Обеспечение безопасности с помощью приложения AXIS Device Manager

Версия 1.0

AXIS COMMUNICATIONS

Оглавление

1. Введение

В секторах, связанных с видеонаблюдением и обеспечением безопасности, постоянно возрастает роль такого фактора как кибербезопасность. Для эффективного обеспечения кибербезопасности необходимо предусмотреть достаточную глубину защиты для каждого уровня вашей IP-сети — начиная с выбираемых вами устройств и партнеров для совместной работы до тех требований, которые они вместе с вами устанавливают.

1.1 Три уровня защиты от кибератак

Мы обеспечиваем три уровня защиты от кибератак:

1. Управление безопасностью: данный уровень требует применения средств обеспечения безопасности, необходимых для нейтрализации ваших реальных угроз. Здесь можно выделить две составляющие: средства обеспечения безопасности и экономически эффективное управление ими. Средства обеспечения безопасности — это защитные меры или средства противодействия угрозам, которые применяются, чтобы избежать, обнаружить, создать препятствия или минимизировать риски нарушения безопасности по отношению к физическому имуществу, информации, компьютерным системам или другим активам.

2. Управление уязвимостями: сюда относится все то, что делает компания Axis для реализации самых современных подходов в сфере кибербезопасности применительно к проектированию, разработке и тестированию своих устройств с целью выявления и сокращения количества уязвимых мест, которые могут использовать злоумышленники. В случае обнаружения уязвимостей запускается процесс управления в ходе которого наши специалисты незамедлительно устраняют критически опасные уязвимости и выпускают сообщения с рекомендациями по сохранению безопасности.

3. Обучение и сотрудничество: это уровень взаимодействия между компанией Axis, вашей организацией и партнерами, имеющий отношение к получению единого четкого понимания угроз в вашей IP-сети, а также их возможного влияния и способов защиты сети.

1.2 Назначение данного документа

В этом руководстве по работе с программным приложением AXIS Device Manager описывается его применение для повышения надежности системы и укрепления ее безопасности. В руководстве подробно разобраны ключевые аспекты и даны соответствующие рекомендации.

1.3 О приложении AXIS Device Manager

AXIS Device Manager представляет собой прикладное программное средство, которое развертывается на объекте заказчика и позволяет просто, эффективно и безопасно справляться со всеми главными задачами управления, которые связаны с установкой, обеспечением безопасности и обслуживанием устройств (см. таблицу ниже). Данное приложение может управлять системами, включающими до двух тысяч устройств Axis на одном объекте или несколько тысяч устройств на нескольких объектах. AXIS Device Manager позволяет эффективно развернуть средства обеспечения кибербезопасности для защиты ваших сетевых устройств и привести их в соответствие с инфраструктурой обеспечения безопасности.

Функции управления устройствами приложения AXIS Device Manager

Установка	Обслуживание
> Назначение IP-адреса > Экспортирование списка устройств, контроль и учет активов* > Управление пользователями и паролями* > Управление платформой ACAP > Обновление встроенного ПО* > Управление сертификатами HTTPS* > Распределение сертификатов по стандарту IEEE 802.1x* > Назначение меток устройствам	> Статус устройств > Сбор данных с устройств > Настройка устройств и копирование конфигураций на несколько устройств > Подключение к нескольким серверам/системам > Точки восстановления > Восстановление заводских настроек по умолчанию > Замена устройств > Обновление сертификатов и управление сертификатами* > Усиление кибербезопасности*

** функция управления кибербезопасностью*

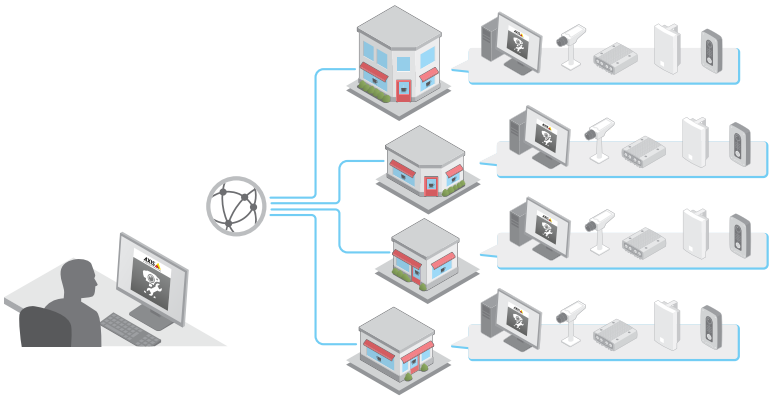


Рис. 1. Управление несколькими объектами

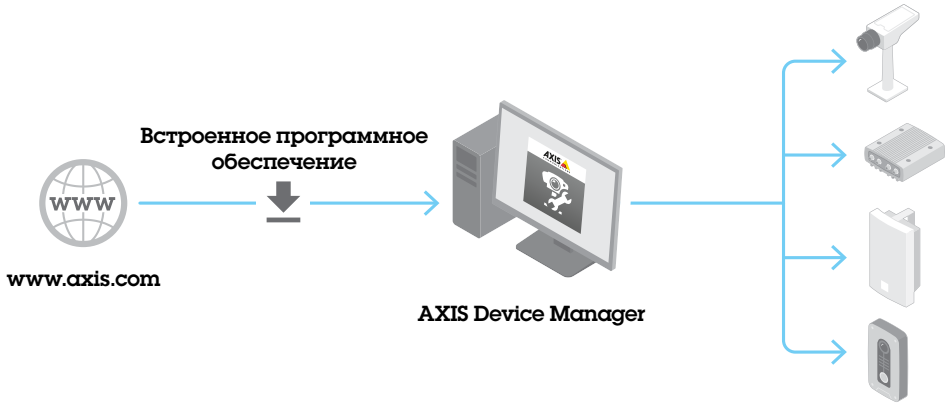


Рис. 2. Обновление встроенного ПО

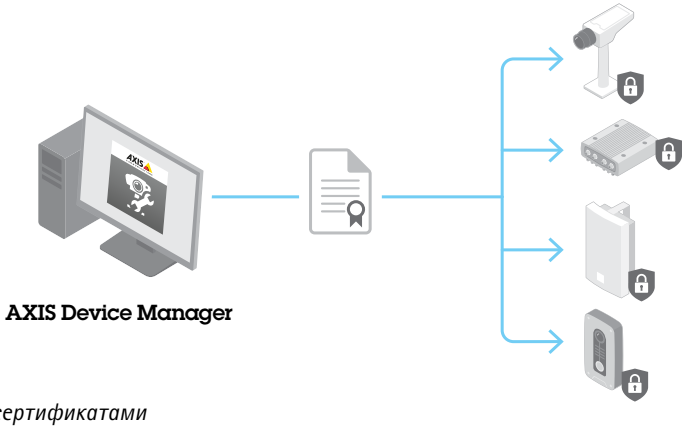


Рис. 3. Управление сертификатами

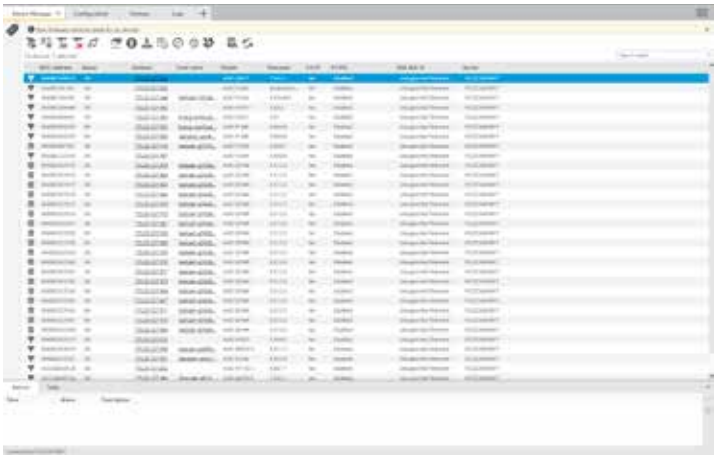
2. Перечень устройств

Фундаментальным аспектом обеспечения безопасности корпоративной сети является поддержание в актуальном состоянии полного перечня всех сетевых устройств. При создании или проверке общей политики обеспечения безопасности важно иметь четкую и документально оформленную информацию о каждом устройстве, а не только о критически важных активах. Это связано с тем, что даже единственное неучтенное устройство может быть использовано для несанкционированного доступа к сети. Нельзя защитить устройство, если его не учли или о нем нет полных данных.

Составление перечня устройств — это важный шаг для обеспечения безопасности корпоративной сети. Приложение AXIS Device Manager помогает обеспечить безопасность благодаря тому, что:

> при работе с аудитами и изучении реагирования в случае инцидента вы получаете простой доступ к актуальному полному перечню ваших сетевых устройств
> вы получаете полный список ваших устройств с сортировкой по общему количеству, типу, номерам моделей и так далее
> приложение указывает статус каждого устройства в вашей сети

Рекомендации
AXIS Device Manager — это автоматическое средство получения доступа к перечню сетевых устройств Axis в режиме реального времени. Приложение позволяет автоматически идентифицировать, составлять список и сортировать устройства. Не менее важной является возможность работы с метками, что позволяет пользователю группировать и сортировать устройства исходя из собственных критериев. Благодаря этому можно легко получить и документально оформить общие сведения о всех устройствах Axis в вашей сети.



AXIS Device Manager дает четкое представление о всех ваших устройствах в виде перечня.

3. Политика управления учетными данными и паролями

В системе защиты сетевых ресурсов важную роль играет проверка подлинности и контроль прав доступа пользователя. Реализация соответствующей политики помогает уменьшить риск случайных или преднамеренных несанкционированных действий на протяжении длительного времени. Ключевым моментом здесь является снижение вероятности раскрытия паролей, поэтому важно серьезно подохдить к их выбору. Однако, сотрудники могут передавать друг другу пароли устройств в пределах организации. Если это происходит, то уже неизвестно, кто получает доступ к тому или иному устройству. Приложение AXIS Device Manager поможет вам легко управлять разными учетными записями и паролями для устройств Axis.

Причины, по которым следует вводить в устройства учетные данные не одного, а нескольких пользователей:

> Это позволяет контролировать уровни доступа для разных типов пользователей (машины и люди)
> Снижается вероятность раскрытия пароля привилегированного пользователя (root)
> Можно выполнить сброс учетных данных для одного типа пользователей, и это не повлияет на остальных пользователей

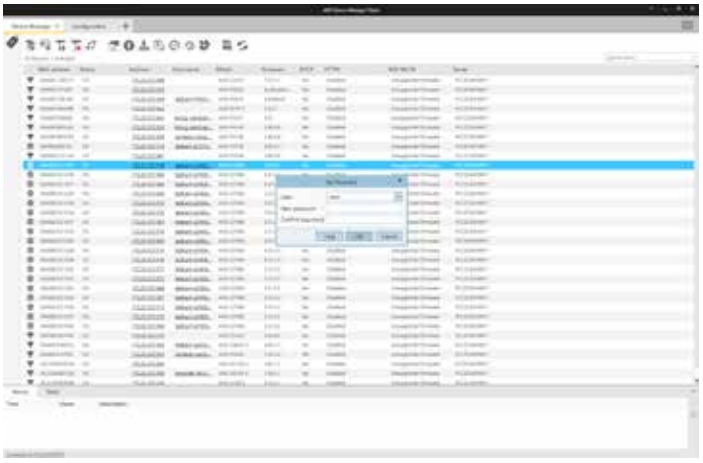
Работа с уровнями доступа в приложении AXIS Device Manager

Устройства Axis в приложении AXIS Device Manager могут поддерживать несколько учетных записей и относиться к одному из трех разных уровней доступа: Наблюдатель, Оператор и Администратор. Управление уровнями доступа в сетевых камерах Axis осуществляется следующим образом.

Пользователи с правами Наблюдателя имеют доступ к видео и PTZ-управлению. Права Оператора позволяют оптимизировать настройки камеры и профили видеопотока. Права Администратора служат для администрирования учетных записей, изменения сетевых параметров и контроля ряда служб, работающих в устройстве. Для каждой роли, имеющей доступ к камере, должна быть создана собственная учетная запись.

Рекомендуемая последовательность действий

> Прежде чем добавить камеры в систему управления видео (VMS), рекомендуется добавить их в приложение AXIS Device Manager
> Выберите все камеры в AXIS Device Manager и создайте новый пароль пользователя с именем "vms" (или другим), задав для него надежный пароль. Права доступа должны соответствовать требованиям VMS — это может быть либо Оператор, либо Администратор (следует уточнить у производителя).
> Добавьте устройства в VMS с учетной записью "vms" и заданным вами паролем
> Вернитесь в приложение AXIS Device Manager и вновь выберите все камеры, после чего сбросьте пароль для учетной записи "root", изменив его на новый надежный пароль. Пароль для учетной записи "root" должен быть известен лишь ограниченному количеству лиц (тех, кто использует AXIS Device Manager).
> Не следует сообщать пароль для учетной записи "root" тем сотрудникам организации, которым необходимо использовать веб-браузер для доступа к устройству с целью обслуживания или диагностики неполадок. В этом случае создайте в AXIS Device Manager новую (временную) учетную запись для выбранного устройства или нескольких устройств с правами доступа Администратора или Оператора. После выполнения соответствующей задачи удалите эту временную учетную запись в приложении AXIS Device Manager.
> AXIS Device Manager поддерживает не только локальных администраторов, но также доменных пользователей и группы. Если доступ к клиенту AXIS Device Manager будет осуществляться только с той же машины, где установлен сервер AXIS Device Manager, то можно использовать локального администратора. Если обслуживающее систему лицо будет использовать удаленные клиенты, то рекомендуется использовать доменных пользователей.



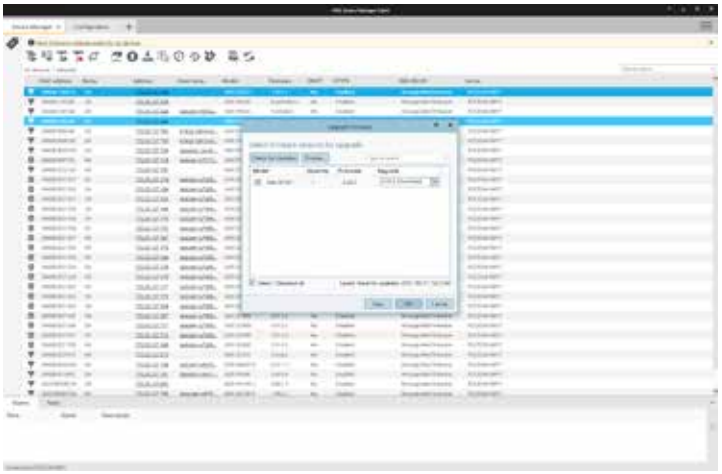
Изменение ролей и паролей пользователя в AXIS Device Manager.

4. Обновления встроенного ПО

В последние версии встроенного ПО входят исправления для известных уязвимостей. Важно всегда работать с самым свежим программным обеспечением, поскольку злоумышленники могут пытаться использовать любые известные уязвимости. Не менее важно и то, что быстрое внедрение нового встроенного ПО существенно улучшает эксплуатационные характеристики и устраняет узкие места, связанные с ручным развертыванием нового выпуска. Приложение AXIS Device Manager подключается к сайту www.axis.com и загружает последнюю версию встроенного ПО или свежие выпуски сервисов. Если вы не хотите загружать файлы из интернета непосредственно в свою сеть, то можно сохранить обновления на флэш-накопитель USB, а затем загрузить их в свой клиент AXIS Device Manager. Кроме того, приложение сообщает о наличии новой версии встроенного ПО и позволяет быстро развернуть обновление на устройствах Axis.

Причины, по которым следует всегда использовать последнюю версию встроенного ПО:

> В этом случае ваша сеть и устройства будут защищены от известных уязвимостей благодаря самым последним исправлениям, внесенным в ПО, что особенно актуально в случае критических уязвимостей
> ПО ваших устройств будет обновлено для реализации доступных улучшений рабочих характеристик; в нем также будут устранены все известные ошибки или упущения
> Вы сразу же получаете доступ к последним функциям и расширенным возможностям



Приложение AXIS Device Manager упрощает процесс обновления встроенного ПО благодаря уведомлениям на экране и интуитивно понятным диалоговым сообщениям.

5. Дополнительное усиление безопасности

Разумная политика управления пользователями и паролями, а также использование последних версий встроенного ПО для работающих устройств позволяют нейтрализовать распространенные риски, связанные с доступом к этим устройствам. В руководстве по усилению безопасности Axis Hardening Guide описаны дополнительные меры для снижения рисков в крупных организациях, выполняющих особо важные функции. К таким мерам относится отключение служб, которые не используются, и включение служб, способствующих обнаружению и отслеживанию возможных проявлений злоумышленных действий или каких-либо нарушений.

AXIS Device Manager упрощает процесс развертывания некоторых из указанных политик. Компания Axis предлагает шаблон настройки конфигурации для задания основных рекомендуемых парметров. С подробной информацией можно ознакомиться на нашем сайте: www.axis.com/products/axis-device-manager/support-and-documentation.

Процедура улучшения защиты устройств согласно руководству по усилению безопасности Axis Hardening Guide:

> Загрузите файл шаблона настройки конфигурации с улучшенными характеристиками безопасности со страницы www.axis.com/products/axis-device-manager/support-and-documentation убрать точку
> Измените файл конфигурации, выбрав в нем необходимые пункты
> Выберите устройства
> Щелкните правой кнопкой мыши и выберите "Настроить устройства | Настройка..."
> Выберите "Файл конфигурации" и выберите загруженный файл
> Задайте необходимые значения параметров

6. Служба "Центр сертификации"

Центр сертификации (ЦС) – это служба, выдающая цифровые сертификаты серверам, клиентам или пользователям. ЦС может быть общедоступным или частным. Для общедоступных служб, к которым относятся открытые веб-сайты и электронная почта, обычно используют публичные доверенные центры сертификации, например Comodo и Symantec (прежнее название Verisign).

Частный ЦС (обычно это служба сертификатов Active Directory) выдает сертификаты для служб внутренних/частных сетей. В системе управления видео это относится, главным образом, к сетевому шифрованию по протоколу Hyper Text Transfer Protocol Secure (HTTPS) и стандарту IEEE 802.1x, который служит для контроля сетевого доступа. Приложение AXIS Device Manager включает в себя службу ЦС для устройств Axis, которая может работать либо как частный корневой ЦС, либо как частный промежуточный ЦС, которые являются частью корпоративной инфраструктуры сертификации открытых ключей (PKI).

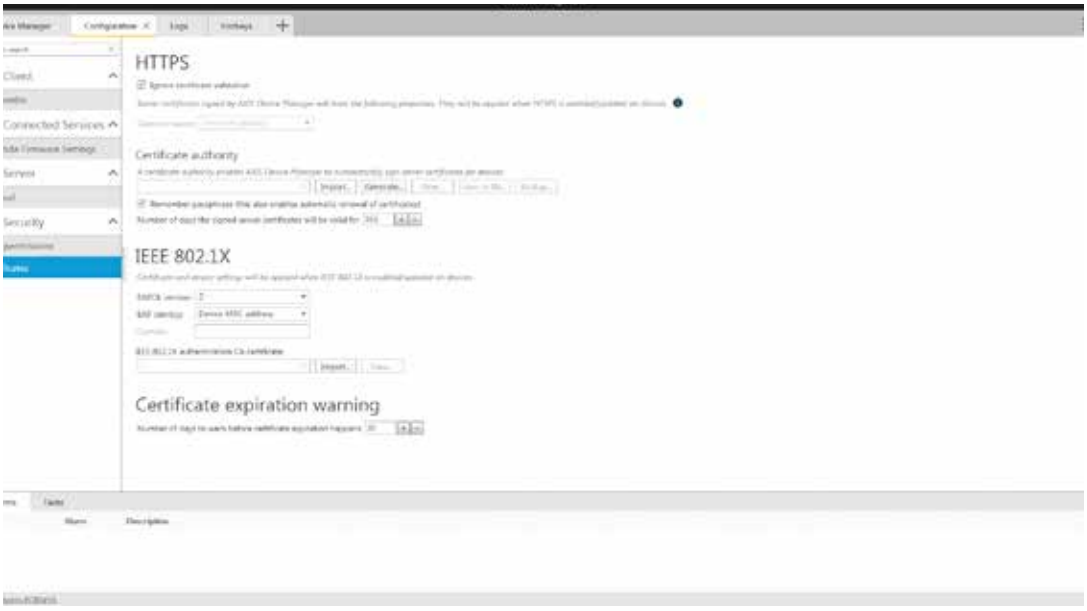
Сертификаты, подписанные ЦС, используются в качестве сертификатов как для IEEE 802.1x (клиент), так и для HTTPS (сервер).

HTTPS

Протокол HTTPS представляет собой безопасную версию протокола HTTP. В случае HTTPS установление связи между клиентом и сервером предусматривает шифрование данных. Для установления зашифрованного соединения достаточно самозаверяемых сертификатов. Принципиальной разницы между уровнем шифрования самозаверяемых сертификатов и сертификатов, подписанных центром сертификации, нет. Основое отличие заключается в том, что самозаверяемые сертификаты не защищают от такой сетевой атаки как спуфинг, когда атакующий компьютер пытается выдать себя за легальный сервер. Сертификаты, подписанные ЦС, повышают для клиентов степень доверия при проверке подлинности для получения доступа к устройству. Следует иметь в виду, что для шифрования видео клиент системы управления видео (VMS) должен поддерживать запросы к видеороликам по HTTPS (RTP по RTSP по HTTPS).

IEEE 802.1X
Этот стандарт, обозначаемый как 802.1X, предотвращает доступ к локальной сети для несанкционированных сетевых устройств. Устройство должно подтвердить свою подлинность, чтобы ему был разрешен доступ к сети (и ее ресурсам). Для этого можно использовать разные методы проверки подлинности, например: MAC-адрес (фильтрация MAC-адресов), имя пользователя и пароль, сертификат клиента. Решение о том, какой метод будет использоваться, принимает владелец системы с учетом реальных угроз, рисков и стоимости.

Эксплуатация инфраструктуры, отвечающей стандарту 802.1X, требует инвестиций. Необходимы управляемые коммутаторы и дополнительные серверы; обычно при этом используется протокол RADIUS (Remote Authentication Dial-In User Service). Использование сертификатов клиентов требует наличия ЦС (частного или общедоступного), который может выдавать такие сертификаты. В большинстве случаев для обслуживания и слежения за работой инфраструктуры требуется персонал.



Настройка сертификатов в AXIS Device Manager.

7. Управление сертификатами на протяжении жизненного цикла

Управление сертификатами на протяжении жизненного цикла — это возможность эффективной работы со всеми процессами и задачами, связанными с выдачей, установкой, проверкой, устранением нарушений и обновлением сертификатов в течение длительного периода времени. AXIS Device Manager обеспечивает эффективное управление сертификатами, поскольку это приложение позволяет администраторам:

> выдавать сертификаты, подписанные ЦС, в случае недоступности какого-либо другого ЦС
> свободно распределять сертификаты, отвечающие стандарту IEEE 802.1X
> без затруднений развертывать сертификаты HTTPS
> следить за окончанием сроков действия сертификатов
> с легкостью обновлять сертификаты до окончания сроков их действия

Рекомендации частных корневых и промежуточных ЦС
Не рекомендуется применять устройства Axis в качестве общедоступных серверов, предназначенных для работы с широкой аудиторией. Следовательно, использование публичного ЦС для частных ресурсов не является экономически эффективным.

Для HTTPS сервер VMS является единственным клиентом, которому необходимо проверять, что он получает доступ к доверенной камере. Клиенты-операторы никогда не получат непосредственный доступ к камерам, поскольку доступ к живому и записанному видео предоставляет сервер VMS. В такой ситуации нет особого смысла встраивать сертификаты сервера камер в существующую корпоративную инфраструктуру PKI.

Наиболее эффективным решением является использование приложения AXIS Device Manager в качестве частного ЦС. После создания сертификата корневого ЦС установите сертификат AXIS Device Manager в хранилище сертификатов сервера VMS. При наличии других клиентов, имеющих непосредственный доступ к камерам (для обслуживания или диагностики), установите корневой ЦС приложения AXIS Device Manager и в эти клиенты.

При использовании стандарта 802.1X у камеры должен быть сертификат клиента, чтобы пройти проверку подлинности на RADIUS-сервере. Рекомендуется, чтобы администратор корпоративной инфраструктуры PKI и (или) ЦС создал сертификат промежуточного ЦС и экспортировал его в виде сертификата PKCS#12 (P12), который можно установить в приложении AXIS Device Manager.

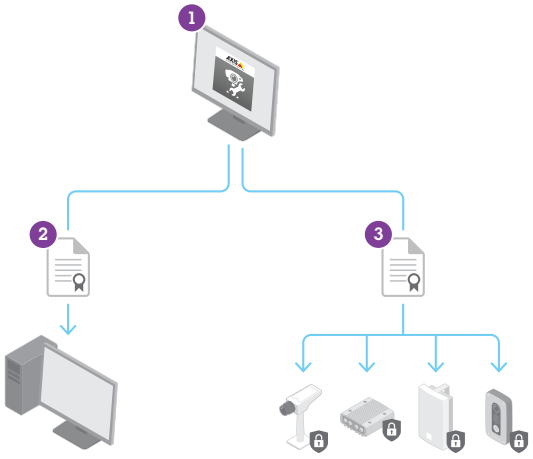


Рис. 4, левая часть. Процедура управления сертификатами HTTPS:
1) создание сертификата корневого или промежуточного ЦС в AXIS Device Manager; 2) экспортирование сертификата ЦС в VMS; 3) загрузка сертификатов сервера на устройства.

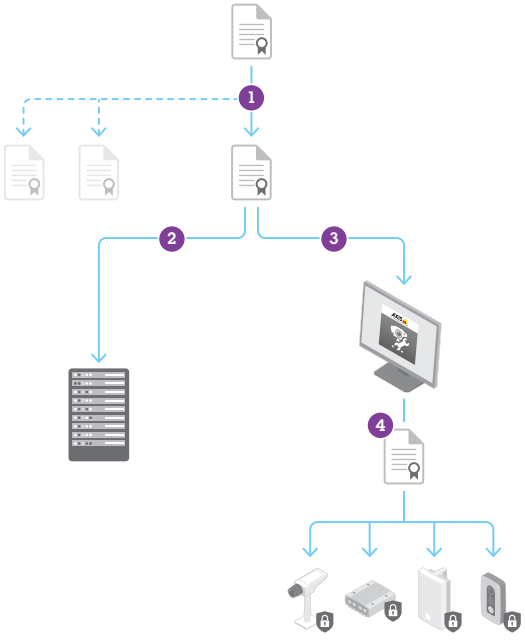


Рис. 5, правая часть. Процедура распределения сертификатов IEEE 802.1X: 1) создание сертификата промежуточного ЦС и сертификата клиента; 2) установка сертификата ЦС на RADIUS-сервере; 3) импортирование сертификата ЦС в AXIS Device Manager; 4) загрузка ЦС и сертификатов клиента на устройства.

8. Заключение

Управление системой обеспечения безопасности и контроль ее работы являются важными составляющими для реализации эффективного подхода, призванного гарантировать кибербезопасность. Каждая составляющая представляет собой непрерывный процесс, требующий поддержания постоянного статуса в сочетании с необходимыми последующими действиями, чтобы нейтрализовать любую потенциальную угрозу, которая может повлиять на работу IP-сети. Приложение AXIS Device Manager — это не просто инструмент для управления вашими устройствами, но и возможность повысить безопасность вашей сети. Для получения более подробной информации или поддержки обращайтесь к местному представителю Axis или ознакомьтесь с сайтом www.axis.com.

О компании Axis Communications

Компания Axis является разработчиком интеллектуальных решений, направленных на построение более разумного и безопасного мира. Будучи лидером на рынке сетевого видео, компания Axis стимулирует развитие отрасли за счет постоянного выпуска инновационных сетевых устройств, созданных на открытой платформе. Благодаря глобальной партнерской сети клиенты получают оперативный доступ ко всем преимуществам наших устройств. Компания Axis имеет долгосрочные отношения с партнерами, предоставляя им информацию и принципиально новые сетевые устройства ля работы как на существующих, так и на новых рынках.

Численность персонала Axis превышает 2 700 специалистов из более чем 50 стран в разных регионах земного шара, а глобальная партнерская сеть насчитывает свыше 90 000 партнеров. Компания Axis была основана в Швеции в 1984 году. Акции компании котируются на Стокгольмской фондовой бирже NASDAQ Stockholm под тикером AXIS.

Более подробную информацию о компании Axis можно найти на нашем веб-сайте www.axis.com.