



# Cyber Protection Guide

## Leitfaden zur optimalen Absicherung Ihres MOBOTIX Videosystems

Kamera • VMS • NAS





### Über dieses Dokument

Die Zahl der über das Internet geführten Cyberattacken gegen Hard- und Software wächst täglich. Um an hochsensible Daten zu gelangen, konzentrieren sich Hacker vorwiegend auf die schwächsten Glieder einer digitalen Absperrkette.

Da Videoüberwachung via IP-Netzwerk heute zu einem Grundbaustein im modernen Gebäudeschutz geworden ist, haben in letzter Zeit auch gezielte Angriffe auf Video-Sicherheitssysteme deutlich zugenommen.

Für MOBOTIX war und ist die Unangreifbarkeit seiner rein IP-basierten Systeme ein grundlegendes Entwicklungsziel. Für ein Höchstmaß an Cybersicherheit nutzen IT-Administratoren heute die auf allen MOBOTIX Systemebenen **serienmäßig integrierten Sicherungs- und Konfigurationstools**.

Die Nutzung dieser Tools – im Verbund mit grundlegenden Sicherheitsmaßnahmen wie Firewalls und Netzwerksegmentierungen – reduziert die möglichen Hacker-Angriffsflächen der im MOBOTIX System eingesetzten Geräte und Anwenderschnittstellen auf ein Minimum.

Dieser Cyber Protection Guide enthält alle entscheidenden Admin-Konfigurationsschritte der Einzelkomponenten (Kamera, VMS, NAS), um die gesamte Videoinfrastuktur optimal vor Fremdzugriffen zu schützen.

**Bitte beachten Sie:** Dieses Dokument gibt dem verantwortlichen Systemadministrator einen Überblick über alle angebotenen Schritte zur Absicherung des MOBOTIX Videosystems. In spezifischen Anwendungsfällen und zur Vermeidung von aufwendigen Umkonfigurationen kann es sinnvoll sein, einzelne Schritte zu überspringen.

**Allgemeine Hinweise:** MOBOTIX übernimmt keine Haftung für technische Fehler, Druckfehler oder Auslassungen.

**Copyright-Hinweise:** Alle Rechte vorbehalten. MOBOTIX, das Logo der MOBOTIX AG und MxAnalytics sind in der EU, den USA und in anderen Ländern eingetragene Marken der MOBOTIX AG © MOBOTIX AG 2018

# Kamera-Konfiguration

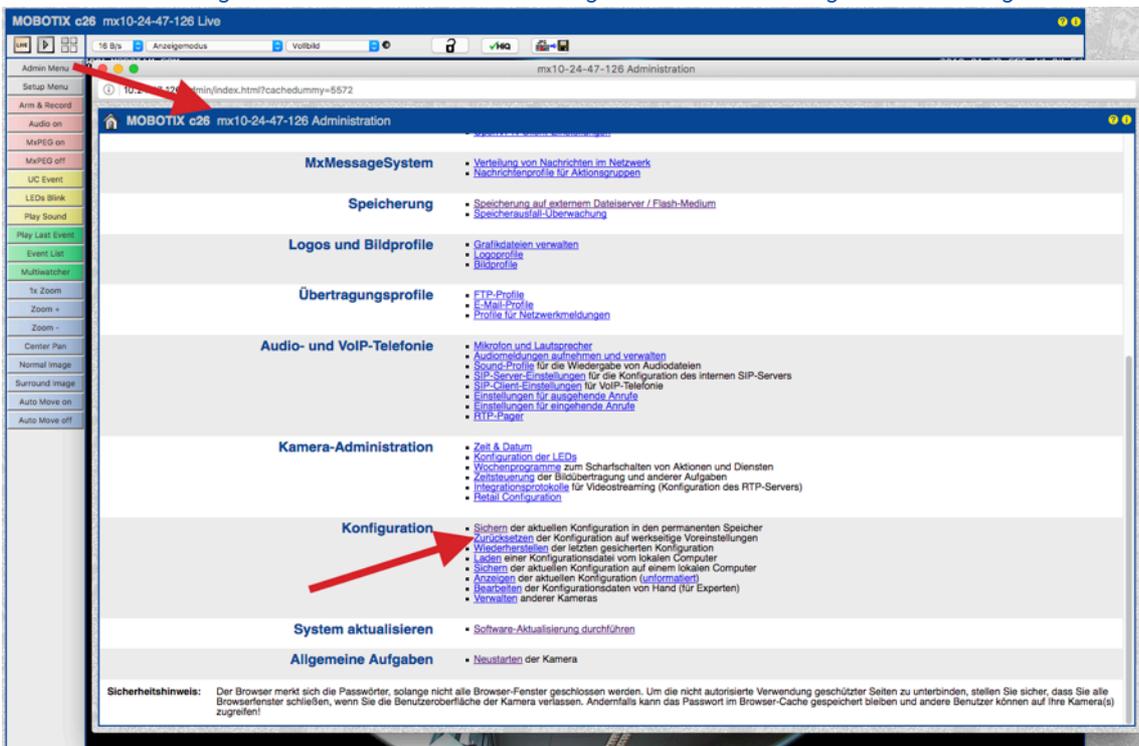


## 1. Kamera-Firmware auf den neuesten Stand bringen

Die kostenlose Firmware kann hier heruntergeladen werden: [www.mobotix.com](http://www.mobotix.com) > Support > Download Center  
Hierzu gibt es unter „Wissen Kompakt“ auch eine Anleitung: [www.mobotix.com](http://www.mobotix.com) > Support > Download Center > Dokumentation > Broschüren & Anleitungen > Wissen Kompakt > Mx CG FirmwareUpdate.pdf

## 2. Zurücksetzen auf Werkseinstellungen (bei Neuinstallation)

Admin Menu > Konfiguration > Zurücksetzen der Konfiguration auf werkseitige Voreinstellungen



### 3. Werksseitige Kamera-Zugangsdaten ändern

Admin Menu > Sicherheit > Benutzer und Passwörter

Benutzer	Gruppe	Passwort	Passwort bestätigen	Bemerkung/Aktion
admin	admins	...	...	<input type="checkbox"/> Entfernen
	Undefiniert			

Es wird **dringend** empfohlen, den Benutzernamen „admin“ und das Standardpasswort „meinsm“ zu ändern.

Denken Sie unbedingt daran, die Konfiguration nach Änderungen bei Benutzern, Passwörter oder Gruppen in den permanenten Speicher der Kamera zu sichern. Ansonsten sind die geänderten Benutzernamen und Passwörter nur bis zum nächsten Neustart der Kamera aktiv. Verwenden Sie den Button „Schließen“ unten im Dialog, da Sie dann zum Sichern der Konfiguration im permanenten Speicher der Kamera aufgefordert werden.

Bewahren Sie Informationen über Passwörter sehr sorgfältig auf. Achten Sie besonders darauf, dass Sie das Passwort für mindestens einen Benutzer in der Gruppe admins kennen. Sie können sonst die Kamera ohne das Passwort nicht mehr verwalten und es gibt keine Möglichkeit, diese Passwortabfrage zu umgehen. Ebenso lässt sich das Passwort aus einer permanent gespeicherten Konfiguration nicht wieder herstellen.

#### So erstellen Sie sichere Passwörter:

- Eine Länge von mindestens 8 Zeichen (bis zu 99)
- Mindestens ein Großbuchstabe A – Z
- Mindestens ein Kleinbuchstabe a – z
- Mindestens eine Ziffer 0 – 9
- Mindestens ein Sonderzeichen: ! “ # \$ % & ' ( ) \* + , - . / : ; < = > ? @ [ \ ] ^ \_ ` { | } ~
- Keine geläufigen Wörter oder Daten verwenden (Name, Geburtsdatum o. ä.)

**Passwort bei Verlust zurücksetzen:** Ist das Administrator-Passwort nicht mehr verfügbar, muss die Kamera bei MOBOTIX kostenpflichtig zurückgesetzt werden!

### 4. Anlegen von Benutzergruppen mit unterschiedlichen Benutzerrechten

Admin Menu > Sicherheit > Benutzer und Passwörter

Üblicherweise benötigen nicht alle Anwender exakt die selben Rechte. Daher können für jede Kamera bis zu 25 verschiedene Benutzergruppen angelegt werden. Die Rechtevergabe erfolgt danach tabellarisch über [Admin Menu > Sicherheit > Gruppen-Zugriffskontrolle \(ACL\)](#) – siehe unten bei Punkt 6.

### 5. Benutzer einzeln anlegen und in unterschiedliche Gruppen einordnen

Admin Menu > Sicherheit > Benutzer und Passwörter

Es empfiehlt sich, jede einzelne Person, die Zugriff auf die Kamera erhalten soll, hier als Benutzer anzulegen. Es können bis zu 100 Benutzer pro Kamera angelegt werden. Damit werden dann die ausgeführten Aktionen der autorisierten Benutzer in einer Webserver-Logdatei gespeichert ([Admin Menu > Sicherheit > Webserver-Logdatei](#)); so lassen sich strittige Situationen jederzeit einfach aufklären („Ich war das nicht“).

Beachten Sie dabei unsere in Punkt 3 aufgeführten Empfehlungen zur Erstellung sicherer Passwörter.

### 6. Öffentlichen Zugriff deaktivieren

Admin Menu > Sicherheit > Gruppen-Zugriffskontrolle (ACL)

MOBOTIX c26 mx10-24-47-126 Gruppen-Zugriffskontrolle (ACL) ? i

Zugriffsrechte	Browser-Ansicht / Anzeige					MxMC & VMS		Konfiguration		
	Gast	Live	Player	Multiview	PDA	Event Stream-Verbindung	HTTP-API	Admin	Bildeinstellungen	Ereignisse
Öffentlicher Zugriff	<input type="checkbox"/>									
<b>Gruppen</b>										
admins	<input checked="" type="checkbox"/>									
es_admins	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>						
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"/>
es_users	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
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"/>
www_users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
	<input type="checkbox"/>									

Öffnen Sie den Dialog [Benutzer und Passwörter](#), um die Benutzer zu verwalten und Gruppen zuzuweisen.

„Öffentlicher Zugriff“ bedeutet, dass die hier per Checkbox aktivierten Kamerafunktionen auch ohne Eingabe eines gültigen Benutzernamens und Passworts verfügbar sind. Um nicht-autorisierten Personen den Zugriff auf das Kameralivebild, die Aufzeichnungen oder auf die Kamerakonfiguration zu verweigern, wird dringend empfohlen, die Funktion „Öffentlicher Zugriff“ komplett zu deaktivieren.

### 7. IP-basierte Zugriffsbeschränkung einrichten

Admin Menu > Sicherheit > IP-basierte Zugriffsbeschränkung

MOBOTIX c26 mx10-24-47-126 IP-basierte Zugriffsbeschränkung ? i

**Konfiguration der Zugriffsbeschränkung**

**VORSICHT: Eine fehlerhafte Zugriffsconfiguration kann den Zugriff auf die Kamera unmöglich machen!**

Zugriffsbeschränkung: Aktiviert Zugriffsbeschränkung aktivieren/deaktivieren.

**Zugriffsregeln für Gewähren**

Modus	IP-Adresse/Subnetz/Domain	Beispiele
<span style="border: 1px solid #ccc; padding: 2px;">Gewähren</span>	<input style="width: 150px;" type="text" value="192.168.1.163"/>	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com
<span style="border: 1px solid #ccc; padding: 2px;">Gewähren</span>	<input style="width: 150px;" type="text"/>	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com

**Zugriffsregeln für Verweigern**

Modus	IP-Adresse/Subnetz/Domain	Beispiele
<span style="border: 1px solid #ccc; padding: 2px;">Verweigern</span>	<input style="width: 150px;" type="text" value="192.168.1.145"/>	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com
<span style="border: 1px solid #ccc; padding: 2px;">Verweigern</span>	<input style="width: 150px;" type="text"/>	192.168.1.163, 192.168.1.0/255.255.255.0, ftp.mobotix.com

**Wenn keine Übereinstimmung:**

Gewähren Zugriff von allen nicht aufgeführten IP-Adressen/Subnetzen/Domains.

Setzen
Voreinstellung
Wiederherstellen
Schließen

Im Dialog Zugriffskontrolle verwalten Sie IP-Adressen, Subnetze oder Domainnamen, denen der Zugriff auf die Kamera gewährt oder verweigert werden soll. Diese Möglichkeit der Zugriffsteuerung arbeitet auf der Ebene des IP-Protokolls, ist unabhängig von der Passwort-basierten Benutzer-Authentifikation auf Ebene des HTTP-Protokolls und hat Priorität vor dieser. Hat ein Computer keine Zugriffsrechte auf dieser Kamera, so ist es generell nicht möglich, die Kamera von diesem Computer aus zu erreichen. Hat ein Computer Zugriffsrechte auf dieser Kamera, erfolgt nach dieser Zugangsprüfung noch zusätzlich die Authentifikation des HTTP-Protokolls, wie im Dialog Benutzer und Passwörter festgelegt.

### 8. Intrusion Detection mit Benachrichtigung aktivieren und die IP-Adresse eines Angreifers blockieren

Admin Menu > Netzwerk-Konfiguration > Webserver (für Experten) > Intrusion Detection-Einstellungen

Intrusion Detection-Einstellungen	
Intrusion Detection aktivieren <input checked="" type="checkbox"/>	Benachrichtigung bei wiederholten fehlerhaften Login-Versuchen schicken.
Benachrichtigungsschwelle <input type="text" value="7"/>	Anzahl der fehlerhaften Login-Versuche, nach denen eine Benachrichtigung erfolgt. Mindestwert ist 5.
Zeitüberschreitung <input type="text" value="60"/> Minuten	Leerlauf-Zeitüberschreitung in Minuten. Lassen Sie dieses Feld leer, um den Standardwert (60 Minuten) zu verwenden. Mehrere Zugriffsversuche eines Client innerhalb dieser Zeitspanne werden als ein Zugriff gewertet, der mit Anfangs- und Endzeit gespeichert wird. Außerdem wird ein Zähler hochgesetzt. (Klicken Sie im Dialog <a href="#">Webserver-Logfile</a> auf Mehr.)
Totzeit <input type="text" value="60"/> Minuten	Totzeit zwischen Benachrichtigungen. Lassen Sie dieses Feld leer, um den Standardwert (60 Minuten) zu verwenden. Geben Sie hier eine "0" (null) ein, um nach Erreichen der Schwelle bei jedem Login-Versuch eine Benachrichtigung auszulösen.
IP-Adresse blockieren <input type="checkbox"/>	Blockiert die IP-Adresse des anfragenden Computers mit Hilfe der <b>IP-basierten Zugriffsbeschränkung</b> , wenn die Benachrichtigungsschwelle erreicht wurde. Die Blockade wird durch den nächsten Neustart wieder aufgehoben. Dies funktioniert nur, wenn <a href="#">IP-basierte Zugriffsbeschränkung</a> aktiviert ist.
E-Mail-Benachrichtigung <input type="text" value="AlarmMail"/>	<b>E-Mail-Profil:</b> Versendet eine E-Mail mit Bild. ( <a href="#">E-Mail-Profile</a> )
Netzwerkmeldung <input type="text" value="Aus"/>	<b>Netzwerkmeldungs-Profil:</b> Sendet eine Netzwerkmeldung über das TCP/IP-Protokoll. ( <a href="#">Profile für Netzwerkmeldungen</a> )

Diese Einstellung ermöglicht die direkte Abwehr unerwünschter Angreifer. Falls versucht wird, Benutzernamen und Passwörter der Kamera mit „Brute Force“-Methoden zu erraten, kann die Kamera nach einer gewissen Anzahl von Fehlversuchen eine Alarmierung auslösen und den Kamerazugriff automatisch sperren.

### 9. Web-Crawling nicht zulassen (Einschränkungen für Web-Robots)

Admin Menu > Seiteneinstellungen > Sprache und Startseite > Seitenoptionen

Seitenoptionen	
Sprache <input type="text" value="de"/>	Wählen Sie die Sprache der Dialoge und der Benutzeroberfläche aus. Klicken Sie <a href="#">hier</a> , um eine andere Schriftart hochzuladen.
Pull-Down-Menüs für die Bildsteuerung <input type="text" value="Anzeigen"/>	<i>Anzeigen</i> bzw. <i>Ausblenden</i> der Pull-Down-Menüs auf der <a href="#">Live-Seite</a> zur schnellen Veränderung von Bildparametern.
Bildwiederholrate des Gastzugangs Maximum <input type="text" value="2"/> B/s Standard <input type="text" value="1"/> B/s	Legen Sie die maximale und die Standard-Bildwiederholrate für die <a href="#">Gastseite</a> fest.
Bildwiederholrate des Benutzerzugangs Maximum <input type="text" value="30"/> B/s Standard <input type="text" value="16"/> B/s	Legen Sie die maximale und die Standard-Bildwiederholrate für die <a href="#">Live-Seite</a> fest.
Betriebsart <input type="text" value="Server Push"/>	Legen Sie die Standard-Betriebsart für die <a href="#">Live-Seite</a> fest. Wenn Sie <i>ActiveX</i> wählen, wird <i>ActiveX</i> auch für die Wiedergabe der Ereignisse im <a href="#">Player</a> verwendet.
Vorschau-Buttons <input type="text" value="Ausblenden"/>	Ermöglicht separate Einstellungen der Bildrate je Client/Browser für Verbindungen geringer Bandbreite. Aktivieren Sie Cookies in Ihrem Browser.
Einschränkungen für Web-Robots <input type="text" value="Robots ausschließen"/>	Ermöglicht Web-Crawlern und Suchmaschinen, die Inhalte auf dem Webserver dieser Kamera zu indexieren.

Mit dieser Einstellung können Sie den Suchmaschinen im Internet sowie anderen automatischen Robots und Web-Crawlern untersagen, die Inhalte auf dem Webserver dieser Kamera zu indexieren. Sofern dies nicht explizit gewünscht ist, sollten Sie keine Indexierung der Bilder und Seiten dieser Kamera zulassen. Stellen Sie sicher, dass Sie die Indexierung nur zulassen, wenn Sie sich der zusätzlichen Sicherheitsrisiken bewusst sind und Sie die dadurch generierte Netzwerklast in Kauf nehmen.

### 10. HTTP-Authentifizierungsmethode „Digest“ auswählen

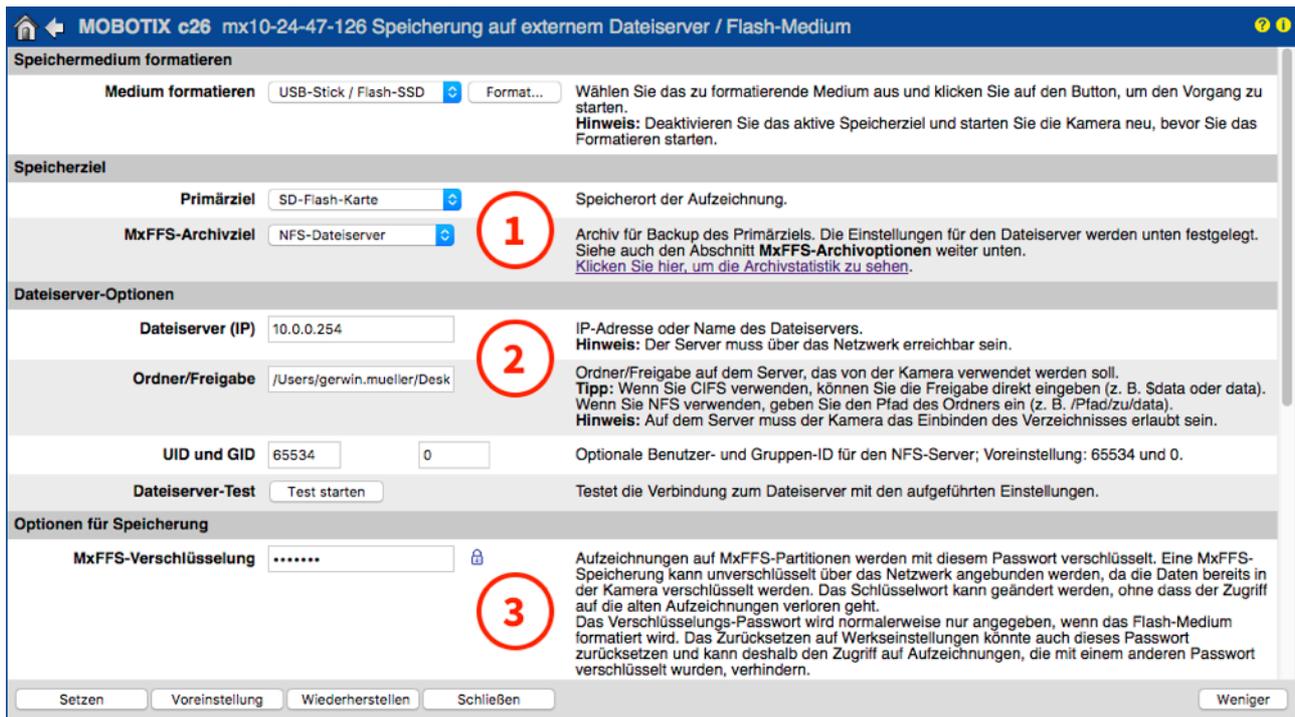
Admin Menu > Netzwerk-Konfiguration > Webserver (für Experten) > Webserver



Diese HTTP-Authentifizierung ist eine anerkannte Methode, mit der sich der Nutzer eines Webbrowsers gegenüber dem Webserver (MOBOTIX Kamera) per Benutzername und Passwort authentifizieren kann. Bei der Digest Access Authentifizierung werden die Zugangsdaten nie im Klartext übermittelt und können so nicht „abgehört“ werden.

### 11. Alle genutzten Speicherziele verschlüsseln

Admin Menu > Speicherung > Speicherung auf externem Dateiserver / Flash-Medium



Über die Kamera-Firmware kann sowohl die Aufzeichnung auf das direkt mit der Kamera verbundene Speichermedium (integrierte microSD-Karte, USB-Stick/Festplatte) als auch auf einen externen Speicher im Netzwerk (Dateiserver SMB NFS) sicher verschlüsselt werden. Ein entwendeter Speicher (Karte, NAS) kann dann nur mit der richtigen Verschlüsselung wieder ausgelesen werden.

## 12. Standard-Passwort für das MxMessageSystem ändern (falls genutzt)

Admin Menu > MxMessageSystem > Verteilung von Nachrichten im Netzwerk

The screenshot shows the 'Allgemeine Konfiguration von MxMessageSystem' window. It includes a dropdown menu for 'Netzwerk' set to 'Deaktiviert', a password field with masked characters, and a 'Broadcast-Port' field set to '19800'. A red warning message states: 'Hinweis: Stellen Sie sicher, dass alle Netzwerkgeräte mithilfe eines Netzwerk-Zeitserverns (NTP) synchronisiert werden.' Buttons at the bottom include 'Setzen', 'Voreinstellung', 'Wiederherstelle', 'Schließen', and 'Mehr'.

Das von MOBOTIX entwickelte MxMessageSystem dient dem Austausch von Nachrichten bzw. Steuerungsbefehlen zwischen den Kameras und Geräten im Netzwerk. Das zur Verschlüsselung dieser Nachrichtenübertragung gewählte Passwort (symmetrischer Schlüssel) sollte eine Mindestlänge von 6 Zeichen haben.

## 13. Benachrichtigung bei Fehlermeldungen einrichten

Admin Menu > System-Informationen > Benachrichtigungen bei Fehlermeldungen

Im Dialog Benachrichtigung bei Fehlern können Sie bestimmen, auf welche Weise und ab welcher Dringlichkeit Fehler und Neustarts der verschiedenen Kamerasysteme automatisch signalisiert werden (per Kamera-LED, E-Mail, Telefonanruf, Netzwerkmeldung etc.). Dank dieser Funktion ist ein Systemadministrator über Änderungen des Systemstatus schnell informiert.

## 14. Speicherausfall-Überwachung einrichten

Admin Menu > Speicherung > Speicherausfall-Überwachung

The screenshot shows the 'Allgemeine Einstellungen' for 'Speicherausfall-Überwachung'. The 'Prüfen' dropdown is set to 'Aktiviert'. Under 'Tests', three options are checked: 'Ping-Test (nur Dateiserver)', 'Übertragung', and 'Verlorene Ereignisse'. A detailed explanation on the right states: 'Wählen Sie die Tests aus, die Sie durchführen möchten. Ping-Test ist nur bei Dateiservern sinnvoll und prüft periodisch, ob der Server auf Datenpakete reagiert. Übertragung prüft, ob das Aufzeichnungsziel tatsächlich Daten zum Speichern annimmt. Verloren gegangene Ereignisse erkennt Ereignisse, die nicht auf dem Aufzeichnungsziel gespeichert werden konnten. Tipp: Sie können die Protokolldatei betrachten.'

Im Dialog Speicherausfall-Überwachung richten Sie die Tests ein, die das von der Kamera als externer Ringspeicher verwendete Speicherziel (Dateiserver bzw. Flash-Medium) laufend kontrollieren. Die Kamera überprüft das verwendete Speicherziel aktiv und signalisiert plötzlich auftretende Probleme mit der Bildspeicherung über die hier festgelegten Meldewege.

### 15. Standard-Ports für den Webserver ändern (für Remote-Zugriff)

Admin Menu > Netzwerk-Konfiguration > Webserver (für Experten)

MOBOTIX c26 mx10-24-47-126 Webserver
?

**Webserver**

Port bzw. Ports für den Webserver <input style="width: 40px;" type="text"/> , <input style="width: 40px;" type="text"/>	<b>Experteneinstellung!</b> Sie können bis zu zwei Ports für den Webserver der Kamera angeben. <b>Achtung:</b> Falsche Eingaben können dazu führen, dass die Kamera nicht mehr angesprochen werden kann. Im Zweifelsfall lassen Sie diese Felder leer. Schließen Sie den Dialog und speichern Sie die Einstellungen im Flash-Speicher. Neue Einstellungen werden erst nach einem Neustart wirksam.
HTTP aktivieren <input type="checkbox"/>	Unverschlüsseltes HTTP auf dieser Kamera aktivieren.
Authentifizierungsmethode <span style="border: 1px solid #ccc; padding: 2px;">Digest</span>	Authentifizierungsmethode für diese Kamera auswählen.

**HTTPS-Einstellungen**

HTTPS aktivieren <input checked="" type="checkbox"/>	Verschlüsseltes HTTPS (SSL/TLS) auf dieser Kamera aktivieren.
SSL/TLS-Port für HTTPS-Server <input style="width: 40px;" type="text"/>	<b>Experteneinstellung! Warnung:</b> Falsche Eingaben können dazu führen, dass die Kamera nicht mehr angesprochen werden kann. Im Zweifelsfall lassen Sie dieses Feld leer. Schließen Sie den Dialog und speichern Sie die Einstellungen im Flash-Speicher. Neue Einstellungen werden erst nach einem Neustart wirksam.
X.509-Zertifikat herunterladen <span style="border: 1px solid #ccc; padding: 2px 5px;">Herunterladen</span>	Von der Kamera verwendetes X.509-Zertifikat und privaten Schlüssel herunterladen (kann eine optionale Zertifikatskette enthalten).
X.509-Zertifikat-Anfragedatei herunterladen <span style="border: 1px solid #ccc; padding: 2px 5px;">Herunterladen</span>	Vom Benutzer in der Kamera hinterlegte X.509-Zertifikat-Anfrage herunterladen. Die X.509-Zertifikat-Anfrage stimmt mit den unten aufgeführten Daten überein. <b>Es steht momentan keine X.509-Zertifikat-Anfrage des Benutzers zur Verfügung.</b>

**MxWeb-Einstellungen**

MxWeb aktivieren <input checked="" type="checkbox"/>	Benutzeroberfläche MxWeb auf dieser Kamera aktivieren. <b>Hinweis:</b> Diese Option wird automatisch (erneut) aktiviert, wenn <b>ONVIF</b> aktiviert ist.
Port für den HTTP-/WS-Server von MxWeb <input style="width: 40px;" type="text"/>	<b>Experteneinstellung! Warnung:</b> Falsche Eingaben können dazu führen, dass die Kamera nicht mehr angesprochen werden kann. Im Zweifelsfall lassen Sie dieses Feld leer. Der Standard-Port für HTTP-/Web Socket-Verbindungen ist 8080. Wenn Sie diesen Port für den Standard-Webserver der Kamera verwenden, müssen Sie einen anderen Port festlegen. Schließen Sie den Dialog und speichern Sie die Einstellungen im Flash-Speicher. Neue Einstellungen werden erst nach einem Neustart wirksam.

Die Verwendung der Standard-Ports (80 TCP für HTTP und 443 TCP for HTTPS) macht die Kamera anfälliger für Hackerangriffe. Zur Erhöhung der Systemsicherheit sollten Sie daher eigene Ports einrichten.

### 16. Eigenes X.509 -Zertifikat generieren und hochladen

Admin Menu > Netzwerk-Konfiguration > Webserver (für Experten)

**Von der Kamera verwendete X.509-Dateien mit dem Zertifikat und dem privaten Schlüssel ersetzen**

X.509-Zertifikat löschen <input type="radio"/>	Vom Benutzer in der Kamera hinterlegte X.509-Dateien mit dem Zertifikat und dem privaten Schlüssel löschen. Die Kamera wird wieder das werkseitige X.509-Zertifikat verwenden.
X.509-Zertifikat und privaten Schlüssel hochladen <input type="radio"/>	X.509-Zertifikat und privaten Schlüssel des Benutzers hochladen. <b>Die von der Kamera verwendeten X.509-Dateien mit dem Zertifikat und dem privaten Schlüssel werden überschrieben.</b> Wenn Sie diese Dateien sichern möchten, laden Sie diese zuerst herunter.
X.509-Zertifikat hochladen <input type="radio"/>	Vom Benutzer bereitgestelltes X.509-Zertifikat in die Kamera laden, das der Zertifikat-Anfrage in der Kamera entspricht. <b>Das aktuelle X.509-Zertifikat in der Kamera wird überschrieben.</b> Wenn Sie diese Datei sichern möchten, laden Sie diese zuerst herunter.
Generieren <input checked="" type="radio"/>	Diese Aktion <b>erzeugt neue X.509-Dateien und überschreibt</b> alle X.509-Dateien (Zertifikat, Zertifikat-Anforderung und privater Schlüssel), die in der Kamera hinterlegt sind. Wenn Sie diese Dateien sichern möchten, laden Sie diese zuerst herunter. <b>Hinweis: Das Generieren wird mehrere Sekunden dauern.</b>
Datei mit X.509-Zertifikat hochladen: <span style="border: 1px solid #ccc; padding: 2px 5px;">Durchsuchen...</span> Keine Datei ausgewählt.	Lädt das X.509-Zertifikat des Benutzers in die Kamera. Wählen Sie hier die X.509-Zertifikatdatei im PEM-Format aus. Wenn das X.509-Zertifikat und X.509-Privatschlüssel in einer Datei vorliegen, wählen Sie diese Datei zum Hochladen aus.
Datei mit X.509-Privatschlüssel hochladen: <span style="border: 1px solid #ccc; padding: 2px 5px;">Durchsuchen...</span> Keine Datei ausgewählt.	Lädt den X.509-Privatschlüssel des Benutzers in die Kamera. Wählen Sie hier die X.509-Privatschlüssel-Datei im PEM-Format aus. Wenn das X.509-Zertifikat und X.509-Privatschlüssel in einer Datei vorliegen, wählen Sie diese Datei zum Hochladen aus. Geben Sie die Passphrase ein, wenn der X.509-Privatschlüssel mit einer Passphrase verschlüsselt wurde.

Durch Hochladen eines von einer externen Autorität signierten X.509-Zertifikats sind die Verbindungen zum Webserver via HTTPS (SSL/TLS) am sichersten verschlüsselt.

### 17. OpenVPN-Verbindung für sicheren Kamera-Fernzugriff einrichten

*Admin Menu > Netzwerk-Konfiguration > OpenVPN Client-Einstellungen*



Für sichere Fernzugriffs-Verbindungen über einen sogenannten VPN-Tunnel (Virtual Private Network), muss die Verwendung von OpenVPN auf dieser Kameras aktiviert werden.

Um eine OpenVPN-Verbindung aufzubauen, benötigen Sie einen entsprechenden Server, der einen sicheren Zugang zur Kamera ermöglicht. Hierzu könnten Sie einen eigenen OpenVPN-Server betreiben oder die Dienste eines OpenVPN-Providers in Anspruch nehmen.

Weitere Informationen über OpenVPN finden Sie auf der Website der [OpenVPN-Community](https://openvpn.com/).

### 18. Kamera nur ins Internet einbinden, wenn unbedingt erforderlich

Der Fernzugriff auf die Kamera sollte immer nur bewusst erfolgen, um das Risiko von Angriffen zu reduzieren. Wenn ein Fernzugriff erforderlich ist, beachten Sie die oben für sicheren Fernzugriff aufgeführten Konfigurationsschritte, um nur Verbindungen mit dafür vorgesehenen Benutzern zu ermöglichen.

### 19. VLANs für separate Videonetze nutzen (Enterprise Security Level)

In Unternehmensumgebungen empfiehlt es sich, das Videonetzwerk (IP-Kameras, NVR- und VMS-Workstations) vom Rest der Hosts zu trennen, um unbefugte Zugriffe zu verhindern und Datenstaus zu vermeiden.

### 20. IEEE 802.1X aktivieren (Enterprise Security Level)

*Admin Menu > Netzwerk-Konfiguration > Ethernet-Schnittstelle*

Dieser internationale Standard wird für Port-basierte Netzwerk-Zugriffskontrolle (Network Access Control, NAC) verwendet. Bei diesem Verfahren müssen sich die Netzwerkgeräte (also auch die MOBOTIX Kamera) am jeweiligen Switch anmelden, um Zugriff auf das Netzwerk zu erhalten. Nicht authentifizierte Netzwerkgeräte werden abgewiesen.

Ob IEEE 802.1X unterstützt wird bzw. notwendig ist, weiß in der Regel der Netzwerk-Administrator. Der Switch (Authenticator), an dem die Kamera angeschlossen ist, muss entsprechend konfiguriert sein. In der Regel benötigt der Switch (Authenticator) darüber hinaus noch einen Authentifizierungs-Server, z. B. einen RADIUS-Server. Das zu verwendende Verfahren wird durch den Authentifizierungs-Server bestimmt. Kamera und Authentifizierungs-Server müssen immer dasselbe Verfahren verwenden.

## 21. Webserver-Logdatei in regelmäßigen Abständen überprüfen

Admin Menu > Sicherheit > Webserver-Logdatei

Host-Name	IP-Adresse	Status	Benutzername	Datum & Uhrzeit ↓↑
10.0.30.29	10.0.30.29	Erfolgreich	admin	Heute 11:19:02
			-	09:49:49
			admin	09:49:48
			-	2018-02-05 15:51:57
			admin	10:14:53
			-	10:14:41
			admin	10:14:41
10.1.1.102	10.1.1.102	Erfolgreich	admin	2018-02-02 11:57:24
10.0.30.29	10.0.30.29	Erfolgreich	admin	2018-02-01 16:31:46
10.1.1.102	10.1.1.102	Erfolgreich	admin	16:09:47
10.0.30.29	10.0.30.29	Erfolgreich	admin	16:06:39
			-	11:42:35
			admin	11:42:34
10.1.1.102	10.1.1.102	Erfolgreich	admin	08:32:24
10.0.30.29	10.0.30.29	Erfolgreich	admin	2018-01-31 13:08:34
10.1.1.102	10.1.1.102	Erfolgreich	admin	11:43:55
10.0.30.29	10.0.30.29	Erfolgreich	admin	11:41:32
			-	2018-01-30 14:09:54
			admin	12:30:38
10.1.1.102	10.1.1.102	Erfolgreich	admin	2018-01-29 16:38:48
10.0.30.29	10.0.30.29	Erfolgreich	admin	15:40:57
			-	14:05:24
10.1.1.102	10.1.1.102	Erfolgreich	admin	12:30:16
10.0.30.29	10.0.30.29	Erfolgreich	admin	2018-01-25 11:48:58
			-	11:48:16
			admin	11:48:13
10.1.1.102	10.1.1.102	Erfolgreich	admin	11:33:09
10.0.30.29	10.0.30.29	Erfolgreich	admin	2018-01-22 13:57:20
169.254.57.119	169.254.57.119	Erfolgreich	admin	13:45:35
			-	13:44:23
			admin	13:44:23
10.0.30.29	10.0.30.29	Erfolgreich	admin	13:28:55

Die Webserver-Logdatei stellt die Protokolldatei des Kamera-Webserver in übersichtlicher Form dar. In dieser Datei werden sämtliche Zugriffe auf die Kamera mit den entsprechenden Statusmeldungen des Webserver sowie Datum/Uhrzeit des Zugriffs und der Hostname des zugreifenden Computers protokolliert. Nicht autorisierte Zugriffsversuche dienen auch als Alarmsignal für Systemadministratoren, um den Schutz ihres Netzwerks weiter zu verbessern.

## 22. Sicherungskopie der aktuellen Kamerakonfiguration an sicherem Ort ablegen

Admin Menu > Konfiguration > Sichern der aktuellen Konfiguration auf einem lokalen Computer

**Konfiguration**

- **Sichern** der aktuellen Konfiguration in den permanenten Speicher
- **Zurücksetzen** der Konfiguration auf werkseitige Voreinstellungen
- **Wiederherstellen** der letzten gesicherten Konfiguration
- **Laden** einer Konfigurationsdatei vom lokalen Computer
- **Sichern** der aktuellen Konfiguration auf einem lokalen Computer
- **Anzeigen** der aktuellen Konfiguration (**unformatiert**)
- **Bearbeiten** der Konfigurationsdaten von Hand (für Experten)
- **Verwalten** anderer Kameras

**System aktualisieren**

- **Software-Aktualisierung durchführen**

Auch wenn die Anmeldedaten der Kamera (Benutzer und Passwörter) in der Kamerakonfigurations-Datei nur verschlüsselt enthalten sind, sollten alle Sicherungskopien an einem sicheren Ort aufbewahrt werden. Darüber hinaus ist es ratsam, die Datei mit einem Passwort als zusätzliche Sicherheitsstufe zu verschlüsseln.

Herzlichen Glückwunsch – die Cybersicherheit Ihrer MOBOTIX Kamera ist jetzt hergestellt!

## VMS-Konfiguration (Video Management System)



1. Erstellen Sie Benutzerkonten auf dem verwendeten Computer
2. Erstellen Sie Benutzerkonten im VMS (MxManagementCenter)
3. Passen Sie die Benutzerrechte im VMS an
4. Verwenden Sie ein Admin-Benutzerkonto nicht zum Kamerazugriff
5. Aktivieren Sie die automatische Abmeldung (Auto log-off)

Herzlichen Glückwunsch – die Cybersicherheit Ihrer Videomanagement-Software ist jetzt hergestellt!

## NAS-Konfiguration (Network Attached Storage)



1. Positionieren Sie das Speichergerät an einem besonders sicheren Ort
2. Erstellen Sie ein starkes (komplexes) Passwort für das Administratorkonto
3. Erstellen Sie ein Benutzerkonto mit eingeschränkten Rechten für die MOBOTIX Kameras
4. Verschlüsseln Sie die Speichervolumen
5. Verwenden Sie eine RAID-Stufe, die Datenredundanz gewährleistet

Herzlichen Glückwunsch – die Cybersicherheit Ihres NAS-Dateiservers ist jetzt hergestellt!