MAKE THE
WORLD SEE

Milestone Systems

Сервер XProtect® Mobile 2025 R1

Руководство администратора

milestone

Содержание

Copyright, товарные знаки и ограничение ответственности

Copyright © 2025 Milestone Systems A/S

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 версии сервера XProtect Mobile 2023 R3

Сведения о подключении.

- Проверьте, есть ли доступ к мобильному серверу из Интернета. См. раздел Сведения о подключении на стр. 14.

Сигналы тревоги:

- Добавьте тревоги «Оповещение о чрезвычайной ситуации», чтобы пользователи могли получать сигналы тревоги с наиболее высоким уровнем серьезности в клиенте XProtect Mobile. См. раздел Добавление сигналов тревоги «Оповещение о чрезвычайной ситуации» на стр. 54.

В версии сервера XProtect Mobile 2023 R2

Общий доступ к отметкам и видео в режиме реального времени.

- Чтобы отметками и видео в режиме реального времени можно было делиться в клиенте XProtect Mobile, нужно включить шифрование на сервере управления. См. раздел Требования к использованию функции «Поделиться» на стр. 10.

Уведомления.

- Сведения о регистрации устройства можно удалить из базы данных VMS. См. раздел Удаление одного или всех зарегистрированных устройств из списка «Зарегистрированные устройства» на стр. 41.

В версии сервера XProtect Mobile 2022 R3

Внешний поставщик удостоверений:

- Теперь с помощью внешнего IDP можно войти в XProtect Web Client и клиент XProtect Mobile. См. раздел Внешний IDP и XProtect Mobile на стр. 53

Управление мобильными устройствами (MDM).

- Теперь клиент XProtect Mobile поддерживает управлением мобильными устройствами. С помощью MDM можно защищать устройства, приложения и данные из управлять ими с одной консоли. Дополнительные сведения приведены в разделе Управление мобильными устройствами (MDM) на стр. 51

Push-уведомления.

- При включении этой функции появится предупреждение, что ваша система, возможно, не соответствует требованиям GDPR.

В версии сервера XProtect Mobile 2022 R2

Уведомления.

- По умолчанию уведомления отключены.

Установка.

- При установке Mobile Server можно подключиться к системе наблюдения, используя базового пользователя.

XProtect Mobile

XProtect Mobile состоит из пяти компонентов:

Клиент XProtect Mobile

Клиент XProtect Mobile — это мобильное приложение для наблюдения, которое можно установить и использовать на устройстве Android или Apple. Клиент XProtect Mobile можно устанавливать неограниченное количество раз.

XProtect Web Client

XProtect Web Client позволяет просматривать видео в режиме реального времени в вашем веб-браузере и загружать записи. XProtect Web Client устанавливается автоматически во время установки сервера XProtect Mobile.

Сервер XProtect Mobile

Сервер XProtect Mobile обрабатывает попытки входа в систему с клиента XProtect Mobile или XProtect Web Client.

Сервер XProtect Mobile распределяет видеопотоки, направленные с сервера записи к клиенту XProtect Mobile или XProtect Web Client. Таким образом обеспечивается защищенная конфигурация без подключения серверов записи к Интернету. Когда сервер XProtect Mobile получает видеопоток от серверов записи, он также проводит сложное преобразование кодеков и форматов для воспроизведения видео на мобильном устройстве.

Встраиваемое расширение XProtect Mobile

Встраиваемое расширение XProtect Mobile — это часть компонента XProtect Mobile Server. Встраиваемое расширение XProtect Mobile позволяет просматривать мобильные серверы в системе VMS и управлять ими из узла **Серверы** в XProtect Management Client.

Встраиваемое расширение XProtect Mobile устанавливается на любой компьютер с XProtect Management Client, откуда вы будете управлять мобильными серверами.

Mobile Server Manager

Используйте Mobile Server Manager, чтобы получить информацию о службе, проверить состояние службы Mobile Server, просмотреть журналы или сообщения о статусе и запустить и остановить службу.

В этом руководстве рассматривается сервер XProtect Mobile, встраиваемое расширение XProtect Mobile и Mobile Server Manager.

Требования и рекомендации

Перед установкой сервера XProtect Mobile

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

Milestone рекомендует устанавливать сервер XProtect Mobile на отдельный компьютер. Перед установкой и началом использования компонента XProtect Mobile Server проверьте следующее:

- Вы настроили камеры и представления в XProtect Management Client.
- Компьютер мобильного сервера сопоставляет имена хостов компьютеров, на которых запущены другие компоненты сервера VMS.
- Компьютер сервера управления сопоставляет имя хоста компьютера мобильного сервера.
- Система VMS установлена и работает.
- Вы настроили по крайней мере одного пользователя VMS. Для подключения к системе наблюдения роли, в которую добавлен пользователь, требуются следующие разрешения для сервера управления:
  - **Подключение**
  - **Прочитать**
  - **Редактировать**
- При обновлении системы убедитесь, что версия встраиваемого расширения XProtect Mobile совпадает с версией мобильного сервера. Если версии встраиваемого расширения и мобильного сервера не совпадают, в работе системы возможны нарушения.

Требования к настройке уведомлений

Для уведомления пользователей о событиях должны выполняться следующие условия:

- Нужно связать один или несколько сигналов тревоги с одним или несколькими событиями или правилами. Это требование не применяется к системным уведомлениям.
- У вас должно быть действующее соглашение Milestone Care™ с Milestone Systems.
- Ваша система должна иметь доступ к Интернету.

Дополнительная информация:

Настройка push-уведомлений на сервере XProtect Mobile на стр. 40

Вкладка «Уведомления» на стр. 28

Требования к настройке интеллектуального соединения Smart Connect

Для использования Smart Connect и проверки правильности настройки XProtect Mobile вам потребуется:

- Общедоступный IP-адрес для сервера XProtect Mobile. Адрес может быть статическим или динамическим, но обычно для этой цели хорошо подходят статические IP-адреса.
- Действующая лицензия Smart Connect
- Действующее соглашение Milestone Care™ с Milestone Systems

Требования к настройке двухэтапной проверки пользователей

Настройка двухэтапной проверки пользователей по электронной почте:

- Установите сервер SMTP.
- Добавьте пользователей и группы в систему XProtect в Management Client в узле **Роли** на панели **Навигация по сайту**. В соответствующей роли выберите вкладку **Пользователи и группы**.
- Если вы перешли на новую версию системы с предыдущей версии XProtect, перезапустите службу Mobile Server, чтобы включить двухэтапную проверку.

Дополнительная информация:

Настройка двухэтапной проверки пользователей по электронной почте на стр. 49

Вкладка «Двухэтапная проверка» на стр. 29

Требования к настройке Video Push

Для потоковой передачи видео с камеры мобильного устройства в систему наблюдения XProtect требуется:

- лицензия на устройство для каждого используемого канала.

Требования к прямому потоковому воспроизведению

XProtect Mobile поддерживает прямое потоковое воспроизведение в режиме трансляции. Для использования прямого потокового воспроизведения в XProtect Web Client и клиенте XProtect Mobile камеры должны быть настроены следующим образом:

- Камеры должны поддерживать кодек H.264 или H.265.

  XProtect Web Client поддерживает только H.264.

- Рекомендуется установить значение **Размер GOP 1 секунда**, а настройка **FPS** должна иметь значение выше **10** к/с.

Требования к использованию функции «Поделиться»

Пользователи могут делиться отметками и видео в режиме реального времени в приложении клиента XProtect Mobile. Эти функции доступны после:

- включения шифрования на сервере управления.

Установка

Установка сервера XProtect Mobile

После установки сервера XProtect Mobile можно использовать клиент XProtect Mobile и XProtect Web Client с вашей системой. Чтобы снизить общее потребление ресурсов системы на компьютере, на котором установлен сервер управления, установите сервер XProtect Mobile на отдельный компьютер.

На сервере управления предусмотрена встроенная общедоступная веб-страница установки. На этой веб-странице администраторы и конечные пользователи могут загружать и устанавливать необходимые компоненты системы XProtect с сервера управления или любого другого компьютера в системе.

Сервер XProtect Mobile устанавливается автоматически при выборе варианта установки «Один компьютер».

Загрузка программы установки сервера XProtect Mobile

1. Введите в браузер следующий URL-адрес: *http://[адрес сервера управления]/installation/admin*, где [адрес сервера управления] — это IP-адрес или имя хоста сервера управления.
2. Для программы установки сервера XProtect Mobile выберите **Все языки**.

Установка сервера XProtect Mobile

1. Запустите загруженный файл. Затем ответьте **Да** на все предупреждения.
2. Выберите язык программы установки. Затем нажмите **Продолжить**.
3. Ознакомьтесь и примите условия лицензионного соглашения. Затем нажмите **Продолжить**.
4. Выберите тип установки:
   - Выберите **Обычная**, чтобы установить сервер XProtect Mobile и встраиваемое расширение.
   - Выберите **Пользовательская**, чтобы установить только сервер или только встраиваемое расширение. Например, установка только встраиваемого расширения может потребоваться, если вы хотите использовать Management Client для управления серверами XProtect Mobile, но вам не нужен сервер XProtect Mobile на этом компьютере.

     Встраиваемое расширение XProtect Mobile требуется на компьютере с Management Client для управления серверами XProtect Mobile в Management Client.

5. Только для пользовательской установки: Выберите компоненты, которые нужно установить. Затем нажмите **Продолжить**.
6. Выберите учетную запись службы для мобильного сервера. Затем нажмите **Продолжить**.

   Чтобы впоследствии изменить или отредактировать данные учетной записи службы, потребуется переустановить мобильный сервер.

7. Только для пользовательской установки: Войдите, используя существующую учетную запись пользователя VMS, при подключении к системе наблюдения:
   - **Учетная запись службы** — это учетная запись, которую вы выбрали в шаге 8. Для подключения с помощью этой учетной записи убедитесь, что учетная запись службы входит в домен, к которому имеет доступ сервер управления.
   - **Базовый пользователь**. Если учетная запись службы не входит в домен, к которому у сервера управления есть доступ, выберите базового пользователя.

   Чтобы впоследствии изменить или отредактировать учетные данные базового пользователя, потребуется переустановить мобильный сервер.

   Нажмите **Продолжить**.
8. В поле **URL-адрес сервера** введите адрес основного сервера управления.

   Только для пользовательской установки: Укажите порты для обмена данными с мобильным сервером. Затем нажмите **Продолжить**. При обычной установке портам подключения присваиваются номера портов по умолчанию (8081 для порта HTTP и 8082 для порта HTTPS).
9. 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**.
10. Укажите шифрование мобильного сервера. Затем нажмите **Продолжить**.

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**.
- Между мобильным сервером и клиентами. Чтобы включить шифрование между мобильным сервером и клиентами, получающими потоки данных с этого сервера, выберите сертификат в разделе **Сертификат потоковых мультимедиа**.

Если не включить шифрование, некоторые функции в некоторых клиентах будут недоступны. Дополнительные сведения см. в разделе Требования к шифрованию мобильного сервера для клиентов.

Дополнительные сведения о настройке безопасного обмена данных в системе см.:

- Шифрование данных на мобильном сервере (объяснение)
- Руководство Milestone по сертификатам

Шифрование также можно включить после завершения установки с помощью значка Mobile Server Manager на панели задач операционной системы (см. Включить шифрование на мобильном сервере на стр. 35).

11. Выберите местонахождение файла и язык продукта, затем нажмите **Установить**.

    После завершения установки появится список успешно установленных компонентов.

Конфигурация

Параметры мобильного сервера

В Management Client можно настраивать и редактировать список параметров сервера XProtect Mobile. Получить доступ к этим параметрам можно в нижней панели инструментов раздела **Свойства** мобильного сервера. В этом разделе можно:

- включать и отключать общие конфигурации компонентов сервера (см. Вкладка «Общая информация» на стр. 15);
- Настройка параметров подключения сервера (см. Вкладка «Подключение» на стр. 18)
- Настройка функции интеллектуального соединения (см. Вкладка «Подключение» на стр. 18)
- просматривать текущий статус сервера и список активных пользователей (см. Вкладка «Состояние сервера» на стр. 20);
- настраивать параметры производительности для включения прямого потокового воспроизведения и адаптивного потокового воспроизведения или для установки ограничений перекодированных видеопотоков (см. Вкладка «Производительность» на стр. 22);
- настраивать параметры расследований (см. Вкладка «Исследования» на стр. 25);
- настраивать параметры Video Push (см. Вкладка Video Push на стр. 27);
- Настройка, включение и отключение системных уведомлений и push-уведомлений (см. Вкладка «Уведомления» на стр. 28)
- включать и настраивать дополнительный этап авторизации для пользователей (см. Вкладка «Двухэтапная проверка» на стр. 29).

Сведения о подключении

В следующих таблицах описаны статусы и сообщения мобильного сервера, которые отображаются на всех вкладках.

Сервер доступен через Интернет

Цвет	Статус	Описание
Оранжевый	Н/Д	Мобильный сервер не настроен так, чтобы к нему можно было получить доступ из местоположений за пределами локальной сети.

Цвет	Статус	Описание
Красный	Нет	Пользователи клиента XProtect Web Client и XProtect Mobile не могут подключиться к мобильному серверу из Интернета.
Зеленый	Да	Пользователи клиента XProtect Web Client и XProtect Mobile могут подключиться к мобильному серверу из Интернета.

Подключение к серверу

Цвет	Сообщение	Описание
Оранжевый	**Недопустимый сертификат HTTPS**	Встраиваемое расширение XProtect Mobile не распознает сертификат мобильного сервера.
Оранжевый	**HTTP/HTTPS недоступен**	XProtect Management Client не может получить доступ к мобильному серверу.
Красный	**HTTP/HTTPS не подключен**	XProtect Management Client обнаруживает мобильный сервер, но не может к нему подключиться.
Зеленый	**HTTP/HTTPS**	XProtect Management Client установлено соединение с мобильным сервером.

Вкладка «Общая информация»

В следующей таблице описаны параметры этой вкладки.

Общая информация

Имя	Описание
Имя сервера	Введите имя сервера XProtect Mobile.

Имя	Описание
Описание	Введите дополнительное описание сервера XProtect Mobile.
Мобильный сервер	Просмотр имени текущего выбранного сервера XProtect Mobile.

Функции

В следующей таблице описано, как управлять доступностью функций XProtect Mobile.

Имя	Описание
Включить XProtect Web Client	Включение доступа к XProtect Web Client. Эта функция включена по умолчанию.
Включить представление со всех камер для клиента XProtect Mobile	В этом представлении отображаются все камеры, которые пользователь может просматривать на сервере записи. Эта функция включена по умолчанию.
Включить отметки	Включение функции отметок для быстрого поиска эпизодов видео в клиенте XProtect Mobile и XProtect Web Client. Эта функция включена по умолчанию.
Включить действия (выходы и события)	Включение доступа к действиям в клиенте XProtect Mobile и XProtect Web Client. Эта функция включена по умолчанию. Если отключить эту функцию, пользователи клиента не смогут видеть выходные данные и события даже при правильных настройках.
Включить входящий звук	Включение функции входящей звуковой информации в XProtect Web Client и клиенте XProtect Mobile. Эта функция включена по умолчанию.

Имя	Описание
Включить PTT	Включение функции PTT в XProtect Web Client и клиенте XProtect Mobile. Эта функция включена по умолчанию.
Запретить встроенной роли Администраторы доступ к серверу XProtect Mobile	Включите эту функцию, чтобы запретить пользователям со встроенной ролью администратора доступ к видео на клиенте XProtect Mobile или XProtect Web Client.

Настройки журналов

Можно просмотреть информацию о параметрах журналов.

Имя	Описание
Расположение файла журнала	Отображение местоположения, где система хранит файлы журналов.
Срок хранения журналов	Отображение количества дней хранения журналов. По умолчанию срок составляет три дня.

Резервная копия конфигурации

Если в системе несколько серверов XProtect Mobile, функцию резервного копирования можно использовать для экспорта и импорта текущих параметров на серверах XProtect Mobile.

Имя	Описание
Импорт	Импорт XML-файла с новой конфигурацией сервера XProtect Mobile.
Экспорт	Экспорт конфигурации сервера XProtect Mobile. Система хранит конфигурацию в XML-файле.

Вкладка «Подключение»

Параметры на вкладке **Подключение** используются для решения следующих задач:

- Настройка параметров подключения на стр. 38
- Отправка пользователям электронных писем на стр. 39
- Включение подключений в сложной сети на стр. 38
- Включение функции обнаружения UPnP на маршрутизаторе на стр. 38

Дополнительные сведения приведены в разделе Smart Connect на стр. 37.

> Можно настроить, каким образом клиент XProtect Mobile и пользователи XProtect Web Client будут подключаться к серверу XProtect Mobile, если открыть **Server Configurator** в ходе установки или нажать правой кнопкой мыши значок Mobile Server Manager на панели задач после установки. Возможный тип подключения — HTTPS или HTTP. Дополнительные сведения приведены в разделе Включить шифрование на мобильном сервере на стр. 35.

Общая информация

Имя	Описание
Время ожидания клиента	Укажите период времени, в течение которого клиент XProtect Mobile и XProtect Web Client должны сообщить серверу XProtect Mobile, что они подключены и работают. Значение по умолчанию — 30 секунд. Milestone рекомендует не увеличивать время ожидания.
Включить обнаружение UPnP	Это позволит обнаруживать сервер XProtect Mobile в сети с помощью протоколов UPnP. Клиент XProtect Mobile включает функцию сканирования для обнаружения серверов XProtect Mobile с помощью UPnP.
Разрешить автоматическое сопоставление портов	Если сервер XProtect Mobile защищен брандмауэром, на маршрутизаторе требуется выполнить сопоставление портов, чтобы клиенты могли получить доступ к серверу из Интернета. Параметр **Разрешить автоматическое сопоставление портов** позволяет

Имя	Описание
	серверу XProtect Mobile самостоятельно выполнять сопоставление портов, если это предусмотрено на маршрутизаторе.
Включить Smart Connect	Интеллектуальное соединение Smart Connect позволяет проверить правильность настройки сервера XProtect Mobile без входа с мобильного устройства или планшета. Также упрощается процесс подключения для пользователей клиента.

Доступ в Интернет

Имя	Описание
Настроить пользовательский доступ к Интернету	Укажите **IP-адрес или имя хоста** и номер порта, который будет использоваться для подключения. Например, это можно сделать, если ваш маршрутизатор не поддерживает UPnP или если у вас цепочка маршрутизаторов.
• **HTTP** • **HTTPS**	Выберите тип подключения.
Выберите, чтобы получить IP-адрес динамически	Установите этот флажок, если у вас часто меняются IP-адреса.
Используйте только настроенные URL-адреса	Установите этот флажок, чтобы подключаться к мобильному серверу, используя только указанный пользователем

Имя	Описание
	IP-адрес или имя хоста.
Адреса серверов	Список всех URL-адресов, подключенных к мобильному серверу.

Уведомления Smart Connect

Имя	Описание
Приглашение по эл. почте для	Укажите адрес электронной почты получателя уведомлений об интеллектуальном соединении.
Язык эл. почты	Укажите язык электронной почты.
Smart Connect номер	Уникальный идентификатор, используемый пользователями мобильных устройств для подключения к серверу XProtect Mobile.
Соединение с Smart Connect	Ссылка, используемая пользователями мобильных устройств для подключения к серверу XProtect Mobile.

Вкладка «Состояние сервера»

Отображение подробных сведений о состоянии сервера XProtect Mobile. Подробные сведения доступны только для чтения:

Имя	Описание
Активность на сервере с	Время и дата последнего запуска сервера XProtect Mobile.

Имя	Описание
Загрузка ЦП	Текущая загрузка центрального процессора на мобильном сервере.
Ширина внешнего канала	Текущая используемая полоса пропускания между клиентом XProtect Mobile или XProtect Web Client и мобильным сервером.

Активные пользователи

Отображение подробных сведений о состоянии клиента XProtect Mobile или XProtect Web Client, которые в настоящее время подключены к серверу XProtect Mobile.

Имя	Описание
Имя пользователя	Имя пользователя для каждого клиента XProtect Mobile или пользователя XProtect Web Client, подключенного к мобильному серверу.
Состояние	Текущая связь между сервером XProtect Mobile и рассматриваемым клиентом XProtect Mobile или пользователем XProtect Web Client. Возможные состояния: • **Подключено**. Начальное состояние, когда клиенты и сервер обмениваются ключами и учетными данными для шифрования. • **Вход выполнен**. Клиент XProtect Mobile или пользователь XProtect Web Client вошел в систему XProtect.
Использование видеоканала (кБ/с)	Общая пропускная способность видеопотоков, которые в настоящее время открыты для каждого клиента XProtect Mobile или пользователя XProtect Web Client.
Использование аудиоканала (кБ/с)	Общая пропускная способность аудиопотоков, которые в настоящее время открыты для каждого пользователя XProtect Web Client.
Транскодированные	Общее количество перекодированных видеопотоков, которые в

Имя	Описание
видеопотоки	настоящее время открыты для каждого клиента XProtect Mobile или пользователя XProtect Web Client.
Прямые потоки	Общее количество прямых видеопотоков, которые в настоящее время открыты для каждого клиента XProtect Mobile или пользователя XProtect Web Client (только для XProtect Expert и XProtect Corporate).
Транскодированные аудиопотоки	Общее количество перекодированных аудиопотоков, которые в настоящее время открыты для каждого пользователя XProtect Web Client.

Вкладка «Производительность»

На вкладке **Производительность** можно задать следующие параметры и ограничения производительности сервера XProtect Mobile:

Параметры потоковой передачи видео (только для XProtect Expert или XProtect Corporate)

Имя	Описание
Включить прямое потоковое воспроизведение	Включите прямую потоковую передачу в XProtect Web Client и клиенте XProtect Mobile (только для XProtect Expert и XProtect Corporate). Эта функция включена по умолчанию.
Включить адаптивное потоковое воспроизведение	Включите адаптивное потоковое воспроизведение в XProtect Web Client и клиенте XProtect Mobile (только для XProtect Expert и XProtect Corporate). Эта функция включена по умолчанию.
Режимы потоковой передачи	После включения адаптивного потокового воспроизведения можно выбрать режим потоковой передачи из списка:

Имя	Описание
	• **Оптимизация качества видео (по умолчанию)** — функция выбирает поток с самым низким доступным разрешением, которое выше запрошенного разрешения или соответствует ему. • **Оптимизация производительности сервера** — функция уменьшает запрошенное разрешение, а затем выбирает поток с самым низким доступным разрешением, которое выше уменьшенного запрошенного значения или соответствует ему. • **Оптимизация разрешения для низкой пропускной способности** — функция выбирает поток с самым низким доступным разрешением (рекомендуется в сетях 3G и нестабильных сетях).

Ограничения транскодированных видеопотоков

Уровень 1

Уровень 1 — это ограничение, которое применяется к серверу XProtect Mobile по умолчанию. Все ограничения, установленные здесь, всегда применяются к перекодированным видеопотокам XProtect Mobile.

Имя	Описание
Уровень 1	Установите этот флажок, чтобы применить первый уровень ограничений к производительности сервера XProtect Mobile.
Макс. к/с	Задайте ограничение по максимальному количеству кадров в секунду (к/с) при отправке с сервера XProtect Mobile клиентам.
Макс. разрешение изображения	Задайте ограничение разрешения изображения при отправке с сервера XProtect Mobile клиентам.

Уровень 2

Если нужно задать другой уровень ограничений, отличный от уровня, заданного по умолчанию в пункте **Уровень 1**, установите флажок **Уровень 2**. Нельзя задать параметры, значения которых будут выше, чем у параметров на первом уровне. Например, если макс. значение к/с составляет 45 на **Уровне 1**, на **Уровне 2** макс. значение к/с может быть не выше 44.

Имя	Описание
Уровень 2	Установите этот флажок, чтобы применить второй уровень ограничений к производительности сервера XProtect Mobile.
Ограничение процессора	Задайте пороговое значение нагрузки центрального процессора на сервере XProtect Mobile до применения системой ограничений видеопотока.
Ограничение пропускной способности	Задайте пороговое значение нагрузки полосы пропускания на сервере XProtect Mobile до применения системой ограничений видеопотока.
Макс. к/с	Задайте ограничение по максимальному количеству кадров в секунду (к/с) при отправке с сервера XProtect Mobile клиентам.
Макс. разрешение изображения	Задайте ограничение разрешения изображения при отправке с сервера XProtect Mobile клиентам.

Уровень 3

Можно установить флажок **Уровень 3**, чтобы создать третий уровень ограничений. Нельзя задать параметры, значения которых будут выше, чем у параметров на **Уровне 1** и **Уровне 2**. Например, если **макс. значение к/с** составляет 45 на **Уровне 1** и 32 на **Уровне 2**, то на **Уровне 3 макс. значение к/с** может быть не выше 31.

Имя	Описание
Уровень 3	Установите этот флажок, чтобы применить третий уровень ограничений к производительности сервера XProtect Mobile.
Ограничение	Задайте пороговое значение нагрузки центрального процессора на сервере

Имя	Описание
процессора	XProtect Mobile до применения системой ограничений видеопотока.
Ограничение пропускной способности	Задайте пороговое значение нагрузки полосы пропускания на сервере XProtect Mobile до применения системой ограничений видеопотока.
Макс. к/с	Задайте ограничение по максимальному количеству кадров в секунду (к/с) при отправке с сервера XProtect Mobile клиентам.
Макс. разрешение изображения	Задайте ограничение разрешения изображения при отправке с сервера XProtect Mobile клиентам.

Системе нужно какое-то время для переключения с одного уровня на другой. Если пороговое значение для центрального процессора или полосы пропускания выше или ниже указанных уровней меньше чем на пять процентов, продолжает применяться текущий уровень.

Вкладка «Исследования»

Параметры расследований

Можно включить расследования, чтобы пользователи могли использовать клиент XProtect Mobile или XProtect Web Client для решения следующих задач:

- Доступ к записанному видео
- Расследование инцидентов
- Подготовка и загрузка видеодоказательств

Имя	Описание
Подключить исследования	Установите этот флажок, чтобы пользователи могли создавать расследования.

Имя	Описание
Папка исследований	Отображение местонахождения экспортированных видео, хранящихся на жестком диске.
Просмотр исследований, сделанных другими пользователями	Установите этот флажок, чтобы пользователи могли получать доступ к расследованиям, которые они не создавали.
Включить ограничение на размер папки исследований	Установите этот флажок, чтобы задать ограничение размера папки расследований и ввести максимальное количество мегабайт, которое может содержать эта папка. Размер по умолчанию — 2000 МБ.
Установить время хранения расследований	Установите этот флажок, чтобы задать время хранения расследований. По умолчанию время хранения составляет семь дней.
Форматы экспорта	Установите флажок формата экспорта, который вы хотите использовать. Доступные форматы экспорта: • **Формат AVI** • **Формат XProtect** • **Формат MKV** По умолчанию флажки не установлены.
Включить временные метки для экспорта AVI	Установите этот флажок, чтобы указывать дату и время загрузки AVI-файла.
Используемый кодек для экспорта AVI	Выберите, какой формат сжатия будет использоваться при подготовке пакетов AVI для загрузки. В зависимости от операционной системы доступные для выбора кодеки могут отличаться. Если вам не удается найти нужный кодек, можно добавить его в список, установив его на компьютер, на котором выполняется сервер XProtect Mobile.

Имя	Описание
Частота дискретизации звука для экспорта AVI	Выберите в списке соответствующую частоту дискретизации при добавлении звуковой информации в экспортируемое видео. По умолчанию частота дискретизации равна 160 000 Гц.

Исследования

Имя	Описание
Исследования	Список текущих расследований, которые настроены в системе. Если вы больше не хотите хранить расследования, используйте кнопку **Удалить** или **Удалить все**. Эта функция может пригодиться, если, например, вам нужно освободить дисковое пространство на сервере.
Подробности	Чтобы удалить отдельные видеофайлы, которые экспортировались для расследования, но не удалять само расследование, выберите расследование в списке. В группе **Подробности расследования** выберите значок удаления справа от **XProtect**, поля **AVI** или **MKV** для экспорта.

Вкладка Video Push

При включении Video Push можно задать следующие параметры:

Имя	Описание
Push-видеопоток	Включите Video Push на мобильном сервере.
Количество каналов	Количество включенных каналов Video Push в вашей системе XProtect.

Имя	Описание
Канал	Номер соответствующего канала. Не редактируется.
Порт	Номер порта для соответствующего канала Video Push.
MAC-адрес	MAC-адрес для соответствующего канала Video Push.
Имя пользователя	Введите имя пользователя, связанного с соответствующим каналом Video Push.
Имя камеры	Имя камеры, если камера определена.

После выполнения всех необходимых действий (см. Настройка Video Push для передачи видео на стр. 44) выберите **Найти камеры**, чтобы выполнить поиск соответствующей камеры.

Вкладка «Уведомления»

Используйте вкладку **Уведомления**, чтобы включать и отключать системные и push-уведомления.

По умолчанию уведомления отключены.

Если вы включили уведомления и настроили один или несколько сигналов тревоги и событий, XProtect Mobile будет уведомлять пользователей о событии. Если приложение открыто, уведомления приходят в XProtect Mobile на мобильном устройстве. Push-уведомления служат для оповещения пользователей при закрытом XProtect Mobile. Эти уведомления приходят на мобильное устройство.

Дополнительная информация: Включение отправки push-уведомлений на некоторые или все мобильные устройства на стр. 41

В следующей таблице описаны параметры этой вкладки.

Имя	Описание
Уведомления	Установите этот флажок, чтобы включить уведомления.
Сохранять регистрацию устройства	Установите этот флажок, чтобы сохранять информацию об устройствах и пользователях, которые подключаются к этому серверу. Система отправляет уведомления на эти устройства.

Имя	Описание
	Если снять этот флажок, список устройств удаляется. Чтобы пользователи снова начали получать уведомления, потребуется установить флажок, а пользователи должны будут снова подключить устройства к серверу.

Зарегистрированные устройства

Имя	Описание
Включено	Установите этот флажок, чтобы начать отправлять уведомления на устройство.
Название устройства	Список мобильных устройств, которые подключены к этому серверу. Можно включить или отключить отправку уведомлений на определенные устройства, установив или сняв флажок **Включено**.
Пользователь	Имя пользователя, который будет получать уведомления.

Вкладка «Двухэтапная проверка»

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/).

Используйте вкладку **Двухэтапная проверка**, чтобы включить дополнительный этап входа в систему для пользователей:

- приложения XProtect Mobile на мобильных устройствах iOS или Android.
- XProtect Web Client

Первый этап проверки — ввод пароля. Второй этап проверки — ввод проверочного кода, который можно отправлять пользователям по электронной почте.

Дополнительные сведения приведены в разделе Настройка двухэтапной проверки пользователей по электронной почте на стр. 49.

В следующих таблицах описаны параметры этой вкладки.

Параметры поставщика > **Электронная почта**

Имя	Описание
Сервер SMTP	Для отправки электронных писем для двухэтапной проверки введите IP-адрес или имя хоста сервера SMTP.
Порт сервера SMTP	Укажите порт сервера SMTP для отправки электронных писем. По умолчанию без SSL используется номер порта 25, с SSL — 465.
Использовать SSL	Установите этот флажок, если ваш сервер SMTP поддерживает шифрование SSL.
Имя пользователя	Укажите имя пользователя для входа на сервер SMTP.
Пароль	Укажите пароль для входа на сервер SMTP.
Использовать безопасную проверку пароля (SPA)	Установите этот флажок, если ваш сервер SMTP поддерживает SPA.
Адрес электронной почты отправителя	Укажите адрес электронной почты для отправки проверочных кодов.
Тема сообщения электронной почты	Укажите тему электронного письма. Пример: Ваш код двухэтапной проверки.
Текст сообщения электронной почты	Введите сообщение, которое хотите отправить. Пример: Ваш код — {0}. Если вы забудете добавить переменную {0}, код добавится в конце текста по умолчанию.

Параметры проверочного кода

Имя	Описание
Время ожидания повторного подключения (0–30 минут)	Укажите период, в течение которого пользователям клиента XProtect Mobile не нужно повторно выполнять вход, например в случае отключения сети. Период по умолчанию — три минуты. Этот параметр не распространяется на XProtect Web Client.
Срок действия кода истекает через (1–10 минут)	Укажите период, в течение которого пользователь может использовать полученный проверочный код. По истечении этого периода код становится недействительным, и пользователь должен запросить новый код. Период по умолчанию — пять минут.
Количество попыток ввода кода (1–10 попыток)	Укажите максимальное количество попыток ввода кода до того, как полученный код станет недействительным. По умолчанию дано три попытки.
Длина кода (4–6 символов)	Укажите количество символов кода. Длина по умолчанию — шесть символов.
Состав кода	Укажите степень сложности кода, который должна генерировать система. Можно выбрать следующие варианты: • **Латинские прописные буквы (A-Z)** • **Латинские строчные буквы (a-z)** • **Цифры (0-9)** • **Специальные символы (!@#...)**

Параметры пользователя

Имя	Описание
Пользователи и	Список пользователей и групп, добавленных в систему XProtect.

Имя	Описание
группы	Если группа настроена в Active Directory, мобильный сервер использует данные Active Directory, например адреса электронной почты. Группы Windows не поддерживают двухэтапную проверку.
Метод проверки	Выберите параметры проверки для каждого пользователя или группы. Можно выбрать следующие варианты: • **Вход в систему невозможен** — пользователь не может войти. • **Двухэтапная верификация отсутствует** — пользователь должен ввести имя пользователя и пароль • **Электронная почта** — помимо имени пользователя и пароля, пользователь должен ввести проверочный код.
Сведения о пользователе	Введите адрес электронной почты, на который каждый пользователь будет получать коды.

Прямое потоковое воспроизведение

XProtect Mobile поддерживает прямое потоковое воспроизведение в режиме трансляции.

Прямое потоковое воспроизведение — это технология потоковой передачи видео, передающая видео из системы XProtect на клиенты напрямую в кодеке H.264, поддерживаемом большинством современных IP-камер. Клиент XProtect® Mobile также поддерживает кодек H.265. Прямое потоковое воспроизведение не требует перекодирования и поэтому позволяет снизить нагрузку на систему XProtect.

Технология прямого потокового воспроизведения является противоположностью параметра перекодирования в XProtect, когда система XProtect декодирует видео из кодека, используемого камерой, в JPEG-файлы. Включение этой функции позволяет снизить потребление ресурсов ЦП для той же конфигурации камер и видеопотоков. Прямое потоковое воспроизведение также повышает производительность потоковой передачи оборудования (максимум в пять раз), передающего несколько параллельных видеопотоков, по сравнению с перекодированием.

Для передачи видео с камер, которые поддерживают кодек H.265, непосредственно в клиент XProtect Mobile можно также использовать функцию прямого потокового воспроизведения.

В Management Client можно включить или отключить прямое потоковое воспроизведение для клиентов (см. Параметры мобильного сервера на стр. 14).

Видеопоток переключается с прямого потокового воспроизведения на перекодирование в следующих случаях:

- Функция прямого потокового воспроизведения отключена в Management Client, или не соблюдены требования (см. Требования к прямому потоковому воспроизведению на стр. 9).
- На камерах, передающих потоковое видео, используется кодек, отличный от H.264 (для всех клиентов) или от H.265 (только для клиентов XProtect Mobile).
- Воспроизведение видео не начинается в течение более 10 секунд.
- На камере, передающей потоковое видео, задана частота кадров «один кадр в секунду» (1 FPS).
- Потеряно соединение с сервером или камерой.
- Вы используете функцию конфиденциальной маскировки при трансляции видео.

Адаптивное потоковое воспроизведение

XProtect Mobile поддерживает адаптивное потоковое воспроизведение в режиме трансляции.

Адаптивное потоковое воспроизведение удобно при просмотре нескольких транслируемых видеопотоков в одном представлении камер. Эта функция оптимизирует производительность сервера XProtect Mobile и повышает скорость декодирования и производительность устройств, на которых выполняется клиент XProtect Mobile и XProtect Web Client.

Для адаптивного потокового воспроизведения на камерах должно быть определено несколько потоков с разным разрешением. В таком случае функция обеспечивает следующие преимущества:

- Оптимизация качества видео — функция выбирает поток с самым низким доступным разрешением, которое выше запрошенного разрешения или соответствует ему.
- Оптимизация производительности сервера — функция уменьшает запрошенное разрешение, а затем выбирает поток с самым низким доступным разрешением, которое выше уменьшенного запрошенного значения или соответствует ему.
- Оптимизация разрешения для низкой пропускной способности — функция выбирает поток с самым низким доступным разрешением (рекомендуется в сетях 3G и нестабильных сетях).

При увеличении всегда запрашивается видеопоток с максимально высоким доступным разрешением.

Снижение разрешения запрошенного видеопотока часто позволяет уменьшить объем передаваемых данных. Объем передаваемых данных также зависит от других параметров конфигурации видеопотоков.

Включить или отключить адаптивное потоковое воспроизведение и настроить предпочтительный режим потокового воспроизведения для функции можно на вкладке **Производительность** в параметрах мобильного сервера в Management Client (см. Параметры мобильного сервера на стр. 14).

Шифрование данных на мобильном сервере (объяснение)

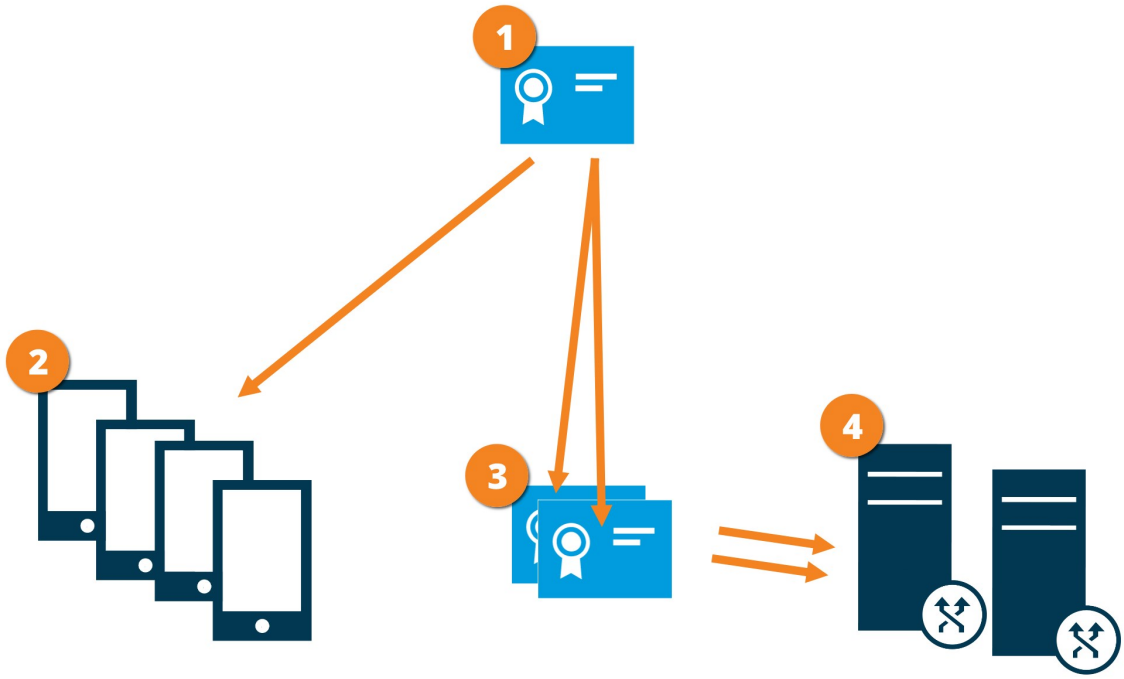
В целях обеспечения безопасности Milestone рекомендует настроить безопасный обмен данными между мобильным сервером и клиентами при управлении параметрами учетных записей пользователей.

Если при использовании HTTP-подключения шифрование не включено, функция PTT в XProtect Web Client будет недоступна.

В VMS XProtect включение и отключение шифрования выполняется для каждого мобильного сервера. Включив шифрование на мобильном сервере, можно использовать зашифрованные подключения ко всем клиентам, службам и модулям интеграции, получающим потоки данных.

Распространение сертификатов для мобильных серверов

На рисунке показан общий принцип подписывания, настройки доверия и распространения сертификатов в VMS XProtect для защиты обмена данными с мобильным сервером.



❶ Сертификат ЦС играет роль доверенной третьей стороны, которой доверяет как субъект/владелец (мобильный сервер), так и сторона, проверяющая сертификат (все клиенты).

❷ Сертификату ЦС должны доверять все клиенты. Таким образом клиенты могут проверять действительность сертификатов, выпущенных ЦС.

❸ Сертификат ЦС используется для организации защищенного подключения между мобильным сервером и клиентами и службами.

❹ Сертификат ЦС необходимо установить на компьютере, где выполняется мобильный сервер.

Требования к сертификату ЦС:

- В сертификате должно содержаться имя хоста мобильного сервера в качестве субъекта/владельца или в списке имен DNS, которым выдается сертификат.
- Сертификату должны доверять все устройства, на которых выполняются службы, получающие потоки данных с мобильного сервера.
- Учетная запись службы, от имени которой выполняется мобильный сервер, должна иметь доступ к закрытому ключу сертификата ЦС.

Дополнительные сведения см. в руководстве по сертификатам, посвященном защите систем XProtect VMS.

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.

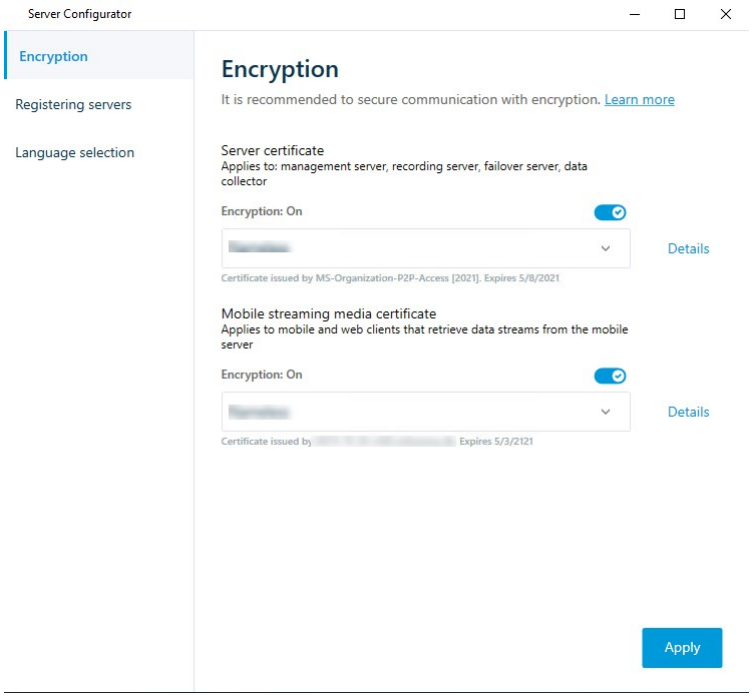
2. В **Server Configurator** в разделе **Сертификат мобильных потоковых мультимедиа** включите **Шифрование**.

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 и родительские/дочерние сайты

Milestone Federated Architecture объединяет несколько отдельных систем в иерархию федеративных сайтов, включающую родительские и дочерние сайты.

Для получения доступа ко всем сайтам с помощью XProtect Mobile или XProtect Web Client установите сервер XProtect Mobile на родительском сайте.

Пользователи клиента XProtect Mobile или XProtect Web Client должны подключиться к серверу управления на родительском сайте.

Smart Connect

Интеллектуальное соединение Smart Connect позволяет проверить правильность настройки XProtect Mobile без входа с мобильного устройства или планшета. Также упрощается процесс подключения для клиента XProtect Mobile и пользователей XProtect Web Client.

Для работы этой функции ваш сервер XProtect Mobile должен использовать общедоступный IP-адрес, а система должна иметь лицензию пакета подписки Milestone Care Plus.

Система незамедлительно отправляет ответ в Management Client, если настройка удаленного подключения выполнена успешно, и подтверждает, что к серверу XProtect Mobile есть доступ через Интернет.

Функция интеллектуального соединения позволяет серверу XProtect Mobile беспрепятственно переключаться между внутренними и внешними IP-адресами и подключаться к XProtect Mobile из любого местонахождения.

Для упрощения настройки мобильных клиентов можно отправлять электронные письма конечным пользователям напрямую из Management Client. Электронное письмо содержит ссылку, которая напрямую добавляет сервер в XProtect Mobile. Таким образом настройка не требует перехода по сетевым адресам и портам.

Настройка интеллектуального соединения Smart Connect

Чтобы настроить функцию интеллектуального соединения, выполните следующие действия:

1. В пункте Management Client на панели навигации разверните узел **Серверы** и выберите **Мобильные серверы**.
2. Выберите мобильный сервер и перейдите на вкладку **Подключение**.
3. Включите функцию обнаружения UPnP на маршрутизаторе.
4. Настройте параметры подключения.
5. Отправьте пользователям электронное письмо.
6. Включите подключения в сложной сети.

Включение функции обнаружения UPnP на маршрутизаторе

Для упрощения подключения мобильных устройств к серверам XProtect Mobile можно включить функцию UPnP (Universal Plug and Play) на маршрутизаторе. UPnP позволяет серверу XProtect Mobile автоматически настроить переадресацию портов. При этом переадресацию портов можно настроить вручную на маршрутизаторе с помощью веб-интерфейса. В зависимости от маршрутизатора процесс настройки сопоставления портов может отличаться. Если вы не знаете, как настроить переадресацию портов на вашем маршрутизаторе, ознакомьтесь с документацией к этому устройству.

Каждые пять минут служба XProtect Mobile Server проверяет, доступен ли сервер пользователям в Интернете. Статус отображается в верхнем левом углу панели **Свойства**: 

.

Включение подключений в сложной сети

Если у вас сложная сеть с пользовательскими параметрами, вы можете предоставлять информацию, необходимую пользователям для подключения.

На вкладке **Подключение** в группе **Доступ в Интернет** укажите следующую информацию:

- Если вы используете сопоставление портов UPnP, для переадресации на определенное подключение установите флажок **Настроить пользовательский доступ к Интернету**. Затем укажите **IP-адрес или имя хоста** и порт, который будет использоваться для подключения. Например, это можно сделать, если ваш маршрутизатор не поддерживает UPnP или если у вас цепочка маршрутизаторов
- Если у вас часто меняются IP-адреса, установите флажок **Отметить, чтобы получить IP-адрес динамически**.

Настройка параметров подключения

1. В пункте Management Client на панели навигации разверните узел **Серверы** и выберите **Мобильные серверы**.
2. Выберите сервер и перейдите на вкладку **Подключение**.

3. Используйте параметры в группе **Общее**, чтобы указать следующее:
    - Для упрощения подключения клиента XProtect Mobile и пользователей XProtect Web Client к серверам XProtect Mobile установите флажок **Включить Smart Connect**.
    - Укажите период времени, в течение которого клиент XProtect Mobile и XProtect Web Client должны сообщить мобильному серверу, что они подключены и работают.
    - Чтобы сервер XProtect Mobile обнаруживался в сети протоколами UPnP, установите флажок **Включить функцию обнаружения UPnP**.
    - Чтобы сервер XProtect Mobile самостоятельно выполнял сопоставление портов (если это предусмотрено настройками маршрутизатора), установите флажок **Разрешить автоматическое сопоставление портов**.

Отправка пользователям электронных писем

Для упрощения настройки клиентов XProtect Mobile и XProtect Web Client можно отправлять электронные письма конечным пользователям напрямую из Management Client. Электронное письмо содержит ссылку, которая напрямую добавляет сервер в XProtect Mobile. Таким образом настройка не требует перехода по сетевым адресам и портам.

1. В поле **Приглашение по эл. почте для** введите адрес электронной почты получателя уведомления Smart Connect и укажите язык.
2. Затем сделайте следующее:
    - Чтобы отправить сообщение, нажмите **Отправить**.
    - Скопируйте информацию в вашу программу обмена сообщениями.

Дополнительная информация:

Требования к настройке интеллектуального соединения Smart Connect на стр. 9

Вкладка «Подключение» на стр. 18

Уведомления

В XProtect Mobile можно настроить уведомление пользователей о возникновении событий, например об активации тревог или возникновении ошибок устройств или серверов.

Уведомления доставляются вне зависимости от того, работает ли приложение. При открытии XProtect Mobile на мобильном устройстве приложение отправляет уведомление. Системные уведомления приходят, даже если приложение не запущено. Пользователи могут указать, какие типы уведомлений хотят получать. Например, пользователь может выбрать следующие уведомления:

- Все тревоги
- только назначенные ему сигналы тревоги;
- только сигналы тревоги, связанные с системой.

  Такие сигналы могут отправляться, когда сервер отключается от сети или снова подключается к ней.

Для уведомления пользователей, у которых не открыт компонент XProtect Mobile, можно также использовать push-уведомления. Эти уведомления называют push-уведомлениями. Push-уведомления доставляются на мобильное устройство. Они очень удобны для информирования пользователей, пока они занимаются другими делами.

По умолчанию уведомления отключены.

Использование push-уведомлений

> Для использования push-уведомлений у вашей системы должен быть доступ в Интернет.

Для отправки push-уведомлений используются облачные службы Apple, Microsoft и Google:

- служба push-уведомлений Apple (APN);
- центр уведомлений Microsoft Azure;
- служба push-уведомлений Google Cloud Messaging.

Существует ограничение на количество уведомлений, которые система может отправить за определенный период времени. Если ваша система превысит это ограничение, она сможет отправлять только одно уведомление раз в 15 минут в течение следующего периода. Уведомление будет содержать список событий, которые произошли за 15 минут. По истечении следующего периода это ограничение снимается.

Также см. Требования к настройке уведомлений на стр. 8 и Вкладка «Уведомления» на стр. 28.

Настройка push-уведомлений на сервере XProtect Mobile

Чтобы настроить уведомления, выполните следующие действия:

1. В Management Client выберите мобильный сервер и перейдите на вкладку **Уведомления**.
2. Чтобы отправлять уведомления на все мобильные устройства, которые подключаются к серверу, установите флажок **Уведомления**. Чтобы продолжить, прочтите предупреждение о персональных данных и нажмите **Да**.
3. Чтобы сохранять информацию о пользователях и мобильных устройствах, которые подключаются к серверу, установите флажок **Сохранять регистрацию устройства**.

Сервер отправляет уведомления только на мобильные устройства из этого списка. Если снять флажок **Сохранять регистрацию устройства** и сохранить изменения, система очистит список. Чтобы снова получать push-уведомления, пользователям потребуется повторно подключить устройство.

Включение отправки push-уведомлений на некоторые или все мобильные устройства

Чтобы настроить в XProtect Mobile уведомление пользователей о событиях путем отправки push-уведомлений на некоторые или все мобильные устройства, выполните следующие действия:

1. В Management Client выберите мобильный сервер и перейдите на вкладку **Уведомления**.
2. Выполните одно из следующих действий:
    - Чтобы выбрать отдельные устройства, установите флажок **Включено** для каждого мобильного устройства в таблице **Зарегистрированные устройства**.
    - Чтобы выбрать все мобильные устройства, установите флажок **Уведомления**. Чтобы продолжить, прочтите предупреждение о персональных данных и нажмите **Да**.

Прекращение отправки push-уведомлений на некоторые или все мобильные устройства

Прекратить отправку push-уведомлений на некоторые или все мобильные устройства можно несколькими способами.

1. В Management Client выберите мобильный сервер и перейдите на вкладку **Уведомления**.
2. Выполните одно из следующих действий:
    - Чтобы прекратить отправку на отдельные устройства, снимите флажок **Включено** для каждого мобильного устройства. Пользователь может подключить к серверу XProtect Mobile другое устройство.
    - Чтобы прекратить отправку на все мобильные устройства, снимите флажок **Уведомления**.

Чтобы временно приостановить отправку на все устройства, снимите флажок **Сохранять регистрацию устройства** и сохраните изменения. После повторного подключения пользователя система снова начнет отправлять уведомления.

Удаление одного или всех зарегистрированных устройств из списка «Зарегистрированные устройства»

При удалении приложения XProtect Mobile или отключении устройства данные устройства могут по-прежнему храниться в базе данных VMS.

VMS удаляет регистрационные данные устройств в следующих случаях:

- когда вы удаляете пользователя из системы;
- если продление Milestone Care Plus не выполнялось более 180 дней.

Тем не менее, в некоторых случаях регистрационные данные устройств не удаляются автоматически.

Вам потребуется вручную удалить одно или все зарегистрированные устройства в следующих случаях:

- если пользователь потерял телефон;
- если вы намерены полностью удалить мобильный сервер и его данные;
- если пользователь перестает использовать уведомления или клиентское приложение XProtect Mobile;
- если вы добавили в роль VMS группу Active Directory (AD), и разрешения для пользователя изменились. При добавлении группы AD VMS неизвестно, каким пользователям назначается данная роль. Если вы удаляете пользователя из группы AD или запрещаете ему доступ к мобильному серверу, вам также потребуется вручную удалить устройство этого пользователя из списка.

Чтобы удалить зарегистрированное устройство, выполните следующие действия:

1. В Management Client выберите мобильный сервер и перейдите на вкладку **Уведомления**.
2. Выполните одно из следующих действий:
    - Чтобы удалить отдельные устройства, выберите устройство и нажмите **Удалить**.
    - Чтобы удалить все устройства, нажмите **Удалить все**.

Настройка расследований

Настройте расследования, чтобы пользователи могли использовать XProtect Web Client или XProtect Mobile для доступа к записанным видео и расследования инцидентов, а также для подготовки и загрузки видеодоказательств.

Чтобы настроить расследования, выполните следующие действия:

1. В Management Client выберите мобильный сервер и перейдите на вкладку **Исследования**.
2. Установите флажок **Подключить исследования**. Этот флажок установлен по умолчанию.
3. В поле **Папка исследований** укажите, где сохранять видео для расследований.
4. Дополнительно: Чтобы пользователи могли получить доступ к расследованиям, созданным другими пользователями, установите флажок **Просмотр исследований, сделанных другими пользователями**. Если этот флажок не установлен, пользователи будут видеть только собственные расследования.
5. Установите флажок **Включить ограничение на размер папки исследований**, чтобы задать максимальное количество мегабайт, которое может содержать папка расследований.

6. Установите флажок **Установить время хранения расследований**, чтобы задать время хранения расследований. По умолчанию время хранения составляет семь дней.
7. В разделе **Форматы экспорта** установите флажок рядом с форматом экспорта, который хотите использовать. Доступные форматы экспорта:
   - **Формат AVI**
   - **Формат XProtect**
   - **Формат MKV**

   По умолчанию флажки не установлены.

8. (Необязательно) Чтобы добавить дату и время загрузки видео, установите флажок **Включить временные метки для экспорта AVI**.
9. В поле **Используемый кодек для экспорта AVI** выберите формат сжатия для подготовки пакетов AVI к загрузке.

   В зависимости от вашей операционной системы кодеки в списке могут отличаться. Если вам не удается найти нужный кодек, можно установить его на компьютер, на котором выполняется Management Client, и он появится в списке.

   Кроме того, кодеки могут использовать разную степень сжатия, что влияет на качество видео. При более высокой степени сжатия требуется меньше места для хранения, но и качество может ухудшиться. При меньшей степени сжатия требуется больше места для хранения и более высокая производительность сети, но качество будет выше. Рекомендуется изучить разные кодеки, прежде чем сделать выбор.

10. В списке **Частота дискретизации звука для экспорта AVI** выберите соответствующую частоту дискретизации при добавлении звуковой информации в экспортируемое видео. По умолчанию частота дискретизации равна 160 000 Гц.

    Чтобы пользователи могли сохранять расследования, у роли безопасности, назначенной пользователям, должно быть разрешение **Экспорт**.

Удаление расследований

Расследования или экспортированные видео, которые больше не нужны, можно удалить. Эта функция может понадобиться, если, например, вам нужно освободить дисковое пространство на сервере.

- Чтобы удалить расследование и все экспортированные видео, созданные для него, выберите расследование в списке и нажмите **Удалить**.
- Чтобы удалить отдельные видеофайлы, которые экспортировались для расследования, но не удалять само расследование, выберите расследование в списке. В группе **Подробности расследования** выберите значок **Удалить** справа от полей **XProtect**, **AVI** или **MKV** для экспортированных видео.

Использование Video Push для потоковой передачи видео

Video Push можно настроить таким образом, чтобы пользователи могли сообщать другим людям о ситуации или записывать видео для дальнейшего расследования, передавая его с камеры мобильного устройства в вашу систему наблюдения XProtect. Видеопоток может также сопровождаться звуковой информацией.

Также см. Вкладка Video Push на стр. 27 и Требования к настройке Video Push на стр. 9.

Настройка Video Push для передачи видео

Чтобы пользователи могли передавать видео с мобильных устройств в систему XProtect, настройте Video Push на сервере XProtect Mobile.

В Management Client выполните эти действия в следующем порядке:

1. На вкладке **Video Push** установите флажок **Video Push**, чтобы включить функцию.
2. Добавьте канал Video Push для потоковой передачи видео.
3. Добавьте драйвер Video Push как аппаратное устройство на Recording Server. Драйвер моделирует камеру, и вы сможете передавать видео на Recording Server.
4. Добавьте устройство драйвера Video Push в канал, предусмотренный для Video Push.

Добавление канала Video Push для потоковой передачи видео

Чтобы добавить канал, выполните следующие действия:

1. На панели навигации выберите **Мобильные серверы** и соответствующий мобильный сервер.
2. На вкладке **Video Push** установите флажок **Video Push**.
3. В разделе **Сопоставление каналов** в нижнем левом углу нажмите **Добавить**, чтобы добавить канал Video Push.

4. В появившемся диалоговом окне введите имя пользователя учетной записи (добавляется в пункте **Роли**), которая будет использовать канал. Эта учетная запись пользователя должна иметь разрешение на доступ к серверу XProtect Mobile и серверу записи (на вкладке **Общая безопасность**).

   Для использования Video Push пользователи должны войти в XProtect Mobile с мобильного устройства, используя имя пользователя и пароль этой учетной записи.

   При добавлении нового канала Video Push на мобильный сервер система генерирует номер порта и MAC-адрес канала, которые используются, когда канал добавляется на сервер записи как аппаратное устройство. Система также генерирует пароль, который используется для подключения Recording Server к Mobile Server. Пароль по умолчанию — **Milestone**.

5. Запишите номер порта. Он вам потребуется при добавлении драйвера Video Push в качестве аппаратного устройства на сервер записи.
6. Нажмите **OK**, чтобы закрыть диалоговое окно «Канал Video Push».
7. Чтобы сохранить канал, нажмите **Сохранить** в верхнем левом углу панели навигации.

Редактирование канала Video Push

Настройки добавленного канала Video Push можно редактировать:

1. В разделе **Сопоставление каналов** выберите канал, в который нужно внести изменения, и нажмите **Изменить**.
2. По завершении редактирования нажмите **OK**, чтобы закрыть диалоговое окно «Канал Video Push».
3. Чтобы сохранить изменения, нажмите **Сохранить** в верхнем левом углу панели навигации.

При изменении номера порта и MAC-адреса канала Video Push необходимо также заменить данные канала Video Push, которые вы ранее добавляли на сервер записи, новыми данными. В противном случае не удастся установить соединение между Recording Server и Mobile Server.

Удаление канала Video Push

Каналы, которые больше не используются, можно удалять:

1. В разделе **Сопоставление каналов** выберите канал, который нужно удалить, и нажмите **Удалить**.
2. Чтобы сохранить изменения, нажмите **Сохранить** в верхнем левом углу панели навигации.

Изменить пароль

Автоматически созданный пароль, который используется для подключения Recording Server к Mobile Server, можно изменить:

1. В разделе **Сопоставление каналов** в нижнем правом углу нажмите **Изменить пароль**.
2. В диалоговом окне **Изменить пароль Video Push** введите новый пароль в первом поле и повторите его во втором поле, затем нажмите **OK**.
3. Чтобы сохранить изменения, нажмите **Сохранить** в верхнем левом углу панели навигации.

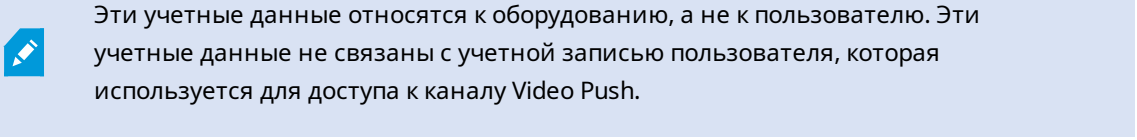
При изменении пароля канала Video Push это изменение применяется ко всем каналам Video Push, которые уже есть в списке или будут добавлены в будущем. Даже если удалить все существующие каналы Video Push из списка, новый пароль останется действующим и будет применяться к будущим каналам.

После сохранения изменения все существующие каналы Video Push перестают работать из-за разрыва соединения между Recording Server и Mobile Server. Чтобы восстановить соединение, на панели навигации нажмите правой кнопкой мыши вкладку **Серверы записи**, запустите мастер **замены оборудования** и введите новый пароль драйвера Video Push, который вы добавили в качестве аппаратного устройства на Recording Server.

Добавление драйвера Video Push как аппаратного устройства на сервер записи

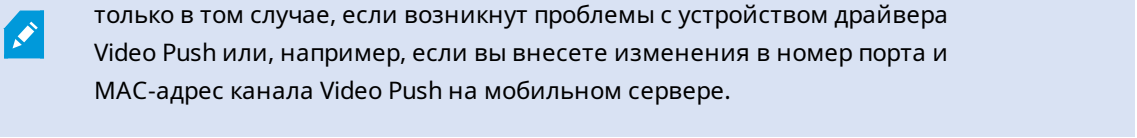
1. На панели навигации нажмите **Серверы записи**.
2. Правой кнопкой мыши нажмите сервер, на который вы хотите передать видео, и нажмите **Добавить оборудование**, чтобы открыть мастер **добавления оборудования**.
3. Выберите способ определения оборудования **Вручную** и нажмите **Далее**.

4. Введите учетные данные драйвера Video Push:
   - Имя пользователя: Не заполняйте это поле, чтобы использовать имя пользователя по умолчанию.
   - Пароль: Введите **Milestone** — пароль, созданный системой. Если вы меняли пароль при добавлении канала Video Push на мобильном сервере, введите свой пароль. Затем нажмите **Далее**.

   Эти учетные данные относятся к оборудованию, а не к пользователю. Эти учетные данные не связаны с учетной записью пользователя, которая используется для доступа к каналу Video Push.

5. В списке драйверов разверните **Milestone**, установите флажок **Драйвер Video Push** и нажмите **Далее**.
6. В поле **Адрес** введите IP-адрес компьютера, на котором установлен сервер XProtect Mobile.

   Рекомендуется использовать MAC-адрес, созданный системой. Меняйте его только в том случае, если возникнут проблемы с устройством драйвера Video Push или, например, если вы внесете изменения в номер порта и MAC-адрес канала Video Push на мобильном сервере.

7. В поле **Порт** введите номер порта канала, который вы создали для потоковой передачи видео. Номер порта назначается при создании канала.
8. В столбце **Модель оборудования** выберите **Драйвер Video Push** и нажмите **Далее**.
9. Когда система обнаружит новое оборудование, нажмите **Далее**.
10. В поле **Шаблон имени оборудования** укажите, что будет отображаться: модель оборудования и IP-адрес или только модель.

11. Установите флажок **Включено**, если хотите включить связанные устройства. Связанные устройства можно добавить в список **Драйвер Video Push**, даже если они не включены. Можно включить их позже.

    > Если при потоковой передаче видео вы хотите использовать информацию о местонахождении, включите порт **Метаданные**.

    > Если вы хотите во время потоковой передачи видео воспроизводить звуковую информацию, включите микрофон, связанный с камерой, которая используется для потоковой передачи видео.

12. Выберите группы по умолчанию для связанных устройств слева или выберите группу в поле **Добавить в группу**. Если добавить устройства в группу, это позволит применять настройки сразу ко всем устройствам или заменять устройства.

Добавление устройства драйвера Video Push в канал Video Push

Чтобы добавить устройство драйвера Video Push в канал, предусмотренный для Video Push, выполните следующие действия:

1. На панели **Навигация по сайту** нажмите **Мобильные серверы** и перейдите на вкладку **Video Push**.
2. Нажмите **Найти камеры**. Если камера найдена, название камеры драйвера Video Push появится в поле **Имя камеры**.
3. Сохраните настройки.

Включение звуковой информации для существующего канала Video Push

После выполнения всех требований к включению звуковой информации в Video Push (см. Требования к настройке Video Push на стр. 9) в Management Client сделайте следующее:

1. На панели **Навигация по сайту** разверните узел **Серверы** и нажмите **Серверы записи**.
2. На панели обзора выберите папку соответствующего сервера записи, разверните папку **Драйвер Video Push** и нажмите правой кнопкой мыши микрофон, связанный с Video Push.
3. Выберите **Включено**, чтобы включить микрофон.
4. В той же папке выберите камеру, связанную с Video Push.
5. На панели **Свойства** перейдите на вкладку **Клиент**.
   Дополнительные сведения см. в разделе Вкладка «Клиент» (устройства).

6. В правой части поля **Связанный микрофон** нажмите  . Откроется диалоговое окно **Выбранное устройство**.
7. На вкладке **Серверы записи** разверните папку сервера записи и выберите микрофон, связанный с Video Push.
8. Нажмите кнопку **OK**.

Настройка двухэтапной проверки пользователей по электронной почте

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 принудительно активировать дополнительный этап авторизации для пользователей клиента XProtect Mobile или XProtect Web Client, настройте двухэтапную проверку на сервере XProtect Mobile. Кроме стандартного имени пользователя и пароля, пользователь должен будет ввести проверочный код, полученный по электронной почте.

Двухэтапная проверка повышает уровень безопасности вашей системы наблюдения.

Выполните следующие действия в Management Client:

1. Ввод информации о сервере SMTP на стр. 49.
2. Задание кода проверки, отправляемого пользователям на стр. 50.
3. Назначение метода проверки пользователей и групп Active Directory на стр. 50.

Также см. Требования к настройке двухэтапной проверки пользователей на стр. 9 и Вкладка «Двухэтапная проверка» на стр. 29.

Ввод информации о сервере SMTP

Поставщик использует информацию о сервере SMTP:

1. На панели навигации нажмите **Мобильные серверы** и выберите соответствующий мобильный сервер.
2. На вкладке **Двухэтапная проверка** установите флажок **Включить двухэтапную проверку**.
3. На вкладке **Электронная почта** под разделом **Параметры поставщика** введите информацию о сервере SMTP и укажите адрес электронной почты. На этот адрес система будет отправлять электронные письма пользователям клиента при входе в систему с двухэтапной проверкой.

Дополнительные сведения приведены в разделе Вкладка «Двухэтапная проверка» на стр. 29.

Задание кода проверки, отправляемого пользователям

Настройка сложности кода проверки:

1. На вкладке **Двухэтапная проверка** в разделе **Параметры проверочного кода** укажите период, в течение которого пользователям клиента XProtect Mobile не нужно повторно подтверждать авторизацию, например в случае отключения сети. Период по умолчанию — три минуты.
2. Укажите период, в течение которого пользователь может использовать полученный проверочный код. По истечении этого периода код становится недействительным, поэтому пользователь должен запросить новый код. Период по умолчанию — пять минут.
3. Укажите максимальное количество попыток ввода кода до того, как полученный код станет недействительным. По умолчанию дано три попытки.
4. Укажите количество символов кода. Длина по умолчанию — шесть символов.
5. Укажите степень сложности кода, который должна генерировать система.

Дополнительные сведения приведены в разделе Вкладка «Двухэтапная проверка» на стр. 29.

Назначение метода проверки пользователей и групп Active Directory

На вкладке **Двухэтапная проверка** в разделе **Параметры пользователя** отображается список пользователей и групп, добавленных в систему XProtect.

1. В столбце **Метод проверки** выберите подходящий метод для каждого пользователя или группы.
2. В поле **Сведения о пользователе** добавьте данные доставки кода, например адреса электронной почты отдельных пользователей. При следующем входе в приложение XProtect Web Client или XProtect Mobile пользователю потребуется указать дополнительный компонент авторизации.
3. Если группа настроена в Active Directory, сервер XProtect Mobile использует данные Active Directory, например адреса электронной почты.

   Группы Windows не поддерживают двухэтапную проверку.

4. Сохраните настройки.

Настройка двухэтапной проверки пользователей по электронной почте завершена.

Дополнительные сведения приведены в разделе Вкладка «Двухэтапная проверка» на стр. 29.

Действия

Вы можете управлять доступностью вкладки **Действия** в клиенте XProtect Mobile или в XProtect Web Client, включая или отключая действия на вкладке **Общая информация**. **Действия** включены по умолчанию, и все действия, доступные для подключенных устройств, отображаются на этой вкладке.

Дополнительные сведения приведены в разделе Вкладка «Общая информация» на стр. 15.

Управление мобильными устройствами (MDM)

Управление мобильными устройствами (MDM) — это программное обеспечение, обеспечивающее защиту, мониторинг, управление и поддержку мобильных устройств, развернутых в сетях операторов мобильной связи, поставщиков услуг и крупных предприятий.

Как правило, решение управления мобильными устройствами включает серверный компонент, передающий команды управления на мобильные устройства, и клиентский компонент, работающий на управляемых устройствах, который получает и выполняет команды управления.

Эта функция позволяет распространять клиент XProtect Mobile и добавлять собственные политики на устройства в вашей организации.

Чтобы использовать функции управления мобильными устройствами на мобильном устройстве, нужно задать сведения о мобильном сервере на платформе MDM. К ним относятся: имя сервера, адрес сервера, порт сервера и протокол типа подключения.

Если вы изменили сведения для уже добавленного мобильного сервера, оператору потребуется вручную удалить этот сервер из списка **Серверы** и перезапустить приложение XProtect Mobile.

Настройка сведений о мобильном сервере на платформе управления мобильными устройствами (администраторы)

Чтобы иметь возможность распространять клиент XProtect Mobile и управлять им на мобильных устройствах с помощью платформы управления мобильными устройствами (MDM), необходимо добавить сведения о сервере. Дополнительные сведения о настройке приведены в документации ПО для управления мобильными устройствам.

Если вы не ввели обязательные сведения о сервере или предоставили неверные сведения, мобильный сервер не будет добавлен в приложение XProtect Mobile.

Для пользователей Android

Данные сервера можно указать в интерфейсе пользователя платформы MDM. Вы можете загрузить управляемый файл конфигурации с данными сервера.

Сведения о сервере:

- **Имя сервера** — (обязательное поле) введите имя сервера.
- **Адрес сервера** — (обязательное поле) введите адрес сервера.
- **Порт сервера** — (обязательное поле) введите номер порта сервера.
- **Тип протокола подключения** — включите, если используете подключение по HTTPS. Отключите, если используете подключение по HTTP. По умолчанию используется подключение по HTTPS.

Чтобы загрузить файл на платформу управления мобильными устройствами, выполните следующие действия:

1. В конце этого руководства в Приложении А найдите управляемый шаблон конфигурации для устройств Android. Скопируйте содержимое.
2. Откройте любой текстовый редактор и вставьте содержимое.
3. Укажите сведения о сервере в полях **android:description**.
4. Сохраните файл в формате XML.
5. Откройте платформу управления мобильными устройствами и загрузите управляемый файл конфигурации.

Для пользователей iOS

Для управления устройствами iOS из платформы управления мобильными устройствами необходимо указать сведения о подключении в управляемом файле конфигурации.

1. В конце этого руководства в Приложении Б найдите управляемый шаблон конфигурации для устройств iOS. Скопируйте содержимое.
2. Откройте любой текстовый редактор и вставьте содержимое.

3. Укажите сведения о сервере:
   - **versionConfig** — (обязательное поле) введите версию конфигурации приложения **1.0.0** по умолчанию.
   - **serverNameConfig** — (обязательное поле) введите имя сервера.
   - **serverAddressConfig** — (обязательное поле) введите адрес сервера.
   - **serverPortConfig** — (обязательное поле) введите номер порта сервера.
   - **serverConnectionProtocolTypeConfig** — по умолчанию используется подключение типа **HTTPS**; для использования незащищенного подключения введите **HTTP**.
4. Сохраните файл в формате XML.
5. Откройте платформу управления мобильными устройствами и загрузите управляемый файл конфигурации.

Присвоение имени группам вывода для использования в клиенте XProtect Mobile и XProtect Web Client

Чтобы действия корректно отображались с текущей камерой, необходимо создать группу вывода, которая будет называться так же, как и камера.

Пример:

Если вы создаете группу вывода, где выходные данные привязаны к камере с именем «AXIS P3301 - 10.100.50.110 - Камера 1», нужно ввести это же имя в поле **Имя** (в разделе **Информация о группе устройств**).

В поле **Описание** можно добавить дополнительное описание, например «AXIS P3301 - 10.100.50.110 - Камера 1 - выключатель освещения».

> ⚠ Если не следовать этим правилам присвоения имен, действия в списке действий не будут доступны для соответствующего представления камеры. Вместо этого действия будут отображаться в списке других действий на вкладке **Действия**.

Дополнительные сведения см. в разделе Выходные данные.

Внешний IDP и XProtect Mobile

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.

Вы можете войти в XProtect Web Client или в клиент XProtect Mobile через внешний IDP, используя XProtect не ниже версии 2022 R3.

Чтобы войти с помощью внешнего IDP в XProtect Web Client или в клиент XProtect Mobile, нужно использовать подключение HTTPS.

Перед настройкой входа во внешний IDP для XProtect Web Client и клиента XProtect Mobile убедитесь, что вы сделали следующее:

- настроили внешний IDP;
- зарегистрировали заявки;
- связали заявки с ролями.

Дополнительную информацию см. в руководстве администратора для XProtect VMS.

Чтобы войти в XProtect Web Client через внешний IDP, нужны дополнительные настройки. См. раздел Настройка входа через внешний IDP для XProtect Web Client на стр. 54.

Настройка входа через внешний IDP для XProtect Web Client

Возможность входа через внешний IDP в XProtect Web Client доступна только для подключений по HTTPS.

1. В Management Client выберите пункт **Инструменты** > **Параметры**, а затем перейдите на вкладку **Внешний IDP**.
2. В разделе **URI переадресации для веб-клиентов** выберите **Добавить**.
3. Введите адреса для XProtect Web Client в формате `https://[address]:[номер порта]/index.html`:
    - В качестве адреса введите имя хоста или IP-адрес компьютера, на котором выполняется мобильный сервер.
    - В качестве номера порта введите порт, который XProtect Web Client использует для взаимодействия с мобильным сервером. Для подключений по HTTPS номер порта по умолчанию — 8082.

Добавление сигналов тревоги «Оповещение о чрезвычайной ситуации»

При обнаружении потенциальной опасности функция «Оповещение о чрезвычайной ситуации» позволяет пользователям клиента XProtect Mobile получать уведомления о сигналах тревоги с наиболее высоким уровнем серьезности, просматривать подробную информацию о сигнале тревоги и оперативно принимать меры. Оповещение о чрезвычайной ситуации — это тип сигнала тревоги, который задается в XProtect Management Client.

Для работы этой функции необходимы push-уведомления. Push-уведомления доступны только в том случае, если вы приобрели лицензию Milestone Care Plus.

Эта функция доступна только в некоторых продуктах VMS XProtect. Просмотреть полных список функций, который приводится на странице обзора продукта, на веб-странице Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Чтобы добавить такой сигнал тревоги, необходимо сделать следующее:

1. Добавьте новую категорию сигналов тревоги с уровнем 99 в разделе **Сигналы тревоги** > **Настройки данных сигналов тревоги**. Можно создавать неограниченное количество категорий уровня 99.
2. Добавьте определение тревоги с этой категорией.

Обслуживание

Mobile Server Manager

Mobile Server Manager — это функция, которая находится на панели задачи и подключается к мобильному серверу. При нажатии значка Mobile Server Manager в области уведомлений правой кнопкой мыши откроется меню, в котором можно получить доступ к функциям мобильного сервера.

Вы можете выполнять следующие действия:

- Доступ к XProtect Web Client на стр. 56
- Запуск, остановка и перезапуск службы Mobile Server на стр. 57
- Изменение пароля для защиты данных на стр. 57
- Отображение/изменение номеров портов на стр. 58
- Включить шифрование на мобильном сервере на стр. 35 с помощью **Server Configurator**
- Открыть сегодняшний файл журнала (см. Доступ к журналам и расследованиям на стр. 58)
- Открыть папку журналов (см. Доступ к журналам и расследованиям на стр. 58)
- Открыть папку расследований (см. Доступ к журналам и расследованиям на стр. 58)
- Изменение папки расследований на стр. 59
- Просматривать статус XProtect Mobile Server (см. Показать статус на стр. 60)

Доступ к XProtect Web Client

Если на вашем компьютере установлен сервер XProtect Mobile, XProtect Web Client можно использовать для доступа к камерам и представлениям. Так как устанавливать XProtect Web Client не нужно, вы можете войти с компьютера, где установлен сервер XProtect Mobile, или с любого компьютера, который вы хотите использовать для этой цели.

1. Настройте сервер XProtect Mobile в Management Client.
2. Если вы используете компьютер, на котором установлен сервер XProtect Mobile, нажмите правой кнопкой мыши значок Mobile Server Manager в области уведомлений и выберите **ОткрытьXProtect Web Client**.
3. Если на компьютере, который вы используете, не установлен сервер XProtect Mobile, вы можете войти через браузер. Продолжайте с пункта 4 этого процесса.
4. Откройте интернет-браузер (Microsoft Edge, Mozilla Firefox, Google Chrome или Safari).

5. Введите внешний IP-адрес, т.е. внешний адрес или порт сервера, на котором работает сервер XProtect Mobile.

   Пример: Сервер XProtect Mobile установлен на сервере с IP-адресом 127.2.3.4 и настроен на прием подключений по HTTP через порт 8081 и подключений по HTTPS через порт 8082 (параметры программы установки по умолчанию).

   В адресной строке браузера введите **http://127.2.3.4:8081**, если нужно использовать стандартное подключение по HTTP, или **https://127.2.3.4:8082**, чтобы использовать безопасное подключение по HTTPS. Теперь можно приступать к использованию XProtect Web Client.

6. Для упрощения доступа к XProtect Web Client в дальнейшем добавьте адрес в закладки браузера. Если вы используете XProtect Web Client на локальном компьютере, на котором установлен сервер XProtect Mobile, вы также можете использовать ярлык на рабочем столе, который создает программа установки. Нажмите ярлык, чтобы запустить браузер по умолчанию, и откройте XProtect Web Client.

Перед использованием новой версии XProtect Web Client нужно очистить кэш интернет-браузера, в котором работает XProtect Web Client. Системные администраторы должны попросить пользователей XProtect Web Client очистить кэш браузера после обновления или принудительно выполнить это действие дистанционно (это можно сделать только в браузере Internet Explorer в домене).

Запуск, остановка и перезапуск службы Mobile Server

При необходимости можно запустить, остановить или перезапустить службу Mobile Server с Mobile Server Manager.

- Чтобы выполнить эти задачи, нажмите правой кнопкой мыши значок Mobile Server Manager и выберите **Запустить службу Mobile Server**, **Остановить службу Mobile Server** или **Перезапустить службу Mobile Server**, соответственно

Изменение пароля для защиты данных

Пароль для защиты данных сервера мобильной связи используется 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.

Чтобы изменить пароль для защиты данных мобильного сервера, выполните следующие действия:

1. Нажмите правой кнопкой мыши значок Mobile Server Manager и выберите **Изменить параметры пароля защиты данных**. Откроется диалоговое окно.
2. В поле **Новый пароль** введите новый пароль.
3. Введите новый пароль еще раз в поле **Подтвердить новый пароль**.

4. (Необязательно) 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**.
5. Нажмите кнопку **OK**.

> Этот пароль необходимо хранить в надежном месте. Если этого не сделать, вам может не удаться восстановить данные мобильного сервера.

Отображение/изменение номеров портов

1. Нажмите правой кнопкой мыши значок Mobile Server Manager и выберите **Показать/изменить номера портов**.
2. Чтобы изменить номер порта, введите соответствующий номер. Можно указать стандартный номер порта для подключений HTTP или номер защищенного порта для подключений HTTPS, а также оба.
3. Нажмите кнопку **OK**.

Доступ к журналам и расследованиям

Mobile Server Manager позволяет быстро получить доступ к файлу журнала за день, открыть папку, где сохраняются файлы журналов и открыть папку, где сохраняются расследования.

Чтобы открыть любой из этих элементов, нажмите значок Mobile Server Manager правой кнопкой мыши и выберите:

- **Открыть сегодняшний журнал**
- **Открыть папку журналов**
- **Открыть папку расследований**

Контрольные журналы создаются для каждого действия, которое еще не зарегистрировано в Management Server или Recording Server.

Следующие действия всегда регистрируются в журналах (даже если расширенная регистрация в контрольных журналах не включена):

- все действия администрирования (эти сообщения в контрольном журнале содержат старое и новое значения);
- все действия, связанные с созданием, редактирование и удалением расследований, а также подготовкой и загрузкой экспортированных материалов, изменением соответствующих параметров. Контрольный журнал содержит подробные сведения о выполненных действиях.

Передача видеопотока регистрируется в журнале, только если включена расширенная регистрация в контрольном журнале.

При удалении сервера XProtect Mobile с вашего компьютера его файлы журналов не удаляются. Администраторы с соответствующими пользовательскими разрешениями могут получить доступ к этим файлам журналов позже или удалить их, если они больше не нужны. По умолчанию файлы журналов находятся в папке **ProgramData**. Если изменить местонахождение файлов журналов по умолчанию, существующие журналы не скопируются в новое местонахождение и не удалятся.

Изменение папки расследований

По умолчанию расследования хранятся в папке **ProgramData**. Если изменить местонахождение папки расследований по умолчанию, существующие расследования автоматически не копируются в новое местонахождение и не удаляются. Чтобы изменить папку для хранения экспортированных данных расследований на жестком диске, выполните следующие действия:

1. Нажмите правой кнопкой мыши значок Mobile Server Manager и выберите **Изменить папку расследований**.

   Откроется новое окно **Расположение исследований**.

2. Нажмите значок папки рядом с полем **Папка**, в котором отображается текущее местонахождение, чтобы перейти к существующей папке или создать новую папку. Затем нажмите **OK**.

3. В списке **Старые исследования** выберите действие, которое хотите применить к существующим расследованиям, хранящимся в текущей папке. Доступные варианты:

   - **Переместить** — перемещение существующих расследований в новую папку.

     Если не переместить существующие расследования в новую папку, вы больше не сможете просматривать их.

   - **Удалить** — удаление существующих расследований.
   - **Ничего не делать** — существующие расследования останутся в текущей папке. После изменения местонахождения папки расследований по умолчанию вы больше не сможете их просматривать.

4. Нажмите **Применить**, а затем **OK**.

Показать статус

Нажмите значок Mobile Server Manager и выберите **Показать статус** или дважды нажмите значок Mobile Server Manager, чтобы открыть окно, в котором отображается статус сервера XProtect Mobile. Можно использовать следующую информацию:

Имя	Описание
Сервер запущен с	Время и дата, когда сервер XProtect Mobile запускался последний раз.
Подключенные пользователи	Количество пользователей, которые в настоящее время подключены к серверу XProtect Mobile.
Аппаратное декодирование	Указывает, применяется ли на сервере XProtect Mobile аппаратно-ускоренное декодирование.
Загрузка ЦП	Доля ресурсов центрального процессора (%), в настоящее время используемая сервером XProtect Mobile.
Журнал загрузки процессора	График, подробно описывающий историю загрузки центрального процессора сервером XProtect Mobile.

Использовать балансировщик нагрузки для мобильного сервера

В качестве дополнительного шага безопасности XProtect Mobile использует идентификаторы при обмене данными между сервером и мобильным приложением. Когда пользователь впервые подключается к мобильному серверу из приложения XProtect Mobile, идентификатор мобильного сервера копируется на устройство пользователя. При каждой попытке подключения к мобильному серверу идентификаторы серверов сравниваются с полученными изначально.

По умолчанию каждый сервер имеет уникальный идентификатор. Чтобы добавить мобильный сервер в группу балансировки нагрузки, необходимо убедиться, что идентификатор мобильного сервера совпадает с идентификатором, используемым другими мобильными серверами в группе.

На хосте в группе балансировки нагрузки

Чтобы скопировать идентификаторы сервера с хоста:

1. Перейдите в `C:\ProgramFiles\Milestone\Milestone Mobile Server` и скопируйте файл **VideoOS.MobileServer.Service.exe.config**.
2. Вставьте файл на рабочий стол и откройте его в любом текстовом редакторе.

3. Найдите в файле тег `ServerSettings`. Он должен выглядеть следующим образом:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

4. Скопируйте значения **ServiceID** и **ReportedServiceID**.

На других хостах, входящих в группу

На хосте, входящем в группу балансировки нагрузки:

1. Перейдите в `C:\ProgramFiles\Milestone\Milestone Mobile Server` и откройте файл **VideoOS.MobileServer.Service.exe.config** в любом текстовом редакторе.
2. Найдите в файле тег `ServerSettings` замените значения **ServiceID** и **ReportedServiceID** значениями из исходного файла конфигурации.
3. Чтобы применить изменения, перезапустите службу Mobile Server.
4. Попросите пользователей клиента XProtect Mobile снова добавить мобильный сервер.

Повторите эти действия на всех хостах, входящих в группу балансировки нагрузки.

Перенос мобильного сервера на другой хост

В качестве дополнительного шага безопасности XProtect Mobile использует идентификаторы при обмене данными между сервером и мобильным приложением. Когда пользователь впервые подключается к мобильному серверу из приложения XProtect Mobile, идентификатор мобильного сервера копируется на устройство пользователя. Каждый раз, когда приложение пытается подключиться к мобильному серверу, он сравнивает идентификаторы серверов с полученными изначально. Если идентификаторы серверов не совпадают, подключение не устанавливается.

При переносе мобильного сервера на другой хост и сохранении его исходного адреса необходимо сохранить идентификатор старого сервера.

На старом хосте

Перед переносом мобильного сервера необходимо выполнить следующее:

1. Перейдите в `C:\ProgramFiles\Milestone\Milestone Mobile Server`, скопируйте файл **VideoOS.MobileServer.Service.exe.config** и откройте его в любом текстовом редакторе.
2. Найдите в файле тег `ServerSettings`. Он должен выглядеть следующим образом:

```
<ServerSetings>
 <Identification>
  <add key="ServiceId" value="4d644654-95f5-4382-b582-0005864391ee">
  <add key="ServiceIdS" value="10353810-803F-4880-BC22-417B37F1A1C8">
  <add key="ReportedServiceId" value="10353810-803F-4880-BC22-417B37F1A1C8">
 </Identification>
---
</ServerSettings>
```

3. Скопируйте значения **ServiceID** и **ReportedServiceID**.

Теперь все готово к переносу мобильного сервера.

На новом хосте

После установки и настройки мобильного сервера на новом хосте выполните следующее:

1. Перейдите в `C:\ProgramFiles\Milestone\Milestone Mobile Server` и откройте файл **VideoOS.MobileServer.Service.exe.config** в любом текстовом редакторе.
2. Найдите в файле тег `ServerSettings` замените значения **ServiceID** и **ReportedServiceID** значениями из исходного файла конфигурации.
3. Чтобы применить изменения, перезапустите службу Mobile Server.
4. Попросите пользователей клиента XProtect Mobile снова добавить мобильный сервер.

Способ устранения

Диагностика и устранение неполадок XProtect Mobile

Подключения

Почему я не могу подключиться из клиента XProtect Mobile к моим записям/серверу XProtect Mobile?

Чтобы подключиться к вашим записям, сервер XProtect Mobile должен быть установлен на сервере, на котором выполняется ваша система XProtect, или на выделенном сервере. Также нужны соответствующие параметры XProtect Mobile в конфигурации управления видео XProtect. Они устанавливаются как встраиваемые расширения или вместе с продуктом или обновлением. Более подробно о том, как установить сервер XProtect Mobile и интегрировать параметры, связанные с клиентом XProtect Mobile, в вашу систему XProtect, см. в разделе «Конфигурация» (см. Параметры мобильного сервера на стр. 14).

В поле адреса сервера должно быть указано допустимое имя хоста при использовании на устройстве iOS. Допустимое имя хоста может содержать буквы ASCII от a до z (с учетом регистра), цифры от 0 до 9, точку и дефис (-).

Не удается подключить мобильное устройство к серверу сразу после включения брандмауэра. Почему?

Если брандмауэр был выключен во время установки сервера XProtect Mobile, нужно вручную включить обмен данными по протоколам TCP и UDP.

Как избежать предупреждений о безопасности при запуске XProtect Web Client с соединением HTTPS?

Предупреждение появляется из-за того, что информация об адресе сервера в сертификате неверна. Соединение будет по-прежнему зашифровано.
Самозаверяющий сертификат на сервере XProtect Mobile нужно заменить собственным сертификатом, который соответствует адресу сервера, используемому для подключения к серверу XProtect Mobile. Эти сертификаты можно получить в официальных центрах сертификатов, таких как Verisign. Обратитесь в выбранный ЦС, чтобы узнать подробную информацию. Сервер
XProtect Mobile не использует Microsoft IIS. Это означает, что инструкции по созданию файлов запроса на подпись сертификата (CSR) ЦС с использованием IIS неприменимы к серверу XProtect Mobile. Вам нужно вручную создать CSR-файл с помощью инструментов создания сертификата в командной строке или других подобных сторонних приложениях. Этот процесс выполняется только системными администраторами или опытными пользователями.

Адрес мобильного сервера не менялся, но пользователи клиента XProtect Mobile больше не могут к нему подключиться. Почему?

Клиенты XProtect Mobile подключаются к мобильному серверу, используя уникальный идентификатор службы. Даже если имя хоста и IP-адрес компьютера, на котором установлен мобильный сервер, не меняются, идентификатор службы может не совпадать с идентификатором, хранящимся в клиентах, например в следующих случаях:

- Вы перезагрузили компьютер и переустановили мобильный сервер.
- Вы перенесли мобильный сервер на другой компьютер, но сохранили исходную конфигурацию сервера.

Чтобы восстановить соединение, можно выполнить следующие действия:

- Обновите идентификатор службы на новом мобильном сервере, чтобы он совпадал с идентификатором службы из предыдущей конфигурации. См. https://developer.milestonesys.com/s/article/unable-to-establish-connection-to-XProtect-Mobile-Server-using-Android-iOS-client.
- Попросите пользователей клиента XProtect Mobile повторно подключиться к мобильному серверу.

Качество изображения

Почему иногда при просмотре видео в клиенте XProtect Mobile качество изображения недостаточно хорошее?

Сервер XProtect Mobile автоматически регулирует качество изображения в зависимости от доступной полосы пропускания между сервером и клиентом. Если качество изображения ниже, чем в XProtect® Smart Client, возможно, пропускной способности недостаточно для получения изображений с полным разрешением через клиент XProtect Mobile. Это может быть связано либо со слишком малой пропускная способность в восходящем направлении от сервера или со слишком малой пропускной способностью в нисходящем направлении на стороне клиента. Дополнительные сведения см. в руководстве пользователя XProtect Smart Client.

Если вы работаете в беспроводной среде, где доступны каналы с разными значениями пропускной способности, вы можете заметить, что качество изображений улучшается, если перейти в место с лучшим качеством подключения.

Почему качество изображения бывает недостаточно хорошим при подключении к домашней системе управления видео XProtect через Wi-Fi из офиса?

Проверьте пропускную способность домашнего Интернета. Для частных интернет-подключений характерны разные значения пропускной способности загрузки и отправки, например 20 мбит/2 мбит. Это связано с тем, что дома пользователям нечасто приходится выгружать большие объемы данных, но они часто загружают много данных. Системе управления видео XProtect нужно отправить видео в клиент XProtect Mobile, и она ограничена скоростью отправки вашего подключения. Если низкое качество изображения наблюдается постоянно в разных местах с достаточной скоростью загрузки в сети клиента XProtect Mobile, проблему можно решить увеличением скорости отправки домашнего интернет-подключения.

Аппаратно-ускоренное декодирование

Мой процессор поддерживает аппаратно-ускоренное декодирование?

Аппаратно-ускоренное декодирование поддерживается только более новыми процессорами Intel. Перейдите на веб-сайт Intel (https://www.intel.com/content/www/us/en/ark/featurefilter.html?productType=873&0_QuickSyncVideo=True), чтобы узнать, поддерживает ли ваш процессор аппаратно-ускоренное декодирование.

Убедитесь, что в меню в пункте **Технологии** > **Intel Quick Sync Video** установлено значение **Да**.

Аппаратно-ускоренное декодирование включено по умолчанию, если ваш процессор поддерживает его. Текущий статус можно проверить в пункте **Показать статус** в Mobile Server Manager (см. Показать статус на стр. 60).

Моя операционная система поддерживает аппаратно-ускоренное декодирование?

Все операционные системы, которые поддерживаются XProtect, также поддерживают аппаратно-ускоренное декодирование.

Убедитесь, что в вашей системе установлены последние версии графических драйверов. Этих драйверов нет в Центре обновления Windows.

Как отключить аппаратно-ускоренное декодирование на мобильном сервере? (Advanced)

- Если процессор на мобильном сервере поддерживает аппаратно-ускоренное декодирование, оно включено по умолчанию. Чтобы отключить аппаратно-ускоренное декодирование, сделайте следующее:

  1. Найдите файл VideoOS.MobileServer.Service.exe.config. Обычно он размещается по следующему пути: `C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config`.
  2. Откройте файл в программе «Блокнот» или аналогичном текстовом редакторе. При необходимости свяжите тип файла CONFIG с программой «Блокнот».
  3. Найдите поле `<add key="HardwareDecodingMode" value="Auto" />`.
  4. Замените значение Auto (Авто) на Off (Выкл.).
  5. Сохраните и закройте файл.

Уведомления

Настройки уведомлений не менялись, но зарегистрированные устройства больше не получают уведомления. Почему?

Если вы обновили лицензию или подписку Milestone Care, нужно перезапустить службу Mobile Server.

Приложения

Приложение A

Управляемый шаблон конфигурации для Android

```
<?xml version="1.0" encoding="utf-8"?>

<restrictions xmlns:android="http://schemas.android.com/apk/res/android">

    <restriction
        android:defaultValue="1.0.0"
        android:description="The current version of the app configuration"
        android:key="version_config"
        android:restrictionType="hidden"
        android:title="Version" />

    <restriction
```

```
        android:description="(Mandatory) Enter the server name."
        android:key="server_name_config"
        android:restrictionType="string"
        android:title="Server name" />

    <restriction
        android:description="(Mandatory) Enter the server address."
        android:key="server_address_config"
        android:restrictionType="string"
        android:title="Server address" />

    <restriction
        android:description="(Mandatory) Enter the server port."
```

```
        android:key="server_port_config"

        android:restrictionType="integer"

        android:title="Server port" />


    <restriction

        android:description="Enable when you use an HTTPS connection. Disable
when you use an HTTP connection."

        android:key="server_secure_connection_config"

        android:restrictionType="bool"

        android:title="Connection protocol type"

        android:defaultValue="true"/>


</restrictions>
```

Приложение Б

Управляемый шаблон конфигурации для iOS

```
<managedAppConfiguration>
    <version>1</version>
    <bundleId>com.milestonesys.XProtect</bundleId>
    <dict>
        <string keyName="versionConfig">
            <defaultValue>
                <value>1.0.0</value>
            </defaultValue>
        </string>
        <string keyName="serverNameConfig">
        </string>
        <string keyName="serverAddressConfig">
        </string>
```

```
        <string keyName="serverPortConfig">
        </string>
        <string keyName="serverConnectionProtocolTypeConfig">
            <defaultValue>
                <value>HTTPS</value>
            </defaultValue>
        </string>
    </dict>
    <presentation defaultLocale="en-US">
        <field keyName="versionConfig" type="input">
            <label>
                <language value="en-US">Version</language>
            </label>
            <description>
```

```
                <language value="en-US">The current version of the app
configuration</language>

            </description>

        </field>

    <fieldGroup>

        <name>

            <language value="en-US">Mobile server</language>

        </name>

        <field keyName="serverNameConfig" type="input">

            <label>

                <language value="en-US">Server name</language>

            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
name.</language>
```

```
            </description>
        </field>
        <field keyName="serverAddressConfig" type="input">
            <label>
                <language value="en-US">Server address</language>
            </label>
            <description>
                <language value="en-US">(Mandatory) Enter the server
address.</language>
            </description>
        </field>
        <field keyName="serverPortConfig" type="input">
            <label>
                <language value="en-US">Server port</language>
```

```
            </label>

            <description>

                <language value="en-US">(Mandatory) Enter the server
port.</language>

            </description>

        </field>

        <field keyName="serverConnectionProtocolTypeConfig" type="input">

            <label>

                <language value="en-US">Connection protocol type</language>

            </label>

            <description>

                <language value="en-US">To specify the connection protocol
type, enter HTTPS or HTTP.</language>

            </description>

        </field>
```

```
    </fieldGroup>

    </presentation>

</managedAppConfiguration>
```

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/.