	Выбранные микрофоны будут отображаться в клиентах.
Прослушать прямую трансляцию	Позволяет прослушивать звуковую информацию в режиме реального времени с выбранных микрофонов в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение предоставляется как часть разрешений приложения. Укажите профиль времени или оставьте значение по умолчанию.

Имя	Описание
Прослушать звук в реальном времени с ограниченным доступом	Позволяет прослушивать звук видеозаписей в режиме реального времени с ограниченным доступом с выбранных микрофонов в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение предоставляется как часть разрешений приложения. Укажите профиль времени или оставьте значение по умолчанию.
Воспроизведение > На временной шкале	Позволяет воспроизводить записанную звуковую информацию с выбранных микрофонов в клиентах. Укажите профиль времени или оставьте значение по умолчанию.
Воспроизведение > Воспроизвести до	Позволяет воспроизводить записанную звуковую информацию с выбранных микрофонов в клиентах. Если необходимо, укажите ограничение воспроизведения.
Воспроизводить записи с ограничением	Позволяет воспроизводить записанную звуковую информацию с ограниченным доступом с выбранных микрофонов в клиентах. Укажите профиль времени или оставьте значение по умолчанию.
Прочитать эпизоды	Позволяет читать информацию об эпизодах, например, связанную с обозревателем эпизодов, в клиентах.
Экспорт	Позволяет пользователю экспортировать записи из клиентов.
Начать запись вручную	Позволяет запускать запись звуковой информации вручную с выбранных микрофонов в клиентах.
Остановить запись	Позволяет останавливать запись звуковой

Имя	Описание
вручную	информации вручную с выбранных микрофонов в клиентах.
Прочитать отметки	Позволяет выполнять поиск и чтение сведений об отметках в клиентах.
Редактировать отметки	Позволяет редактировать отметки в клиентах.
Создать отметки	Позволяет добавлять отметки в клиентах.
Удаление закладок	Позволяет удалять отметки в клиентах.
Создать и расширить защиту доказательств	Позволяет пользователю клиента: • Добавлять микрофон к новым или существующим защитам доказательств. • Увеличивать срок действия существующей защиты доказательств • Увеличивать защищенный интервал существующей защиты доказательств. Требуются разрешения пользователя на все устройства, включенные в защиту доказательств.
Удалить и снизить защиту доказательств	Позволяет пользователю клиента: • Удалять микрофон из существующей защиты доказательств • Удалять существующие защиты доказательств • Уменьшать срок действия существующей защиты доказательств

Имя	Описание
	• Уменьшать защищенный интервал существующей защиты доказательств. Требуются разрешения пользователя на все устройства, включенные в защиту доказательств.
Прочитать защиты доказательств	Позволяет пользователю клиента выполнять поиск и чтение сведений о защите доказательств.
Создать и расширить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Создавать ограничение на прямую трансляцию на микрофоне • Создавать ограничение на воспроизведение аудиозаписей • Добавлять новый микрофон в ограничение на прямую трансляцию или воспроизведение • Увеличивать период ограничения для аудиозаписей Требуются разрешения пользователя на все устройства, включенные в ограничение.
Считать ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Просматривать список существующих ограничений на прямую трансляцию и воспроизведение на микрофоне

Имя	Описание
	• Настраивать фильтры и выполнять поиск в списке ограничений на прямую трансляцию и воспроизведение на микрофоне
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Удалять ограничение на прямую трансляцию на микрофоне • Удалять ограничение на воспроизведение аудиозаписей • Уменьшать период ограничения для аудиозаписей • Изменять настройки ограничения на прямую трансляцию или воспроизведение Требуются разрешения пользователя на все устройства, включенные в ограничение.

Разрешения, связанные с динамиком

Здесь настраиваются следующие разрешения для динамиков:

Имя	Описание
Прочитать	Выбранные динамики отображаются в клиентах.
Прослушать прямую трансляцию	Позволяет прослушивать звуковую информацию в режиме реального времени с выбранных динамиков в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение

Имя	Описание
	предоставляется как часть разрешений приложения. Укажите профиль времени или оставьте значение по умолчанию.
Прослушать звук в реальном времени с ограниченным доступом	Позволяет прослушивать звук видеозаписей в режиме реального времени с ограниченным доступом с выбранных динамиков в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение предоставляется как часть разрешений приложения. Укажите профиль времени или оставьте значение по умолчанию.
Воспроизведение > На временной шкале	Позволяет воспроизводить записанную звуковую информацию с выбранных динамиков в клиентах. Укажите профиль времени или оставьте значение по умолчанию.
Воспроизведение > Воспроизвести до	Позволяет воспроизводить записанную звуковую информацию с выбранных динамиков в клиентах. Если необходимо, укажите ограничение воспроизведения.
Воспроизводить записи с ограничением	Позволяет воспроизводить записанную звуковую информацию с ограниченным доступом с выбранных динамиков в клиентах. Укажите профиль времени или оставьте значение по умолчанию.
Прочитать эпизоды	Позволяет читать информацию об эпизодах, например, связанную с обозревателем эпизодов, в клиентах.
Экспорт	Позволяет пользователю экспортировать записи из клиентов.

Имя	Описание
Начать запись вручную	Позволяет запускать запись звуковой информации вручную с выбранных динамиков в клиентах.
Остановить запись вручную	Позволяет останавливать запись звуковой информации вручную с выбранных динамиков в клиентах.
Прочитать отметки	Позволяет выполнять поиск и чтение сведений об отметках в клиентах.
Редактировать отметки	Позволяет редактировать отметки в клиентах.
Создать отметки	Позволяет добавлять отметки в клиентах.
Удаление закладок	Позволяет удалять отметки в клиентах.
Создать и расширить защиту доказательств	Позволяет пользователю клиента: • Добавлять динамик к новым или существующим защитам доказательств • Увеличивать срок действия существующей защиты доказательств • Увеличивать защищенный интервал существующей защиты доказательств. Требуются разрешения пользователя на все устройства, включенные в защиту доказательств.
Удалить и снизить защиту доказательств	Позволяет пользователю клиента: • Удалять динамик из существующей защиты доказательств • Удалять существующие защиты доказательств

Имя	Описание
	• Уменьшать срок действия существующей защиты доказательств • Уменьшать защищенный интервал существующей защиты доказательств. Требуются разрешения пользователя на все устройства, включенные в защиту доказательств.
Прочитать защиты доказательств	Позволяет пользователю клиента выполнять поиск и чтение сведений о защите доказательств.
Создать и расширить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Создавать ограничение на прямую трансляцию на динамиках • Создавать ограничение на воспроизведение аудиозаписей • Добавлять новый микрофон в ограничение на прямую трансляцию или воспроизведение • Увеличивать период ограничения для аудиозаписей Требуются разрешения пользователя на все устройства, включенные в ограничение.
Считать ограничения на просмотр/прослушивание в режиме реального времени и	Позволяет пользователю клиента: • Просматривать список существующих ограничений на прямую трансляцию и воспроизведение на динамиках

Имя	Описание
воспроизведение	• Настраивать фильтры и выполнять поиск в списке ограничений на прямую трансляцию и воспроизведение на динамиках
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Удалять ограничение на прямую трансляцию на динамиках • Удалять ограничение на воспроизведение аудиозаписей • Уменьшать период ограничения для аудиозаписей • Изменять настройки ограничения на прямую трансляцию или воспроизведение  Требуются разрешения пользователя на все устройства, включенные в ограничение.

Разрешения, связанные с метаданными

Здесь настраиваются следующие разрешения для устройств метаданных:

Имя	Описание
Прочитать	Предоставляет разрешение на просмотр устройств метаданных и получение данных от них в клиентах.
Редактировать	Предоставляет разрешение на изменение свойств метаданных. Также разрешение позволяет пользователям включать или отключать устройства метаданных в

Имя	Описание
	Management Client с помощью MIP SDK.
Просмотр прямой трансляции	Предоставляет разрешение на просмотр метаданных в режиме реального времени с камер в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение предоставляется как часть разрешений приложения.
Просмотреть прямую передачу в режиме реального времени с ограничениями	Предоставляет разрешение на просмотр метаданных в режиме реального времени с ограниченным доступом с камер в клиентах. Для XProtect Smart Client требуется, чтобы у роли было разрешение на просмотр вкладки **Наблюдение** в клиентах. Это разрешение предоставляется как часть разрешений приложения.
Воспроизведение	Предоставляет разрешение на воспроизведение в клиентах записанных данных из устройств метаданных.
Воспроизводить записи с ограничением	Предоставляет разрешение на воспроизведение в клиентах записанных данных с из устройств метаданных с ограниченным доступом.
Прочитать эпизоды	Предоставляет разрешение на использование функции «Эпизоды» при просмотре записанных данных из устройств метаданных в клиентах.
Экспорт	Предоставляет разрешение на экспорт записанной звуковой информации из устройств метаданных в клиентах.

Имя	Описание
Создать и расширить защиту доказательств	Предоставляет разрешение на создание и расширение защиты доказательств для метаданных в клиентах.
Прочитать защиты доказательств	Предоставляет разрешение на просмотр защиты доказательств для метаданных в клиентах.
Удалить и снизить защиту доказательств	Предоставляет разрешение на удаление или снижение защиты доказательств для метаданных в клиентах.
Начать запись вручную	Предоставляет разрешение на запуск записи метаданных вручную в клиентах.
Остановить запись вручную	Предоставляет разрешение на остановку записи метаданных вручную в клиентах.
Создать и расширить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Создавать ограничение на прямую трансляцию на устройстве метаданных • Создавать ограничение на воспроизведение на устройстве метаданных • Добавлять новые метаданные в ограничение на прямую трансляцию или воспроизведение • Увеличивать период ограничения для устройств метаданных Требуются разрешения пользователя на все устройства, включенные в ограничение.

Имя	Описание
Считать ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Просматривать список существующих ограничений на прямую трансляцию и воспроизведение на устройстве метаданных • Настраивать фильтры и выполнять поиск в списке ограничений на прямую трансляцию и воспроизведение на устройстве метаданных
Удалить и уменьшить ограничения на просмотр/прослушивание в режиме реального времени и воспроизведение	Позволяет пользователю клиента: • Удалять ограничение на прямую трансляцию на устройстве метаданных • Удалять ограничение на воспроизведение на устройстве метаданных • Уменьшать период ограничения для устройств метаданных • Изменять настройки ограничения на прямую трансляцию или воспроизведение  Требуются разрешения пользователя на все устройства, включенные в ограничение.

Разрешения, связанные с устройствами ввода

Настройте следующие разрешения для устройств ввода:

Имя	Описание
Прочитать	Выбранные устройства ввода будут отображаться в клиентах.

Разрешения, связанные с устройствами вывода

Настройте следующие разрешения для устройств вывода:

Имя	Описание
Прочитать	Выбранные устройства вывода будут отображаться в клиентах. Отображаемые устройства вывода можно выбрать в списке в клиентах.
Активация	Выбранные устройства вывода можно активировать из Management Client и в клиентах. Укажите профиль времени или оставьте значение по умолчанию.

Вкладка PTZ (роли)

Разрешения для поворотных камер с трансфокатором (PTZ) настраиваются на вкладке **PTZ**. Вы можете указать функции, которые пользователи/группы могут использовать в клиентах. Также можно выбрать отдельные PTZ-камеры или группы устройств, содержащие PTZ-камеры.

Здесь можно настроить следующие разрешения для PTZ:

Имя	Описание
Ручная сессия PTZ	Определяет, может ли выбранная роль использовать функции PTZ и приостанавливать патрулирование на выбранной камере. Укажите профиль времени, выберите **Всегда** или оставьте значение по умолчанию, которое соответствует профилю времени по умолчанию, определенному на вкладке **Информация** для данной роли.
Активировать исходную предустановку PTZ или профиль патрулирования	Определяет, может ли выбранная роль перемещать выбранную камеру в исходные предустановки, запускать и останавливать профили патрулирования, а также приостанавливать патрулирование. Укажите профиль времени, выберите **Всегда** или оставьте значение по умолчанию, которое соответствует профилю времени по умолчанию, определенному на вкладке **Информация** для данной роли.

Имя	Описание
	Чтобы разрешить пользователю с этой ролью использовать на камере другие функции PTZ, включите разрешение **Ручная сессия PTZ**.
Приоритет PTZ	Определяет приоритет при управлениями PTZ-камерами. Если несколько пользователей системы наблюдения хотят одновременно управлять одной и той же PTZ-камерой, могут возникнуть конфликты. Этой ситуации можно избежать, указав приоритет использования выбранных PTZ-камер пользователями/группами с выбранной ролью. Укажите приоритет от 1 до 32 000, где 1 — самый низкий приоритет. Приоритет по умолчанию — 3000. Пользователь, роль которого обладает наивысшим приоритетом, может управлять PTZ-камерой.
Управление исходными предустановками PTZ или профилями патрулирования	Определяет разрешение на добавление, изменение и удаление исходных предустановок PTZ и профилей патрулирования на выбранной камере в Management Client и XProtect Smart Client. Чтобы разрешить пользователю с этой ролью использовать на камере другие функции PTZ, включите разрешение **Ручная сессия PTZ**.
Заблокировать/разблокировать исходные предустановки PTZ	Определяет, может ли роль блокировать и разблокировать исходные предустановки для выбранной камеры.
Зарезервировать сессии PTZ	Определяет разрешение на перевод выбранной камеры в режим зарезервированной сессии PTZ. В зарезервированной сессии PTZ или сессиях патрулирования другие пользователи с более высоким PTZ-приоритетом не смогут осуществлять функции управления. Чтобы разрешить пользователю с этой ролью использовать на камере другие функции PTZ, включите разрешение **Ручная сессия PTZ**.

Имя	Описание
Освободить сеансы PTZ	Определяет, может ли выбранная роль освобождать сессии PTZ других пользователей из Management Client. Вы всегда можете освобождать собственные сеансы PTZ — данное разрешение не требуется.

Вкладка «Речь» (роли)

Актуально только в том случае, если в системе используются динамики. Здесь настраиваются следующие разрешения для динамиков:

Имя	Описание
Говорить	Определяет, могут ли пользователи разговаривать через выбранные динамики. Укажите профиль времени или оставьте значение по умолчанию.
Приоритет речи	Когда несколько пользователей клиента хотят одновременно разговаривать через один и тот же динамик, могут возникнуть конфликты. Проблему можно решить, указав приоритет использования выбранных динамиков пользователями/группами с выбранной ролью. Укажите приоритет от **Очень низкого** до **Очень высокого**. Роли с наивысшим приоритетом смогут использовать динамик раньше других ролей. Если два пользователя с одной и той же ролью хотят разговаривать одновременно, применяется принцип очереди.

Вкладка «Дистанционные записи» (роли)

Здесь настраиваются следующие разрешения для дистанционных записей:

Имя	Описание
Получить дистанционные записи	Предоставляет разрешение на получение записей в клиентах с камер, микрофонов, динамиков и устройств метаданных на удаленных объектах или из накопителей для хранения данных на камерах.

Вкладка Smart Wall (роли)

С помощью ролей можно предоставить пользователям клиента разрешения, связанные с Smart Wall:

Имя	Описание
Прочитать	Позволяет пользователям просматривать выбранные Smart Wall в XProtect Smart Client.
Редактировать	Позволяет пользователям изменять выбранные Smart Wall в Management Client.
Удалить	Позволяет пользователям удалять выбранные Smart Wall в Management Client.
Управление	Позволяет пользователям применять макеты к выбранным Smart Wall в XProtect Smart Client и к активным препозициям.
Воспроизведение	Разрешить пользователям воспроизводить записанные данные на основе выбранных Smart Wall в XProtect Smart Client.

Вкладка «Внешнее событие» (роли)

Здесь настраиваются следующие внешние разрешения событий:

Имя	Описание
Прочитать	Позволяет пользователям выполнять поиск и просматривать выбранное внешнее системное событие в клиентах и Management Client.
Редактировать	Позволяет пользователям изменять выбранное внешнее системное событие в Management Client.
Удалить	Позволяет пользователям удалять выбранное внешнее системное событие в Management Client.
Активировать	Позволяет пользователям активировать выбранное внешнее системное событие в клиентах.

Вкладка «Группа отображений» (роли)

На вкладке **Группа отображений** можно указать, какие группы отображений могут использовать в клиентах пользователи и группы пользователей с выбранной ролью.

Здесь настраиваются следующие разрешения для групп отображений:

Имя	Описание
Прочитать	Предоставляет разрешение на просмотр групп отображений в клиентах и в Management Client. Группы отображений создаются в Management Client.
Редактировать	Предоставляет разрешение на изменение свойств групп отображений в Management Client.
Удалить	Предоставляет разрешение на удаление групп отображений в Management Client.
Управление	Предоставляет разрешение на использование групп отображений в XProtect Smart Client, то есть на создание и удаление подгрупп и отображений.

Вкладка «Серверы» (роли)

Настройка разрешений ролей на вкладке **Серверы** актуальна только в том случае, если ваша система работает в Milestone Federated Architecture.

Имя	Описание
Объекты	Предоставляет разрешение на просмотр выбранного объекта в Management Client. Подключенные объекты соединяются с помощью Milestone Federated Architecture. Чтобы редактировать свойства, вам необходимы разрешения «Редактирование» на сервере управления на каждом объекте.

Дополнительные сведения приведены в разделе Настройка Milestone Federated Architecture на стр. 105.

Вкладка Matrix (роли)

Если вы настроили получателей Matrix в своей системе, также можно настроить разрешения ролей Matrix. Из клиента вы можете отправить видео выбранным получателям Matrix. Получателей можно выбрать на вкладке Matrix.

Доступны следующие разрешения:

Имя	Описание
Прочитать	Определяет, могут ли пользователи и группы с выбранной ролью выбирать и отправлять видео получателю Matrix из клиентов.

Вкладка «Сигналы тревоги» (роли)

Если вы используете сигналы тревоги в конфигурации системы для обеспечения централизованного обзора и управления установкой (включая любые другие серверы XProtect), то на вкладке **Сигналы тревоги** можно указать разрешения на сигналы тревоги для пользователей и групп с выбранной ролью, которая необходима, например, для обработки сигналов тревоги в клиентах.

На вкладке **Сигналы тревоги** настраиваются следующие разрешения для сигналов тревоги:

Разрешение безопасности	Описание
Управление	Предоставляет разрешение на управление сигналами тревоги в Smart Client. Например, изменение приоритетов сигналов тревоги, повторное назначение сигналов тревоги другим пользователям, подтверждение сигналов тревоги, изменение состояния нескольких сигналов тревоги (например, с **Новый** на **Назначено**). Чтобы изменить настройки сигнала тревоги, вам также потребуется разрешение **Изменение настроек сигнала тревоги**. Вкладка **Сигналы тревоги и события** появляется в диалоговом окне **Опции** только если данное разрешение предоставлено.
Представление	Предоставляет разрешение на просмотр вкладки **Диспетчер сигналов тревоги** в XProtect Smart Client и получение сигналов тревоги и их настроек через API.

Разрешение безопасности	Описание
	Чтобы просмотреть сигналы тревоги в XProtect Smart Client, необходимо предоставить разрешение **Просмотр** хотя бы для одного определения тревоги. По умолчанию вы просматриваете сигналы тревоги из решений сторонних производителей.
Отключить оповещения	Предоставляет разрешение на отключение сигналов тревоги.
Получать уведомления	Предоставляет разрешение на получение уведомлений о сигналах тревоги в клиентах XProtect Mobile и XProtect Web Client.
Изменение настроек сигнала тревоги	Предоставляет разрешение на изменение определений тревоги, состояний сигналов тревоги, категорий сигналов тревоги, звуков сигналов тревоги, хранения сигналов тревоги и хранения событий. Чтобы изменить настройки сигнала тревоги, также потребуется разрешение **Управление**.

В разделе **Определения тревоги** вы можете настроить разрешения для конкретного определения тревоги:

Имя	Описание
Представление	Предоставляет разрешение на просмотр определений тревоги, состояний сигналов тревоги, категорий сигналов тревоги, звуков сигналов тревоги, хранения сигналов тревоги и хранения событий.
Запись	Включает разрешение **Просмотр**.

Вкладка «Управление доступом» (роли)

При добавлении или редактировании базовых пользователей, пользователей Windows или групп можно настроить параметры управления доступом:

Имя	Описание
Использовать контроль доступа	Предоставляет пользователю разрешение на использование любых функций, связанных с управлением доступом, в клиентах.
Просмотреть список владельцев карт	Позволяет пользователю просматривать список владельцев карт на вкладке **Управление доступом** в клиентах.
Получать уведомления	Позволяет пользователю получать уведомления о запросах доступа в клиентах.

Вкладка LPR (роли)

Если ваша система работает с XProtect LPR, укажите следующие разрешения для пользователя:

Имя	Описание
Использовать LPR	Предоставляет разрешение на использование всех функций распознавания номерного знака (LPR) в клиентах
Управление списками соответствия номерных знаков	Предоставляет разрешение на добавление, импорт, изменение, экспорт и удаление списков соответствия номерных знаков в Management Client
Считать списки соответствия номерных знаков	Предоставляет разрешение на просмотр списков соответствия номерных знаков.

Вкладка «Инциденты» (роли)

При наличии XProtect Incident Manager можно указать следующие разрешения для тех или иных ролей.

Чтобы предоставить роли администратора Management Client разрешения на просмотр свойств инцидентов и управление ими, выберите узел **Свойства инцидентов**.

Чтобы предоставить оператору XProtect Smart Client разрешение на просмотр заданных свойств инцидентов, выберите **Свойства инцидентов** и предоставьте разрешение **Просмотр**. Чтобы предоставить общие разрешения на просмотр проектов с инцидентами и управление ими, выберите

узел **Проект с инцидентом**. Разверните узел **Проект с инцидентом** и выберите один или несколько подузлов, чтобы предоставить разрешения для конкретных дополнительных функций или возможностей.

Имя	Описание
Управление	Разрешение на управление (просмотр, создание, редактирование и удаление) параметрами и свойствами, связанными с функцией, или просмотр элементов пользовательского интерфейса, представленных выбранным узлом в Management Client или XProtect Smart Client.
Представление	Разрешение на просмотр (но не создание, редактирование и удаление) параметров и свойств, связанных с функцией, просмотр заданных свойств инцидентов или просмотр элементов пользовательского интерфейса, представленных выбранным узлом в Management Client или XProtect Smart Client.

Вкладка MIP (роли)

С помощью MIP SDK сторонние разработчики могут подключать к вашей системе собственные встраиваемые расширения, например, для интеграции внешних систем управления доступом и других подобных задач. Встраиваемые расширения сторонних производителей будут иметь свои собственные настройки на отдельных вкладках.

Изменяемые настройки зависят от конкретного встраиваемого расширения. Пользовательские настройки для встраиваемого расширения можно найти на вкладке **MIP**.

Базовый пользователь (узел «Безопасность»)

В VMS Milestone XProtect существует два типа учетных записей пользователей: базовый пользователь и пользователь Windows.

Базовыми пользователями являются учетные записи пользователей, создаваемые в VMS Milestone XProtect. Это специальная системная учетная запись пользователя, предусматривающая аутентификацию на основе пароля и имени базового пользователя для отдельных пользователей.

Пользователи Windows — это учетные записи пользователей, добавляемые через Microsoft Active Directory.

Между базовыми пользователями и пользователями Windows есть несколько различий:

- Аутентификация базовых пользователей выполняется по комбинации имени пользователя и пароля, они создаются только для одной системы или сайта. Учтите, что даже если у базового пользователя на одном федеративном сайте то же имя и пароль, что у базового пользователя на другом федеративном сайте, базовый пользователь имеет доступ только к сайту, на котором он был создан.
- Аутентификация пользователей Windows в основана на имени для входа Windows, и они привязаны к компьютеру.

Узел «Информационная панель системы»

Узел «Информационная панель системы»

В разделе **Информационная панель системы** можно воспользоваться различными функциями управления системой и ее компонентами.

Имя	Описание
Текущая задача	Получите комплексное представление о выполняемых задачах на выбранном сервере записи.
Системный монитор	Отслеживайте состояние серверов и камер по заданным параметрам.
Пороговые значения системного монитора	Устанавливайте пороговые значения для отслеживаемых параметров на сервере и отслеживайте плитки, используемые в системном мониторе.
Защита доказательств	Получите комплексное представление обо всех защищенных данных в системе.
Отчеты о конфигурации	Распечатайте отчет с конфигурацией системы Вы можете решить, что именно будет включено в отчет.

Текущие задачи (раздел «Информационная панель системы»)

В окне **Текущие задачи** показан обзор текущих задач для выбранного сервера записи. Если вы запустили задачу, которая занимает много времени и выполняется в фоновом режиме, вы можете открыть окно **Текущие задачи** и проверить ход ее выполнения. К длительным задачам, запускаемым пользователем, относятся, например, обновления прошивки и перемещение оборудования. В окне доступна информация о времени начала, примерном времени завершения и ходе выполнения задачи.

Сведения в окне **Текущие задачи** не обновляются динамически. Это скорее снимок состояния текущих задач на момент открытия окна. Если окно оставалось открытым в течение какого-то времени, обновите данные, нажав кнопку **Обновить** в нижнем правом углу окна.

Системный монитор (узел «Информационная панель системы»)

Функции **Системного монитора** позволяют быстро получить визуальное представление текущего состояния серверов и камер системы.

Окно «Информационная панель системного монитора»

Плитки

В верхней части окна **Информационная панель системного монитора** есть цветные плитки, которые обозначают состояние оборудования серверов и камер в системе.

Плитки меняют состояние и, соответственно, цвет в зависимости от пороговых значений, заданных в узле **Пороговые значения системного монитора**. Дополнительные сведения приведены в разделе Пороговые значения системного монитора (узел «Информационная панель системы») на стр. 629. Задайте пороговые значения, которые будут указываться следующими цветами плиток:

Цвет плитки	Описание
Зеленый	Состояние **Норма**. Система работает штатно.
Желтый	Состояние **Предупреждение**. Как минимум один контролируемый параметр превышает пороговое значение для состояния **Норма**.
Красный	**Критическое** состояние. Как минимум один контролируемый параметр превышает пороговое значение для состояния **Норма** и **Предупреждение**.

Список оборудования с контролируемыми параметрами

Если нажать плитку, в нижней части окна **Информационная панель системного монитора** будет выведено состояние выбранного контролируемого параметра для каждой единицы оборудования, представленной плиткой.

Пример: Контролируемые параметры скорости прямой передачи с камеры достигли состояния «Предупреждение».

Настройка окна информационной панели

Выберите **Настроить** в верхнем правом углу окна, чтобы открыть окно **Настроить информационную панель**.

В окне **Настроить информационную панель** можно выбрать плитку, которую нужно создать, изменить или удалить. При создании и изменении плиток можно выбрать, какое оборудование и контролируемые параметры будут отображаться на плитке.

Окно «Сведения»

Выберите плитку, затем в списке оборудования с контролируемыми параметрами нажмите кнопку **Сведения** справа от камеры или сервера. В зависимости от выбранного оборудования вы сможете просматривать информацию о системе и создавать следующие отчеты:

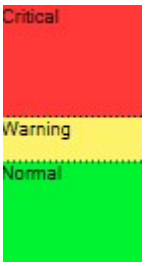
Оборудование	Информация
Сервер управления	Данные о: • Загрузка ЦП • Доступная память Выберите **История**, чтобы просмотреть архив состояний оборудования и создать отчет по указанным выше данным.
Серверы записи	Данные о: • Загрузка ЦП • Доступная память • Диски • Хранение • Сеть • Камеры Выберите **История**, чтобы просмотреть архив состояний оборудования и создать отчет по указанным выше данным.
Серверы записи обработки отказа	Данные о: • Загрузка ЦП • Доступная память

Оборудование	Информация
	• Серверы записи под мониторингом Выберите **История**, чтобы просмотреть архив состояний оборудования и создать отчет по указанным выше данным.
Серверы регистрации, серверы событий и прочее	Данные о • Загрузка ЦП • Доступная память Выберите **История**, чтобы просмотреть архив состояний оборудования и создать отчет по указанным выше данным.
Камеры	Данные о: • Хранение • Используемое место • Динамический режим: кадров/с (по умолчанию) • Запись: кадров/с • Динамический режим: формат видео • Запись: формат видео • Получено медиаданных (Кбит/с) • Доступная память Выберите имя камеры, чтобы просмотреть архив ее состояний и создать отчет о следующих данных: • Данные, полученные с камеры • Использование диска камерой

Если вы получаете доступ к данным системного монитора из операционной системы сервера, может появляться сообщение о **конфигурации усиленной безопасности Internet Explorer**. Перед продолжением выполните инструкции по добавлению страницы **системного монитора** в **зону надежных сайтов**.

Пороговые значения системного монитора (узел «Информационная панель системы»)

Используя пороговые значения системного монитора, можно задать и скорректировать пороговые значения изменения состояния оборудования, визуально отображаемого на плитках в **информационной панели системного монитора**. Например, при изменении состояния загрузки ЦП сервера с нормального (зеленый цвет) на состояние предупреждения (желтый цвет) или с состояния предупреждения (желтый цвет) на критическое состояние (красный цвет).



Пример сравнения пороговых значений для трех состояний

Можно менять пороговые значения для серверов, камер, дисков и хранилища. Для всех пороговых значений используются одинаковые кнопки и параметры.

Общие элементы пользовательского интерфейса

Кнопки и параметры	Описание	Устройство
Интервал расчета	При подключении к оборудованию часто случаются кратковременные сбои. Если задать интервал расчета равным 0, все эти сбои будут активировать оповещения об изменении состояния оборудования. Поэтому интервал расчета должен иметь некоторую величину. Если интервал расчета задать равным одной (1) минуте, вы будете получать оповещения, только если среднее значение за минуту превысит пороговое значение. При правильно заданном интервале расчета вы не будете получать ложные оповещения. Вам будут приходить оповещения только о длительных проблемах, таких как загрузка ЦП или потребление памяти. Изменение значений интервалов расчета описано в Изменение пороговых значений, задающих моменты изменения состояния оборудования на стр. 324.	сек.

Кнопки и параметры	Описание	Устройство
Advanced	С помощью кнопки **Advanced** можно определить пороговые значения и интервалы расчета для отдельных серверов, камер, дисков и хранилища. Дополнительные сведения приведены ниже.	-
Создать правило	Можно комбинировать события из **Системного монитора** и правил для активации действий, например при критической загрузке ЦП сервера или нехватке свободного места на диске. Дополнительные сведения приведены в разделах Правила и события (объяснение) на стр. 88 и Добавление правил на стр. 296.	-

Пороговые значения серверов

Пороговое значение	Описание	Устройство
Загрузка ЦП	Пороговые значения загрузки ЦП на отслеживаемых серверах.	%
Доступная память	Пороговые значения используемого ОЗУ на отслеживаемых серверах.	МБ
Декодирование NVIDIA	Пороговые значения использования декодирования NVIDIA на отслеживаемых серверах.	%
Память NVIDIA	Пороговые значения используемого ОЗУ NVIDIA на отслеживаемых серверах.	%
Визуализация NVIDIA	Пороговые значения использования визуализации NVIDIA на отслеживаемых серверах.	%

Пороговые значения камер

Пороговое значение	Описание	Устройство
Прямая передача FPS	Пороговые значения количества кадров в секунду для используемых камер при воспроизведении видео в режиме реального времени с отслеживаемых камер.	%
Запись: кадров/с	Пороговые значения количества кадров в секунду для используемых камер при записи видео на отслеживаемые камеры.	%
Используемое место	Пороговые значения пространства, которое используется отслеживаемыми камерами.	ГБ

Пороговые значения дисков

Пороговое значение	Описание	Устройство
Свободное пространство	Пороговые значения доступного пространства на отслеживаемых дисках.	ГБ

Пороговые значения хранилища

Пороговое значение	Описание	Устройство
Время хранения	Пороговое значение, которое показывает прогнозируемое время, когда в хранилище закончится место. Состояние отображается исходя из настроек системы и обновляется дважды в день.	Дни

Защита доказательств (раздел «Информационная панель системы»)

В разделе **Защита доказательств** узла **Информационная панель системы** содержится обзор всех защищенных данных текущей системы наблюдения.

Для всех видов защиты доказательств доступны следующие метаданные:

- Начальная и конечная дата для защищенных данных
- Пользователь, защищающий доказательство
- Момент прекращения защиты доказательства
- Место хранения данных
- Размер каждой единицы защиты доказательств

Вся информация, отображаемая в окне **Защита доказательств**, представляет собой снимки. Нажмите F5 для обновления информации.

Отчеты о конфигурации (раздел «Информационная панель системы»)

При установке и настройке ПО для управления видео (VMS) вы задаете много параметров: возможно, их потребуется задокументировать. Кроме того, по прошествии времени бывает трудно вспомнить, какие именно параметры вы изменяли с момента установки и первоначальной настройки или даже за последние месяцы. Именно поэтому в системе есть возможность напечатать отчет со всеми настроенными параметрами.

При создании и печати отчетов о конфигурации доступны следующие настройки:

Имя	Описание
Отчеты	Список элементов, которые можно включить в отчет о конфигурации.
Выбрать все	Добавляет в отчет о конфигурации все элементы списка **Отчеты**.
Очистить все	Удаляет из отчета о конфигурации все элементы списка **Отчеты**.
Титульный лист	Настройте титульную страницу отчета.
Форматирование	Форматирование отчета.
Удалить конфиденциальные данные	Удаляет из отчета о конфигурации персональную информацию, например адреса электронной почты и другие виды конфиденциальных данных, для обеспечения его соответствия GDPR. Информация о владельце лицензии всегда исключается из отчета.
Экспорт	Выберите место для сохранения отчета и создайте его в формате PDF.

Узел «Журналы сервера»

Узел «Журналы сервера»

Системные журналы (вкладка)

Каждая строка в журнале представляет собой запись журнала. Запись журнала содержит ряд информационных полей:

Имя	Описание
Уровень ведения журнала	Информация, предупреждение или ошибка.
Местное время	Временная отметка по местному времени сервера вашей системы.
Текст сообщения	Идентификационный номер зарегистрированного инцидента.
Категория	Тип зарегистрированного инцидента.
Тип источника	Тип оборудования, на котором возник зарегистрированный инцидент, например сервер или устройство.
Имя источника	Название оборудования, на котором произошел зарегистрированный инцидент.
Тип событий	Тип события, к которому относится зарегистрированный инцидент.

Контрольные журналы (вкладка)

Каждая строка в журнале представляет собой запись журнала. Запись журнала содержит ряд информационных полей:

Имя	Описание
Местное время	Временная отметка по местному времени сервера вашей системы.
Текст сообщения	Описание зарегистрированного инцидента.
Разрешение	Информация о том, имеется ли у удаленного пользователя разрешение на то или иное действие.
Категория	Тип зарегистрированного инцидента.
Тип источника	Тип оборудования, на котором возник зарегистрированный инцидент, например сервер или устройство.
Имя источника	Название оборудования, на котором произошел зарегистрированный инцидент.
Пользователь	Имя удаленного пользователя, у которого возник зарегистрированный инцидент.
Местоположение пользователя	IP-адрес или имя хоста компьютера, на котором у удаленного пользователя произошел зарегистрированный инцидент.

Журналы на основе правил (вкладка)

Каждая строка в журнале представляет собой запись журнала. Запись журнала содержит ряд информационных полей:

Имя	Описание
Местное время	Временная отметка по местному времени сервера вашей системы.
Текст сообщения	Описание зарегистрированного инцидента.
Категория	Тип зарегистрированного инцидента.

Имя	Описание
Тип источника	Тип оборудования, на котором возник зарегистрированный инцидент, например сервер или устройство.
Имя источника	Название оборудования, на котором произошел зарегистрированный инцидент.
Тип событий	Тип события, к которому относится зарегистрированный инцидент.
Имя правила	Имя правила, которое активирует запись в журнале.
Имя службы	Название службы, в которой произошел зарегистрированный инцидент.

Узел «Метаданные»

Метаданные и поиск по метаданным

Сведения об управлении устройствами хранения метаданных и настройке этих устройств см. в разделе Отображение или скрытие категорий поиска по метаданным и фильтров поиска на стр. 326.

Что такое метаданные?

Метаданные — это данные о данных, например данные, описывающие видеоизображение, содержимое объектов на изображении или место записи изображения.

Метаданные могут формироваться:

- самим устройством, передающим данным, например камерой, передающей видео;
- системой или интеграцией сторонних производителей через универсальный драйвер метаданных.

Поиск метаданных

Поиск по метаданным — это любой поиск видеозаписей в XProtect Smart Client, в котором применяются категории поиска и фильтры поиска, связанные с метаданными.

Категории поиска по метаданным в Milestone, применяемые по умолчанию:

- Местонахождение: Пользователи могут задавать географические координаты и радиус поиска относительно этих координат.
- Люди: Пользователи могут искать по полу и приблизительному росту и возрасту, а также, при желании, отображать результаты с лицами.
- Транспортные средства: Пользователи могут искать по цвету, скорости и типу транспортных средств, а также по конкретному номерному знаку.

Требования для поиска по метаданным

Для получения результатов необходимо иметь одно из следующего:

- Не менее одного устройства системы видеонаблюдения, которое может осуществлять видеоаналитику и правильно настроено.
- Служба обработки видео в системе видеонаблюдения, которая создает метаданные

В каждом из случаев метаданные должны соответствовать необходимому формату.

Дополнительные сведения см. в документации по интеграции поиска метаданных.

Узел «Управление доступом»

Свойства управления доступом

Вкладка «Общие настройки» (управление доступом)

Имя	Описание
Включить	По умолчанию системы включены, то есть они доступны в XProtect Smart Client для пользователей с соответствующими разрешениями, и система XProtect получает события управления доступом. Вы можете отключить систему, например на время технического обслуживания, чтобы исключить срабатывание излишних сигналов тревоги.
Имя	Имя интеграции управления доступом, которое отображается в приложении для управления и на клиентах. Вы можете перезаписать существующее имя и задать новое.
Описание	Описание интеграции системы управления доступом. Не обязательно.

Имя	Описание
Встраиваемое расширение интеграции	Тип системы управления доступом, выбранный при первоначальной интеграции.
Последнее обновление конфигурации	Дата и время последнего импорта конфигурации из системы управления доступом.
Обновить конфигурацию	Нажмите эту кнопку, чтобы отразить изменения конфигурации, внесенные в систему управления доступом, в XProtect, например если вы добавили или удалили дверь. Откроется сводка изменений в конфигурации системы управления доступом. Прежде чем применить новую конфигурацию, изучите список, чтобы убедиться, что параметры системы управления доступом правильно отражены.
Требуется имя пользователя оператора	Включите дополнительное имя пользователя для пользователей клиента, если система управления доступом поддерживает дифференцированные разрешения пользователей. Если включить этот параметр, система управления доступом в клиенте XProtect Mobile будет недоступна. Это параметр доступен только в том случае, если встраиваемое расширение интеграции поддерживает дифференцированные разрешения пользователей.

Имена и содержимое следующих полей импортируются из встраиваемого расширения интеграции. Ниже приведены примеры типичных полей:

Имя	Описание
Адрес	Введите адрес сервера, на котором размещается интегрированная система управления доступом.
Порт	Укажите номер порта на сервере, к которому подключена система управления доступом.
Имя пользователя	Введите имя пользователя согласно требованиям системы управления доступом. Этот пользователь будет администратором интегрированной системы в XProtect.
Пароль	Задайте пароль для этого пользователя.

Вкладка «Двери и соответствующие камеры» (управление доступом)

На этой вкладке отображаются связи между точками доступа к дверям и камерами, микрофонами и динамиками. Сопоставить камеры можно в мастере интеграции: эти настройки можно изменить в любой момент. Сопоставление с микрофонами и динамиками происходит автоматически по соответствующему микрофону или динамику на камере.

Имя	Описание
Двери	Списки доступных точек доступа для дверей, определенных в системе управления доступом, с группировкой по дверям. Для более удобной навигации между дверями отфильтруйте двери в системе управления доступом с помощью раскрывающегося списка в верхней части экрана. **Включено**: Двери с лицензией по умолчанию включены. Чтобы освободить лицензию, достаточно отключить дверь. **Лицензия**: Информация о наличии соответствующей лицензии на дверь или об истечении ее срока действия. Если дверь отключена, это поле будет пустым. **Удалить**: Нажмите **Удалить**, чтобы удалить камеру из точки доступа. Если удалить все камеры, автоматически снимается флажок у связанных с ними камер.
Камеры	Список камер, настроенных в системе XProtect. Выберите камеру из списка и перетащите ее в соответствующую точку доступа, чтобы связать точку доступа с камерой.

Вкладка «Событие контроля доступа» (управление доступом)

Категории событий обеспечивают возможность группировки событий. Конфигурация категорий событий влияет на функционирование управления доступом в системе XProtect, с ее помощью вы можете, к примеру, задать сигнал тревоги, который будет срабатывать по нескольким типам событий.

Имя	Описание
Событие контроля доступа	Список событий контроля доступа, импортированных из системы управления доступом. Встраиваемое расширение интеграции по умолчанию обеспечивает включение и отключение событий. После интеграции вы можете в любое время отключить или включить события.

Имя	Описание
	Если событие включено, оно сохраняется в базе данных событий XProtect, а также доступно, например, для фильтрации в XProtect Smart Client.
Тип источника	Устройство контроля доступа, которое активирует событие контроля доступа.
Категория события	Вы можете назначать событиям контроля доступа одну или несколько категорий событий или не назначать их вовсе. В процессе интеграции система автоматически сопоставляет соответствующие категории с событиями. Таким образом обеспечивается настройка системы XProtect по умолчанию. Сопоставление можно изменить в любой момент. Встроенные категории событий: • Доступ запрещен • Доступ разрешен • Запрос доступа • Тревога • Ошибка • Предупреждение Кроме того, выводятся события и категории событий, заданные встраиваемым расширением интеграции. Также можно задать пользовательские категории событий, подробнее см. в разделе **Пользовательские категории**. ⚠ При изменении категорий событий в XProtect Corporate убедитесь, что существующие правила управления доступом продолжают действовать.
Категории пользователя	Создание, изменение или удаление пользовательских категорий событий. Если встроенные категории событий не отвечают вашим требованиям, вы можете создать собственные. Например, при определении инициирующих событий для действий управления доступом. Категории универсальны для всех систем интеграции, добавленных в систему XProtect. Они обеспечивают возможность межсистемного взаимодействия,

Имя	Описание
	например при определении тревог. При удалении пользовательской категории событий, которая используется какой-либо интеграцией, появится соответствующее предупреждение. При подтверждении удаления все конфигурации, созданные с помощью этой категории, включая действия управления доступом, перестанут работать.

Вкладка «Уведомление запроса доступа» (управление доступом)

С ее помощью можно задать уведомления запроса доступа, которые будут появляться на экране XProtect Smart Client при наступлении определенного события.

Имя	Описание
Имя	Введите имя уведомления запроса доступа.
Добавить уведомление запроса доступа	Нажмите, чтобы добавить и настроить уведомления запроса доступа. Чтобы удалить уведомление, нажмите значок **X** в правой части. Если пользователь XProtect Smart Client авторизуется на родительском сайте в иерархии Milestone Federated Architecture, в XProtect Smart Client также отображаются уведомления запроса доступа с дочерних сайтов.
Сведения уведомления запроса доступа	Укажите, какие камеры, микрофоны и динамики будут отображаться в уведомлениях запроса доступа при наступлении определенного события. Задайте звуковой сигнал, который будет оповещать пользователя о всплывающем уведомлении.
Добавить команду	Выберите команды, которые должны быть доступны в виде кнопок в диалоговых окнах уведомления запроса доступа в XProtect Smart Client. Связанные команды запроса доступа: • Активация всех команд, связанных с операциями запроса доступа, доступных на исходном устройстве. Например, **Открыть дверь**.

Имя	Описание
	Все связанные команды: • Активация всех команд на исходном устройстве. Команда контроля доступа: • Активация выбранной команды контроля доступа. Команда системы: • Активация команды, предустановленной в системе XProtect. Чтобы удалить команду, нажмите значок **X** в правой части.

Вкладка «Владельцы карт» (управление доступом)

Используйте вкладку **Владельцы карт** для просмотра соответствующей информации в системе управления доступом.

Имя	Описание
Поиск владельца карты	Введите имя владельца карты: если такое имя существует, оно появится в списке.
Имя	Список имен владельцев карт, полученных из системы управления доступом.
Тип	Список типов владельцев карт, например: • Сотрудник • Охрана • Гость

Если ваша система управления доступом поддерживает добавление/удаление изображений в системе XProtect, вы можете добавить соответствующие фотографии для владельцев карт. Это удобно, если в системе управления доступом отсутствуют фотографии владельцев карт.

Имя	Описание
Выберите изображение	Укажите путь к файлу с фотографией владельца карты. Эта кнопка не доступна, если изображения обрабатываются системой управления доступом. Допустимые форматы файлов: BMP, PNG и JPG. Размер изображений корректируется, чтобы обеспечить оптимальное представление. Milestone рекомендует использовать квадратное изображение.
Удалить изображение	Нажмите, чтобы удалить изображение. Если изображение хранилось в системе управления доступом, оно будет отображаться после удаления.

Узел «Инциденты»

Свойства инцидента (узел «Инциденты»)

Ниже приведено описание параметров, связанных с XProtect Incident Manager.

На этих вкладках задаются все свойства инцидентов для операторов XProtect Smart Client:

- Типы
- Статусы
- Категории
- Категория 1–5

Все свойства инцидентов имеют следующие параметры:

Имя	Описание
Имя	Названия свойств инцидентов не обязательно должны быть уникальными. Однако в большинстве ситуаций целесообразно использовать уникальные и описательные названия таких свойств.
Описание	Дополнительное объяснение заданного свойства инцидента. Например, вы создали категорию *Местонахождение*. Описание категории может быть таким: *Где произошел инцидент?*

Узел Transact

Источники транзакций (узел Transact)

В следующей таблице описаны свойства источников транзакций.

Дополнительные сведения о добавлении источника см. в разделе Добавление источника транзакции (мастер).

Источники транзакций (свойства)

Имя	Описание
Включить	Снимите этот флажок, чтобы отключить источник транзакции. Поток данных транзакции остановится, при этом данные, которые уже импортированы, останутся на сервере событий. Транзакции из отключенного источника транзакции по-прежнему можно просматривать в XProtect Smart Client в течение периода хранения.  Даже для отключенного источника транзакций необходима соответствующая лицензия на источник транзакций.
Имя	Чтобы изменить имя, введите новое имя в этом поле.
Коннектор	Коннектор, выбранный при создании источника транзакции, изменить нельзя. Чтобы выбрать другой коннектор, потребуется создать новый источник транзакции и, работая с мастером, выбрать нужный коннектор.
Определение транзакции	Вы можете выбрать другое определение транзакции, которое определяет, каким образом преобразуются данные транзакции, полученные в транзакциях и их строках. Среди прочего настраивается следующее: • начало и окончание транзакции; • способ отображения транзакции в XProtect Smart Client.
Период хранения	Укажите период хранения данных транзакции на сервере событий (в днях). Период хранения по умолчанию составляет 30 дней. По истечении периода хранения данные автоматически удаляются. Это позволяет избежать

Имя	Описание
	проблем, связанных с превышением емкости базы данных. Минимальное значение — 1 день, а максимальное — 1000 дней.
Коннектор клиента TCP	Если выбран **коннектор клиента TCP**, задайте следующие параметры: • **Имя хоста** — введите имя хоста TCP-сервера, связанного с источником транзакции. • **Порт** — введите номер порта TCP-сервера, связанного с источником транзакции.
Коннектор последовательного порта	Если выбран **коннектор последовательного порта**, задайте следующие параметры и убедитесь, что они соответствуют параметрам источника транзакции: • **Последовательный порт** — выберите COM-порт. • **Скорость (бит/с)** — укажите скорость в битах, передаваемых в секунду. • **Равный** — укажите метод выявления ошибок при передаче (контроль четности). По умолчанию задан вариант **Нет**. • **Бит данных** — укажите число бит, представляющих один символ данных. • **Стоповые биты** — укажите число бит, которое будет указывать на передачу одного байта. Для большинства устройств требуется указать 1 бит. • **Подтверждение связи** — укажите метод подтверждения связи, определяющий протокол связи между источником транзакции и сервером событий

Определения транзакций (узел Transact)

В следующей таблице описаны свойства определений, которые используются с источниками транзакций.

Дополнительные сведения о создании и добавлении определений транзакций см. в разделе Создание и добавление определений транзакции.

Определения транзакций (свойства)

Имя	Описание
Имя	Укажите имя.
Кодировка	Выберите набор символов, используемых источником транзакции, например кассовым аппаратом. Это поможет XProtect Transact преобразовывать данные транзакции в понятный текст, с которым вы сможете работать при настройке определения. Если выбрать кодировку неправильно, данные могут отображаться в виде бессмысленного текста.
Начать сбор данных	Сбор данных транзакции из подключенного источника транзакции. Данные можно использовать для настройки определения транзакции. Дождитесь завершения хотя бы одной, а лучше нескольких транзакций.
Закончить сбор данных	После сбора достаточного объема данных для настройки определения нажмите эту кнопку.
Загрузить из файла	Чтобы импортировать данные из существующего файла, нажмите эту кнопку. Как правило, это созданный ранее файл в формате CAPTURE. Формат файла может быть другим. Важно то, чтобы кодировка импортируемого файла совпадала с кодировкой, выбранной для текущего определения.
Сохранить в файл	Нажмите эту кнопку, чтобы сохранить собранные необработанные данные в файл. Их можно будет использовать позднее.
Тип сопоставления	Выберите тип соответствия, который будет использоваться для поиска шаблона начала и шаблона остановки в собираемых необработанных данных: • Использовать точное совпадение. Функция поиска будет находить строки, которые содержат именно те символы, которые вы ввели в полях **Шаблон начала** и **Шаблон остановки**.

Имя	Описание
	• Использовать групповые символы. Функция поиска будет находить строки, которые содержат символы, введенные в полях **Шаблон начала** и **Шаблон остановки** в сочетании с подстановочными знаками (*, #, ?) *, заменяющими любое число символов. Например, если ввести «Начать тра*цию», функция поиска найдет строки, которые содержат текст «Начать транзакцию». # соответствует строго одной цифре. Например, если ввести «# арбуз», функция поиска найдет строки, содержащие, например «1 арбуз». ? соответствует строго одному символу. Например, поисковый запрос «Начать транз?кцию» можно использовать для поиска строк, содержащих «Начать транзакцию». • Использовать стандартное выражение. Этот тип сопоставления помогает находить строки, содержащие конкретные способы или типы обозначений, например формат даты или номер кредитной карты. Дополнительные сведения см. на сайте Microsoft (https://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/).
Необработанные данные	В этом разделе отображаются строки данных транзакции из подключенного источника транзакции.
Шаблон начала	Задайте шаблон начала, чтобы указать, где начинается транзакция. В поле **предварительного просмотра** отображаются горизонтальные линии, отмечающие начало и конец транзакции и разделяющие отдельные транзакции.
Шаблон остановки	Задайте шаблон остановки, чтобы указать, где заканчивается транзакция. Шаблон остановки задавать необязательно, но он может пригодиться, если получаемые данные, помимо фактических транзакций, содержат несущественную информацию, например о времени работы или специальных предложениях. Если не указывать шаблон остановки, окончание чека определяется в терминах начала следующего чека. Начало определяется текстом, введенным в поле **Шаблон начала**.
Добавить фильтр	Используйте кнопку **Добавить фильтры**, чтобы указать символы, которые

Имя	Описание
	требуется пропускать в XProtect Smart Client или заменять другими символами либо разрывом строки. Замена символов может быть удобна, когда строка источника транзакции содержит управляющие символы, не подлежащие печати. Добавление разрывов строк необходимо, чтобы чеки в XProtect Smart Client выглядели как исходные чеки.
Фильтрация текста	Отображает символы, выбранные в разделе **Необработанные данные**. Если вам известно, какие символы нужно пропускать или заменять, но они не отображаются в полученной строке необработанных данных, их можно ввести вручную в поле **Символ**. Если символ является управляющим символом, его значение потребуется ввести в шестнадцатеричном формате. Если символ содержит больше байт, используйте следующий формат значения: {XX} и {XX, XX,...}.
Действие	Для каждого добавляемого фильтра необходимо указать способ обработки выбранных символов. • «Пропустить» — выбранные символы отфильтровываются. • «Заменить» — выбранные символы заменяются заданными символами. • «Добавить разрыв строки» — выбранные символы заменяются разрывом строки.
Подстановка	Введите текст, который будет заменять выбранные символы. Применимо, только если выбрано действие **Заменить**.
Удалить управляющие символы, которые не определены в качестве текста фильтра	Удаление непечатаемых символов, которые остались после добавления фильтров. На панели **Необработанные данные** и **Предв. просмотр** можно увидеть, как изменяются строки данных транзакции при включении и отключении этого параметра.
Предв. просмотр	В разделе **Предв. просмотр** можно убедиться, что нежелательные символы выбраны и отфильтрованы. Выходные данные в этом разделе похожи на реальные чеки, отображаемые в XProtect Smart Client.

Узел «Сигналы тревоги»

Определения сигналов тревоги (раздел «Сигналы тревоги»)

Можно указать, что система должна создавать сигнал тревоги в XProtect Smart Client при фиксации произошедшего в ней событие. Прежде чем использовать сигналы тревоги, их необходимо задать. Это осуществляется на основании событий, зарегистрированных на серверах системы. Также можно использовать пользовательские события для активации сигналов тревоги, а также использовать одно и то же событие для активации нескольких разных сигналов тревоги.

Настройки определений сигналов тревоги:

Имя	Описание
Включить	По умолчанию определение сигналов тревоги включено. Для отключения снимите отметку в поле.
Имя	Имена сигналов тревоги могут быть неуникальными, однако в большинстве случаев удобно использовать уникальные и наглядные имена.
Инструкции	Введите описание сигнала тревоги, а также сведения о том, как следует решать проблему, ставшую его причиной. Этот текст отображается в XProtect Smart Client, когда пользователь работает с сигналом тревоги.
Событие срабатывания	Выберите сообщение о событии, которое будет использовано при активации сигнала тревоги. Выберите из двух раскрывающихся меню: • Первое раскрывающееся меню: Выберите тип события (например, событие аналитики или системное событие) • Второе раскрывающееся меню: Выберите конкретное сообщение о событии, которое необходимо использовать. Доступные сообщения зависят от типа события, выбранного вами в первом раскрывающемся меню
Источники	Укажите источники, из которых возникают события. Помимо камер и других устройств, в их число также могут входить источники, определяемые встраиваемыми расширениями (например, инструментами анализа видео (VCA) и MIP). Возможные варианты зависят от типа выбранного вами события.

Активатор сигнала тревоги:

Имя	Описание
Профиль времени	Выберите кнопку-переключатель **Профиль времени**, чтобы задать интервал времени, в течение которого будет активно определение сигнала тревоги. В списке отображается только тот профиль времени, который задан в разделе **Правила и события**. Если он не задан, доступен только вариант **Всегда**.
На основе события	Если вы хотите, чтобы сигнал тревоги срабатывал в зависимости от события, выберите эту кнопку-переключатель. После выбора укажите инициирующее и завершающее событие. Можно выбрать аппаратные события, заданные на камерах, видеосерверах и устройствах ввода. Также см. раздел Обзор событий. Также можно использовать глобальные/активируемые вручную события. Также см. раздел Пользовательские события (объяснение).

Требуется действие оператора:

Имя	Описание
Лимит времени	Выберите лимит времени для ситуаций, в которых требуется действие оператора. Значение по умолчанию — 1 минута. Лимит времени активен только после привязки события в раскрывающемся меню **События активированы**.
События запущены	Выберите, какое событие должно активироваться по истечении лимита времени.

Карты:

Имя	Описание
Представление диспетчера сигналов	Назначьте сигналу тревоги интеллектуальную карту или карту, когда сигнал тревоги включен в список XProtect Smart Client > **Диспетчер сигналов тревоги**.

Имя	Описание
тревоги	На интеллектуальной карте отображаются сигналы тревоги при их активации устройством, добавленным на интеллектуальную карту.

Прочее:

Имя	Описание
Связанные камеры	Выберите до 15 камер, которые будут включены в определение сигнала тревоги, даже если они сами по себе не активируют сигнал тревоги. Это может быть актуально, например, если в качестве источника сигнала тревоги выбрано внешнее сообщение о событии (например, об открытии двери). Задав определение одной или нескольких камер, расположенных около двери, можно привязать сделанные этими камерами записи инцидента к сигналу тревоги.
Исходный владелец сигнала тревоги	Выберите пользователя по умолчанию, ответственного за сигнал тревоги.
Исходный приоритет сигнала тревоги	Выберите приоритет для сигнала тревоги. Используйте эти приоритеты в XProtect Smart Client для задания степени важности сигнала тревоги.
Категория сигнала тревоги	Выберите категорию для сигнала тревоги, например **Ложная тревога** или **Требуется расследование**.
События, активированные сигналом тревоги	Задайте событие, которое сигнал тревоги может активировать в XProtect Smart Client.

Имя	Описание
Автоматически закрывать сигнал тревоги	Если требуется, чтобы определенное событие автоматически закрывало сигнал тревоги, поставьте отметку в этом поле. Не все события могут активировать сигналы тревоги. Снимите отметку в этом поле, чтобы отключить новый сигнал тревоги с самого начала.
Сигналы тревоги, назначаемые администраторам	Поставьте отметку в этом поле, чтобы включить пользователей с ролью администратора в список **Кому назначено**. Список **Кому назначено** находится в разделе сведений о сигнале тревоги на вкладке **Диспетчер сигналов тревоги** в XProtect Smart Client. Снимите отметку в поле, чтобы исключить пользователей с ролью администратора из списка **Кому назначено** и сократить его.

Настройки данных сигналов тревоги (раздел «Сигналы тревоги»)

При настройке данных сигналов тревоги необходимо указать следующее:

Вкладка «Уровни данных сигналов тревоги»

Приоритеты

Имя	Описание
Уровень	Добавьте новые приоритеты с выбранными вами номерами уровней или используйте/измените уровни приоритета, заданные по умолчанию (номера 1, 2 или 3). Эти уровни приоритета используются для настройки параметра **Исходный приоритет сигнала тревоги**.
Имя	Введите имя объекта. Вы можете создать такое их количество, которое необходимо.
Звук	Выберите звук, который будет сопровождать сигнал тревоги. Используйте один из

Имя	Описание
	звуков, заданных по умолчанию, или добавьте новые звуки в разделе **Настройки звуков**.
Повторить звук	Решите, должен ли звук воспроизводиться однократно либо повторяться в XProtect Smart Client до тех пор, пока оператор не нажмет имя сигнала в списке сигналов тревоги.
Включить уведомления на рабочем столе	Для каждого приоритета сигналов тревоги можно включить или отключить уведомления на рабочем столе. Если вы используете ПО для управления видео XProtect, которое поддерживает профили Smart Client, необходимо включить уведомления в требуемых профилях Smart Client. См. раздел Вкладка «Диспетчер сигналов тревоги» (профили Smart Client) на стр. 517.

Состояния

Имя	Описание
Уровень	В дополнение к уровням состояний, заданным по умолчанию (номера**1**, **4**, **9** и**11**, которые невозможно изменить или использовать повторно), добавьте новые состояния с номерами уровней, которым вы отдаете предпочтение. Эти уровни состояний видны в XProtect Smart Client только в пункте *Список сигналов тревоги*.

Категории

Имя	Описание
Уровень	Добавьте новые категории с номерами уровней, которым вы отдаете предпочтение. Эти уровни категорий используются для настройки параметра **Исходная категория сигнала тревоги**.  Уровень 99 зарезервирован для сигнала тревоги при оповещении о чрезвычайной ситуации в клиенте XProtect Mobile.
Имя	Введите имя объекта. Вы можете создать такое их количество, которое необходимо.

Вкладка «Настройка списка сигналов тревоги»

Имя	Описание
Доступные столбцы	Используйте >, чтобы выбрать столбцы, которые должны быть доступны в XProtect Smart Client в пункте *Список сигналов тревоги*. Используйте <, чтобы отменить выбор. В результате этого пункт **Выбранные столбцы** должен содержать элементы, которые необходимо включить.

Вкладка «Причины закрытия»

Имя	Описание
Включить	Выберите, чтобы перед закрытием сигналов тревоги требовалось указать причину их закрытия.
Причина	Добавьте причины закрытия, из которых пользователь может сделать выбор при закрытии сигналов тревоги. Например: *Нарушитель. Проблема решена* или *Ложная тревога*. Вы можете создать такое их количество, которое необходимо.

Параметры звука (узел «Сигналы тревоги»)

При настройке звука нужно указать следующее:

Имя	Описание
Звуки	Выберите звук, который будет сопровождать сигнал тревоги. В списке звуков есть ряд звуков Windows по умолчанию. Можно добавлять новые звуки (в формате WAV или MP3).
Добавить	Добавьте звуки. Выполните поиск звукового файла на устройстве и загрузите один или несколько файлов в формате WAV или MP3.
Удалить	Удалите выбранный звук из списка добавленных вручную звуков. Звуки по умолчанию нельзя удалить.
Проверка	Проверьте звук. Выберите звук из списка. Звук воспроизводится один раз.

Иерархия федеративных сайтов

Свойства федеративных сайтов

В этом разделе приведено описание вкладки **Общая информация** и вкладки **Родительский сайт**.

Вкладка «Общая информация»

Вы можете изменить некоторую информацию, связанную с сайтом, на который вы вошли.

Имя	Описание
Имя	Введите имя сайта.
Описание	Введите описание сайта.
URL-адреса	С помощью списка можно добавлять и удалять URL-адреса для этого сайта и указывать, являются ли они внешними адресами или нет. Внешние адреса могут быть доступны за пределами локальной сети.
Версия	Номер версии сервера управления этого сайта.
Служебная учетная запись	Служебная учетная запись, под которой работает сервер управления.
Время последней синхронизации	Время и дата последней синхронизации иерархии.
Статус последней синхронизации	Статус последней синхронизации иерархии. Возможны варианты **Успешно** или **Сбой**.

Вкладка «Родительский сайт»

На этой вкладке отображается информация о родительском сайте того сайта, на который вы в данный момент вошли. Вкладка не отображается, если у этого сайта отсутствует родительский сайт.

Имя	Описание
Имя	Имя родительского сайта.
Описание	Описание родительского сайта (необязательно).
URL-адреса	Список URL-адресов родительского сайта с указанием внешних адресов. Внешние адреса могут быть доступны за пределами локальной сети.
Версия	Номер версии сервера управления этого сайта.
Служебная учетная запись	Служебная учетная запись, под которой работает сервер управления.
Время последней синхронизации	Время и дата последней синхронизации иерархии.
Статус последней синхронизации	Статус последней синхронизации иерархии. Возможны варианты **Успешно** или **Сбой**.

Milestone Husky IVO System Health

Husky IVO System Health (узел)

Узел отображает данные о состоянии системы со всех устройств Husky IVO, которые успешно подключились к XProtect Management Client, с указанием имен их компьютеров и общего состояния каждого устройства.

Выберите название устройства в узле, чтобы отобразить основную статистику состояния системы для этого устройства на новой странице.

В узле могут отображаться только данные о состоянии системы от Husky IVO устройств.

Узел Husky IVO System Health доступен только после установки встраиваемого расширения Husky IVO System Health на машину XProtect Management Client.

Husky IVO System Health в настоящее время доступно как бета-версия. Внешний вид и функции окончательной версии могут отличаться от бета-версии.

Индикаторы состояния системы

Общие индикаторы состояния, отображаемые в узле:

- **Все в порядке**: Нет никаких обнаруженных проблем, о которых нужно сообщить.
- **Требует проверки**: Обнаружена одна или несколько проблем, требующих проверки.
- **Отсутствуют данные**: Невозможно сообщить о статусе из-за недостаточности данных.

Обновление данных о состоянии системы

Данные о состоянии системы будут автоматически обновляться через фиксированные промежутки в 5 минут, и их нельзя обновить вручную.

Дополнительные сведения приведены в разделе Husky IVO System Health на стр. 58

helpfeedback@milestone.dk

О компании Milestone

Milestone Systems — ведущий разработчик программного обеспечения для управления видео на открытой платформе.Наши технологии помогают миру увидеть, как обеспечить безопасность, защитить имущество и повысить эффективность бизнеса. Milestone Systems поддерживает сообщество пользователей открытой платформы для коллективного развития инновационных сетевых видеотехнологий.Мы предлагаем надежные и масштабируемые решения, зарекомендовавшие себя на более чем 150 000 площадок по всему миру. Компания Milestone Systems, основанная в 1998 году, является отдельной компанией в Canon Group. Дополнительные сведения приведены на сайте https://www.milestonesys.com/.