Руководство по киберзащите

Методы защиты видеосистем MOBOTIX

Камера • VMS • NAS

MOBOTIX

О данном руководстве

Кибератаки на подключенное к Интернету программное и аппаратное обеспечение являются растущей проблемой. В последние годы злоумышленники все чаще выискивают слабые звенья в периметре безопасности для доступа к критическим приложениям и конфиденциальным данным.Технологии видеонаблюдения являются важной частью систем безопасности любых объектов и часто встраиваются в распределенные корпоративные сети. Поэтому устройства видеонаблюдения все чаще становятся объектами скоординированных кибератак. Приняв во внимание эту новую тенденцию, компания MOBOTIX разработала комплект **встроенных инструментов и функций**, который позволяет администраторам ИТ-безопасности настраивать каждое устройство в качестве части многоуровневой системы кибербезопасности. Эти инструменты, используемые совместно с другими элементами безопасности, такими как брандмауэры и сегментация сети, могут уменьшить поверхность атаки, приходящуюся на долю устройств MOBOTIX, в рамках политики безопасного доступа для администраторов и пользователей.

В этом руководстве представлены практические рекомендации по настройке устройств MOBOTIX для обеспечения максимальной защиты от кибератак, а также рекомендации по эффективной практике создания безопасной инфраструктуры видеонаблюдения.

Примечание. Настоящий документ предназначен для ознакомления ответственного администратора со всеми возможными мерами защиты системы MOBOTIX. Учитывая особенности различных областей применения и во избежание неоправданного изменения конфигурации, может оказаться нецелесообразным выполнять все процедуры, описанные в этом руководстве.

Настройка камеры

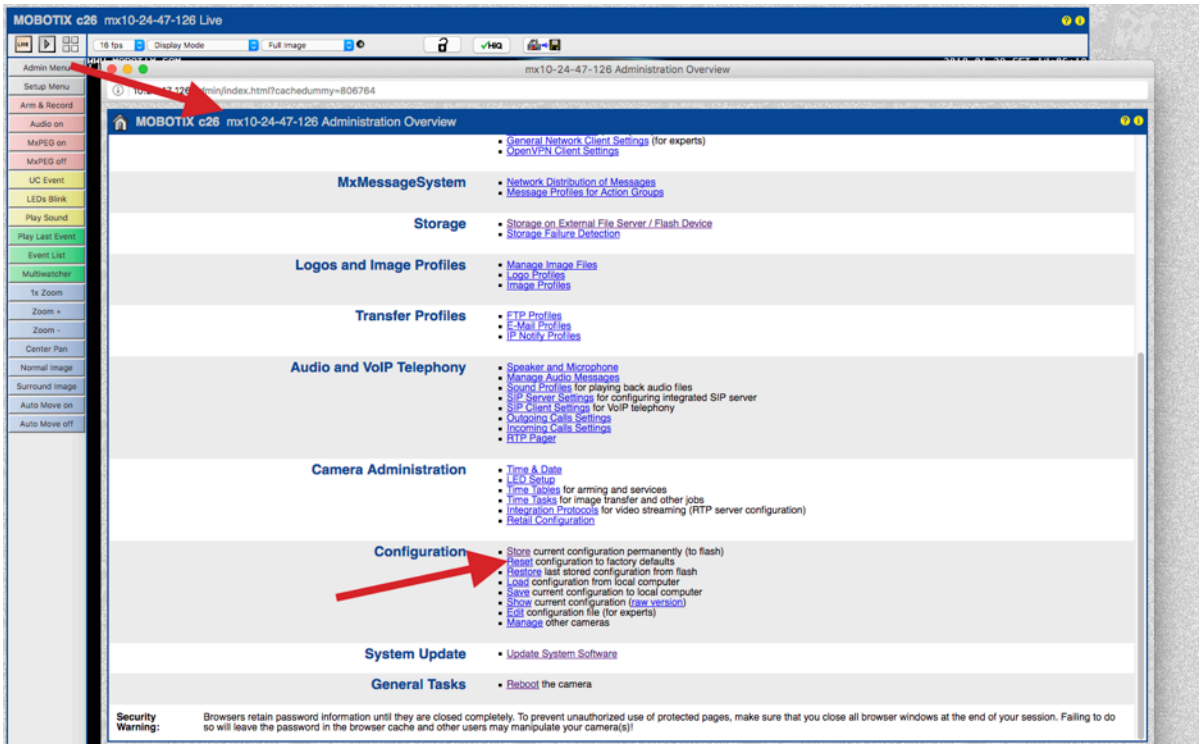
1. Своевременно обновляйте встроенное ПО камер

Встроенное ПО MOBOTIX можно бесплатно загрузить на нашем сайте: www.mobotix.com > Поддержка > Download Center

Не знаете, как поступить? Обратитесь к следующей краткой инструкции: www.mobotix.com > Поддержка > Download Center > Документация > Брошюры и информация > Краткая инструкция > Mx_CG_FirmwareUpdate.pdf

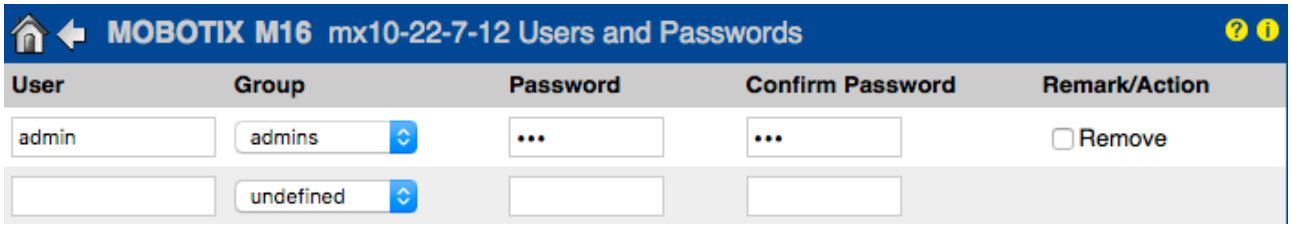
2. Восстановите заводские настройки

Admin Menu > Конфигурация > Сброс конфигурации до заводских настроек



3. Смените пароль администратора, установленный по умолчанию

Admin Menu > Безопасность > Пользователи и пароли



При первом вызове камеры пароль по умолчанию "meinsm" необходимо всегда менять.

Закончив настройку учетных данных пользователей, паролей и групп, следует обязательно сохранить параметры в постоянной памяти камеры. В противном случае измененная конфигурация будет действовать только до следующей перезагрузки камеры. Пользуйтесь кнопкой Close в заключительной части диалогового окна: после нажатия на эту кнопку система автоматически предлагает сохранить конфигурацию в постоянной памяти камеры.

Храните информацию о своем пароле в надежном месте. Особое внимание нужно обратить на то, чтобы сохранить пароль хотя бы одного пользователя из группы администраторов. Без пароля доступ к камере с правами администратора становится невозможным, а обойти пароль нельзя. Также невозможно получить пароль из данных конфигурации, сохраненных в постоянной памяти.

Правила создания надежного пароля

- Используйте не менее 8 символов (и не более 99)
- По меньшей мере один символ в верхнем регистре
- По меньшей мере один символ в нижнем регистре
- По меньшей мере одна цифра
- По меньшей мере один специальный символ: ! “ # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ `{ | } ~
- Не используйте обычные слова и даты

Политика сброса пароля: если пароль администратора больше не доступен, камера должна быть сброшена через MOBOTIX за дополнительную плату!

4. Создайте несколько групп пользователей с разными правами

Admin Menu > Безопасность > Пользователи и пароли

По большому счету некоторые права большинству пользователей не нужны. Можно создать не более 25 групп пользователей с помощью страницы Admin Menu > Group Access Control List.

5 . Создайте несколько пользовательских учетных записей и причислите их к соответствующим группам

Admin Menu > Безопасность > Пользователи и пароли

Всегда желательно создавать учетную запись пользователя для каждого лица, которому разрешен доступ к камере. Можно создать не более 100 учетных записей пользователей. Действия, выполняемые уполномоченными пользователями, регистрируются в файле журнала веб-сервера: при возникновении разногласий это помогает определить, «кто что сделал».

Правила создания надежных паролей см. выше.

6. Запретите общий доступ

Admin Menu > Безопасность > Списки контроля доступа групп

MOBOTIX M16 mx10-22-7-12 Group Access Control Lists

Access Rights	Browser Screen / View: Guest	Live	Player	MultiView	PDA	MxMC & VMS: Event Stream	HTTP API	Configuration: Admin	Image Setup	Event Setup	
Public Access	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	Disable all
Groups											**Remove Group**
admins	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐
es_admins	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐
es_guests	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐
es_users	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐
www_guests	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
www_users	☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☐
	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Open Users and Passwords to manage users and to assign groups.

Общий доступ позволяет обращаться к определенным ресурсам камеры без аутентификации. Настоятельно рекомендуется запрещать общий доступ, чтобы посторонние не могли просматривать прямую трансляцию, вести запись или управлять камерой (например, изменять конфигурацию или выполнять какие-либо действия).

7. Активируйте список контроля доступа по IP

Admin Menu > Безопасность > Ограничение доступа на основе IP-адреса

MOBOTIX c26 mx10-24-47-126 IP-Level Access Control

Access Control Configuration

WARNING: A faulty access configuration may render the camera inaccessible!

Access Control: Enabled — Enable or disable Access Control.

Access Rules for Allow

Mode	IP Address/Subnet/Domain	Examples
Allow	192.168.1.163	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com
Allow		192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com

Access Rules for Deny

Mode	IP Address/Subnet/Domain	Examples
Deny	192.168.1.163	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com
Deny		192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com

If no match is found:

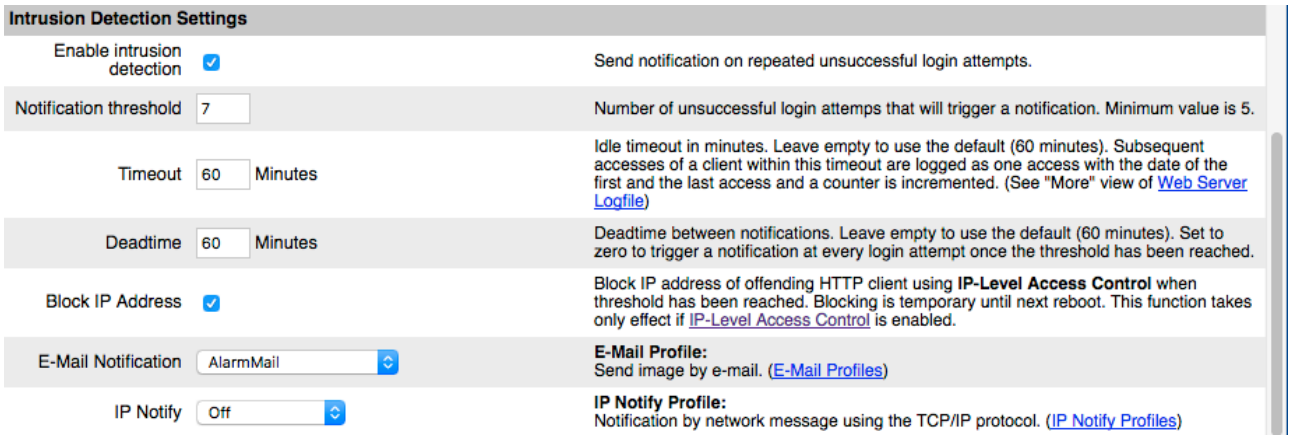
Allow — Access from all IP addresses/subnets/domains not listed above.

Set | Factory | Restore | Close

Диалоговое окно Access Control позволяет устанавливать IP-адреса, подсети и доменные имена, с которых разрешен (или запрещен) доступ к камере. В этой функции контроля доступа к камере используется уровень протокола IP. Функция не зависит от аутентификации пользователя по паролю (на уровне протокола HTTP) и превалирует над аутентификацией по паролю. Если с какого-либо компьютера нет доступа к камере на уровне IP, то с помощью этого компьютера невозможно связаться с камерой. Если на компьютере есть доступ к камере на уровне IP, то аутентификация по паролю является следующим этапом (это отражено в диалоговом окне Users and Passwords).

8. Активируйте обнаружение несанкционированного доступа (с уведомлением и блокировкой подозрительного IP-адреса)

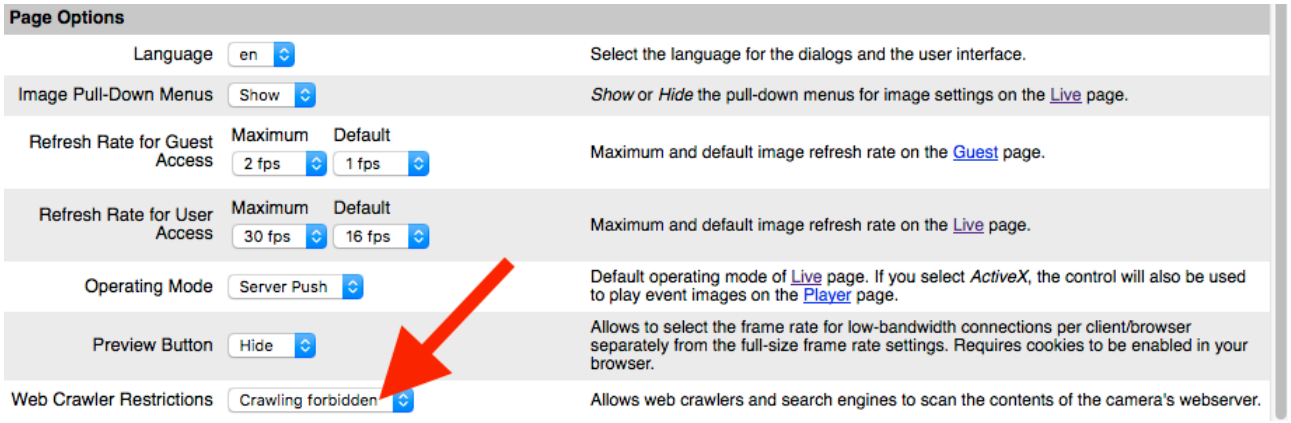
Admin Menu > Конфигурация сети > Веб-сервер (для экспертов) > Настройки функции обнаружения непредусмотренного появления



Эта функция обеспечивает автоматическую защиту от атак. Если злоумышленник попытается получить доступ к камере с помощью «грубой силы», подбирая имена пользователей и пароли, камера отправит оповещение и автоматически заблокирует подозрительный IP-адрес после определенного количества неудачных попыток.

9. Убедитесь, что веб-сканирование запрещено

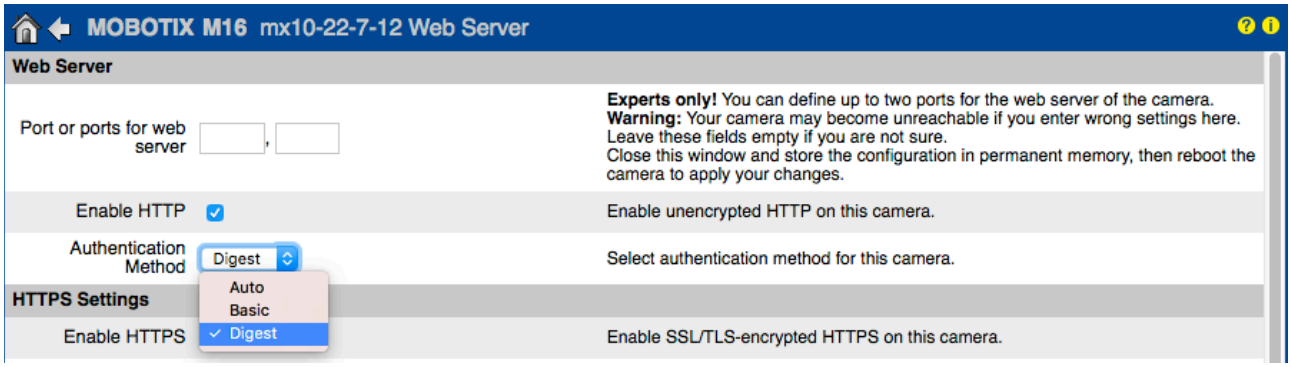
Admin Menu > Настройки страниц > Язык и начальная страница > Опции страницы



Используя этот параметр, можно запретить поисковым системам, другим автоматическим роботам и веб-сканерам сканировать содержимое веб-сервера камеры. Вряд ли вы захотите, чтобы поисковая система индексировала все изображения и страницы, найденные в камере. Разрешайте сканирование только в том случае, если осознаете дополнительные риски безопасности и учитываете рост сетевого трафика, обусловленный работой сканеров.

10. Активируйте дайджест-проверку подлинности

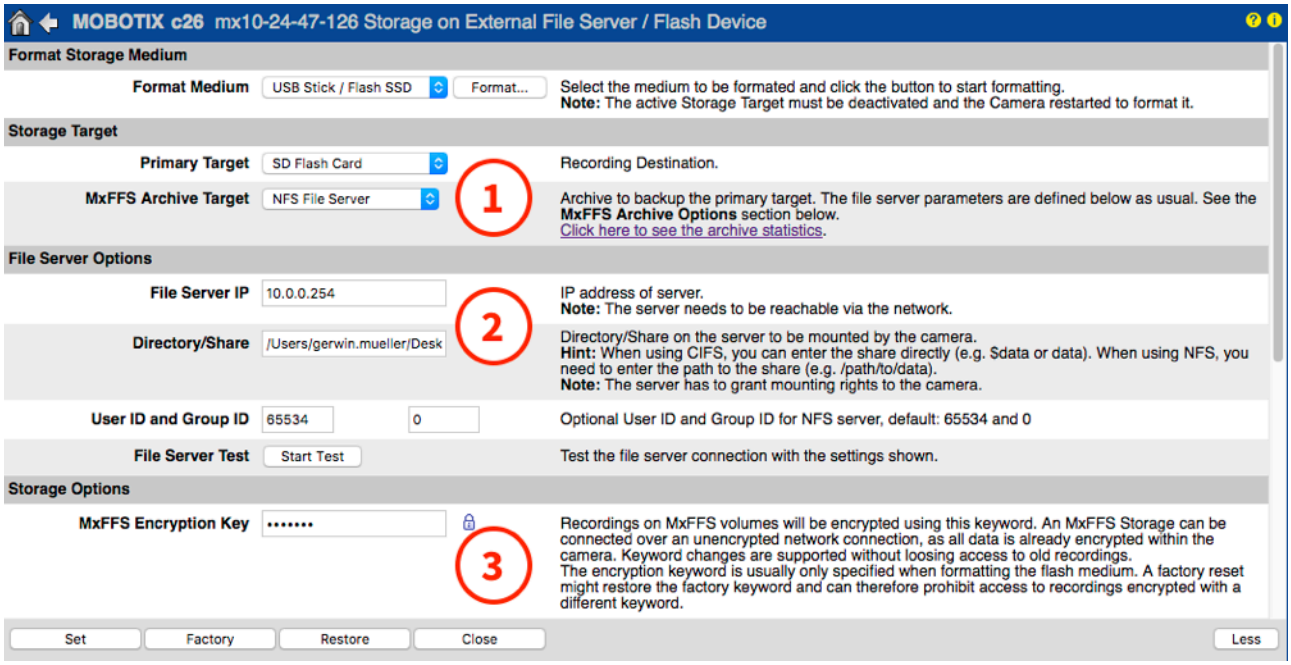
Admin Menu > Конфигурация сети > Веб-сервер (для экспертов) > Веб-сервер



Дайджест-проверка подлинности является одним из общепринятых методов, которые веб-сервер (камера MOBOTIX) может использовать для согласования учетных данных, таких как имя пользователя или пароль, с клиентом (веб-браузером). При дайджест-проверке подлинности пароль никогда не отправляется в открытом виде, а имя пользователя может быть хэшировано.

11. Задайте ключ шифрования для записей

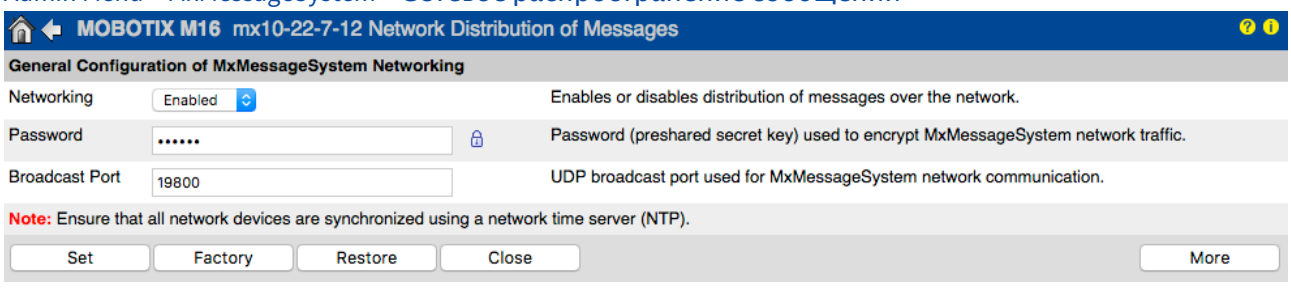
Admin Menu > Storage > Сохранение на внешнем файловом сервере / во флэш-памяти



Ключ шифрования можно задать для шифрования записей, хранящихся во внутреннем хранилище (карта microSD или USB-накопитель), а также для записей, архивируемых на внешнем файловом сервере (SMB или NFS).

12. Измените пароль по умолчанию для системы MxMessage (если она активирована)

Admin Menu > MxMessageSystem > Сетевое распространение сообщений



Система MxMessageSystem обеспечивает передачу сообщений между камерами в сети. Для шифрования передаваемых сообщений следует установить пароль (симметричный ключ) не менее чем из 6 символов.

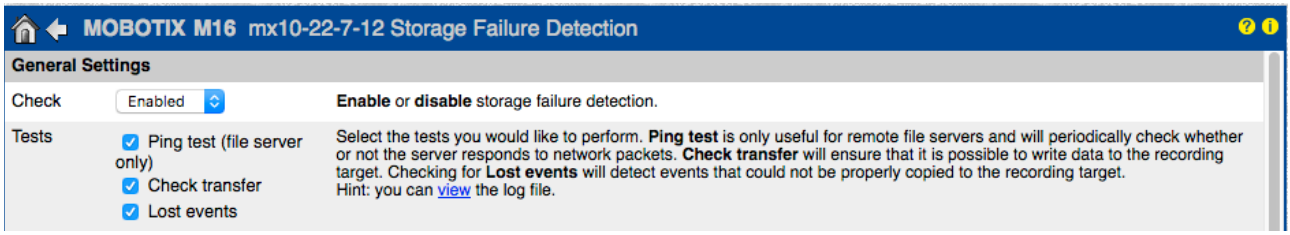
13. Активируйте уведомления об ошибках

Admin Menu > Информация о системен > Уведомление при сообщениях об ошибках

Диалоговое окно Error Notification позволяет выбрать несколько вариантов получения уведомлений (по эл. почте, с помощью IP-уведомлений, звонков VoIP и т. п.) в случае перезагрузки или обнаружения ошибок в различных системах камеры. Посредством этого инструмента системные администраторы следят за исправностью функционирования камер MOBOTIX.

14. Активируйте обнаружение сбоев хранилища

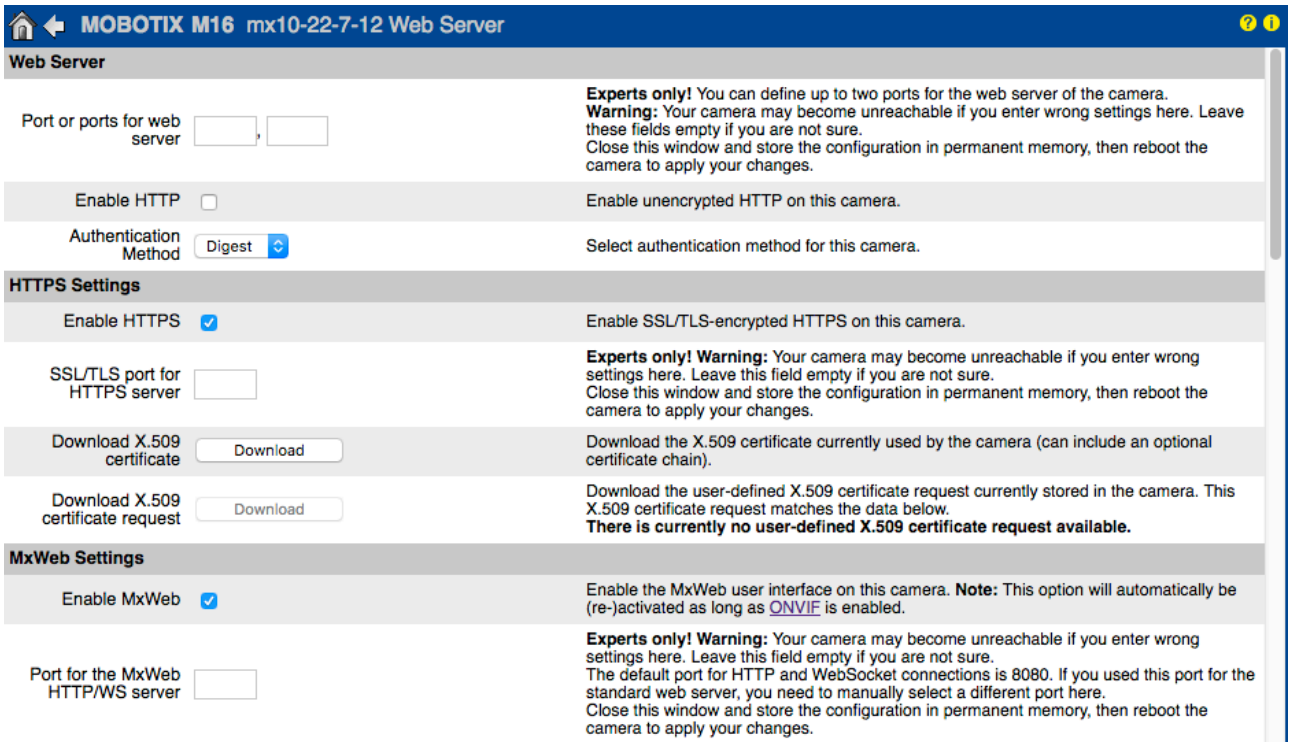
Admin Menu > Storage > Контроль за выходом памяти из строя



Используйте диалоговое Storage Failure Detection, чтобы настроить проверки для постоянного контроля внешнего хранилища (файлового сервера или флеш-накопителя), которое камера использует в качестве внешнего циклического буфера. Камера будет активно отслеживать объект хранения и сообщать о проблемах с видеозаписью, используя методы уведомления, которые указаны в этом диалоговом окне.

15. Измените стандартные порты веб-сервера (для удаленного доступа)

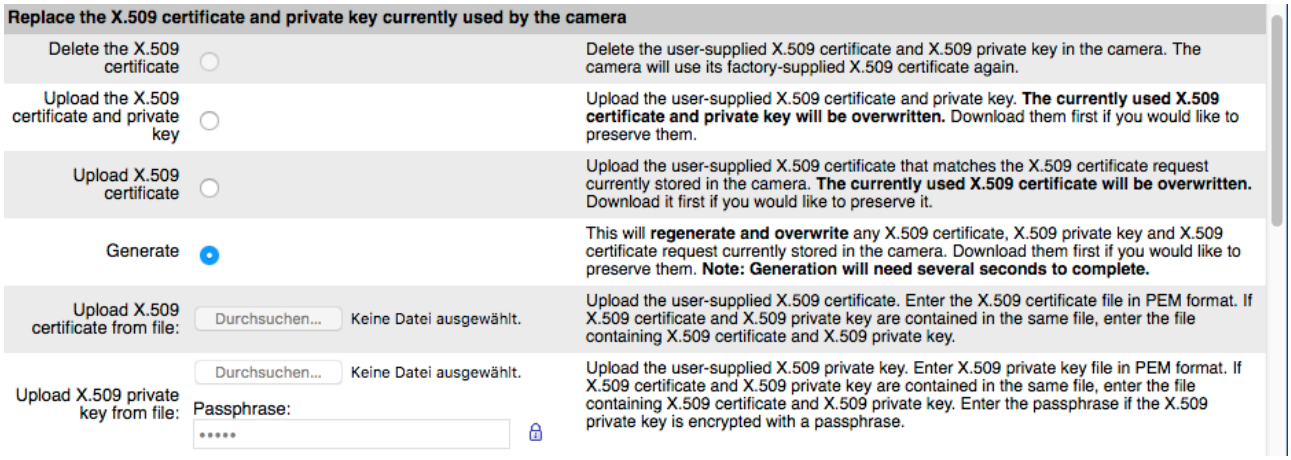
Admin Menu > Конфигурация сети > Веб-сервер (для экспертов)



Стандартные порты (80 TCP для HTTP и 443 TCP для HTTPS) особо подвержены атакам. Замена стандартных портов на пользовательские дополнительно повысит безопасность камеры.

16. Сгенерируйте и загрузите пользовательские сертификаты X.509

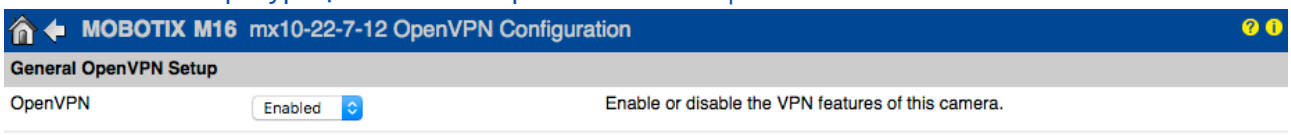
Admin Menu > Конфигурация сети > Веб-сервер (для экспертов)



Загрузка пользовательского сертификата, подписанного доверенным CA (центром сертификации), обеспечит конфиденциальность и подлинность всех соединений, установленных через HTTPS (SSL/TLS).

17. Настройте клиент OpenVPN для удаленных подключений

Admin Menu > Конфигурация сети > Настройки клиента OpenVPN



Чтобы оптимизировать безопасность при работе с удаленными подключениями, можно использовать встроенный клиент OpenVPN для создания туннеля VPN (виртуальной частной сети) между камерой и удаленным хостом.

Чтобы создать соединение OpenVPN, требуется соответствующий сервер, обеспечивающий безопасный доступ к камере. Для этого можно запустить собственный сервер OpenVPN или использовать эту услугу, предоставляемую поставщиком OpenVPN.
Чтобы подробнее узнать о технологии OpenVPN, посетите сайт сообщества OpenVPN.

18. Избегайте открывать камеру для Интернета без крайней необходимости

Чтобы сократить риск атак, предоставляйте удаленный доступ к камере осознанно. Если удаленный доступ необходим, в обязательном порядке соблюдайте изложенные выше правила, ограничивая возможность подключения кругом уполномоченных пользователей.

19. Используйте технологию VLAN для отделения сети системы видеонаблюдения (на корпоративном уровне безопасности)

В корпоративной среде рекомендуется отделять сеть CCTV (IP-камеры, рабочие станции NVR и VMS) от остальных узлов, чтобы предотвратить несанкционированный доступ и избежать перегрузки сети.

20. Активируйте стандарт IEEE 802.1X (на корпоративном уровне безопасности)

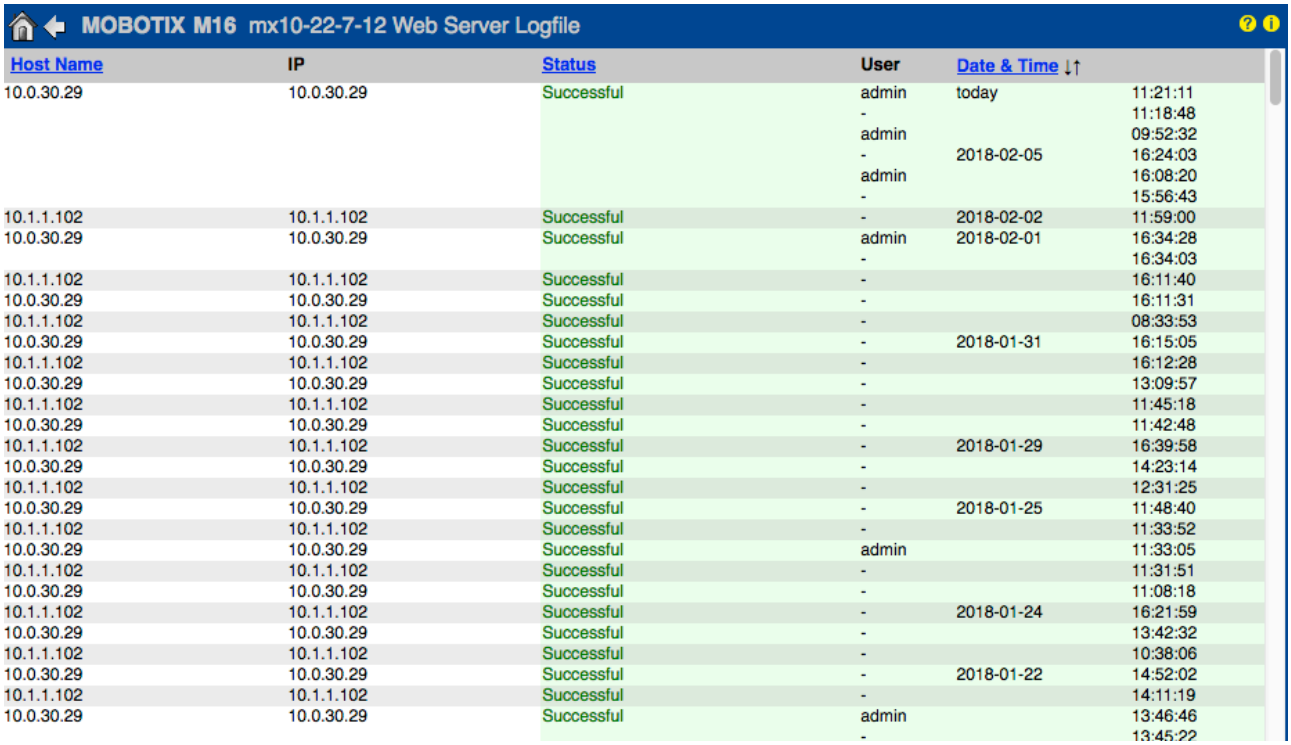
Admin Menu > Конфигурация сети > Интерфейс Ethernet (для экспертов) > IEEE 802.1X

Этот международный стандарт используется для управления сетевым доступом в режиме портов (NAC). Смысл процедуры заключается в том, что для подключения к сети любые сетевые устройства (в том числе камеры MOBOTIX) проходят аутентификацию на коммутаторе. Доступ сетевых устройств без должной аутентификации отклоняется.

Спросите у сетевого администратора, поддерживается ли (и требуется ли) стандарт IEEE 802.1X. Убедитесь, что коммутатор, к которому подключена камера (аутентификатор), настроен соответствующим образом. В общем случае для работы коммутатора (аутентификатора) необходим также сервер аутентификации, такой как сервер RADIUS. Процедура аутентификации контролируется сервером аутентификации. Следите за тем, чтобы камера и сервер аутентификации всегда использовали одну и ту же процедуру.

21. Регулярно проверяйте файл журнала веб-сервера

Admin Menu > Безопасность > Файл журнала веб-сервера



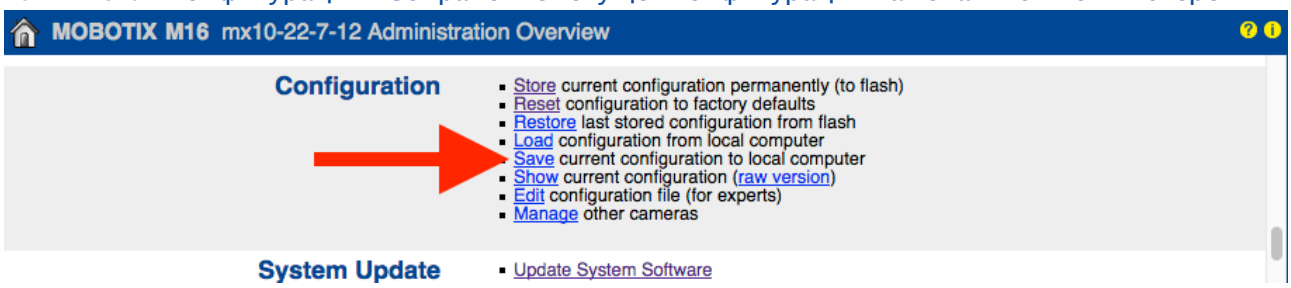
MOBOTIX M16 mx10-22-7-12 Web Server Logfile

Host Name	IP	Status	User	Date & Time ↓↑	
10.0.30.29	10.0.30.29	Successful	admin	today	11:21:11
			-		11:18:48
			admin		09:52:32
			-	2018-02-05	16:24:03
			admin		16:08:20
			-		15:56:43
10.1.1.102	10.1.1.102	Successful	-	2018-02-02	11:59:00
10.0.30.29	10.0.30.29	Successful	admin	2018-02-01	16:34:28
			-		16:34:03
10.1.1.102	10.1.1.102	Successful	-		16:11:40
10.0.30.29	10.0.30.29	Successful	-		16:11:31
10.1.1.102	10.1.1.102	Successful	-		08:33:53
10.0.30.29	10.0.30.29	Successful	-	2018-01-31	16:15:05
10.1.1.102	10.1.1.102	Successful	-		16:12:28
10.0.30.29	10.0.30.29	Successful	-		13:09:57
10.1.1.102	10.1.1.102	Successful	-		11:45:18
10.0.30.29	10.0.30.29	Successful	-		11:42:48
10.1.1.102	10.1.1.102	Successful	-	2018-01-29	16:39:58
10.0.30.29	10.0.30.29	Successful	-		14:23:14
10.1.1.102	10.1.1.102	Successful	-		12:31:25
10.0.30.29	10.0.30.29	Successful	-	2018-01-25	11:48:40
10.1.1.102	10.1.1.102	Successful	-		11:33:52
10.0.30.29	10.0.30.29	Successful	admin		11:33:05
10.1.1.102	10.1.1.102	Successful	-		11:31:51
10.0.30.29	10.0.30.29	Successful	-		11:08:18
10.1.1.102	10.1.1.102	Successful	-	2018-01-24	16:21:59
10.0.30.29	10.0.30.29	Successful	-		13:42:32
10.1.1.102	10.1.1.102	Successful	-		10:38:06
10.0.30.29	10.0.30.29	Successful	-	2018-01-22	14:52:02
10.1.1.102	10.1.1.102	Successful	-		14:11:19
10.0.30.29	10.0.30.29	Successful	admin		13:46:46
			-		13:45:22

В файле журнала веб-сервера регистрируются все попытки доступа и информация о дате (времени) с соответствующими сообщениями о состоянии веб-сервера, а также имени хоста подключившегося компьютера. Попытки несанкционированного доступа должны стать сигналом тревоги для системного администратора и побудить его к дополнительному укреплению сети.

22. Храните резервные файлы конфигурации в безопасном месте

Admin Menu > Конфигурация > Сохранение текущей конфигурации на локальном компьютере



Учетные данные камеры (пароли пользователей) в файле конфигурации камеры хэшируются, однако любая резервная копия файла конфигурации должна храниться в надежном месте. Кроме того, рекомендуется шифровать файл с помощью пароля для дополнительного повышения безопасности.

Поздравляем! Кибербезопасность вашей камеры MOBOTIX обеспечена!

Настройка системы управления видео (VMS)

1. **Создайте учетные записи пользователей на используемом компьютере.**
2. **Создайте учетные записи пользователей в MxMC.**
3. **Ограничьте права пользователей системы VMS.**
4. **Избегайте использовать учетную запись администратора для доступа к камерам через MxMC.**
5. **Активируйте функцию «автоматического выхода из системы».**

Поздравляем! Кибербезопасность вашей системы управления видео обеспечена!

MOBOTIX

Настройка сетевого устройства хранения (NAS)

1. **Разместите устройство, используемое для хранения видеозаписей, в безопасном месте.**
2. **Установите надежный пароль для учетной записи администратора.**
3. **Создайте стандартную учетную запись пользователя (с ограниченными правами) для устройств MOBOTIX.**
4. **Шифруйте тома хранилищ.**
5. **Используйте уровень RAID, обеспечивающий дублирование данных.**

Поздравляем! Кибербезопасность вашего сетевого устройства хранения обеспечена!