



www.cactusconcept.com

# Руководство по киберзащите

Методы защиты  
видеосистем MOBOTIX  
Камера • VMS • NAS





### 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.

**Общая информация.** Компания MOBOTIX не несет ответственности за технические ошибки, опечатки и пропуски.

**Уведомление об авторских правах.** Все права защищены. [Надпись](#) MOBOTIX, логотипы MOBOTIX AG и MxAnalytics являются зарегистрированными товарными знаками компании MOBOTIX AG в Европейском союзе, США и других странах. © MOBOTIX AG, 2018.

## Настройка камеры



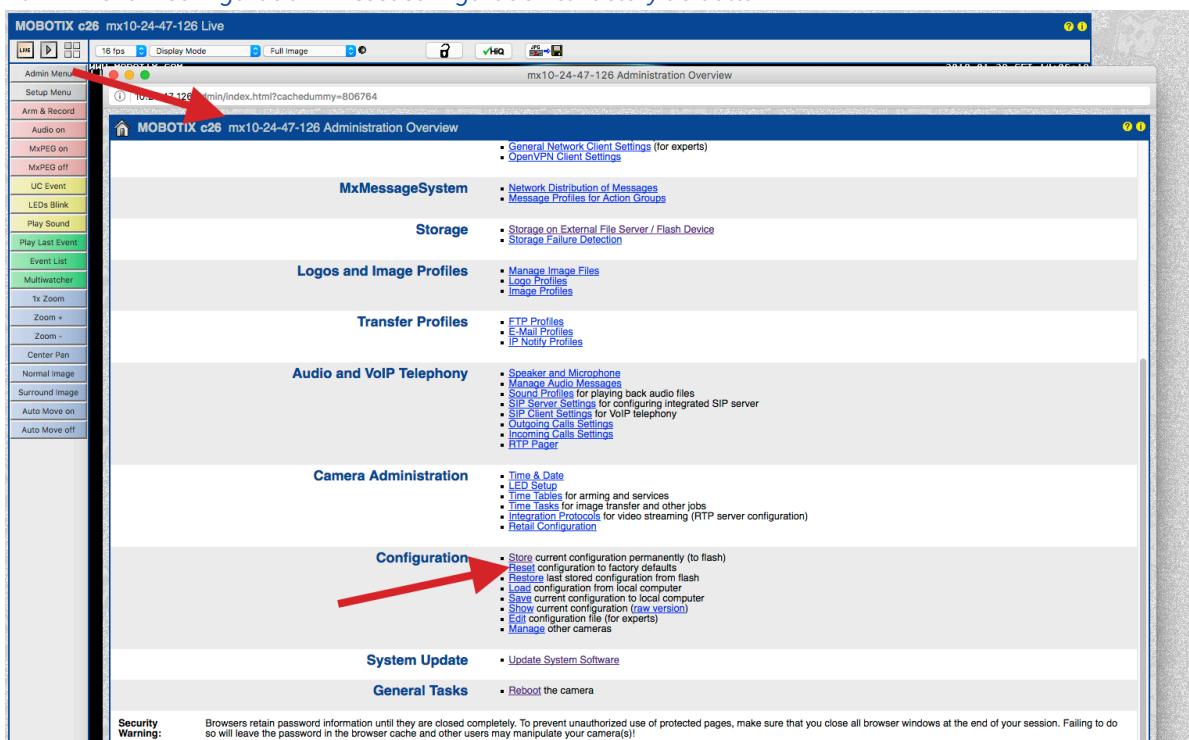
### 1. Своевременно обновляйте встроенное ПО камер

Встроенное ПО MOBOTIX можно бесплатно загрузить на нашем сайте: [www.mobotix.com](http://www.mobotix.com) > [Поддержка](#) > [Download Center](#)

Не знаете, как поступить? Обратитесь к следующей краткой инструкции: [www.mobotix.com](http://www.mobotix.com) > [Поддержка](#) > [Download Center](#) > [Документация](#) > [Брошюры и информация](#) > [Краткая инструкция](#) > [Mx CG FirmwareUpdate.pdf](#)

### 2. Восстановите заводские настройки

*Admin Menu > Configuration > Reset configuration to factory defaults*





### 3. Смените пароль администратора, установленный по умолчанию

Admin Menu > Security > Users and Passwords

User	Group	Password	Confirm Password	Remark/Action
admin	admins	...	...	<input type="checkbox"/> Remove
	undefined			

Настоятельно рекомендуется сменить имя пользователя (admin) и пароль, используемый по умолчанию (meinsm).

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 утерян, камеру необходимо вернуть в компанию MOBOTIX для сброса пароля.

### 4. Создайте несколько групп пользователей с разными правами

Admin Menu > Security > Users and Passwords

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 > Security > Users and Passwords

Всегда желательно создавать учетную запись пользователя для каждого лица, которому разрешен доступ к камере. Можно создать ~~не более~~ до 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 > Security > Group Access Control Lists

MOBOTIX M16 mx10-22-7-12 Group Access Control Lists											
Access Rights	Browser Screen / View					MxMC & VMS		Configuration			
	Guest	Live	Player	MultiView	PDA	Event Stream	HTTP API	Admin	Image Setup	Event Setup	
Public Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Disable all"/>
Groups											Remove Group
<input type="text" value="admins"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="es_admins"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="es_guests"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="es_users"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="www_guests"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="www_users"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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 > Security > IP-Level Access Control

**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  Disabled 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  Deny Access from all IP addresses/subnets/domains not listed above.

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 > Network Setup > Web Server (for experts) > Intrusion Detection Settings*

**Intrusion Detection Settings**

Enable intrusion detection  Send notification on repeated unsuccessful login attempts.

Notification threshold  Number of unsuccessful login attempts that will trigger a notification. Minimum value is 5.

Timeout  Minutes Idle timeout in minutes. Leave empty to use the default (60 minutes). Subsequent accesses of a client within this timeout are logged as one access with the date of the first and the last access and a counter is incremented. (See "More" view of [Web Server Logfile](#))

Deadtime  Minutes Deadtime between notifications. Leave empty to use the default (60 minutes). Set to zero to trigger a notification at every login attempt once the threshold has been reached.

Block IP Address  Block IP address of offending HTTP client using **IP-Level Access Control** when threshold has been reached. Blocking is temporary until next reboot. This function takes only effect if [IP-Level Access Control](#) is enabled.

E-Mail Notification   **E-Mail Profile:**  
Send image by e-mail. ([E-Mail Profiles](#))

IP Notify   **IP Notify Profile:**  
Notification by network message using the TCP/IP protocol. ([IP Notify Profiles](#))

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 > Page Administration > Language and Start Page > Page Options*

Page Options		
Language	en	Select the language for the dialogs and the user interface.
Image Pull-Down Menus	Show	Show or Hide the pull-down menus for image settings on the <a href="#">Live</a> page.
Refresh Rate for Guest Access	Maximum: 2 fps Default: 1 fps	Maximum and default image refresh rate on the <a href="#">Guest</a> page.
Refresh Rate for User Access	Maximum: 30 fps Default: 16 fps	Maximum and default image refresh rate on the <a href="#">Live</a> page.
Operating Mode	Server Push	Default operating mode of <a href="#">Live</a> page. If you select <i>ActiveX</i> , the control will also be used to play event images on the <a href="#">Player</a> page.
Preview Button	Hide	Allows to select the frame rate for low-bandwidth connections per client/browser separately from the full-size frame rate settings. Requires cookies to be enabled in your browser.
Web Crawler Restrictions	Crawling forbidden	Allows web crawlers and search engines to scan the contents of the camera's webserver.

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 > Network Setup > Web Server (for experts) > Web Server*

Web Server	
Port or ports for web server	<input type="text"/> <input type="text"/>
Enable HTTP	<input checked="" type="checkbox"/>
Authentication Method	Digest
Enable HTTPS	<input checked="" type="checkbox"/>
HTTPS Settings	Digest

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 > Storage on External File Server / Flash Device*



**Format Storage Medium**  
Format Medium: USB Stick / Flash SSD [Format...]  
Select the medium to be formatted and click the button to start formatting.  
**Note:** The active Storage Target must be deactivated and the Camera restarted to format it.

**Storage Target**  
Primary Target: SD Flash Card  
Recording Destination.  
MxFFS Archive Target: NFS File Server **1**  
Archive to backup the primary target. The file server parameters are defined below as usual. See the **MxFFS Archive Options** section below.  
[Click here to see the archive statistics.](#)

**File Server Options**  
File Server IP: 10.0.0.254  
IP address of server.  
**Note:** The server needs to be reachable via the network.  
Directory/Share: /Users/gerwin.mueller/Desk **2**  
Directory/Share on the server to be mounted by the camera.  
**Hint:** When using CIFS, you can enter the share directly (e.g. \$data or data). When using NFS, you need to enter the path to the share (e.g. /path/to/data).  
**Note:** The server has to grant mounting rights to the camera.  
User ID and Group ID: 65534 0  
Optional User ID and Group ID for NFS server, default: 65534 and 0  
File Server Test: Start Test  
Test the file server connection with the settings shown.

**Storage Options**  
MxFFS Encryption Key: ..... **3**  
Recordings on MxFFS volumes will be encrypted using this keyword. An MxFFS Storage can be connected over an unencrypted network connection, as all data is already encrypted within the camera. Keyword changes are supported without losing access to old recordings.  
**Hint:** The encryption keyword is usually only specified when formatting the flash medium. A factory reset might restore the factory keyword and can therefore prohibit access to recordings encrypted with a different keyword.

Set Factory Restore Close Less

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 > Network Distribution of Messages*

**MOBOTIX M16 mx10-22-7-12 Network Distribution of Messages**

**General Configuration of MxMessageSystem Networking**

Networking: Enabled  
Enables or disables distribution of messages over the network.

Password: .....  
Password (preshared secret key) used to encrypt MxMessageSystem network traffic.

Broadcast Port: 19800  
UDP broadcast port used for MxMessageSystem network communication.

**Note:** Ensure that all network devices are synchronized using a network time server (NTP).

Set Factory Restore Close More

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

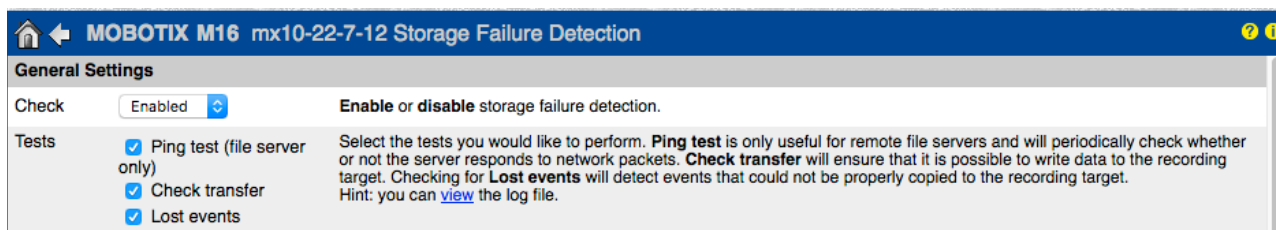
### 13. Активируйте уведомления об ошибках

*Admin Menu > System Information > Error Notification*

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

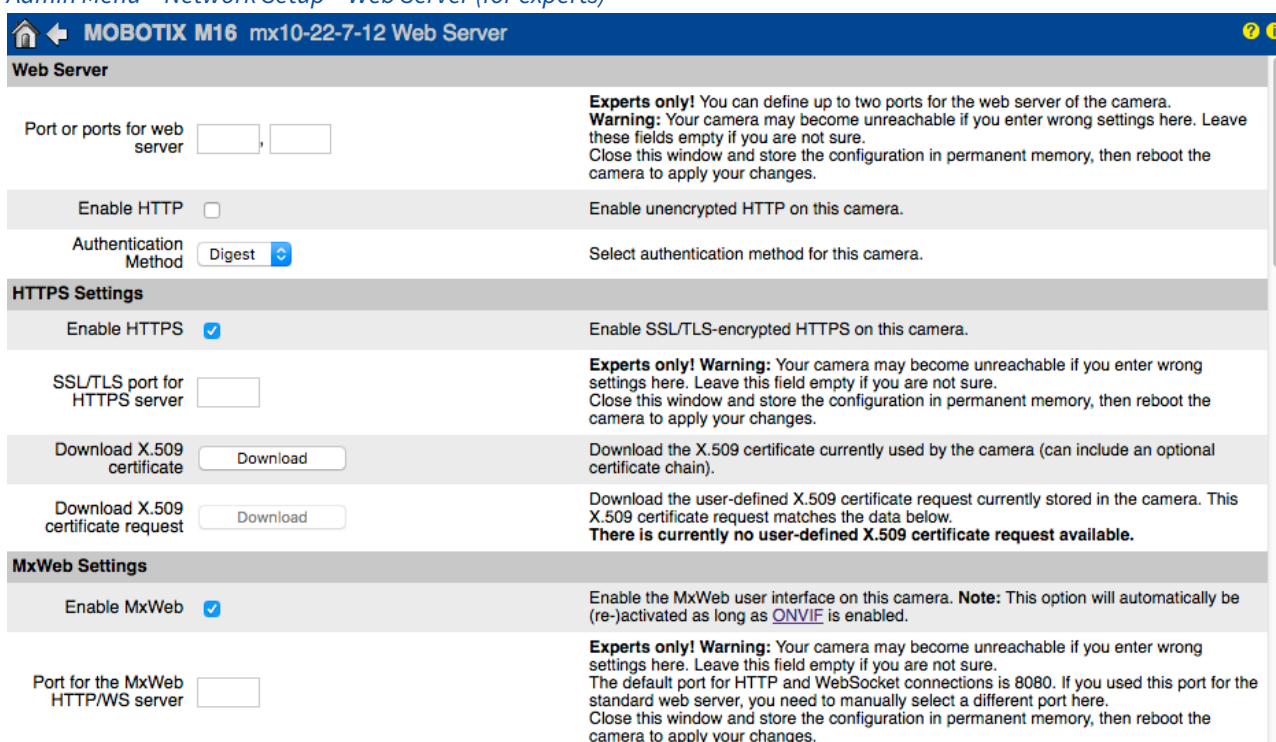
*Admin Menu > Storage > Storage Failure Detection*



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 > Network Setup > Web Server (for experts)*



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 > Network Setup > Web Server (for experts)*

Replace the X.509 certificate and private key currently used by the camera		
Delete the X.509 certificate	<input type="radio"/>	Delete the user-supplied X.509 certificate and X.509 private key in the camera. The camera will use its factory-supplied X.509 certificate again.
Upload the X.509 certificate and private key	<input type="radio"/>	Upload the user-supplied X.509 certificate and private key. <b>The currently used X.509 certificate and private key will be overwritten.</b> Download them first if you would like to preserve them.
Upload X.509 certificate	<input type="radio"/>	Upload the user-supplied X.509 certificate that matches the X.509 certificate request currently stored in the camera. <b>The currently used X.509 certificate will be overwritten.</b> Download it first if you would like to preserve it.
Generate	<input checked="" type="radio"/>	This will <b>regenerate and overwrite</b> any X.509 certificate, X.509 private key and X.509 certificate request currently stored in the camera. Download them first if you would like to preserve them. <b>Note: Generation will need several seconds to complete.</b>
Upload X.509 certificate from file:	<input type="text" value="Durchsuchen..."/> Keine Datei ausgewählt.	Upload the user-supplied X.509 certificate. Enter the X.509 certificate file in PEM format. If X.509 certificate and X.509 private key are contained in the same file, enter the file containing X.509 certificate and X.509 private key.
Upload X.509 private key from file:	<input type="text" value="Durchsuchen..."/> Keine Datei ausgewählt. Passphrase: <input type="password" value="*****"/>	Upload the user-supplied X.509 private key. Enter X.509 private key file in PEM format. If X.509 certificate and X.509 private key are contained in the same file, enter the file containing X.509 certificate and X.509 private key. Enter the passphrase if the X.509 private key is encrypted with a passphrase.

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

### 17. Настройте клиент OpenVPN для удаленных подключений

*Admin Menu > Network Setup > OpenVPN Client Settings*

MOBOTIX M16 mx10-22-7-12 OpenVPN Configuration

General OpenVPN Setup

OpenVPN  Enable or disable the VPN features of this camera.

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 > Network Setup > Ethernet Interface (for experts) > 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 > Security > Web Server Logfile*

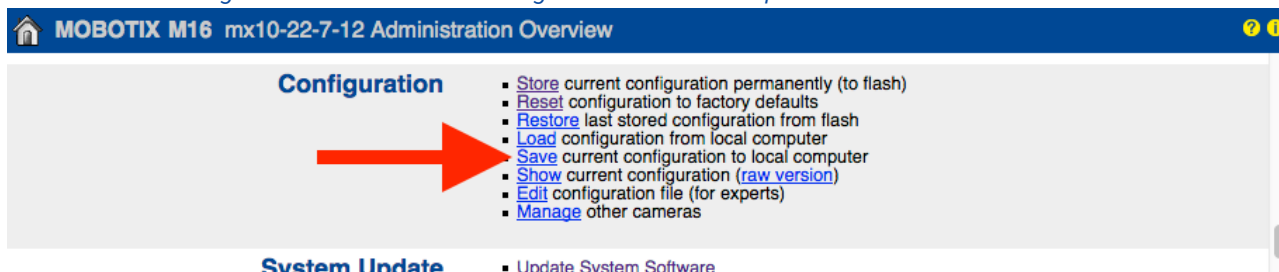


Host Name	IP	Status	User	Date & Time
10.0.30.29	10.0.30.29	Successful	admin	today 11:21:11
			-	11:18:48
			admin	09:52:32
			-	2018-02-05 16:24:03
			admin	16:08:20
			-	15:56:43
10.1.1.102	10.1.1.102	Successful	-	2018-02-02 11:59:00
10.0.30.29	10.0.30.29	Successful	admin	2018-02-01 16:34:28
			-	16:34:03
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 > Configuration > Save current configuration to local computer*



**Configuration**

- Store current configuration permanently (to flash)
- Reset configuration to factory defaults
- Restore last stored configuration from flash
- Load configuration from local computer
- Save current configuration to local computer
- Show current configuration (raw version)
- Edit configuration file (for experts)
- Manage other cameras

**System Update**

- Update System Software

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!

## 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!