

MAKE THE
WORLD SEE

Milestone Systems

XProtect® Access 2024 R1

Руководство администратора



Содержание

Copyright, товарные знаки и ограничение ответственности	3
Поддерживаемые продукты и версии VMS	4
Обзор	5
XProtect Access	5
Лицензирование	6
Лицензии на XProtect Access	6
Подробнее о лицензиях	6
Конфигурация	7
Настройка интегрированной системы управления доступом	7
Мастер интеграции системы управления доступом	7
Создать интеграцию системы контроля доступа	8
Подключение к системе управления доступом	8
Связанные камеры	8
Сводка	8
Свойства управления доступом	9
Вкладка «Общие настройки» (управление доступом)	9
Вкладка «Двери и соответствующие камеры» (управление доступом)	10
Вкладка «Событие контроля доступа» (управление доступом)	11
Вкладка «Уведомление запроса доступа» (управление доступом)	12
Вкладка «Владельцы карт» (управление доступом)	13
Настройка запросов доступа	14

Copyright, товарные знаки и ограничение ответственности

Copyright © 2024 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.

Поддерживаемые продукты и версии VMS

В этом руководстве описываются функции, поддерживаемые следующими продуктами XProtect VMS:

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

Milestone проверяет функции, описанные в этом документе, на продуктах XProtect в текущей версии и двух предыдущих версиях выпусков.

Если новые функции поддерживаются только в текущей версии и ни в каких предыдущих версиях, вы можете найти сведения об этом в описании функций.

Документацию по клиентам и расширениям XProtect, поддерживаемым в ранее упомянутых устаревших продуктах VMS XProtect, можно найти на странице загрузки Milestone (<https://www.milestonesys.com/downloads/>).

- XProtect Enterprise
- XProtect Professional
- XProtect Express
- XProtect Essential

Обзор

XProtect Access



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



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

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

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

Преимущества XProtect Smart Client для оператора:

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

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

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

Лицензирование

Лицензии на XProtect Access

Для XProtect Access потребуются следующие лицензии, связанные с управлением доступом:

- Одна базовая лицензия для XProtect Access на неограниченное количество серверов доступа
- По одной лицензии управления доступом для каждой двери, которую нужно интегрировать и контролировать в XProtect Access. При установке XProtect Access лицензии для дверей устанавливаются автоматически.



Установленные лицензии для дверей по умолчанию отключены. Необходимо включить двери, которые вы хотите использовать. Количество включенных дверей должно соответствовать количеству лицензий.

Пример

Вы хотите добавить 10 дверей, при этом у вас есть только 5 лицензий управления доступом для дверей. После добавления первых 5 дверей вы не сможете добавить остальные. Чтобы добавить еще одну дверь, придется удалить одну из уже добавленных дверей.

Пример

Есть одна дверь с двумя точками доступа: устройство для считывания карт на входе и устройство для считывания карт на выходе. Поскольку для каждой двери требуется по одной лицензии управления доступом, в данном случае вам потребуется одна лицензия управления доступом для дверей.

Подробнее о лицензиях

Чтобы получить информацию о текущем состоянии лицензий управления доступом для дверей, разверните узел **Управление доступом**.

Для приобретения дополнительных базовых лицензий XProtect Access или лицензий на двери обратитесь к поставщику.

Конфигурация

Настройка интегрированной системы управления доступом

Требования

- Имеются необходимые лицензии XProtect Access
 - На сервере событий установлено встраиваемое расширение интеграции, соответствующее системе управления доступом
1. Добавьте интегрированную систему управления доступом в систему XProtect. См. раздел [Мастер интеграции системы управления доступом на стр. 7](#). Мастер поможет вам выполнить все основные действия.
 2. Укажите дополнительные свойства для интеграции с системой управления доступом, в частности, для событий контроля доступа может потребоваться сопоставить события из системы управления доступом с категориями событий, которые распознает XProtect. См. раздел [Свойства управления доступом на стр. 9](#).
 3. Создайте роль с соответствующим разрешением на использование функций управления доступом в XProtect Smart Client.
 4. Кроме того, роль необходимо связать с профилем Smart Client.
 5. Система по умолчанию запускает правило, благодаря которому на экране XProtect Smart Client появляются уведомления запроса доступа в случае отказа в доступе. Уведомления запроса доступа можно добавлять и изменять: см. раздел «Уведомление запроса доступа» (свойства) (см. [Вкладка «Уведомление запроса доступа» \(управление доступом\) на стр. 12](#)).
 6. При необходимости можно создать дополнительные правила, основанные на действиях и событиях системы управления доступом.
 7. При необходимости измените общие параметры управления доступом в разделе **Опции > Параметры управления доступом**.

Мастер интеграции системы управления доступом

Мастер создания интеграции с системой управления доступом предназначен для пошаговой настройки начальной интеграции с системой управления доступом. Используйте мастер для выполнения основных действий по настройке. В дальнейшем можно выполнить более детальную настройку.

Прежде чем запустить мастер интеграции управления доступом, убедитесь, что на сервере событий установлено встраиваемое расширение интеграции.

Часть заполняемых полей и их значения по умолчанию наследуются от встраиваемого расширения интеграции. В связи с этим интерфейс мастера может отличаться в зависимости от системы управления доступом, с которой осуществляется интеграция.

Чтобы запустить мастер, выберите **Управление доступом** в дереве, нажмите правой кнопкой мыши и выберите **Создать**.

Создать интеграцию системы контроля доступа

Введите имя и укажите данные подключения системы управления доступом, которую нужно добавить. В зависимости от типа системы указываются такие параметры, как сетевой адрес сервера системы управления доступом, имя пользователя и пароль администратора системы управления доступом.

Система управления видео использует указанные имя пользователя и пароль для входа в систему управления доступом и получения полной конфигурации.

Встраиваемое расширение интеграции может задавать дополнительные параметры, которые не указаны в мастере. Их можно изменить в разделе **Общие настройки** после настройки интеграции. Значения параметров по умолчанию задаются встраиваемым расширением или системой XProtect.

Подключение к системе управления доступом

После успешной интеграции встраиваемого расширения на экране появится краткое описание полученной конфигурации системы управления доступом. Прежде чем перейти к следующему шагу мастера, просмотрите список и убедитесь, что все элементы интегрированы.

Связанные камеры

Сопоставьте точки доступа системы управления доступом с камерами системы XProtect, на которых будут отображаться соответствующие видео событий, связанных с дверьми.

К одной точке доступа можно привязать несколько камер. Пользователь XProtect Smart Client может просматривать видео со всех камер, в частности, при расследовании событий.

Пользователь XProtect Smart Client также может добавить одну из камер при настройке элементов представления в разделе **Контроль доступа**.

Двери с лицензией по умолчанию включены. Чтобы отключить дверь и освободить лицензию управления доступом для дверей, снимите соответствующий флажок.

Сводка

Интеграция системы управления доступом успешно создана в XProtect с параметрами по умолчанию, наследуемыми от встраиваемого расширения интеграции. Чтобы получить доступ к новой системе управления доступом и начать ее использовать, пользователи клиента должны войти в XProtect Smart Client.

При необходимости в конфигурацию можно внести изменения.

Свойства управления доступом

Вкладка «Общие настройки» (управление доступом)

Имя	Описание
Включить	<p>По умолчанию системы включены, то есть они доступны в XProtect Smart Client для пользователей с соответствующими разрешениями, и система XProtect получает события управления доступом.</p> <p>Вы можете отключить систему, например на время технического обслуживания, чтобы исключить срабатывание излишних сигналов тревоги.</p>
Имя	Имя интеграции управления доступом, которое отображается в приложении для управления и на клиентах. Вы можете перезаписать существующее имя и задать новое.
Описание	Описание интеграции системы управления доступом. Не обязательно.
Встраиваемое расширение интеграции	Тип системы управления доступом, выбранный при первоначальной интеграции.
Последнее обновление конфигурации	Дата и время последнего импорта конфигурации из системы управления доступом.
Обновить конфигурацию	<p>Нажмите эту кнопку, чтобы отразить изменения конфигурации, внесенные в систему управления доступом, в XProtect, например если вы добавили или удалили дверь.</p> <p>Откроется сводка изменений в конфигурации системы управления доступом. Прежде чем применить новую конфигурацию, изучите список, чтобы убедиться, что параметры системы управления доступом правильно отражены.</p>
Требуется имя пользователя оператора	<p>Включите дополнительное имя пользователя для пользователей клиента, если система управления доступом поддерживает дифференцированные разрешения пользователей. Если включить этот параметр, система управления доступом в клиенте XProtect Mobile будет недоступна.</p> <p>Это параметр доступен только в том случае, если встраиваемое расширение интеграции поддерживает дифференцированные разрешения пользователей.</p>

Имена и содержимое следующих полей импортируются из встраиваемого расширения интеграции. Ниже приведены примеры типичных полей:

Имя	Описание
Адрес	Введите адрес сервера, на котором размещается интегрированная система управления доступом.
Порт	Укажите номер порта на сервере, к которому подключена система управления доступом.
Имя пользователя	Введите имя пользователя согласно требованиям системы управления доступом. Этот пользователь будет администратором интегрированной системы в XProtect.
Пароль	Задайте пароль для этого пользователя.

Вкладка «Двери и соответствующие камеры» (управление доступом)

На этой вкладке отображаются связи между точками доступа к дверям и камерами, микрофонами и динамиками. Сопоставить камеры можно в мастере интеграции: эти настройки можно изменить в любой момент. Сопоставление с микрофонами и динамиками происходит автоматически по соответствующему микрофону или динамику на камере.

Имя	Описание
Двери	<p>Списки доступных точек доступа для дверей, определенных в системе управления доступом, с группировкой по дверям.</p> <p>Для более удобной навигации между дверями отфильтруйте двери в системе управления доступом с помощью раскрывающегося списка в верхней части экрана.</p> <p>Включено: Двери с лицензией по умолчанию включены. Чтобы освободить лицензию, достаточно отключить дверь.</p> <p>Лицензия: Информация о наличии соответствующей лицензии на дверь или об истечении ее срока действия. Если дверь отключена, это поле будет пустым.</p> <p>Удалить: Нажмите Удалить, чтобы удалить камеру из точки доступа. Если удалить все камеры, автоматически снимается флажок у связанных с ними камер.</p>

Имя	Описание
Камеры	<p>Список камер, настроенных в системе XProtect.</p> <p>Выберите камеру из списка и перетащите ее в соответствующую точку доступа, чтобы связать точку доступа с камерой.</p>

Вкладка «Событие контроля доступа» (управление доступом)

Категории событий обеспечивают возможность группировки событий. Конфигурация категорий событий влияет на функционирование управления доступом в системе XProtect, с ее помощью вы можете, к примеру, задать сигнал тревоги, который будет срабатывать по нескольким типам событий.

Имя	Описание
Событие контроля доступа	<p>Список событий контроля доступа, импортированных из системы управления доступом. Встраиваемое расширение интеграции по умолчанию обеспечивает включение и отключение событий. После интеграции вы можете в любое время отключить или включить события.</p> <p>Если событие включено, оно сохраняется в базе данных событий XProtect, а также доступно, например, для фильтрации в XProtect Smart Client.</p>
Тип источника	Устройство контроля доступа, которое активирует событие контроля доступа.
Категория события	<p>Вы можете назначать событиям контроля доступа одну или несколько категорий событий или не назначать их вовсе. В процессе интеграции система автоматически сопоставляет соответствующие категории с событиями. Таким образом обеспечивается настройка системы XProtect по умолчанию. Сопоставление можно изменить в любой момент.</p> <p>Встроенные категории событий:</p> <ul style="list-style-type: none"> • Доступ запрещен • Доступ разрешен • Запрос доступа • Тревога

Имя	Описание
	<ul style="list-style-type: none"> • Ошибка • Предупреждение <p>Кроме того, выводятся события и категории событий, заданные встраиваемым расширением интеграции. Также можно задать пользовательские категории событий, подробнее см. в разделе Пользовательские категории.</p> <div style="border: 1px solid #ccc; background-color: #fff9e6; padding: 10px; margin-top: 10px;">  <p>При изменении категорий событий в XProtect Corporate убедитесь, что существующие правила управления доступом продолжают действовать.</p> </div>
Категории пользователя	<p>Создание, изменение или удаление пользовательских категорий событий.</p> <p>Если встроенные категории событий не отвечают вашим требованиям, вы можете создать собственные. Например, при определении инициирующих событий для действий управления доступом.</p> <p>Категории универсальны для всех систем интеграции, добавленных в систему XProtect. Они обеспечивают возможность межсистемного взаимодействия, например при определении тревог.</p> <p>При удалении пользовательской категории событий, которая используется какой-либо интеграцией, появится соответствующее предупреждение. При подтверждении удаления все конфигурации, созданные с помощью этой категории, включая действия управления доступом, перестанут работать.</p>

Вкладка «Уведомление запроса доступа» (управление доступом)

С ее помощью можно задать уведомления запроса доступа, которые будут появляться на экране XProtect Smart Client при наступлении определенного события.

Имя	Описание
Имя	Введите имя уведомления запроса доступа.
Добавить	Нажмите, чтобы добавить и настроить уведомления запроса доступа.

Имя	Описание
<p>уведомление запроса доступа</p>	<p>Чтобы удалить уведомление, нажмите значок X в правой части.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;">  <p>Если пользователь XProtect Smart Client авторизуется на родительском сайте в иерархии Milestone Federated Architecture, в XProtect Smart Client также отображаются уведомления запроса доступа с дочерних сайтов.</p> </div>
<p>Сведения уведомления запроса доступа</p>	<p>Укажите, какие камеры, микрофоны и динамики будут отображаться в уведомлениях запроса доступа при наступлении определенного события. Задайте звуковой сигнал, который будет оповещать пользователя о всплывающем уведомлении.</p>
<p>Добавить команду</p>	<p>Выберите команды, которые должны быть доступны в виде кнопок в диалоговых окнах уведомления запроса доступа в XProtect Smart Client.</p> <p>Связанные команды запроса доступа:</p> <ul style="list-style-type: none"> • Активация всех команд, связанных с операциями запроса доступа, доступных на исходном устройстве. Например, Открыть дверь. <p>Все связанные команды:</p> <ul style="list-style-type: none"> • Активация всех команд на исходном устройстве. <p>Команда контроля доступа:</p> <ul style="list-style-type: none"> • Активация выбранной команды контроля доступа. <p>Команда системы:</p> <ul style="list-style-type: none"> • Активация команды, предустановленной в системе XProtect. <p>Чтобы удалить команду, нажмите значок X в правой части.</p>

Вкладка «Владельцы карт» (управление доступом)

Используйте вкладку **Владельцы карт** для просмотра соответствующей информации в системе управления доступом.

Имя	Описание
Поиск владельца карты	Введите имя владельца карты: если такое имя существует, оно появится в списке.
Имя	Список имен владельцев карт, полученных из системы управления доступом.
Тип	Список типов владельцев карт, например: <ul style="list-style-type: none"> • Сотрудник • Охрана • Гость

Если ваша система управления доступом поддерживает добавление/удаление изображений в системе XProtect, вы можете добавить соответствующие фотографии для владельцев карт. Это удобно, если в системе управления доступом отсутствуют фотографии владельцев карт.

Имя	Описание
Выберите изображение	<p>Укажите путь к файлу с фотографией владельца карты. Эта кнопка не доступна, если изображения обрабатываются системой управления доступом.</p> <p>Допустимые форматы файлов: BMP, PNG и JPG.</p> <p>Размер изображений корректируется, чтобы обеспечить оптимальное представление.</p> <p>Milestone рекомендует использовать квадратное изображение.</p>
Удалить изображение	Нажмите, чтобы удалить изображение. Если изображение хранилось в системе управления доступом, оно будет отображаться после удаления.

Настройка запросов доступа

Существует несколько типов событий контроля доступа, например **Доступ запрещен** и **Доступ разрешен**. Чтобы включить уведомления запроса доступа, необходимо связать тип события с

категорией события **Запрос доступа**. Тип **Доступ запрещен** по умолчанию связан с событием **Запрос доступа**: Уведомления запроса доступа отправляются только в случае отказа в доступе. Чтобы изменить этот параметр, выполните действия, описанные в данном разделе.

Требования: Включите уведомления для ролей пользователей клиента. В соответствующей роли перейдите на вкладку **Управление доступом**, выберите **Управление доступом**, а затем установите флажок **Получать уведомления**.

Действия:

1. На панели **Навигация по сайту** выберите **Управление доступом**.
2. На вкладке **События контроля доступа** в столбце **Событие контроля доступа** найдите тип события, который хотите изменить.
3. Чтобы отключить запросы доступа для того или иного типа события, в столбце **Категория события** выберите и снимите флажок **Запрос доступа**.
4. Чтобы включить запросы доступа для дополнительного типа события, в столбце **Категория события** выберите и установите флажок **Запрос доступа**.
5. Сохраните изменения.



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/>.

