MOBOTIX HUB – Hardening Guide

2023 R2 - 30.V2.01_8.2023

Inhaltsverzeichnis

1 Urheberrecht, Marken und Haftungsausschluss

Handelsmarken

MOBOTIX HUB ist eine eingetragene Marke der MOBOTIX AG.
Microsoft und Windows sind eingetragene Marken der Microsoft Corporation. App Store ist eine Dienstleistungsmarke von Apple Inc. Android ist eine Marke von Google Inc.
Alle anderen Marken, die in diesem Dokument erwähnt werden, sind Marken ihrer jeweiligen Eigentümer.

Verzichtserklärung

Dieser Text dient nur zu allgemeinen Informationszwecken und wurde mit der gebotenen Sorgfalt erstellt.
Jedes Risiko, das sich aus der Verwendung dieser Informationen ergibt, liegt beim Empfänger, und nichts in diesem Dokument sollte so ausgelegt werden, dass es irgendeine Art von Garantie darstellt.
Die MOBOTIX AG behält sich das Recht vor, ohne vorherige Ankündigung Anpassungen vorzunehmen.
Alle Namen von Personen und Organisationen, die in den Beispielen in diesem Text verwendet werden, sind fiktiv.
Jede Ähnlichkeit mit einer tatsächlichen Organisation oder Person, ob lebendig oder tot, ist rein zufällig und unbeabsichtigt.
Dieses Produkt kann Software von Drittanbietern verwenden, für die möglicherweise besondere Bedingungen gelten. Wenn dies der Fall ist, finden Sie weitere Informationen in der Datei *3rd_party_software_terms_and_conditions.txt, die* sich in Ihrem Installationsordner für das MOBOTIX HUB-System befindet.

2 Einleitung

Dieser Leitfaden beschreibt Sicherheits- und physische Sicherheitsmaßnahmen sowie Best Practices, die Ihnen helfen können, Ihre XProtect Videomanagement-Software (VMS) vor Cyberangriffen zu schützen. Dazu gehören Sicherheitsüberlegungen für die Hard- und Software von Servern, Clients und Netzwerkgerätekomponenten eines Videoüberwachungssystems.

In diesem Leitfaden werden standardmäßige Sicherheits- und Datenschutzkontrollen übernommen und sie den einzelnen Empfehlungen zugeordnet. Das macht diesen Leitfaden zu einer Ressource für die Einhaltung von Sicherheits- und Netzwerksicherheitsanforderungen in der Branche und in Behörden.

2.1 Was ist "Hardening"?

Die Entwicklung und Implementierung von Sicherheitsmaßnahmen und Best Practices wird als "Sicherung" bezeichnet. Sicherung ist ein kontinuierlicher Prozess, bei dem Sicherheitsrisiken identifiziert und verstanden werden und geeignete Maßnahmen ergriffen werden, um ihnen entgegenzuwirken. Der Prozess ist dynamisch, da sich Bedrohungen und die Systeme, auf die sie abzielen, ständig weiterentwickeln.

Die meisten Informationen in diesem Leitfaden konzentrieren sich auf IT-Einstellungen und -Techniken, aber es ist wichtig, sich daran zu erinnern, dass die physische Sicherheit auch ein wichtiger Bestandteil der Sicherung ist. Verwenden Sie z. B. physische Barrieren für Server und Clientcomputer, und stellen Sie sicher, dass Dinge wie Kameragehäuse, Schlösser, Manipulationsmelder und Zugriffskontrollen sicher sind.

Im Folgenden sind die umsetzbaren Schritte zum Sichern eines VMS aufgeführt:

1. Verstehen der zu schützenden Komponenten
2. Sichern Sie die Komponenten des Überwachungssystems:
    1. Sichern der Server (physisch und virtuell) sowie der Clientcomputer und -geräte
    2. Sichern Sie das Netzwerk6/2
    3. Sichern Sie die Kameras
3. Dokumentieren und pflegen Sie die Sicherheitseinstellungen auf jedem System
4. Schulung und Investition in Mitarbeiter und Fähigkeiten, einschließlich Ihrer Lieferkette.

2.1.1 Zielgruppe

Jeder in einem Unternehmen muss zumindest die Grundlagen der Netzwerk- und Softwaresicherheit verstehen. Versuche, kritische IT-Infrastrukturen zu kompromittieren, werden immer häufiger, daher muss jeder Sicherung und Sicherheit ernst nehmen.

Dieser Leitfaden bietet grundlegende und erweiterte Informationen für Endbenutzer, Systemintegratoren, Berater und Komponentenhersteller.

- Grundlegende Beschreibungen geben einen allgemeinen Einblick in die Sicherheit
- Erweiterte Beschreibungen geben IT-spezifische Anleitungen für die Sicherung von XProtect VMS-Produkten. Neben der Software werden auch Sicherheitsüberlegungen für die Hardware und die Gerätekomponenten des Systems beschrieben.

2.1.2 Ressourcen und Referenzen

Die folgenden Organisationen stellen Ressourcen und Informationen zu bewährten Methoden für die Sicherheit bereit:

- Internationale Organisation für Normung (ISO),
- Vereinigte Staaten (USA) Nationales Institut für Standards und Technologie (NIST)

- Security Technical Implementation Guidelines (STIGs) der US-amerikanischen Defense Information Systems Administration (DISA)
- Zentrum für Internet-Sicherheit
- SANS Institut
- Allianz für Cloud-Sicherheit (CSA)
- Arbeitsgruppe für Internettechnik (IETF)
- Britische Normen

Darüber hinaus stellen Kamerahersteller Anleitungen für ihre Hardwaregeräte zur Verfügung.

Siehe Anhang 1 - Ressourcen auf der Seite 101 für eine Liste von Referenzen und Anhang 2 - Akronyme auf der Seite 101 für eine Liste der Akronyme.

Dieser Leitfaden nutzt länderische, internationale und branchenspezifische Standards und Spezifikationen. Insbesondere bezieht es sich auf die Sonderveröffentlichung 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) des US-Handelsministeriums National Institute of Standards and Technology.

Das NIST-Dokument wurde für die US-Bundesregierung geschrieben. In der Sicherheitsbranche ist es jedoch allgemein als die aktuelle Best Practice anerkannt.

Dieser Leitfaden verweist auf zusätzliche Informationen zu Sicherheitskontrollen und verlinkt diese. Der Leitfaden kann auf branchenspezifische Anforderungen und andere internationale Standards und Rahmenwerke für das Sicherheits- und Risikomanagement verwiesen werden. Das aktuelle NIST Cybersecurity Framework verwendet beispielsweise SP 800-53 Rev4 als Grundlage für die Kontrollen und Anleitungen. Ein weiteres Beispiel ist der Anhang H in SP 800-53 Rev 4, der einen Verweis auf die Anforderungen der ISO/IEC 15408, wie z. B. Common Criteria, enthält.

2.1.3 Hardware und Gerätekomponenten

Zu den Komponenten einer MOBOTIX HUB VMS-Installation gehören neben der Software in der Regel auch Hardwaregeräte, wie z. B.:

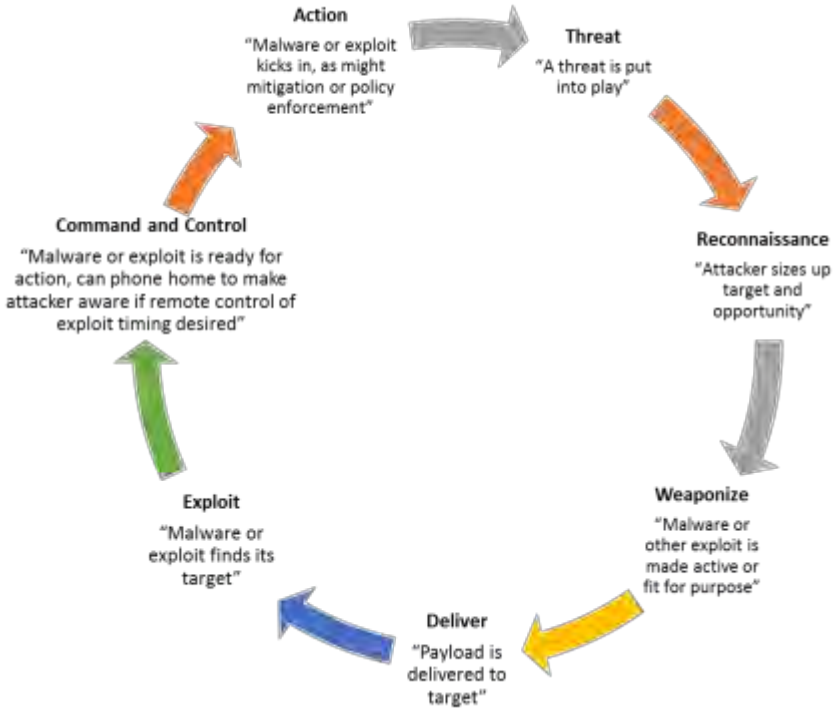
- Fotoapparate
- Encoder
- Produkte für die Vernetzung
- Lagersysteme
- Server und Clientcomputer (physische oder virtuelle Maschinen)
- Mobile Geräte, wie z.B. Smartphones

Es ist wichtig, dass Sie Hardwaregeräte in Ihre Bemühungen einbeziehen, Ihre MOBOTIX HUB VMS-Installation zu Sichern. Zum Beispiel haben Kameras oft Standardpasswörter. Einige Hersteller veröffentlichen diese Passwörter online, damit sie für Kunden leicht zu finden sind. Das bedeutet leider, dass die Passwörter auch Angreifern zur Verfügung stehen.
Dieses Dokument enthält Empfehlungen für Hardwaregeräte.

2.2 Cyberbedrohungen und Cyberrisiken

Es gibt viele Quellen für Bedrohungen für ein VMS, einschließlich geschäftlicher, technologischer, prozessualer und menschlicher Angriffe oder Ausfälle. Bedrohungen finden über einen Lebenszyklus hinweg statt. Der

Bedrohungslebenszyklus, der manchmal auch als "Cyber Kill" oder "Cyber Threat Chain" bezeichnet wird, wurde entwickelt, um die Stadien fortschrittlicher Cyberbedrohungen zu beschreiben.
Jede Phase im Lebenszyklus einer Bedrohung braucht Zeit. Die Zeitspanne für jede Phase hängt von der Bedrohung oder Kombination von Bedrohungen und ihren Akteuren und Zielen ab.



Der Bedrohungslebenszyklus ist wichtig für die Risikobewertung, da er zeigt, wo Sie Bedrohungen abwehren können. Ziel ist es, die Anzahl der Schwachstellen zu reduzieren und sie so früh wie möglich zu beheben. Wenn Sie beispielsweise einen Angreifer entmutigen, der ein System auf Schwachstellen untersucht, kann eine Bedrohung beseitigt werden.
Durch die Sicherung werden Maßnahmen zur Minderung von Bedrohungen für jede Phase des Bedrohungslebenszyklus eingeführt. Während der Erkundungsphase sucht ein Angreifer beispielsweise nach offenen Ports und ermittelt den Status von Diensten, die mit dem Netzwerk und dem VMS in Verbindung stehen. Um dies zu vermeiden, besteht die Sicherungsanleitung darin, nicht benötigte Systemports in MOBOTIX HUB-VMS und Windows-Konfigurationen zu schließen.
Der Prozess der Risiko- und Bedrohungsbewertung umfasst die folgenden Schritte:

- Identifizieren von Informations- und Sicherheitsrisiken
- Risiken bewerten und priorisieren
- Implementieren Sie Richtlinien, Verfahren und technische Lösungen, um diese Risiken zu mindern

Der Gesamtprozess der Risiko- und Bedrohungsbewertung und der Implementierung von Sicherheitskontrollen wird als Risikomanagement-Framework bezeichnet. Dieses Dokument bezieht sich auf NIST-Sicherheits- und Datenschutzkontrollen und andere Veröffentlichungen zu Risikomanagement-Frameworks.

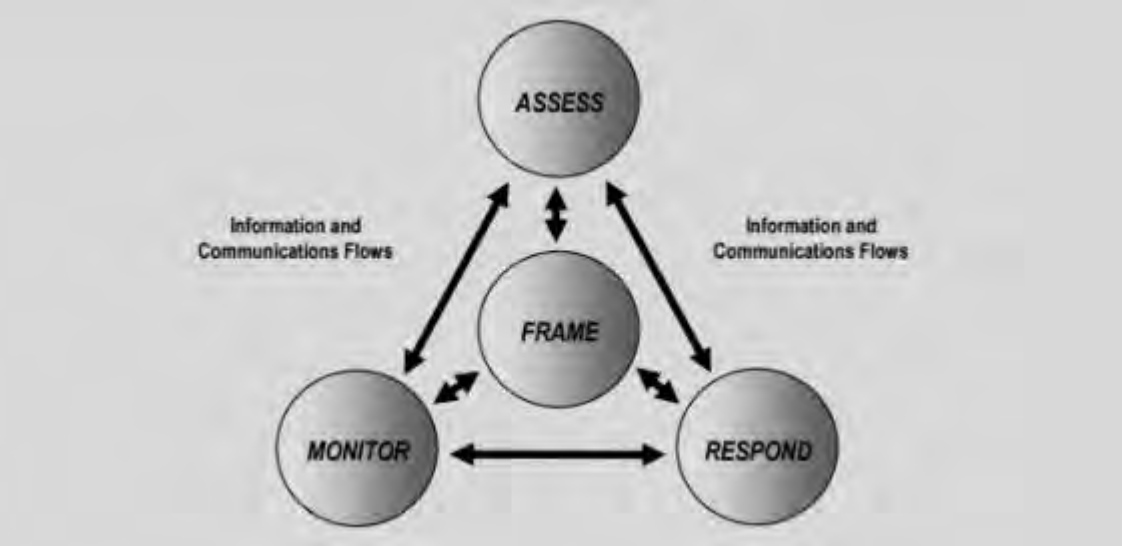
2.2.1 Rahmenwerk für das Cyber-Risikomanagement

Die Sicherheits- und Datenschutzkontrollen in SP 800-53 Revision 4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) sind Teil eines umfassenden Risikomanagement-Frameworks von NIST. Das NIST-Dokument SP800-39 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf) ist ein Leitfaden für die Anwendung eines

Risikomanagement-Frameworks. SP800-36 ist ein grundlegendes Dokument für das NIST Cybersecurity Framework, das im Cybersecurity Framework (http://www.nist.gov/cyberframework/) beschrieben wird.
Die Zahlen hier zeigen:

- Ein Überblick über den Risikomanagementprozess. Es zeigt einen übergeordneten Gesamtansatz auf hohem Niveau.
- Risikomanagement auf betriebswirtschaftlicher Ebene unter Berücksichtigung strategischer und taktischer Überlegungen.
- Der Lebenszyklus eines Risikomanagement-Frameworks und die NIST-Dokumente, die Details zu jedem der Schritte im Lebenszyklus enthalten.

Sicherheits- und Datenschutzkontrollen stellen spezifische Maßnahmen und Empfehlungen dar, die im Rahmen eines Risikomanagementprozesses umgesetzt werden müssen. Es ist wichtig, dass der Prozess die Bewertung der Organisation, die besonderen Anforderungen einer bestimmten Bereitstellung und die Aggregation dieser Aktivitäten in einem Sicherheitsplan umfasst. SP 800-18 Revision 1 (http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf) bietet Referenzen für detaillierte Sicherheitspläne.



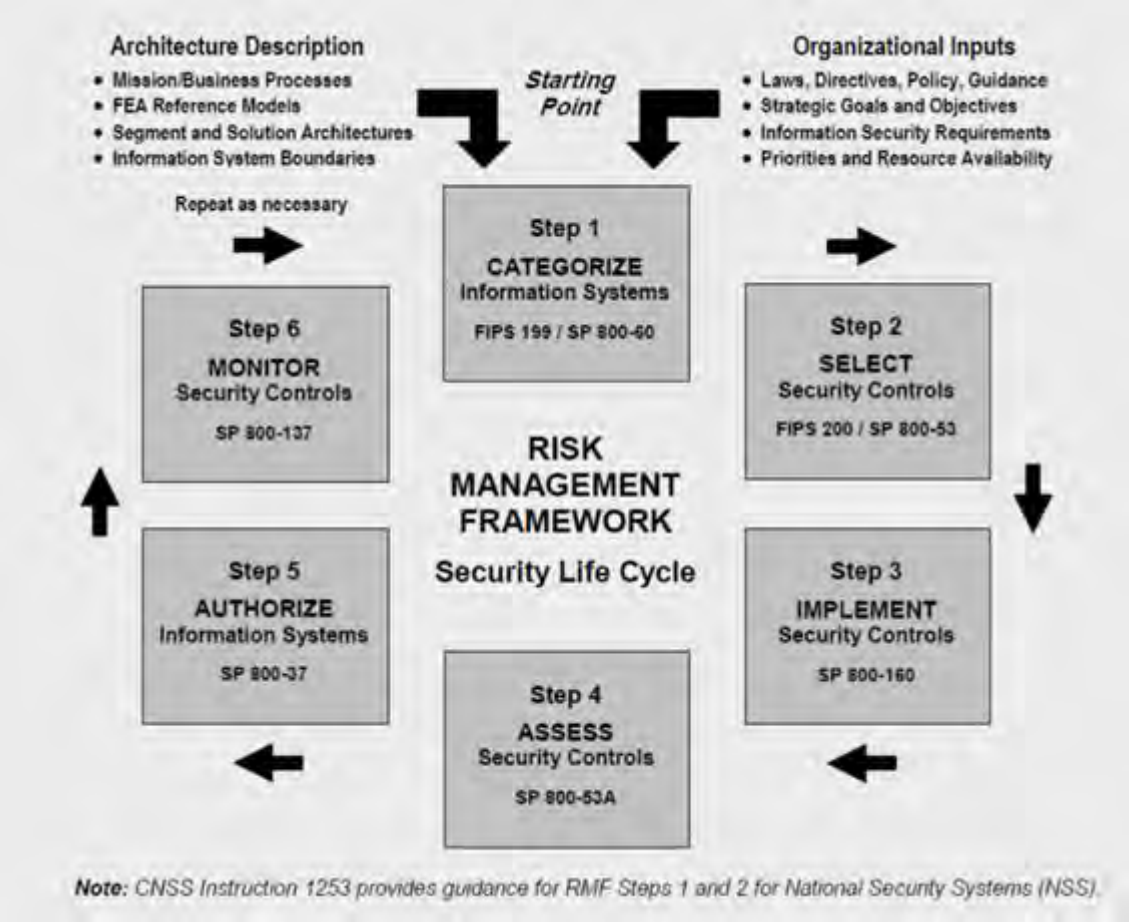
Überblick über das Risikomanagement (SP 800-39, Seite 8 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

Der Prozess ist interaktiv, und die Antworten und ihre Ergebnisse sind iterativ. Sicherheitsbedrohungen, Risiken, Reaktionen und Ergebnisse sind dynamisch und anpassungsfähig, und daher muss auch ein Sicherheitsplan erstellt werden.
Dieses Diagramm zeigt, wie ein Risikomanagement-Framework IT-Systeme, Geschäftsprozesse und die Organisation als Ganzes berücksichtigt, um ein Gleichgewicht für den Sicherheitsplan zu finden.

Balance zwischen Sicherheit und Geschäftszielen (SP 800-39, Seite 9 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

Bei der Sicherung eines Systems wägen Sie die Auswirkungen auf die Produktivität und Benutzerfreundlichkeit des Unternehmens zum Wohle der Sicherheit ab und umgekehrt im Kontext der von Ihnen bereitgestellten Services. Die Sicherheitshinweise sind nicht von anderen Geschäfts- und IT-Aktivitäten isoliert.

Wenn ein Benutzer beispielsweise sein Kennwort bei drei aufeinanderfolgenden Versuchen falsch eingibt, wird das Kennwort blockiert und er kann nicht auf das System zugreifen. Das System ist vor Brute-Force-Angriffen geschützt, aber der unglückliche Benutzer kann das Gerät nicht für seine Arbeit verwenden. Eine Richtlinie für sichere Passwörter, die 30-stellige Passwörter erfordert und Passwörter alle 30 Tage ändert, ist eine bewährte Methode, aber auch schwierig zu verwenden.



Beispiel für ein Rahmenwerk für das Risikomanagement (SP 800-53 Rev 5 Seite 8 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final))

Um sein Risikomanagement zu dokumentieren, hat das NIST mehrere Sonderveröffentlichungen erstellt. Es umfasst die folgenden Komponenten:

1. Kategorisierung (Identifizierung des Risikoniveaus)
2. Auswahl von Sicherheits- und Datenschutzkontrollen
3. Implementierung
4. Bewertung der Wirksamkeit von Sicherheitskontrollen
5. Erstellen eines verbesserten Systemsicherheitsprofils und einer so genannten Authority to Operate (ATO)
6. Überwachung und Bewertung durch Iterationen

Das Risikomanagement-Framework hilft dabei, einen Sicherheitsplan und eine Anleitung in einen Sicherheitskontext zu stellen.

2.3 Sichern von Systemkomponenten

Um Systemkomponenten zu Sichern, ändern Sie die Konfigurationen, um das Risiko eines erfolgreichen Angriffs zu verringern. Angreifer suchen nach einem Weg in das System und suchen nach Schwachstellen in exponierten Teilen des Systems. Überwachungssysteme können 100 oder sogar 1000 Komponenten umfassen. Wenn eine Komponente nicht gesichert wird, kann das System gefährdet werden.

Die Notwendigkeit, Konfigurationsinformationen zu pflegen, wird manchmal übersehen. MOBOTIX HUB VMS bietet Funktionen für die Verwaltung von Konfigurationen, aber Organisationen müssen über eine Richtlinie und einen Prozess verfügen und sich verpflichten, die Arbeit zu erledigen.

Die Sicherung setzt voraus, dass Sie Ihr Wissen über Sicherheit auf dem neuesten Stand halten:

- Achten Sie auf Probleme, die sich auf Software und Hardware auswirken, einschließlich Betriebssysteme, mobile Geräte, Kameras, Speichergeräte und Netzwerkgeräte. Richten Sie einen Ansprechpartner für alle Komponenten im System ein. Verwenden Sie im Idealfall Berichtsverfahren, um Fehler und Schwachstellen für alle Komponenten zu verfolgen.
- Bleiben Sie auf dem Laufenden über allgemeine Sicherheitsanfälligkeiten und Gefährdungen (CVEs) (beschrieben unter Allgemeine Sicherheitsanfälligkeiten und Gefährdungen (https://cve.mitre.org/)) für alle Systemkomponenten. Diese können sich auf Betriebssysteme, Geräte mit fest codierten Wartungskennwörtern usw. beziehen. Beheben Sie Schwachstellen für jede Komponente und warnen Sie Hersteller vor Schwachstellen.
- Pflegen Sie die aktuelle Konfigurations- und Systemdokumentation für das System. Verwenden Sie Änderungskontrollverfahren für die von Ihnen ausgeführte Arbeit, und befolgen Sie bewährte Methoden für die Konfigurationsverwaltung, wie in SP 800-128 (https://csrc.nist.gov/publications/detail/sp/800-128/final) beschrieben.

In den folgenden Abschnitten finden Sie grundlegende und erweiterte Sicherungs- und Sicherheitsempfehlungen für jede Systemkomponente. Die Abschnitte enthalten auch Beispiele dafür, wie sich diese auf bestimmte Sicherheitskontrollen beziehen, die in der NIST-Sonderveröffentlichung 800-53 Revision 4 mit dem Titel *Security and Privacy Controls for Federal Information Systems and Organizations beschrieben sind*.

Zusätzlich zum NIST-Dokument werden die folgenden Quellen referenziert:

- Zentrum für Internet-Sicherheit
- SP 800-53
- ISO 27001
- ISO/IEC 15408 (auch bekannt als Common Criteria, ISO/IEC 15408-1:2022 (https://www.iso.org/standard/72891.html)).

Anhang 1 - Ressourcen auf der Seite 101 Dieses Dokument enthält Empfehlungen von Kameraherstellern. Dies ist eine relativ neue Anstrengung der Hersteller, so dass nur begrenzte Ressourcen zur Verfügung stehen. In den meisten Fällen können die Empfehlungen über Kamerahersteller hinweg verallgemeinert werden.

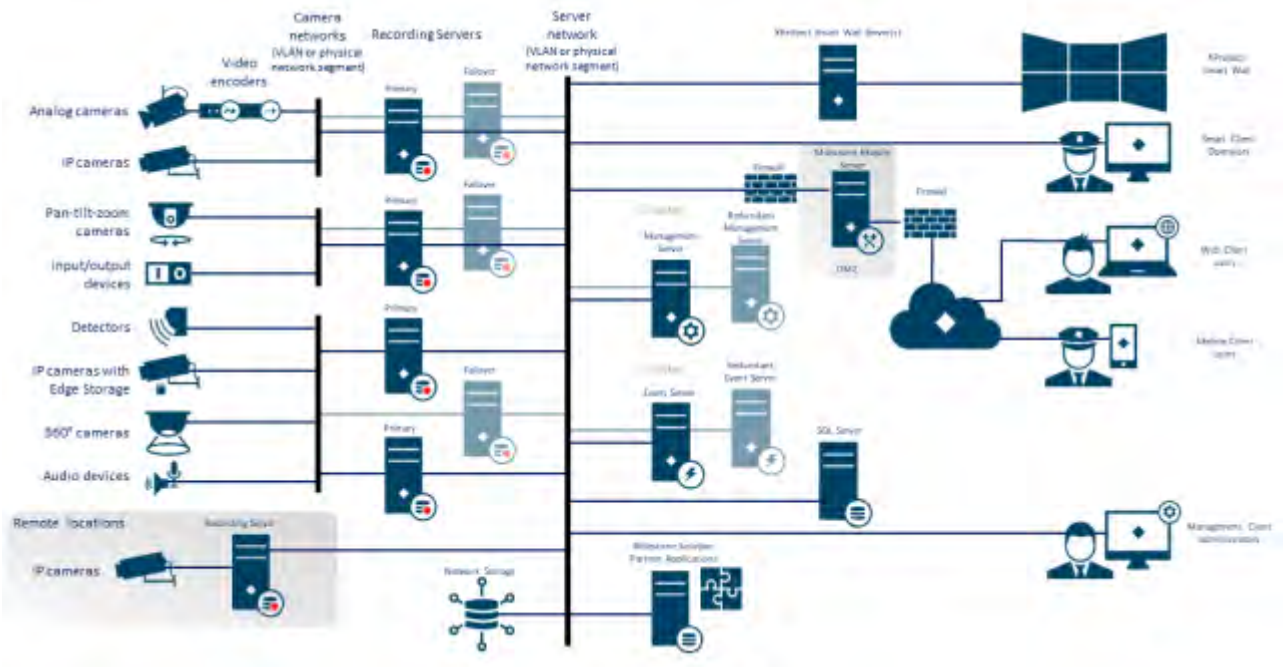
3 Allgemeine Einrichtung

3.1 Überblick

Um Ihr Überwachungssystem zu sichern, empfiehlt MOBOTIX Folgendes:

- Beschränken Sie den Zugriff auf Server. Bewahren Sie Server in verschlossenen Räumen auf und erschweren Sie Eindringlingen den Zugriff auf Netzwerk- und Stromkabel.
  (PE2 und PE3 in den Anhängen D und F in NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (PE Physical and Environment Protection).)
- Entwerfen Sie eine Netzwerkinfrastruktur, die so weit wie möglich physische Netzwerk- oder VLAN-Segmentierung verwendet.
  (SC3 in den Anhängen D und F in NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53 /rev-5/final) (SC System- und Kommunikationsschutz).)
  - Trennen Sie das Kameranetzwerk vom Servernetzwerk, indem Sie auf jedem Aufzeichnungsserver zwei Netzwerkschnittstellen haben: eine für das Kameranetzwerk und eine für das Servernetzwerk.
  - Platzieren Sie den mobilen Server in einer "demilitarisierten Zone" (DMZ) mit einer Netzwerkschnittstelle für den öffentlichen Zugriff und einer für die private Kommunikation mit anderen Servern.
    (SC7 in den Anhängen D und F NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53 /rev-5/final).)
  - Bei der allgemeinen Einrichtung können viele Vorsichtsmaßnahmen getroffen werden. Dazu gehören neben Firewalls auch Techniken zur Segmentierung des Netzwerks und zur Kontrolle des Zugriffs auf die Server, Clients und Anwendungen.
    (AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 in den Anhängen D und F in NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (AC Access Controls), (CM Configuration Management) (IR Incident Response) (SA System and Service Acquisition) (SI Systems and Information Integrity).)
- Konfigurieren Sie das VMS mit Rollen, die den Zugriff auf das System steuern, und legen Sie Aufgaben und Verantwortlichkeiten fest.
  (AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, in den Anhängen D und F in NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (AU Audit and Accountability) (IA Identification and Authentication) (PL Planning).)

Die Abbildung zeigt ein Beispiel für eine allgemeine Einrichtung.



3.1.1 Datenschutz durch Design

MOBOTIX-Produkte sind auf eine sichere End-to-End-Kommunikation ausgelegt. MOBOTIX-Produkte wurden entwickelt, um die Privatsphäre zu schützen und Daten zu sichern. Datenschutz ist immer wichtig, aber vor allem, wenn Sie beabsichtigen, die Datenschutz-Grundverordnung (DSGVO) in der EU einzuhalten.

Gemäß der DSGVO ist der für die Verarbeitung personenbezogener Daten Verantwortliche bei der Verarbeitung dieser Daten verpflichtet, technische oder organisatorische Maßnahmen zu ergreifen, die darauf abzielen, die in der DSGVO festgelegten Datenschutzgrundsätze umzusetzen. Die DSGVO bezeichnet dies als Privacy by Design.

Im Zusammenhang mit einer Überwachungskamera wäre ein relevantes Beispiel für Privacy by Design eine Funktion, die es dem Benutzer digital ermöglicht, die Bilderfassung auf einen bestimmten Bereich zu beschränken und so zu verhindern, dass die Kamera Bilder außerhalb dieses Bereichs aufnimmt, die sonst aufgenommen würden.

In MOBOTIX HUB gibt es Unterstützung für die Maskierung von Privatsphären in zwei Formen: permanente Masken, die nicht entfernt werden können, und anhebbare Masken, die (mit den richtigen Berechtigungen) angehoben werden können, um das Bild hinter der Maske freizulegen.

Der für die Verarbeitung Verantwortliche ist auch verpflichtet, technische oder organisatorische Maßnahmen zu ergreifen, die standardmäßig eine möglichst geringe Verletzung der Privatsphäre der betreffenden personenbezogenen Daten gewährleisten. Die DSGVO bezeichnet dies als datenschutzfreundliche Vorgabe. Im Zusammenhang mit einer Kamera könnte ein relevantes Beispiel für den standardmäßigen Datenschutz die Verwendung von Privatsphärenmaskierung sein, um einen sensiblen Bereich im Sichtfeld der Kamera privat zu halten.

Was sollten Sie tun, um Privacy by Design zu gewährleisten?

- Berücksichtigen Sie die Auflösung verschiedener Punkte in der Kameraszene und dokumentieren Sie diese Einstellungen

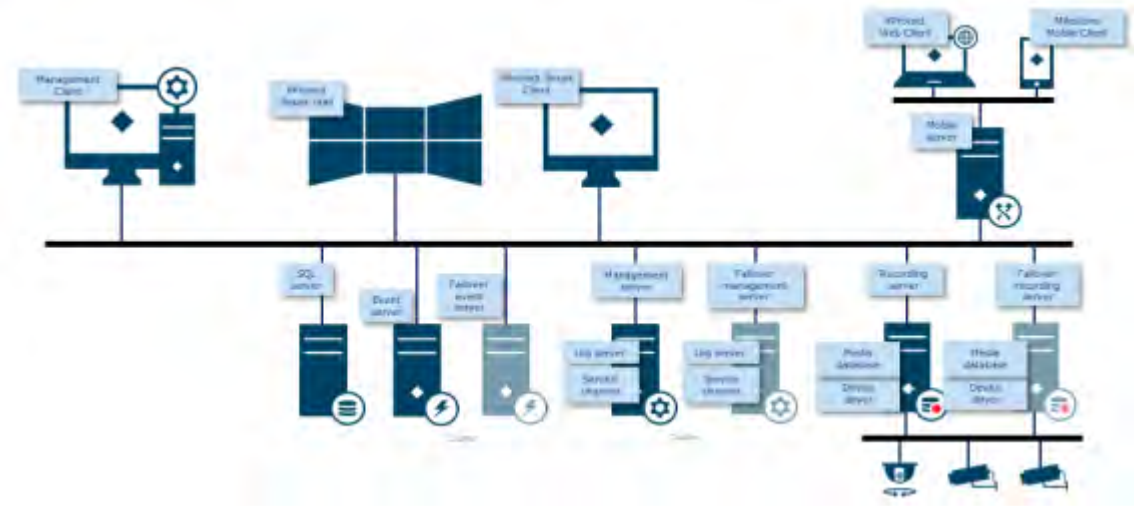
Unterschiedliche Einsatzzwecke erfordern unterschiedliche Bildqualitäten. Wenn eine Identifizierung nicht erforderlich ist, sollten die Kameraauflösung und andere veränderbare Faktoren gewählt werden, um sicherzustellen, dass keine erkennbaren Gesichtsbilder aufgenommen werden.

- Verschlüsseln Sie Ihre Aufzeichnungen
  MOBOTIX empfiehlt, dass Sie Ihre Aufzeichnungen sichern, indem Sie mindestens die Light-Verschlüsselung auf dem Speicher und den Archiven Ihrer Aufnahmeserver aktivieren. MOBOTIX verwendet für die Verschlüsselung den AES-256-Algorithmus. Wenn Sie Leichte Verschlüsselung auswählen, wird nur ein Teil der Aufzeichnung verschlüsselt. Wenn Sie Starke Verschlüsselung auswählen, wird die gesamte Aufzeichnung verschlüsselt.
- Sichern Sie das Netzwerk
  MOBOTIX empfiehlt, Kameras auszuwählen, die HTTPS unterstützen. Es wird empfohlen, dass Sie die Kameras in separaten VLANs einrichten und HTTPS für Ihre Kamera verwenden, um die Serverkommunikation aufzuzeichnen.
  Es wird empfohlen, dass sich MOBOTIX HUB Smart Clients und MOBOTIX HUB Smart Walls im selben VLAN wie die Server befinden.
  Verwenden Sie ein VPN-verschlüsseltes Netzwerk oder ähnliches, wenn Sie Smart Client oder Smart Wall von einem entfernten Standort aus verwenden.
- Aktivieren und dokumentieren Sie die beabsichtigte Aufbewahrungszeit
  Nach Art. 4 Abs. 1 lit. e DSGVO dürfen Aufzeichnungen nicht länger aufbewahrt werden, als es für die konkreten Zwecke, für die sie gemacht wurden, erforderlich ist. MOBOTIX empfiehlt, die Aufbewahrungszeit gemäß den regionalen Gesetzen und Anforderungen festzulegen und in jedem Fall auf maximal 30 Tage festzulegen.
- Sichere Exporte
  MOBOTIX empfiehlt, den Zugriff auf die Exportfunktion nur einer ausgewählten Gruppe von Benutzern zu erlauben, die diese Berechtigung benötigen.
  MOBOTIX empfiehlt außerdem, das Smart Client-Profil so zu ändern, dass nur der Export im MOBOTIX HUB-Format mit aktivierter Verschlüsselung zulässig ist. AVI- und JPEG-Exporte sollten nicht erlaubt sein, da sie nicht sicher gemacht werden können. Dadurch wird der Export von Beweismaterial passwortgeschützt, verschlüsselt und digital signiert, um sicherzustellen, dass forensisches Material echt, unverfälscht und nur vom autorisierten Empfänger eingesehen werden kann.
- Privatsphärenmaskierung aktivieren – dauerhaft oder anhebbar
  Verwenden Sie Privacy Masking, um die Überwachung von Bereichen zu verhindern, die für Ihr Überwachungsziel irrelevant sind.
  MOBOTIX empfiehlt, für sensible Bereiche und an Stellen, an denen die Personenidentifikation nicht erlaubt ist, eine anhebbare Unschärfemaske einzustellen. Erstellen Sie dann eine zweite Rolle, die das Aufheben der Maske autorisieren kann.
- Zugriffsrechte mit Rollen einschränken
  Wenden Sie das Prinzip der geringsten Privilegien (PoLP) an.
  MOBOTIX empfiehlt, den Zugriff auf die Funktionalität nur einer ausgewählten Gruppe von Benutzern zu erlauben, die diese Berechtigung benötigen. Standardmäßig kann nur der Systemadministrator auf das System zugreifen und Aufgaben ausführen. Alle neuen Rollen und Benutzer, die angelegt werden, haben keinen Zugriff auf Funktionen, bis sie von einem Administrator bewusst konfiguriert werden.
  Richten Sie Berechtigungen für alle Funktionen ein, z. B. zum Anzeigen von Live-Videos und -Aufzeichnungen, zum Anhören von Audio, zum Zugriff auf Metadaten, zum Steuern von PTZ-Kameras, zum

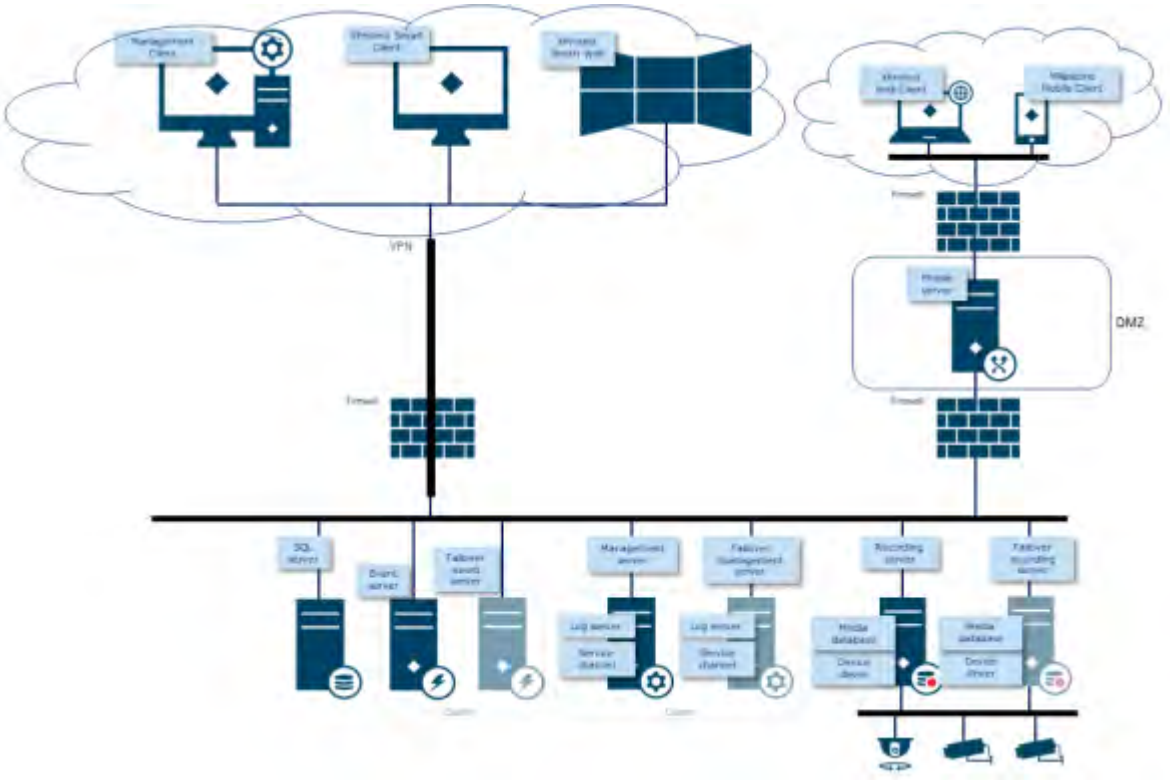
Zugreifen auf und Konfigurieren von Smart Wall, zum Heben von Privatsphärenmasken, Arbeiten mit Exporten, Speichern von Schnappschüssen und so weiter.
Gewähren Sie nur Zugriff auf die Kameras, auf die der jeweilige Bediener zugreifen muss, und beschränken Sie den Zugriff auf aufgezeichnete Video-, Audio- und Metadaten für Bediener entweder vollständig oder gewähren Sie nur Zugriff auf die Video-, Audio- oder Metadaten, die in den letzten Stunden oder weniger aufgezeichnet wurden.
Regelmäßige Bewertung und Überprüfung der Rollen und Verantwortlichkeiten von Bedienern, Ermittlern, Systemadministratoren und anderen Personen mit Zugriff auf das System. Gilt das Prinzip der geringsten Privilegien weiterhin?

- Aktivieren und Verwenden der zweistufigen Überprüfung
  MOBOTIX empfiehlt, für Benutzer von MOBOTIX HUB Mobile oder MOBOTIX HUB Web Client einen zusätzlichen Anmeldeschritt anzugeben, indem Sie die zweistufige Verifizierung aktivieren.
- Einschränken von Administratorberechtigungen
  MOBOTIX empfiehlt, die Anzahl der Benutzer mit der Rolle "Administrator" zu begrenzen. Wenn Sie mehrere Administratorrollen erstellen müssen, können Sie deren Zugriff einschränken, indem Sie Administratorrollen erstellen, die nur ausgewählte Teile des Systems verwalten können, z. B. bestimmte Geräte oder Funktionen.
  MOBOTIX empfiehlt außerdem, dass der VMS-Administrator nicht über vollständige Administratorrechte für den Speicher verfügt, der aufgezeichnete Videos enthält, und dass der Speicheradministrator keinen Zugriff auf die VMS- oder Backup-Verwaltung haben sollte.

Aus Sicherheitsgründen sollten Sie das Netzwerk so segmentieren, dass sich hinter den Aufzeichnungsservern ein Client-/Verwaltungsnetzwerk und Kameranetzwerke befinden:



Um die Sicherheit zu erhöhen, stellen Sie den mobilen Server in eine "demilitarisierte Zone" (DMZ) mit einer Netzwerkschnittstelle für den öffentlichen Zugang und einer für die private Kommunikation mit anderen Servern und verwenden Sie VPN-verschlüsselte Netzwerke für externe Verbindungen oder um die Sicherheit für weniger sichere interne Netzwerke zu erhöhen:


VPN
DMZ

4 Server, Workstations, Clients und Anwendungen

Dieser Abschnitt enthält Anleitungen zur Sicherung basierend auf Microsoft Windows und den Diensten, die von MOBOTIX HUB VMS verwendet werden. Dazu gehören:

- Das MOBOTIX HUB VMS-Produkt, z. B. MOBOTIX HUB® Corporate oder MOBOTIX HUB® Enterprise auf Windows-Servern
- Das auf den Aufzeichnungsservern installierte Gerätepaket
- Die Serverhardware oder virtuelle Plattformen sowie die Betriebssysteme und Dienste
- Die Client-Rechner für MOBOTIX HUB® Smart Client und MOBOTIX HUB® Web Client
- Mobile Endgeräte und deren Betriebssysteme und Anwendungen

4.1 Grundlegende Schritte

4.1.1 Festlegung von Überwachungs- und Sicherheitszielen

MOBOTIX empfiehlt, vor der Implementierung des VMS Überwachungsziele festzulegen. Definieren Sie Ziele und Erwartungen in Bezug auf die Erfassung und Verwendung von Videodaten und zugehörigen Metadaten. Alle Beteiligten sollten die Überwachungsziele verstehen.

Einzelheiten zu den Überwachungszielen finden sich in anderen Dokumenten, z. B. BS EN 62676-1-1: *Videoüberwachungssysteme für den Einsatz in Sicherheitsanwendungen. Systemanforderungen. Allgemein.*

Wenn Überwachungsziele vorhanden sind, können Sie die Sicherheitsziele festlegen. Sicherheitsziele unterstützen die Überwachungsziele, indem sie sich mit den zu schützenden Elementen des VMS befassen. Ein gemeinsames Verständnis der Sicherheitsziele erleichtert die Sicherung des VMS und die Aufrechterhaltung der Datenintegrität. Wenn die Überwachungs- und Sicherheitsziele festgelegt sind, können Sie die betrieblichen Aspekte der Sicherung des VMS leichter angehen, z. B. folgende Vorgehensweisen:

- Verhindern Sie, dass Daten kompromittiert werden
- Reagieren Sie auf Bedrohungen und Vorfälle, wenn sie auftreten, einschließlich Rollen und Verantwortlichkeiten.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 PL-2 Systemsicherheitsplan
- NIST SP 800-53 SA-4 Erfassungsprozess

4.1.2 Erstellen Sie eine formelle Sicherheitsrichtlinie und einen Reaktionsplan

In Übereinstimmung mit NIST SP 800-100 Information Security Handbook: A Guide for Managers (https://csrc.nist.gov/publications/detail/sp/800-100/final) empfiehlt MOBOTIX, dass Sie eine formelle Sicherheitsrichtlinie und einen Reaktionsplan festlegen, die beschreiben, wie Ihr Unternehmen Sicherheitsprobleme in Bezug auf praktische Verfahren und Richtlinien angeht. Eine Sicherheitsrichtlinie kann z. B. Folgendes enthalten:

- Eine Passwortrichtlinie, die von der internen IT-Abteilung definiert wird
- Zutrittskontrolle mit ID-Badges
- Einschränkungen für Smartphones bei der Verbindung mit dem Netzwerk

Übernehmen Sie vorhandene IT-Richtlinien und -Pläne, wenn sie sich an Best Practices für die Sicherheit halten.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 IR-1 Richtlinien und Verfahren für die Reaktion auf Vorfälle
- NIST SP 800-53 PM-1 Plan für das Informationssicherheitsprogramm

4.1.3 Windows-Benutzer mit Active Directory verwenden

Es gibt zwei Arten von Benutzern in MOBOTIX HUB VMS:

- Basisbenutzer: ein dediziertes VMS-Benutzerkonto, das durch eine Kombination aus Benutzername und Kennwort unter Verwendung einer Kennwortrichtlinie authentifiziert wird. Basic-Benutzer stellen eine Verbindung zum VMS über eine SSL-Instanz (Secure Socket Layer) mit der aktuellen TLS-Sicherheitsprotokollsitzung (https://datatracker.ietf.org/wg/tls/charter/ Transport Layer) für die Anmeldung her und verschlüsseln den Inhalt des Datenverkehrs sowie den Benutzernamen und das Kennwort.
- Windows-Benutzer: Das Benutzerkonto ist spezifisch für einen Computer oder eine Domäne und wird basierend auf der Windows-Anmeldung authentifiziert. Windows-Benutzer, die eine Verbindung mit

dem

VMS herstellen, können Microsoft Windows Challenge/Response (NTML) für die Anmeldung, Kerberos (siehe Kerberos-Authentifizierung (erklärt) auf Seite 39) oder andere SSP-Optionen von Microsoft (https://msdn.microsoft.com/en-us /library/windows/desktop/aa380502(v=vs.85).aspx) verwenden.

MOBOTIX empfiehlt, wann immer möglich, Windows-Benutzer in Kombination mit Active Directory (AD) zu verwenden, um den Zugriff auf das VMS zu autorisieren. Auf diese Weise können Sie Folgendes erzwingen:

- Eine Kennwortrichtlinie, die Benutzer dazu verpflichtet, ihr Kennwort regelmäßig zu ändern
- Brute-Force-Schutz, so dass das Windows AD-Konto nach einer Reihe fehlgeschlagener Authentifizierungsversuche gesperrt wird, wiederum in Übereinstimmung mit der Kennwortrichtlinie der Organisation
- Multi-Faktor-Authentifizierung im VMS, insbesondere für Administratoren
- Rollenbasierte Berechtigungen, damit Sie Zugriffskontrollen auf Ihre gesamte Domain anwenden können

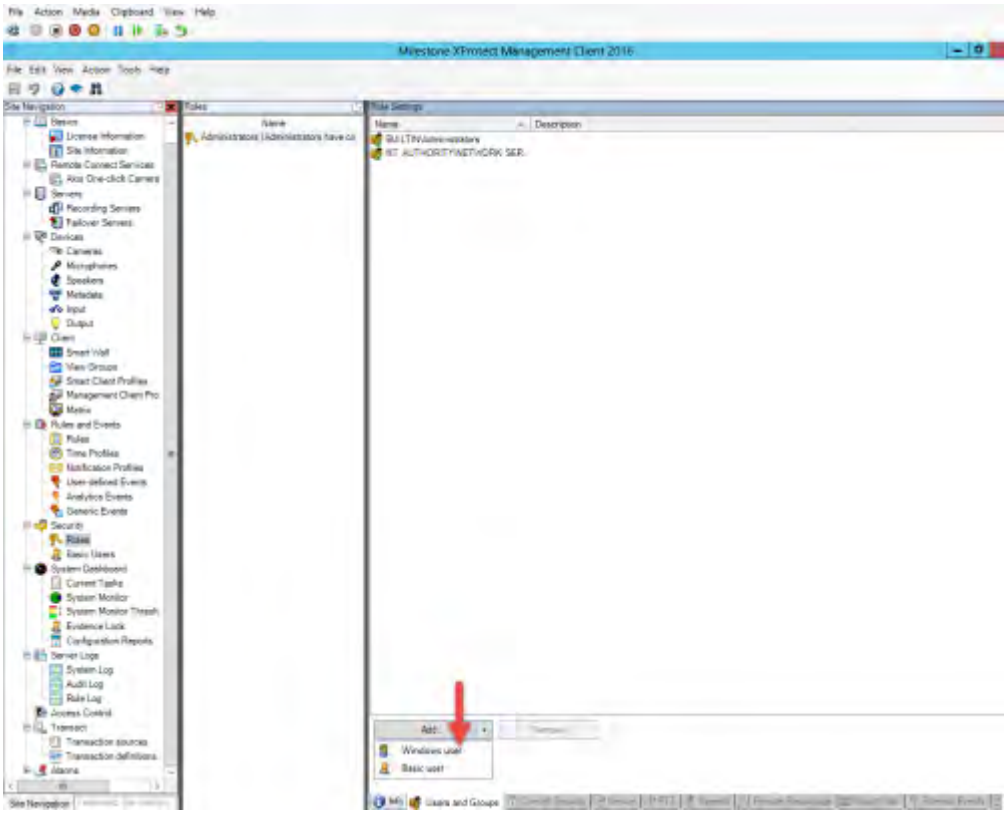
Wenn Ihre Organisation AD nicht verwendet, können Sie stattdessen Windows-Benutzer zu Arbeitsgruppen auf dem Verwaltungsserver hinzufügen. Arbeitsgruppen bieten Ihnen einige der gleichen Vorteile wie Windows-Benutzer mit AD. Sie können eine Kennwortrichtlinie erzwingen, die zum Schutz vor Brute-Force-Angriffen beiträgt, aber MOBOTIX empfiehlt, eine Windows-Domäne zu verwenden, da Sie so eine zentrale Kontrolle über Benutzerkonten haben.

Windows-Benutzer haben den Vorteil, dass sie über das Verzeichnis als eine einzige autoritative Quelle und als Unternehmensdienst für das Netzwerk authentifiziert werden und nicht ad hoc für ihren lokalen Rechner. Auf diese Weise können Sie rollenbasierte Zugriffssteuerungen verwenden, um Benutzern und Gruppen Berechtigungen konsistent in der gesamten Domäne und auf den Computern im Netzwerk zuzuweisen.

Wenn Sie lokale Windows-Benutzer verwenden, muss der Benutzer auf jedem Computer einen lokalen Benutzernamen und ein Kennwort erstellen, was aus Sicherheits- und Benutzerfreundlichkeitsaspekten problematisch ist.

Gehen Sie folgendermaßen vor, um Windows-Benutzer oder -Gruppen zu Rollen im Management-Client hinzuzufügen:

1. Öffnen Sie den Management-Client.
2. Erweitern Sie den Knoten Sicherheit.



3. Wählen Sie die Rolle aus, zu der Sie die Windows-Benutzer hinzufügen möchten.
4. Klicken Sie auf der Registerkarte Benutzer und Gruppen auf Hinzufügen, und wählen Sie Windows-Benutzer aus. Ein Popup-Fenster wird angezeigt.
5. Wenn der Domänenname nicht im Feld Von diesem Standort angezeigt wird, klicken Sie auf Standorte.
6. Geben Sie den Windows-Benutzer an, und klicken Sie dann auf OK.

Um zu überprüfen, ob es sich bei dem Windows-Benutzer um einen AD-Benutzer handelt, muss der Domänenname als Präfix angezeigt werden, z. B. "Domain\John".

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 SA-5 Informationssystem Dokumentation
- NIST SP 800-53 SA-13 Vertrauenswürdigkeit

4.1.4 Sichere Kommunikation (erklärt)

Hypertext Transfer Protocol Secure (HTTPS) ist eine Erweiterung des Hypertext Transfer Protocol (HTTP) für die sichere Kommunikation über ein Computernetzwerk. Bei HTTPS wird das Kommunikationsprotokoll mit Transport Layer Security (TLS) oder seinem Vorgänger Secure Sockets Layer (SSL) verschlüsselt.
In MOBOTIX HUB VMS wird die sichere Kommunikation durch die Verwendung von SSL/TLS mit asymmetrischer Verschlüsselung (RSA) erreicht.
SSL/TLS verwendet ein Schlüsselpaar – einen privaten, einen öffentlichen – um sichere Verbindungen zu authentifizieren, zu sichern und zu verwalten.

Eine Zertifizierungsstelle (Certificate Authority, CA) kann mithilfe eines CA-Zertifikats Zertifikate für Webdienste auf Servern ausstellen. Dieses Zertifikat enthält zwei Schlüssel, einen privaten Schlüssel und einen öffentlichen Schlüssel. Der öffentliche Schlüssel wird auf den Clients eines Web-Service (Service-Clients) installiert, indem ein öffentliches Zertifikat installiert wird. Der private Schlüssel wird zum Signieren von Serverzertifikaten verwendet, die auf dem Server installiert werden müssen. Immer wenn ein Dienstclient den Webdienst aufruft, sendet der Webdienst das Serverzertifikat einschließlich des öffentlichen Schlüssels an den Client. Der Dienstclient kann das Serverzertifikat mithilfe des bereits installierten Zertifikats der öffentlichen Zertifizierungsstelle validieren. Der Client und der Server können nun über das öffentliche und das private Serverzertifikat einen geheimen Schlüssel austauschen und so eine sichere SSL/TLS-Verbindung aufbauen.
Weitere Informationen zu TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security

Zertifikate haben ein Ablaufdatum. MOBOTIX HUB VMS warnt Sie nicht, wenn ein Zertifikat abläuft. Wenn ein Zertifikat abläuft:- Die Clients vertrauen dem Aufzeichnungsserver mit dem abgelaufenen Zertifikat nicht mehr und können daher nicht mehr mit ihm kommunizieren.
Die Aufzeichnungsserver vertrauen dem Management-Server nicht mehr mit dem abgelaufenen Zertifikat und können daher nicht mehr mit ihm kommunizieren
. Die mobilen Geräte vertrauen dem mobilen Server mit dem abgelaufenen Zertifikat nicht mehr und können daher nicht mehr mit ihm
kommunizieren.Um die Zertifikate zu erneuern, führen Sie die Schritte in diesem Leitfaden wie beim Erstellen von Zertifikaten aus.

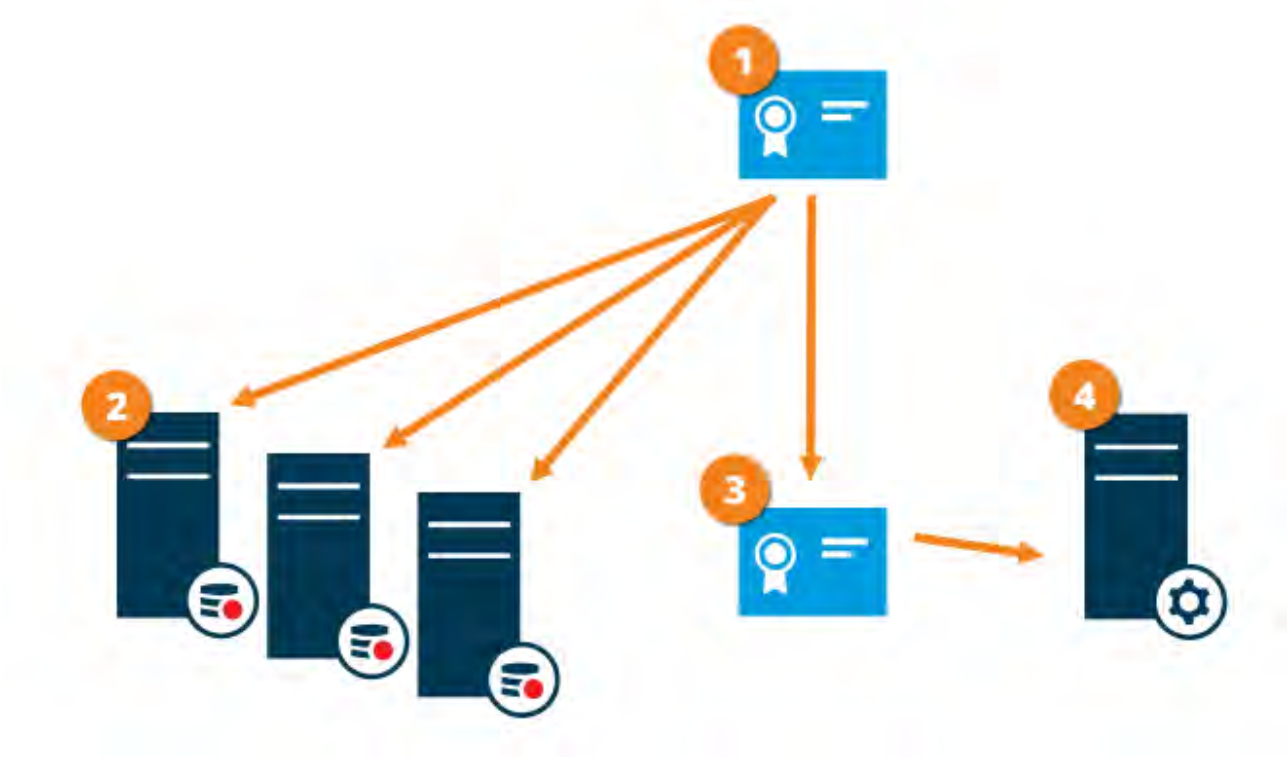
Weitere Informationen finden Sie im Leitfaden für Zertifikate, wie Sie Ihre MOBOTIX Hub VMS-Installationen sichern können .

4.1.5 Verschlüsselung des Management-Servers (erklärt)

Sie können die bidirektionale Verbindung zwischen dem Management-Server und dem Aufzeichnungsserver verschlüsseln. Wenn Sie die Verschlüsselung auf dem Management-Server aktivieren, gilt sie für Verbindungen von allen Aufzeichnungsservern, die eine Verbindung zum Management-Server herstellen. Wenn Sie die Verschlüsselung auf dem Management-Server aktivieren, müssen Sie auch die Verschlüsselung auf allen Aufzeichnungsservern aktivieren. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Management-Server und allen Aufzeichnungsservern installieren.

Zertifikatsverteilung für Management-Server

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in MOBOTIX HUB VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation mit dem Management-Server zu sichern.



❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl der Betreff/Eigentümer (Management-Server) als auch die Partei, die das Zertifikat überprüft (Aufzeichnungsserver), vertrauen

❷ Das CA-Zertifikat muss auf allen Aufzeichnungsservern als vertrauenswürdig eingestuft werden. Auf diese Weise können die Aufzeichnungsserver die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen

❸ Das CA-Zertifikat wird verwendet, um eine sichere Verbindung zwischen dem Management-Server und den Aufzeichnungsservern herzustellen

❹ Das Zertifikat der Zertifizierungsstelle muss auf dem Computer installiert sein, auf dem der Verwaltungsserver ausgeführt wird

Anforderungen an das Zertifikat des privaten Verwaltungsservers:

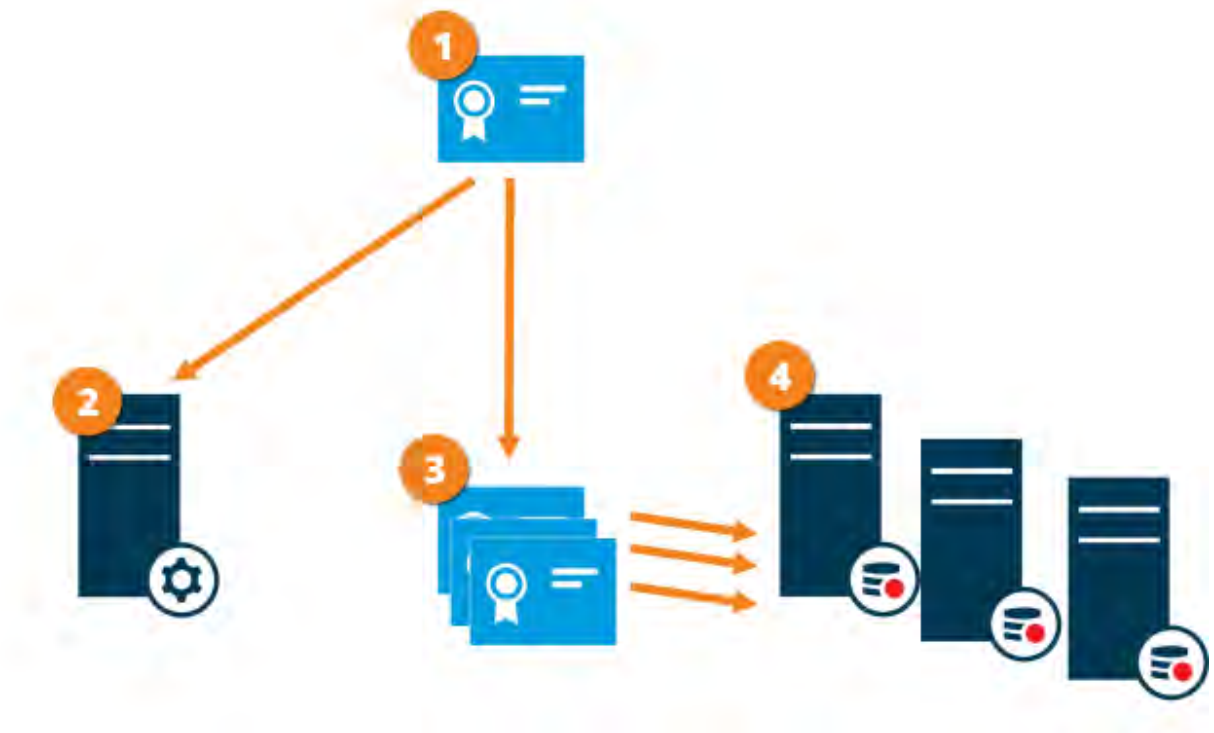
- Wird für den Management-Server ausgestellt, sodass der Hostname des Management-Servers im Zertifikat enthalten ist, entweder als Antragsteller (Besitzer) oder in der Liste der DNS-Namen, für die das Zertifikat ausgestellt wird
- Vertrauenswürdig auf dem Management-Server selbst, indem das CA-Zertifikat als vertrauenswürdig eingestuft wird, das zum Ausstellen des Management-Server-Zertifikats verwendet wurde
- Vertrauenswürdig auf allen Aufzeichnungsservern, die mit dem Management-Server verbunden sind, indem das Zertifikat der Zertifizierungsstelle als vertrauenswürdig eingestuft wird, das zum Ausstellen des Management-Server-Zertifikats verwendet wurde

4.1.6 Verschlüsselung vom Management-Server zum Aufzeichnungsserver (erklärt)

Sie können die bidirektionale Verbindung zwischen dem Management-Server und dem Aufzeichnungsserver verschlüsseln. Wenn Sie die Verschlüsselung auf dem Management-Server aktivieren, gilt sie für Verbindungen von allen Aufzeichnungsservern, die eine Verbindung zum Management-Server herstellen. Die Verschlüsselung dieser Kommunikation muss der Verschlüsselungseinstellung auf dem Management-Server entsprechen. Wenn also die Verschlüsselung des Management-Servers aktiviert ist, muss diese auch auf den Aufzeichnungsservern aktiviert werden und umgekehrt. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Verwaltungsserver und allen Aufzeichnungsservern installieren, einschließlich Failover-Aufzeichnungsservern.

Verteilung von Zertifikaten

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in MOBOTIX HUB VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation vom Management-Server aus zu sichern.



❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl der Betreff/Eigentümer (Aufzeichnungsserver) als auch die Partei, die das Zertifikat überprüft (Management-Server), vertrauen

❷ Das Zertifikat der Zertifizierungsstelle muss auf dem Verwaltungsserver als vertrauenswürdig eingestuft werden. Auf diese Weise kann der Management-Server die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen

❸ Das CA-Zertifikat wird verwendet, um eine sichere Verbindung zwischen den Aufzeichnungsservern und dem Management-Server herzustellen

❹ Das CA-Zertifikat muss auf den Rechnern installiert sein, auf denen die Aufzeichnungsserver ausgeführt werden Voraussetzungen für das Zertifikat des privaten Aufzeichnungsservers:

- Wird an den Aufzeichnungsserver ausgestellt, sodass der Hostname des Aufzeichnungsservers im Zertifikat enthalten ist, entweder als Betreff (Eigentümer) oder in der Liste der DNS-Namen, für die das Zertifikat ausgestellt wird

- Vertrauenswürdig auf dem Management-Server, indem das Zertifikat der Zertifizierungsstelle als vertrauenswürdig eingestuft wird, das zum Ausstellen des Zertifikats des Aufzeichnungsservers verwendet wurde

4.1.7 Verschlüsselung zwischen dem Management-Server und dem Datensammler-Server (Erläuterung)

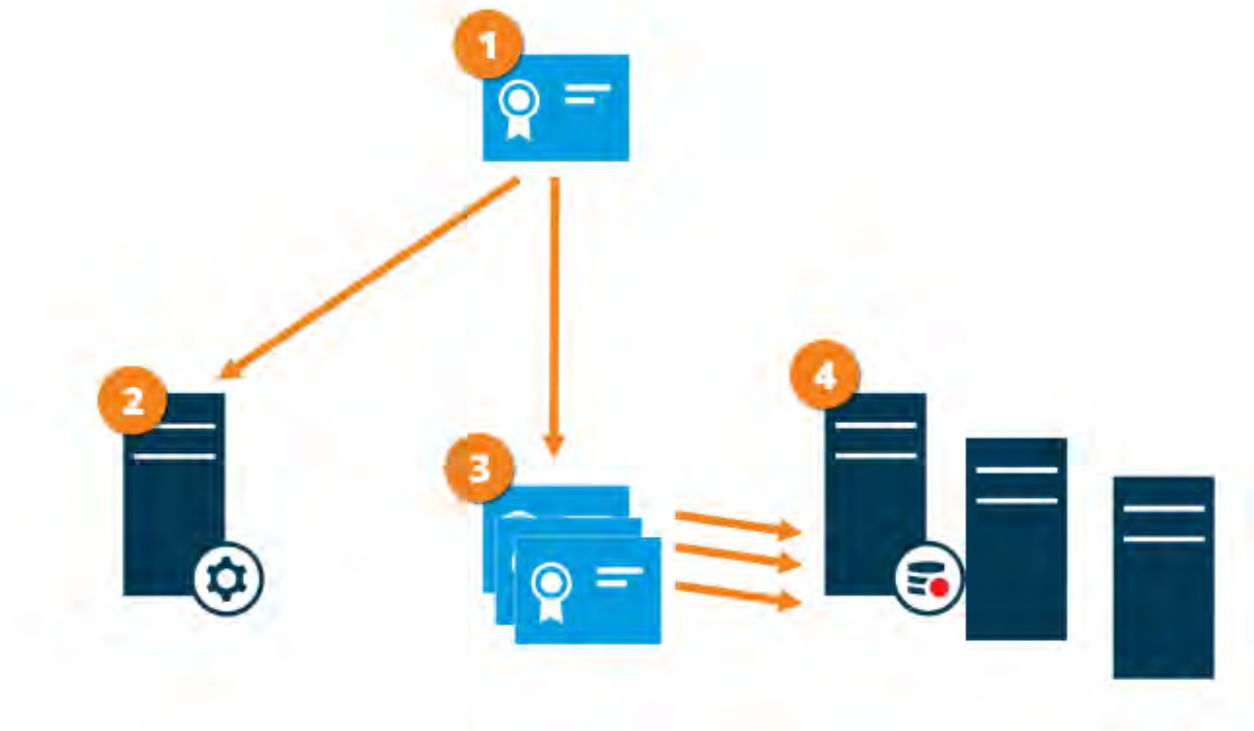
Sie können die bidirektionale Verbindung zwischen dem Management-Server und dem zugehörigen Datensammler verschlüsseln, wenn Sie über einen Remoteserver des folgenden Typs verfügen:

- Aufzeichnungsserver
- Ereignisserver
- Protokollserver
- LPR-Server
- Mobiler Server

Wenn Sie die Verschlüsselung auf dem Verwaltungsserver aktivieren, gilt sie für Verbindungen von allen Datensammlerservern, die eine Verbindung mit dem Verwaltungsserver herstellen. Die Verschlüsselung dieser Kommunikation muss der Verschlüsselungseinstellung auf dem Management-Server entsprechen. Wenn also die Verschlüsselung des Management-Servers aktiviert ist, muss diese auch auf den Data Collector-Servern aktiviert werden, die mit den einzelnen Remote-Servern verbunden sind, und umgekehrt. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Verwaltungsserver und allen Datensammlerservern installieren, die mit den Remoteservern verbunden sind.

Verteilung von Zertifikaten

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in MOBOTIX HUB VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation vom Management-Server aus zu sichern.



❶ Ein Zertifizierungsstellenzertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl der Betreff/Eigentümer (Datensammlerserver) als auch die Partei, die das Zertifikat überprüft (Verwaltungsserver), als vertrauenswürdig eingestuft wird

❷ Das Zertifikat der Zertifizierungsstelle muss auf dem Verwaltungsserver als vertrauenswürdig eingestuft werden. Auf diese Weise kann der Management-Server die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen

❸ Das CA-Zertifikat wird verwendet, um eine sichere Verbindung zwischen den Datensammlerservern und dem Management-Server herzustellen

❹ Das Zertifikat der Zertifizierungsstelle muss auf den Computern installiert sein, auf denen die Datensammlerserver ausgeführt werden

Anforderungen an das Serverzertifikat für den privaten Datensammler:

- Wird für den Datensammlerserver ausgestellt, sodass der Hostname des Datensammlerservers im Zertifikat enthalten ist, entweder als Antragsteller (Besitzer) oder in der Liste der DNS-Namen, für die das Zertifikat ausgestellt wird
- Vertrauenswürdig auf dem Verwaltungsserver, indem das Zertifikat der Zertifizierungsstelle als vertrauenswürdig eingestuft wird, das zum Ausstellen des Datensammlerserverzertifikats verwendet wurde

4.1.8 Verschlüsselung für Clients und Server, die Daten vom Aufzeichnungsserver abrufen (erklärt)

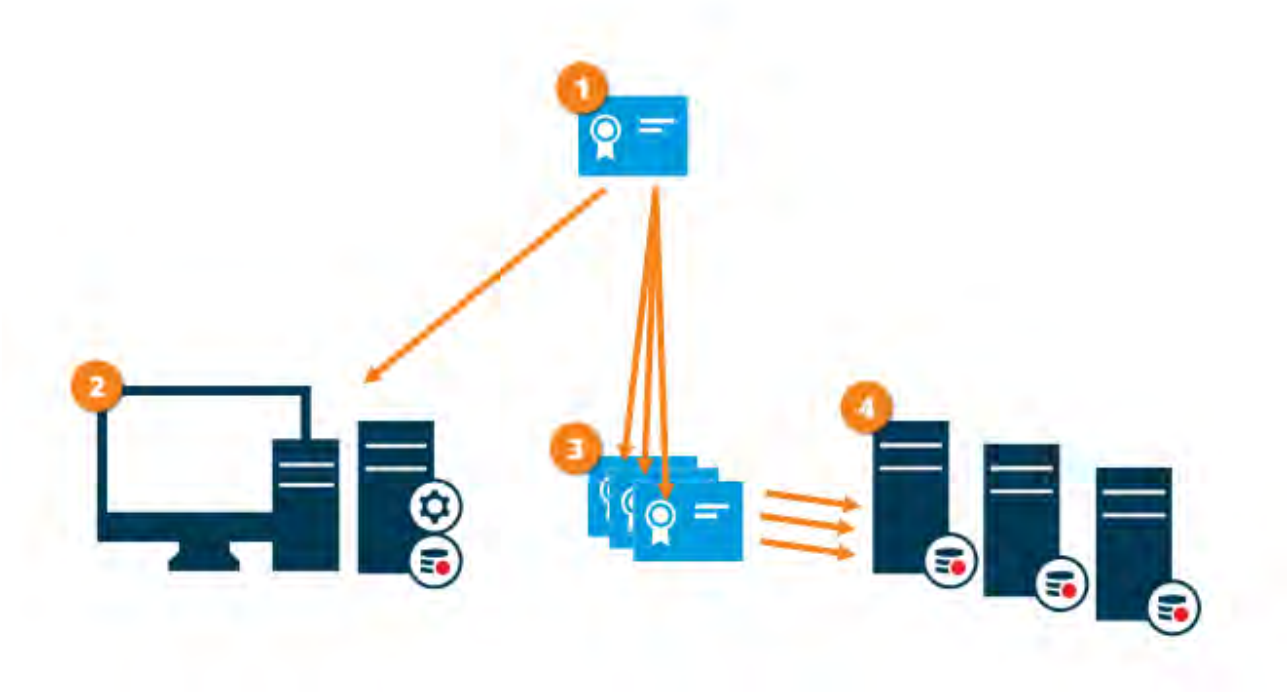
Wenn Sie die Verschlüsselung auf einem Aufzeichnungsserver aktivieren, wird die Kommunikation mit allen Clients, Servern und Integrationen, die Datenströme vom Aufzeichnungsserver abrufen, verschlüsselt. In diesem Dokument, das als "Kunden" bezeichnet wird, gilt Folgendes:

- MOBOTIX HUB Smart Client
- Management-Client
- Management Server (für System Monitor und für Bilder und AVI-Videoclips in E-Mail-Benachrichtigungen)
- MOBOTIX HUB Mobiler Server
- MOBOTIX HUB Ereignisserver
- MOBOTIX HUB LPR
- MOBOTIX Open Network Bridge
- MOBOTIX HUB DLNA Server
- Standorte, die Datenströme vom Aufzeichnungsserver über MOBOTIX Interconnect abrufen
- Einige MIP SDK-Integrationen von Drittanbietern

Für Lösungen, die mit MIP SDK 2018 R3 oder früher erstellt wurden und auf Aufzeichnungsserver zugreifen: Wenn die Integrationen mithilfe von MIP SDK-Bibliotheken vorgenommen werden, müssen sie mit MIP SDK 2019 R1 neu erstellt werden. Wenn die Integrationen direkt mit den Recording Server-APIs kommunizieren, ohne MIP SDK-Bibliotheken zu verwenden, müssen die Integratoren selbst HTTPS-Unterstützung hinzufügen.

Verteilung von Zertifikaten

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in MOBOTIX HUB VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation zum Aufzeichnungsserver abzusichern.



❶ Ein CA-Zertifikat fungiert als vertrauenswürdiger Drittanbieter, der sowohl vom Betreff/Eigentümer (Aufzeichnungsserver) als auch von der Partei, die das Zertifikat überprüft (alle Clients), als vertrauenswürdig eingestuft wird

❷ Das Zertifizierungsstellenzertifikat muss auf allen Clients als vertrauenswürdig eingestuft werden. Auf diese Weise können die Clients die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen

❸ Das CA-Zertifikat wird verwendet, um eine sichere Verbindung zwischen den Aufzeichnungsservern und allen Clients und Diensten herzustellen

❹ Das CA-Zertifikat muss auf den Rechnern installiert sein, auf denen die Aufzeichnungsserver ausgeführt werden

Voraussetzungen für das Zertifikat des privaten Aufzeichnungsservers:

- Wird an den Aufzeichnungsserver ausgestellt, sodass der Hostname des Aufzeichnungsservers im Zertifikat enthalten ist, entweder als Betreff (Eigentümer) oder in der Liste der DNS-Namen, für die das Zertifikat ausgestellt wird
- Vertrauenswürdig auf allen Computern, auf denen Dienste ausgeführt werden, die Datenströme von den Aufzeichnungsservern abrufen, indem das Zertifikat der Zertifizierungsstelle als vertrauenswürdig eingestuft wird, das zum Ausstellen des Zertifikats des Aufzeichnungsservers verwendet wurde
- Das Dienstkonto, auf dem der Aufzeichnungsserver ausgeführt wird, muss Zugriff auf den privaten Schlüssel des Zertifikats auf dem Aufzeichnungsserver haben.

Wenn Sie die Verschlüsselung auf den Aufzeichnungsservern aktivieren und Ihr System Failover-Aufzeichnungsserver einsetzt, empfiehlt MOBOTIX, auch die Failover-Aufzeichnungsserver für die Verschlüsselung vorzubereiten.

4.1.9 Verschlüsselung der Kommunikation mit dem Event Server

Sie können die bidirektionale Verbindung zwischen dem Ereignisserver und den Komponenten, die mit dem Ereignisserver kommunizieren, einschließlich des LPR-Servers, verschlüsseln. Wenn Sie die Verschlüsselung auf dem Ereignisserver aktivieren, gilt sie für Verbindungen von allen Komponenten, die eine Verbindung mit dem

Ereignisserver herstellen. Bevor Sie die Verschlüsselung aktivieren, müssen Sie Sicherheitszertifikate auf dem Ereignisserver und allen Verbindungskomponenten installieren.

Wenn die Event-Server-Kommunikation verschlüsselt ist, gilt dies für die gesamte Kommunikation mit diesem Event-Server. Das heißt, es wird jeweils nur ein Modus unterstützt, entweder http oder https, aber nicht gleichzeitig.

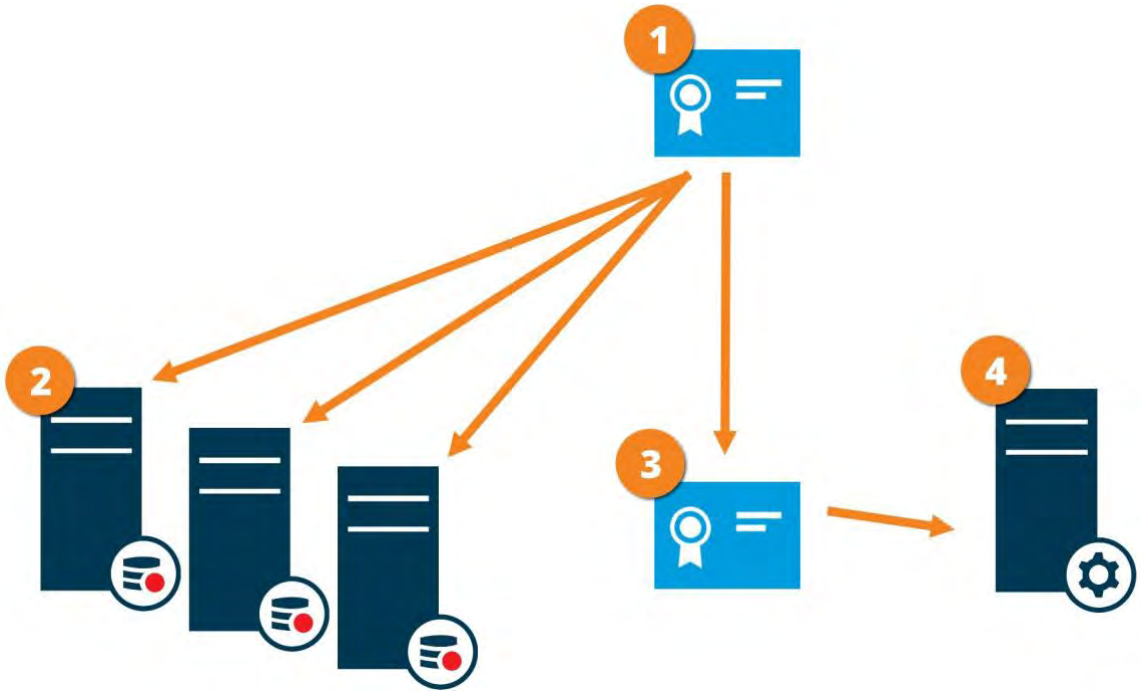
Die Verschlüsselung gilt für jeden Dienst, der auf dem Ereignisserver gehostet wird, einschließlich Transact, Maps, GisMap und Intercommunication.

Bevor Sie die Verschlüsselung im Event Server aktivieren, müssen alle Clients (Smart Client und Management Client) und das XProtect LPR-Plug-In mindestens auf Version 2022 R1 aktualisiert werden.

HTTPS wird nur unterstützt, wenn jede Komponente mindestens auf Version 2022 R1 aktualisiert wurde.

Verteilung von Zertifikaten

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in XProtect VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation mit dem Ereignisserver zu sichern



❶ Ein Zertifizierungsstellenzertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl der Antragsteller/Besitzer (Ereignisserver) als auch die Partei, die das Zertifikat überprüft, als vertrauenswürdig eingestuft wird

❷ Das Zertifizierungsstellenzertifikat muss auf allen Clients als vertrauenswürdig eingestuft werden. Auf diese Weise können die Clients die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen

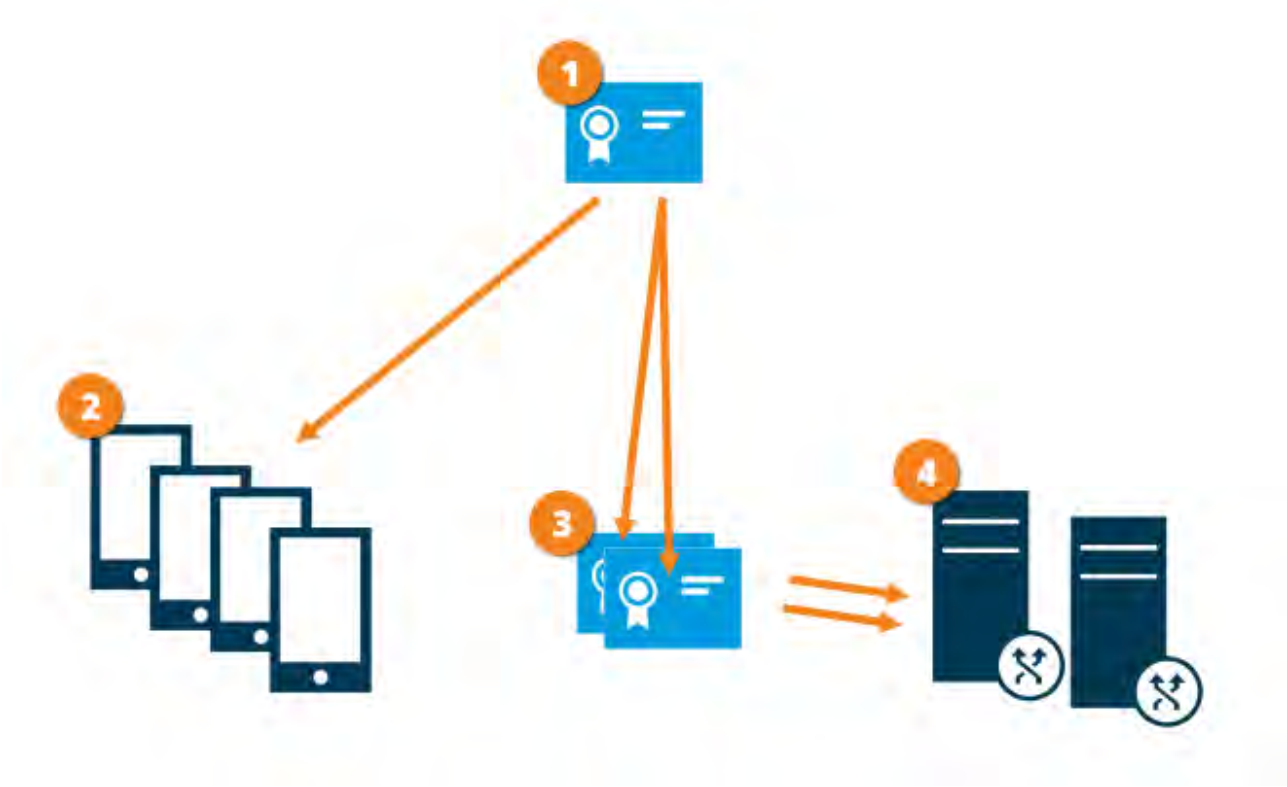
❸ Das Zertifikat der Zertifizierungsstelle wird verwendet, um eine sichere Verbindung zwischen dem Ereignisserver und den Clients herzustellen❹. Das Zertifikat der Zertifizierungsstelle muss auf dem Computer installiert sein, auf dem der Ereignisserver ausgeführt wird.

4.1.10 Datenverschlüsselung mobiler Server (erklärt)

In MOBOTIX HUB-VMS wird die Verschlüsselung pro mobilem Server aktiviert oder deaktiviert. Wenn Sie die Verschlüsselung auf einem mobilen Server aktivieren, haben Sie die Möglichkeit, eine verschlüsselte Kommunikation mit allen Clients, Diensten und Integrationen zu verwenden, die Datenströme abrufen.

Zertifikatsverteilung für mobile Server

Die Grafik veranschaulicht das grundlegende Konzept, wie Zertifikate in MOBOTIX HUB VMS signiert, vertrauenswürdig und verteilt werden, um die Kommunikation mit dem mobilen Server abzusichern.



❶ Ein Zertifizierungsstellenzertifikat fungiert als vertrauenswürdiger Dritter, dem sowohl der Betreff/Besitzer (mobiler Server) als auch die Partei, die das Zertifikat überprüft (alle Clients), als vertrauenswürdig eingestuft wird
❷ Das Zertifizierungsstellenzertifikat muss auf allen Clients als vertrauenswürdig eingestuft werden. Auf diese Weise können Clients die Gültigkeit der von der Zertifizierungsstelle ausgestellten Zertifikate überprüfen
❸ Das CA-Zertifikat wird verwendet, um eine sichere Verbindung zwischen dem mobilen Server und Clients und Diensten herzustellen
❹ Das Zertifikat der Zertifizierungsstelle muss auf dem Computer installiert sein, auf dem der mobile Server ausgeführt wird

Voraussetzungen für das CA-Zertifikat:

- Der Hostname des mobilen Servers muss im Zertifikat enthalten sein, entweder als Betreff/Eigentümer oder in der Liste der DNS-Namen, für die das Zertifikat ausgestellt wurde
- Das Zertifikat muss auf allen Geräten vertrauenswürdig sein, auf denen Dienste ausgeführt werden, die Datenströme vom mobilen Server abrufen

- Das Dienstkonto, auf dem der mobile Server ausgeführt wird, muss Zugriff auf den privaten Schlüssel des Zertifizierungsstellenzertifikats haben

Anforderungen an die Verschlüsselung mobiler Server für Clients

Wenn Sie die Verschlüsselung nicht aktivieren und eine HTTP-Verbindung verwenden, steht die Push-to-Talk-Funktion im MOBOTIX HUB Web Client nicht zur Verfügung.

4.1.11 Kerberos-Authentifizierung (erklärt)

Kerberos ist ein ticketbasiertes Netzwerkauthentifizierungsprotokoll. Es wurde entwickelt, um eine starke Authentifizierung für Client/Server- oder Server/Server-Anwendungen zu ermöglichen.
Verwenden Sie die Kerberos-Authentifizierung als Alternative zum älteren Authentifizierungsprotokoll Microsoft NT LAN (NTLM).
Die Kerberos-Authentifizierung erfordert eine gegenseitige Authentifizierung, bei der sich der Client beim Dienst und der Dienst beim Client authentifiziert. Auf diese Weise können Sie sich sicherer von MOBOTIX HUB-Clients bei MOBOTIX HUB-Servern authentifizieren, ohne Ihr Passwort preiszugeben.
Um die gegenseitige Authentifizierung in Ihren MOBOTIX HUB VMS zu ermöglichen, müssen Sie Service Principal Names (SPN) im Active Directory registrieren. Ein SPN ist ein Alias, der eine Entität, z. B. einen MOBOTIX HUB-Serverdienst, eindeutig identifiziert. Für jeden Dienst, der die gegenseitige Authentifizierung verwendet, muss ein SPN registriert sein, damit Clients den Dienst im Netzwerk identifizieren können. Ohne korrekt registrierte SPNs ist eine gegenseitige Authentifizierung nicht möglich.
In der folgenden Tabelle sind die verschiedenen MOBOTIX-Dienste mit den entsprechenden Portnummern aufgeführt, die Sie für die Registrierung benötigen:

Dienst	Portnummer
Verwaltungsserver – IIS	80 - Konfigurierbar
Management-Server - Intern	8080
Aufzeichnungsserver - Datensammler	7609
Failover-Server	8990
Ereignisserver	22331
LPR-Server	22334

Die Anzahl der Dienste, die Sie im Active Directory registrieren müssen, hängt von Ihrer aktuellen Installation ab. Data Collector wird bei der Installation von Management Server, Recording Server, Event Server, LPR Server oder Failover Server automatisch installiert.

Sie müssen zwei SPNs für den Benutzer registrieren, der den Dienst ausführt: einen mit dem Hostnamen und einen mit dem vollqualifizierten Domänennamen.
Wenn Sie den Dienst unter einem Netzwerkbenutzerdienstkonto ausführen, müssen Sie die beiden SPNs für jeden Computer registrieren, auf dem dieser Dienst ausgeführt wird.
Dies ist das MOBOTIX SPN-Benennungsschema:

```
VideoOS/[DNS-Hostname]:[Port]
VideoOS/[Vollständig qualifizierter Domänenname]:[Port]
```

Folgenden finden Sie ein Beispiel für SPNs für den Aufzeichnungsserverdienst, der auf einem Computer mit den folgenden Details ausgeführt wird:

```
Hostname: Datensatzserver1
Domäne: Surveillance.com
```

Zu registrierende SPNs:

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

4.1.12 Verwenden Sie das Windows-Update

MOBOTIX empfiehlt, dass Sie Windows Update verwenden, um Ihr VMS vor Schwachstellen im Betriebssystem zu schützen, indem Sie sicherstellen, dass die neuesten Updates installiert sind. MOBOTIX HUB VMS ist Windows-basiert, daher sind Sicherheitsupdates von Windows Update wichtig.

Updates können eine Verbindung zum Internet erfordern, daher empfiehlt MOBOTIX, diese Verbindung nur bei Bedarf zu öffnen und auf ungewöhnliche Verkehrsmuster zu überwachen.

Windows-Updates erfordern häufig einen Neustart. Dies kann ein Problem sein, wenn eine hohe Verfügbarkeit erforderlich ist, da der Server während des Neustarts keine Daten von Geräten empfangen kann.

Es gibt mehrere Möglichkeiten, dies zu vermeiden oder die Auswirkungen zu minimieren. Sie können z. B. Updates auf den Server herunterladen und diese dann zu einem Zeitpunkt anwenden, zu dem ein Neustart die Überwachung so wenig wie möglich stört.

Wenn Hochverfügbarkeit ein Problem darstellt, empfiehlt MOBOTIX, Management-Server und Ereignisserver in Clustern auszuführen, die einen oder mehrere Failover-Server enthalten. Der Failover-Server übernimmt die Kontrolle, während der Aufzeichnungsserver neu gestartet wird, und die Überwachung wird nicht unterbrochen. Schließen Sie keine Aufzeichnungsserver in den Cluster ein. Verwenden Sie für Aufzeichnungsserver einen Failover-Aufzeichnungsserver.

MOBOTIX empfiehlt, vor der Implementierung von Windows-Updates in der gesamten Organisation die Updates in einer Testumgebung zu überprüfen. Siehe NIST 800-53 CM-8 *Information system component inventory and sandboxing and SC-44 Detonationskammern*.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SI-2 Fehlerbehebung

4.1.13 Halten Sie Software und Geräte-Firmware auf dem neuesten Stand

MOBOTIX empfiehlt, für die Hardware-Geräte, z. B. die Kameras, die neueste Version von MOBOTIX HUB VMS und Firmware zu verwenden. Dadurch wird sichergestellt, dass Ihr System die neuesten Sicherheitsupdates enthält. Überprüfen Sie bei Hardware, Netzwerkkomponenten und Betriebssystemen die CVE-Datenbank sowie alle von den Herstellern veröffentlichten Updates.

Bevor Sie die Geräte-Firmware aktualisieren, stellen Sie sicher, dass MOBOTIX HUB VMS sie unterstützt. Stellen Sie außerdem sicher, dass das auf den Aufzeichnungsservern installierte Gerätepaket die Gerätefirmware unterstützt. Führen Sie dies in einer Testumgebung für Konfiguration, Integration und Tests durch, bevor Sie es in die Produktionsumgebung einführen.

Gehen Sie folgendermaßen vor, um zu überprüfen, ob das VMS ein Gerät unterstützt:

1. Öffnen Sie diesen Link (https://www.mobotix.com/mobotix_custom_table/hub_compatibility).

2. Wählen Sie den Hersteller Ihres Geräts aus, und klicken Sie dann auf Filter. Die Version der Firmware, die vom Gerätepaket unterstützt wird, wird in der Spalte Getestete Firmware aufgeführt .

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SI-2 Fehlerbehebung

4.1.14 Verwenden Sie Antivirus auf allen Servern und Computern

MOBOTIX empfiehlt, Antivirensoftware auf allen Servern und Computern zu implementieren, die eine Verbindung zu den VMS herstellen. Malware, die in Ihr System eindringt, kann Daten auf den Servern und anderen Geräten im Netzwerk sperren, verschlüsseln oder anderweitig kompromittieren.

Wenn mobile Geräte eine Verbindung zum VMS herstellen, muss sichergestellt werden, dass auf den Geräten die neuesten Betriebssysteme und Patches (wenn auch nicht direkt Antivirenprogramme) installiert sind.

Wenn Sie einen Virenscan durchführen, scannen Sie nicht die Verzeichnisse und Unterverzeichnisse des Aufzeichnungsservers, die Aufzeichnungsdatenbanken enthalten. Darüber hinaus sollten Archivspeicherverzeichnisse nicht auf Viren überprüft werden. Die Suche nach Viren in diesen Verzeichnissen kann sich auf die Systemleistung auswirken.

Informationen zu den Ports, Verzeichnissen und Unterverzeichnissen, die von der Virenprüfung ausgeschlossen werden sollen, finden Sie im Abschnitt *Über die Virenprüfung* im *MOBOTIX HUB VMS - Administratorhandbuch*.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 PL-8 Architektur für Informationssicherheit
- NIST SP 800-53 SI-2 Fehlerbehebung
- NIST SP 800-53 SI-3 Schutz vor bösartigem Code
- NIST SP 800-53 SI Überwachung von Informationssystemen

4.1.15 Überwachen Sie die Protokolle im VMS auf Anzeichen verdächtiger Aktivitäten

MOBOTIX HUB VMS bietet Funktionen zum Generieren und Anzeigen von Protokollen, die Informationen zu Nutzungsmustern, Systemleistung und anderen Problemen enthalten. MOBOTIX empfiehlt, die Protokolle auf Anzeichen verdächtiger Aktivitäten zu überwachen.

Es gibt Tools, die Protokolle für Betriebs- und Sicherheitszwecke nutzen. Viele Unternehmen verwenden Syslog-Server, um Protokolle zu konsolidieren. Sie können Syslog verwenden, um Aktivitäten auf Windows-Ebene zu notieren, MOBOTIX HUB VMS unterstützt Syslog jedoch nicht.

MOBOTIX empfiehlt, das Überwachungsprotokoll in MOBOTIX HUB VMS zu verwenden und die Protokollierung des Benutzerzugriffs im Management Client zu aktivieren. Standardmäßig werden im Überwachungsprotokoll nur Benutzeranmeldungen vermerkt. Sie können jedoch die Protokollierung des Benutzerzugriffs aktivieren, sodass im Überwachungsprotokoll alle Benutzeraktivitäten in allen Clientkomponenten von MOBOTIX HUB VMS-Produkten vermerkt werden. Dazu gehören die Zeitpunkte der Aktivitäten und die Quell-IP-Adressen.

Bei den Clientkomponenten handelt es sich um MOBOTIX HUB Smart Client, Web Client, die MOBOTIX HUB Management Client-Komponente und Integrationen, die mit dem MIP SDK erstellt wurden. Beispiele für Aktivitäten sind Exporte, das Aktivieren von Ausgängen, das Betrachten von Kameras live oder in der Wiedergabe und so weiter.

Das Überwachungsprotokoll vermerkt keine erfolglosen Anmeldeversuche oder wenn sich der Benutzer abmeldet.

Das Protokollieren aller Benutzeraktivitäten in allen Clients erhöht die Belastung des Systems und kann sich auf die Leistung auswirken.

Sie können die Auslastung anpassen, indem Sie die folgenden Kriterien angeben, die steuern, wann das System einen Protokolleintrag generiert:

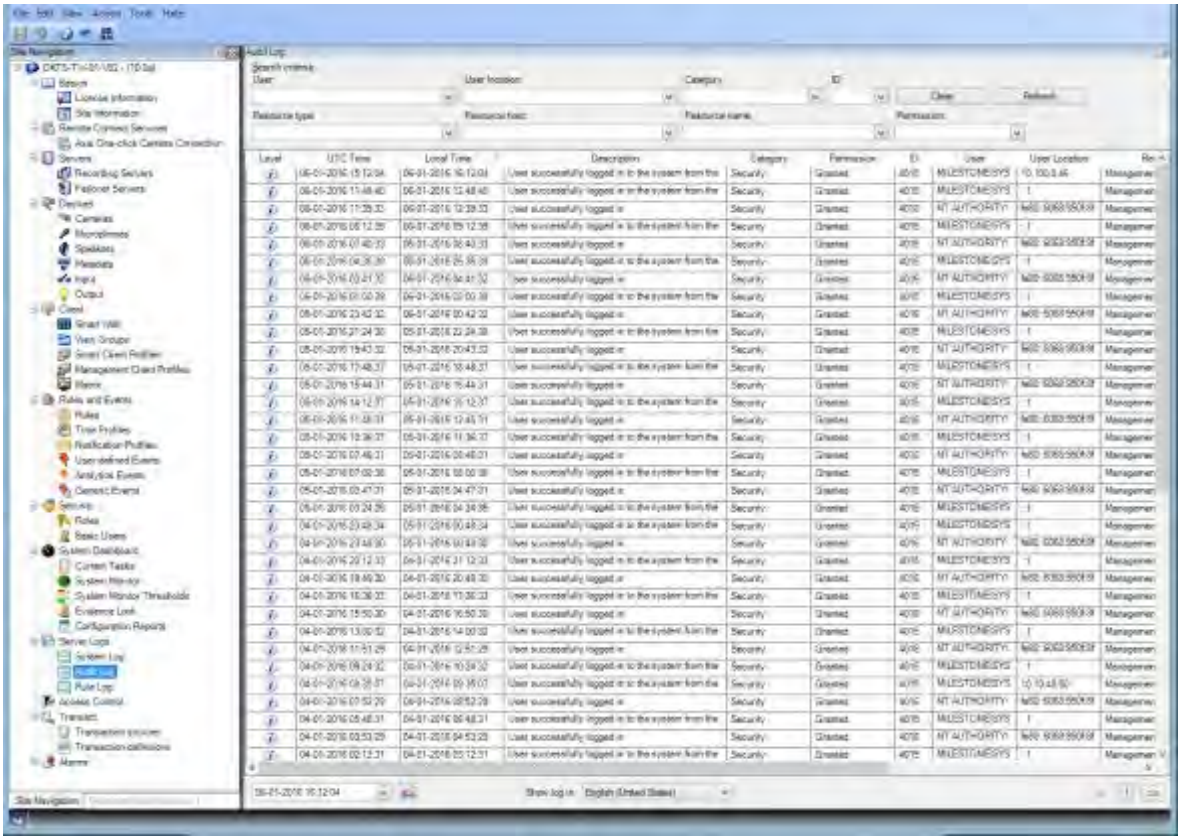
- Die Anzahl der Sekunden, aus denen eine Sequenz besteht. Das VMS generiert einen Protokolleintrag, wenn ein Benutzer ein Video innerhalb der Sequenz wiedergibt.
- Die Anzahl der Frames, die ein Benutzer bei der Wiedergabe von Videos anzeigen muss, bevor das VMS einen Protokolleintrag generiert.

Gehen Sie folgendermaßen vor, um die Protokollierung des erweiterten Benutzerzugriffs zu aktivieren und zu konfigurieren:

1. Klicken Sie im Management-Client auf Extras und wählen Sie Optionen aus.
2. Wählen Sie auf der Registerkarte Serverprotokolle unter Protokolleinstellungen die Option Überwachungsprotokoll aus.
3. Aktivieren Sie unter Einstellungen das Kontrollkästchen Protokollierung des Benutzerzugriffs aktivieren.
4. Optional: Um Einschränkungen für die notierten Informationen festzulegen und die Auswirkungen auf die Leistung zu verringern, treffen Sie eine Auswahl in den Feldern Länge der Protokollierung der Wiedergabesequenz und Vor der Protokollierung gesehene Datensätze.

Gehen Sie folgendermaßen vor, um das Überwachungsprotokoll in MOBOTIX HUB VMS anzuzeigen:

1. Öffnen Sie den Management-Client.
2. Erweitern Sie den Knoten Serverprotokolle.
3. Klicken Sie auf Überwachungsprotokoll.



Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AU-3 Inhalt von Überwachungsdatensätzen
- NIST SP 800-53 RA-5 Schwachstellen-Scan
- NIST SP 800-53 AU-6 Audit-Überprüfung, Analyse und Berichterstattung

4.2 Erweiterte Schritte

4.2.1 Einführung von Standards für sichere Netzwerk- und VMS-Implementierungen

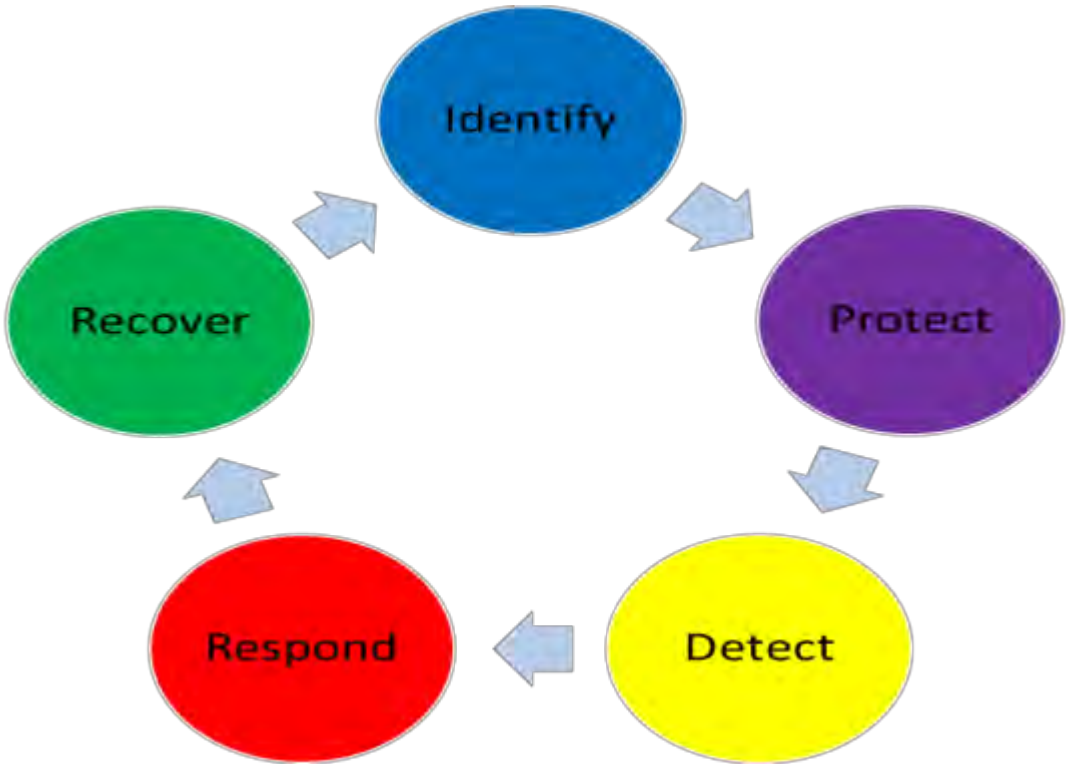
MOBOTIX empfiehlt, Standards für sichere Netzwerke und MOBOTIX HUB-VMS-Implementierungen zu übernehmen. Die Verwendung von Standards ist ein grundlegender Bestandteil der Internet- und Netzwerktechnik

und die Grundlage für Interoperabilität und Systemkonformität. Dies gilt auch für den Einsatz kryptographischer Lösungen, bei denen die auf Standards basierende Kryptographie der am weitesten verbreitete Ansatz ist.

4.2.2 Erstellen eines Incident-Response-Plans

MOBOTIX empfiehlt, mit einer Reihe von Richtlinien und Verfahren zu beginnen und einen Incident-Response-Plan zu erstellen. Beauftragen Sie Mitarbeiter, die den Status des Systems überwachen und auf verdächtige Ereignisse reagieren. Zum Beispiel Aktivitäten, die zu ungewöhnlichen Zeiten stattfinden. Richten Sie mit jedem Ihrer Anbieter, einschließlich MOBOTIX, einen Security Point of Contact (POC) ein.

Das folgende Bild wurde aus dem NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/) übernommen. Es zeigt den Lebenszyklus, der bei der Erstellung eines Plans berücksichtigt werden muss. Das unterstützende Material im Framework enthält Details zum Lebenszyklus und zu den Sicherheitskontrollen für Incident-Response-Pläne.



Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 IR 1-13 Reaktion auf einen Vorfall

4.2.3 Schützen Sie sensible VMS-Komponenten

MOBOTIX empfiehlt, die physische Zugriffskontrolle zu verwenden und das VMS zur Überwachung und zum Schutz der sensiblen VMS-Komponenten zu verwenden. Physische Einschränkungen und rollenbasierte physische Zugriffskontrolle sind Gegenmaßnahmen, die Server und Workstations sicher halten.

Administratoren und Benutzer sollten nur Zugriff auf die Informationen haben, die sie benötigen, um ihre Aufgaben zu erfüllen. Wenn alle internen Benutzer die gleiche Zugriffsebene auf kritische Daten haben, ist es für Angreifer einfacher, auf das Netzwerk zuzugreifen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 PE-1 Richtlinien und Verfahren zum physischen und Umweltschutz
- NIST SP 800-53 PE-2 Physische Zugriffsberechtigungen
- NIST SP 800-53 PE-3 Physische Zugangskontrolle
- NIST SP 800-53 AC-4 mit den geringsten Rechten

4.2.4 Befolgen Sie die Best Practices für die Sicherheit des Microsoft-Betriebssystems

MOBOTIX empfiehlt, dass Sie die bewährten Sicherheitsmethoden für Microsoft-Betriebssysteme befolgen, um Betriebssystemrisiken zu minimieren und die Sicherheit zu gewährleisten. Auf diese Weise können Sie die Sicherheit der Microsoft-Server und Clientcomputer gewährleisten.

Weitere Informationen finden Sie im *Microsoft Security Update Guide* (https://msrc.microsoft.com/update-guide).

4.2.5 Verwenden von Tools zum Automatisieren oder Implementieren der Sicherheitsrichtlinie

MOBOTIX empfiehlt, ein oder mehrere Tools zu finden, die Sie bei der Automatisierung und Implementierung der Sicherheitsrichtlinie unterstützen. Die Automatisierung reduziert das Risiko menschlicher Fehler und erleichtert die Verwaltung der Police. Sie können z. B. die Installation von Sicherheitspatches und Updates auf Servern und Clientcomputern automatisieren.

Eine Möglichkeit, diese Empfehlung zu implementieren, besteht darin, den Microsoft Security Configuration Manager (SCCM) mit dem Security Content Automation Protocol (SCAP) zu kombinieren. (Siehe z. B. *Geek of All Trades: Automatisieren Sie Baseline Security Settings* (https://technet.microsoft.com/en-us/magazine/ff721825.aspx) und *Security Content Automation Protocol (SCAP) Validation Program* (https://csrc.nist.gov/projects/scap-validation-program). Auf diese Weise erhalten Sie ein Framework zum Erstellen, Verteilen und Überprüfen von Sicherheitseinstellungen auf Computern in Ihrem Netzwerk.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 CM-1 Richtlinie und Verfahren für das Konfigurationsmanagement
- NIST SP 800-53 CM-2 Baseline-Konfiguration
- NIST SP 800-53 CM-3 – Kontrolle von Konfigurationsänderungen

4.2.6 Befolgen Sie etablierte Best Practices für die Netzwerksicherheit

MOBOTIX empfiehlt, dass Sie die Best Practices von IT und Anbietern befolgen, um sicherzustellen, dass die Geräte in Ihrem Netzwerk sicher konfiguriert sind. Bitten Sie Ihre Lieferanten, diese Informationen bereitzustellen. Es ist wichtig, einen Sicherheitsdialog zu eröffnen und aufrechtzuerhalten, und eine Diskussion über Best Practices ist ein guter Anfang.

Es ist wichtig, den Zugriff auf das VMS zu verweigern, indem keine anfälligen Netzwerkeinstellungen verwendet werden. Weitere Informationen finden Sie unter *SP 800-128* (https://csrc.nist.gov/publications/detail/sp/800-128/final), *SP 800-41-rev1* (https://csrc.nist.gov/publications/detail/sp/800-41/rev-1/final) (spezifisch für Firewalls) und *ICS-CERT Standards and References* (https://www.cisa.gov/ics) (allgemeine Liste).

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 MA-3 Wartungswerkzeuge

5 Geräte und Netzwerk

Dieser Abschnitt enthält Anleitungen zum Sichern der Geräte und Netzwerkkomponenten im Zusammenhang mit MOBOTIX HUB VMS. Dazu gehören wichtige Teile des Systems wie die Kameras, der Speicher und das Netzwerk. Überwachungssysteme enthalten häufig Kameras am Rand des Netzwerks. Kameras und ihre Netzwerkverbindungen stellen ohne Schutz ein erhebliches Kompromittierungsrisiko dar und ermöglichen Eindringlingen möglicherweise weiteren Zugriff auf das System.

5.1 Grundlegende Schritte – Geräte

5.1.1 Verwenden Sie sichere Passwörter anstelle von Standardpasswörtern

MOBOTIX empfiehlt, die Standardpasswörter auf Geräten, z. B. auf einer Kamera, zu ändern. Verwenden Sie keine Standardkennwörter, da diese häufig im Internet veröffentlicht werden und leicht verfügbar sind.
Verwenden Sie stattdessen sichere Passwörter für Geräte. Sichere Passwörter enthalten acht oder mehr alphanumerische Zeichen, verwenden Groß- und Kleinbuchstaben sowie Sonderzeichen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- Verwaltung des NIST 800-53 IA-4 Authentifikators
- NIST 800-53 IA-8 Authenticator Feedback
- NIST 800-53 SI-11 Fehlerbehandlung

5.1.2 Stoppen Sie ungenutzte Dienste und Protokolle

Um unbefugten Zugriff oder die Offenlegung von Informationen zu vermeiden, empfiehlt MOBOTIX, ungenutzte Dienste und Protokolle auf Geräten zu stoppen. Beispiel: Telnet, SSH, FTP, UPnP, IPv6 und Bonjour.
Es ist auch wichtig, eine starke Authentifizierung für alle Dienste zu verwenden, die auf das VMS, das Netzwerk oder die Geräte zugreifen. Verwenden Sie z. B. SSH-Schlüssel anstelle von Benutzernamen und Kennwörtern, und verwenden Sie Zertifikate von einer Zertifizierungsstelle für HTTPS. Weitere Informationen finden Sie in den Sicherungshandbüchern und anderen Anleitungen des Geräteherstellers.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-17 Fernzugriff (nicht verwendete Protokolle deaktivieren)
- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 CM-7 Geringste Funktionalität
- NIST SP 800-53 IA-2 Identifizierung und Authentifizierung

- NIST SP 800-53 SA-9 Externe Informationsdienste

5.1.3 Erstellen Sie auf jedem Gerät dedizierte Benutzerkonten

Alle Kameras verfügen über ein Standardbenutzerkonto mit einem Benutzernamen und einem Kennwort, die das VMS für den Zugriff auf das Gerät verwendet. MOBOTIX empfiehlt zu Überwachungszwecken, den Standardbenutzernamen und das Standardkennwort zu ändern.

Erstellen Sie ein Benutzerkonto speziell für die Verwendung durch das VMS, und verwenden Sie dieses Benutzerkonto und dieses Kennwort, wenn Sie die Kamera zum VMS hinzufügen. Wenn ein Aufzeichnungsserver eine Verbindung zur Kamera herstellt, verwendet er den Benutzernamen und das Kennwort, die Sie erstellt haben. Wenn die Kamera über ein Protokoll verfügt, zeigt dieses Protokoll an, dass der Aufzeichnungsserver eine Verbindung zur Kamera hergestellt hat.

Mit einem dedizierten Benutzernamen und Kennwort können Sie anhand der Geräteprotokolle feststellen, ob ein Aufnahmeserver oder eine Person auf die Kamera zugegriffen hat. Dies ist relevant, wenn potenzielle Sicherheitsprobleme untersucht werden, die Geräte betreffen.

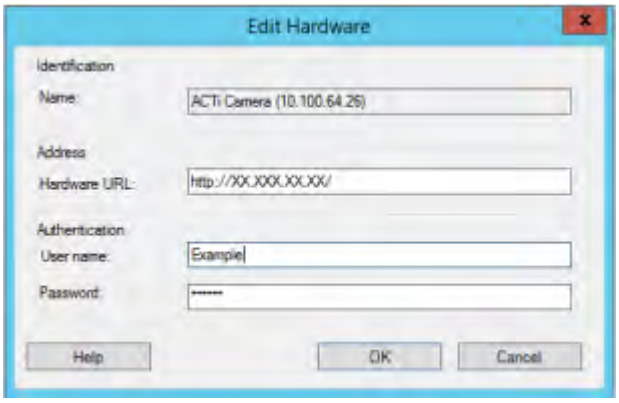
Sie können den Benutzernamen und das Kennwort für ein Gerät ändern, bevor oder nachdem Sie es im Management Client hinzugefügt haben.

Gehen Sie folgendermaßen vor, um den Benutzernamen und das Kennwort zu ändern, bevor Sie das Gerät hinzufügen:

1. Rufen Sie die Weboberfläche des Geräts auf und ändern Sie den Standardbenutzernamen und das Standardkennwort.
2. Fügen Sie im Verwaltungsclient das Gerät hinzu, und geben Sie den Benutzernamen und das Kennwort an.

Gehen Sie folgendermaßen vor, um den Benutzernamen und die Passwörter von Geräten zu ändern, die bereits hinzugefügt wurden:

1. Erweitern Sie im Verwaltungsclient im Bereich Standortnavigation den Knoten Server, und wählen Sie Aufzeichnungsserver aus.
2. Erweitern Sie im Bereich Aufzeichnungsserver den Aufzeichnungsserver, der das Gerät enthält, klicken Sie mit der rechten Maustaste auf das Gerät, und wählen Sie Hardware bearbeiten aus.



3. Geben Sie unter Authentifizierung den neuen Benutzernamen und das Passwort ein.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 AC-4 mit den geringsten Rechten

5.1.4 Nach Geräten suchen

Die Suche nach Geräten (z. B. **Express-Scan oder** Adressbereichsscan **beim Hinzufügen von Hardware) erfolgt mithilfe von Broadcasts, die Benutzernamen und Kennwörter im Klartext enthalten können.**
Sofern es sich nicht um eine Ersteinrichtung handelt, sollte diese Funktion nicht zum Hinzufügen von Geräten zum System verwendet werden. Verwenden Sie stattdessen die **Option Manuell** und wählen Sie den Treiber manuell aus.
Auf sensiblen Systemen sollte die **Funktion zur automatischen Geräteerkennung** auf MOBOTIX HUB Professional VMS (unter **Einstellungen** > **Verbinden von Hardwaregeräten) deaktiviert werden**, da sie in regelmäßigen Abständen Broadcasts sendet, die Benutzernamen und Kennwörter enthalten können.

5.2 Grundlegende Schritte – Netzwerk

5.2.1 Verwenden Sie eine sichere und vertrauenswürdige Netzwerkverbindung

Die Netzwerkkommunikation muss sicher sein, unabhängig davon, ob Sie sich in einem geschlossenen Netzwerk befinden oder nicht. Standardmäßig sollte beim Zugriff auf das VMS eine sichere Kommunikation verwendet werden. Zum Beispiel:

- VPN-Tunnel oder HTTPS standardmäßig
- Neueste Version von Transport Layer Security (https://datatracker.ietf.org/wg/tls/charter/) (TLS, derzeit 1.2) mit gültigen Zertifikaten, die den Best Practices der Branche entsprechen, z. B. von Public-Key Infrastructure (X.509) (https://datatracker.ietf.org/wg/ipsec/documents/) und CA/Browser Forum (https://cabforum.org/).

Andernfalls können Anmeldeinformationen kompromittiert werden, und Eindringlinge könnten sie verwenden, um auf das VMS zuzugreifen.
Konfigurieren Sie das Netzwerk so, dass Clientcomputer sichere HTTPS-Sitzungen oder VPN-Tunnel zwischen den Clientgeräten und den VMS-Servern einrichten können.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SI-2 Fehlerbehebung
- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 SC-23 Session-Authentizität

5.2.2 Verwenden Sie Firewalls, um den IP-Zugriff auf Server und Computer zu beschränken

MOBOTIX empfiehlt die Verwendung sicherer Verbindungen und die folgenden zusätzlichen Schritte:

- Verwenden Sie eine sichere Geräteauthentifizierung

- TLS verwenden
- Verwenden Sie Geräte-Whitelisting, um Geräte zu authentifizieren
- Verwenden Sie Firewalls, um die Netzwerkkommunikation zwischen Servern und Clientcomputern und -programmen einzuschränken.

Alle MOBOTIX HUB Komponenten und die dafür benötigten Ports sind in den einzelnen Abschnitten unten aufgeführt. Um beispielsweise sicherzustellen, dass die Firewall nur unerwünschten Datenverkehr blockiert, müssen Sie die Ports angeben, die von den MOBOTIX HUB-VMS verwendet werden. Sie sollten nur diese Ports aktivieren. Die Listen enthalten auch die Ports, die für lokale Prozesse verwendet werden.
Sie sind in zwei Gruppen unterteilt:

- Serverkomponenten (Dienste): Bieten ihren Dienst auf bestimmten Ports an, weshalb sie auf Clientanforderungen an diesen Ports lauschen müssen. Daher müssen diese Ports in der Windows-Firewall für eingehende Verbindungen geöffnet werden.
- Client-Komponenten (Clients): Initiieren Sie Verbindungen zu bestimmten Ports auf Serverkomponenten. Daher müssen diese Ports für ausgehende Verbindungen geöffnet werden. Ausgehende Verbindungen sind in der Regel standardmäßig in der Windows-Firewall geöffnet.

Wenn nichts anderes angegeben ist, müssen Ports für Serverkomponenten für eingehende Verbindungen und Ports für Clientkomponenten für ausgehende Verbindungen geöffnet werden.
Beachten Sie, dass Serverkomponenten auch als Clients für andere Serverkomponenten fungieren können.
Bei den Portnummern handelt es sich um die Standardnummern, die jedoch geändert werden können. Wenden Sie sich an den MOBOTIX-Support, wenn Sie Ports ändern müssen, die nicht über den Management Client konfigurierbar sind.

Serverkomponenten (eingehende Verbindungen)

In jedem der folgenden Abschnitte werden die Ports aufgelistet, die für einen bestimmten Dienst geöffnet werden müssen. Um herauszufinden, welche Ports auf einem bestimmten Computer geöffnet werden müssen, müssen Sie alle Dienste berücksichtigen, die auf diesem Computer ausgeführt werden.

Beschränken Sie den Remote-Zugriff auf den Management-Server, indem Sie Firewall-Regeln hinzufügen, die nur Aufzeichnungsservern erlauben, eine Verbindung mit dem TCP-Port 9993 herzustellen.

Management Server-Dienst und zugehörige Prozesse

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
80	HTTP (Englisch)	IIS (IIS)	Alle Server sowie der MOBOTIX HUB Smart Client und der Management Client	Der Zweck von Port 80 und Port 443 ist derselbe. Welchen Port das VMS verwendet, hängt jedoch davon ab, ob Sie Zertifikate zum Sichern der Kommunikation verwendet haben. • Wenn Sie die Kommunikation nicht mit Zertifikaten gesichert haben, verwendet das VMS Port 80. • Wenn Sie die Kommunikation mit Zertifikaten gesichert haben , verwendet der virtuelle Computer Port 443, mit Ausnahme der Kommunikation vom Ereignisserver zum Verwaltungsserver. Für die Kommunikation vom Ereignisserver zum Verwaltungsserver werden Windows Secured Framework (WCF) und die Windows-Authentifizierung an Port 80 verwendet.
443	HTTPS	IIS (IIS)		
6473	TCP	Management-Server-Dienst	Taskleistensymbol für den Management-Server-Manager, nur lokale Verbindung.	Anzeigen des Status und Verwalten des Dienstes.
8080	TCP	Verwaltungsserver	Nur lokale Verbindung.	Kommunikation zwischen internen Prozessen auf dem Server.
9000	HTTP (Englisch)	Verwaltungsserver	Dienste des Aufzeichnungsservers	Webservice für die interne Kommunikation zwischen Servern.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
12345	TCP	Management-Server-Dienst	MOBOTIX HUB Smart Client	Kommunikation zwischen dem System und den Matrixempfängern. Sie können die Portnummer im Management Client ändern.
12974	TCP	Management-Server-Dienst	Windows-SNMP-Dienst	Kommunikation mit dem SNMP-Erweiterungsagenten. Verwenden Sie den Port nicht für andere Zwecke, auch wenn Ihr System SNMP nicht anwendet. In MOBOTIX HUB 2014-Systemen oder älter lautete die Portnummer 6475. In MOBOTIX HUB 2019 R2-Systemen und älter lautete die Portnummer 7475.

SQL Server-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
1433	TCP	SQL Server	Management-Server-Dienst	Speichern und Abrufen von Konfigurationen.
1433	TCP	SQL Server	Ereignisserver-Dienst	Speichern und Abrufen von Ereignissen.
1433	TCP	SQL Server	Protokollserver-Dienst	Speichern und Abrufen von Protokolleinträgen.

Datensammler-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
7609	HTTP (Englisch)	IIS (IIS)	Auf dem Verwaltungsserver-Computer: Datensammlungsdienste auf allen anderen Servern. Auf anderen Computern: Datensammlerdienst auf dem Verwaltungsserver.	Systemmonitor.

Ereignisserver-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
1234	TCP/UDP	Ereignisserver-Dienst	Jeder Server, der generische Ereignisse an Ihr MOBOTIX HUB-System sendet.	Lauschen auf generische Ereignisse von externen Systemen oder Geräten.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
				Nur wenn die entsprechende Datenquelle aktiviert ist.
1235	TCP	Ereignisserver-Dienst	Jeder Server, der generische Ereignisse an Ihr MOBOTIX HUB-System sendet.	Lauschen auf generische Ereignisse von externen Systemen oder Geräten. Nur wenn die entsprechende Datenquelle aktiviert ist.
9090	TCP	Ereignisserver-Dienst	Jedes System oder Gerät, das Analyseereignisse an Ihr MOBOTIX HUB-System sendet.	Überwachen von Analyseereignissen von externen Systemen oder Geräten. Nur relevant, wenn die Funktion "Analytics-Ereignisse" aktiviert ist.
22331	TCP	Ereignisserver-Dienst	MOBOTIX HUB Smart Client und der Management Client	Konfiguration, Ereignisse, Alarme und Kartendaten.
22333	TCP	Ereignisserver-Dienst	MIP-Plug-ins und -Anwendungen.	MIP-Nachrichten.

Dienst für den Aufzeichnungsserver

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
25	SMTP	Aufzeichnungsserver-Dienst	Kameras, Encoder und I/O-Geräte.	Lauschen auf Ereignismeldungen von Geräten. Der Port ist standardmäßig deaktiviert. (Veraltet) Wenn Sie diese Option aktivieren, wird ein Port für unverschlüsselte Verbindungen geöffnet, was nicht empfohlen wird.
5210	TCP	Aufzeichnungsserver-Dienst	Failover-Aufzeichnungsserver.	Zusammenführen von Datenbanken nach der Ausführung eines Failover-Aufzeichnungsservers.
5432	TCP	Aufzeichnungsserver-Dienst	Kameras, Encoder und I/O-Geräte.	Lauschen auf Ereignismeldungen von Geräten. Der Port ist standardmäßig deaktiviert.
7563	TCP	Aufzeichnungsserver-Dienst	MOBOTIX HUB Smart Client, Management Client	Abrufen von Video- und Audiostreams, PTZ-Befehlen.
8966	TCP	Aufzeichnungsserver-Dienst	Taskleistensymbol des Aufzeichnungsserver-Managers, nur lokale Verbindung.	Anzeigen des Status und Verwalten des Dienstes.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
9001	HTTP (Englisch)	Aufzeichnungsserver-Dienst	Verwaltungsserver	Webservice für die interne Kommunikation zwischen Servern. Wenn mehrere Recording Server-Instanzen verwendet werden, benötigt jede Instanz einen eigenen Port. Weitere Ports sind 9002, 9003 usw.
11000	TCP	Aufzeichnungsserver-Dienst	Failover-Aufzeichnungsserver	Abrufen des Status von Aufzeichnungsservern.
12975	TCP	Aufzeichnungsserver-Dienst	Windows-SNMP-Dienst	Kommunikation mit dem SNMP-Erweiterungsagenten. Verwenden Sie den Port nicht für andere Zwecke, auch wenn Ihr System SNMP nicht anwendet. In MOBOTIX HUB 2014-Systemen oder älter lautete die Portnummer 6474. In MOBOTIX HUB 2019 R2-Systemen und älter lautete die Portnummer 7474.
65101	UDP	Dienst für den Aufzeichnungsserver	Nur lokale Verbindung	Lauschen auf Ereignisbenachrichtigungen von den Treibern.

Zusätzlich zu den oben aufgeführten eingehenden Verbindungen zum Recording Server-Dienst stellt der Recording Server-Dienst ausgehende Verbindungen zu Kameras, NVRs und Remote-Interconnected-Standorten (MOBOTIX Interconnect ICP) her.

Failover-Server-Dienst und Failover-Aufzeichnungsserver-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
25	SMTP	Failover-Aufzeichnungsserver-Dienst	Kameras, Encoder und I/O-Geräte.	Lauschen auf Ereignismeldungen von Geräten. Der Port ist standardmäßig deaktiviert. (Veraltet) Wenn Sie diese Option aktivieren, wird ein Port für unverschlüsselte Verbindungen geöffnet, was nicht empfohlen wird.

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
5210	TCP	Failover-Aufzeichnungsserver-Dienst	Failover-Aufzeichnungsserver	Zusammenführen von Datenbanken nach der Ausführung eines Failover-Aufzeichnungsservers.
5432	TCP	Failover-Aufzeichnungsserver-Dienst	Kameras, Encoder und I/O-Geräte.	Lauschen auf Ereignismeldungen von Geräten. Der Port ist standardmäßig deaktiviert.
7474	TCP	Failover-Aufzeichnungsserver-Dienst	Windows-SNMP-Dienst	Kommunikation mit dem SNMP-Erweiterungsagenten. Verwenden Sie den Port nicht für andere Zwecke, auch wenn Ihr System SNMP nicht anwendet.
7563	TCP	Failover-Aufzeichnungsserver-Dienst	MOBOTIX HUB Smart Client	Abrufen von Video- und Audiostreams, PTZ-Befehlen.
8844	UDP	Failover-Aufzeichnungsserver-Dienst	Nur lokale Verbindung.	Kommunikation zwischen den Servern.
8966	TCP	Failover-Aufzeichnungsserver-Dienst	Failover Recording Server Manager Taskleistensymbol, nur lokale Verbindung.	Anzeigen des Status und Verwalten des Dienstes.
8967	TCP	Failover-Server-Dienst	Taskleistensymbol des Failover-Server-Managers, nur lokale Verbindung.	Anzeigen des Status und Verwalten des Dienstes.
8990	TCP	Failover-Server-Dienst	Management-Server-Dienst	Überwachen des Status des Failoverserverdiensts.
9001	HTTP (Englisch)	Failover-Server-Dienst	Verwaltungsserver	Webservice für die interne Kommunikation zwischen Servern.

Zusätzlich zu den oben aufgeführten eingehenden Verbindungen mit dem Failover-Server-/Failover-Aufzeichnungsserver-Dienst stellt der Failover-Server-/Failover-Aufzeichnungsserver-Dienst ausgehende Verbindungen zu den regulären Rekordern, Kameras und für Video Push her.

Protokollserver-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
22337	HTTP (Englisch)	Protokollserver-Dienst	Alle MOBOTIX HUB-Komponenten mit Ausnahme des Management Clients und des Aufzeichnungsservers.	Schreiben Sie auf den Protokollserver, lesen Sie ihn und konfigurieren Sie ihn.

Mobiler Server-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
8000	TCP	Mobiler Server-Dienst	Symbol in der Taskleiste von Mobile Server Manager, nur lokale Verbindung.	SysTray-Anwendung.
8081	HTTP (Englisch)	Mobiler Server-Dienst	Mobile Clients, Web-Clients und Management-Client.	Senden von Datenströmen; Video und Audio.
8082	HTTPS	Mobiler Server-Dienst	Mobile Clients und Web-Clients.	Senden von Datenströmen; Video und Audio.
40001 - 40099	HTTP (Englisch)	Mobiler Server-Dienst	Dienst für den Aufzeichnungsserver	Video-Push für mobile Server. Dieser Portbereich ist standardmäßig deaktiviert.

LPR-Serverdienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
22334	TCP	LPR-Serverdienst	Ereignisserver	Abrufen erkannter Nummernschilder und Serverstatus. Damit eine Verbindung hergestellt werden kann, muss auf dem Ereignisserver das LPR-Plug-In installiert sein.
22334	TCP	LPR-Serverdienst	LPR Server Manager Taskleistensymbol, nur lokale Verbindung.	SysTray-Anwendung

MOBOTIX Open Network Bridge-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
580	TCP	MOBOTIX Open Network Bridge Dienst	ONVIF-Kunden	Authentifizierung und Anforderungen für die Konfiguration von Videostreams.
554	RTSP	RTSP-Dienst	ONVIF-Kunden	Streaming des angeforderten Videos an ONVIF-Clients.

MOBOTIX HUB DLNA Server-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
9100	HTTP (Englisch)	DLNA-Serverdienst	DLNA-Gerät	Geräteerkennung und Bereitstellung der Konfiguration von DLNA-Kanälen. Anfragen für Videostreams.
9200	HTTP (Englisch)	DLNA-Serverdienst	DLNA-Gerät	Streaming des angeforderten Videos auf DLNA-Geräte.

MOBOTIX HUB Bildschirmrekorder-Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
52111	TCP	MOBOTIX HUB Bildschirmrekorder	Aufzeichnungsserver-Dienst	Bietet Video von einem Monitor. Sie erscheint und verhält sich wie eine Kamera auf dem Aufzeichnungsserver. Sie können die Portnummer im Management Client ändern.

XProtect Incident Manager Dienst

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
80	HTTP (Englisch)	IIS (IIS)	XProtect Smart Client und der Management Client	Der Zweck von Port 80 und Port 443 ist derselbe. Welchen Port das VMS verwendet, hängt jedoch davon ab, ob Sie Zertifikate zum Sichern der Kommunikation verwendet haben. • Wenn Sie die Kommunikation nicht mit Zertifikaten gesichert haben, verwendet das VMS Port 80.
443	HTTPS			

Portnummer	Protokoll	Prozess	Verbindungen von...	Zweck
				• Wenn Sie die Kommunikation mit Zertifikaten gesichert haben, verwendet das VMS den Port 443

Serverkomponenten (ausgehende Verbindungen)

Management-Server-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
443	HTTPS	Der Lizenzserver, auf dem der Lizenzverwaltungsdienst gehostet wird.	Aktivieren von Lizenzen.

Dienst für den Aufzeichnungsserver

Portnummer	Protokoll	Verbindungen zu...	Zweck
80	HTTP (Englisch)	Kameras, NVRs, Encoder Miteinander verbundene Standorte	Authentifizierung, Konfiguration, Datenströme, Video und Audio. Einloggen
443	HTTPS	Kameras, NVRs, Encoder	Authentifizierung, Konfiguration, Datenströme, Video und Audio.
554	RTSP	Kameras, NVRs, Encoder	Datenströme, Video und Audio.
7563	TCP	Miteinander verbundene Standorte	Datenströme und Ereignisse.
11000	TCP	Failover-Aufzeichnungsserver	Abrufen des Status von Aufzeichnungsservern.
40001 – 40099	HTTP (Englisch)	Mobiler Server-Dienst	Video-Push für mobile Server. Dieser Portbereich ist standardmäßig deaktiviert.

Failover-Server-Dienst und Failover-Aufzeichnungsserver-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
11000	TCP	Failover-Aufzeichnungsserver	Abrufen des Status von Aufzeichnungsservern.

Protokollserver-Dienst

Portnummer	Protokoll	Verbindungen zu...	Zweck
443	HTTPS	Log-Server	Weiterleiten von Nachrichten an den Protokollserver.

API-Schnittstelle

Portnummer	Protokoll	Verbindungen zu...	Zweck
80	HTTP (Englisch)	Verwaltungsserver	RESTful API

Portnummer	Protokoll	Verbindungen zu...	Zweck
443	HTTPS	Verwaltungsserver	RESTful API

Kameras, Encoder und I/O-Geräte (eingehende Verbindungen)

Portnummer	Protokoll	Verbindungen von...	Zweck
80	TCP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Authentifizierung, Konfiguration und Datenströme; Video und Audio.
443	HTTPS	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Authentifizierung, Konfiguration und Datenströme; Video und Audio.
554	RTSP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Datenströme; Video und Audio.

Kameras, Encoder und I/O-Geräte (ausgehende Verbindungen)

Portnummer	Protokoll	Verbindungen zu...	Zweck
25	SMTP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Senden von Ereignisbenachrichtigungen (veraltet).
5432	TCP	Aufzeichnungsserver und Failover-Aufzeichnungsserver	Senden von Ereignisbenachrichtigungen. Der Port ist standardmäßig deaktiviert.
22337	HTTP (Englisch)	Log-Server	Weiterleiten von Nachrichten an den Protokollserver.

Nur wenige Kameramodelle sind in der Lage, ausgehende Verbindungen aufzubauen.

Clientkomponenten (ausgehende Verbindungen)

MOBOTIX HUB Smart Client, MOBOTIX HUB Management Client, MOBOTIX HUB Mobile Server

Portnummer	Protokoll	Verbindungen zu...	Zweck
80	HTTP (Englisch)	Management-Server-Dienst	Authentifizierung
443	HTTPS	Management-Server-Dienst	Authentifizierung von Basisbenutzern.
7563	TCP	Dienst für den Aufzeichnungsserver	Abrufen von Video- und Audiostreams, PTZ-Befehlen.
22331	TCP	Ereignisserver-Dienst	Alarme.

MOBOTIX HUB Web Client, MOBOTIX HUB Mobile Client

Portnummer	Protokoll	Verbindungen zu...	Zweck
8081	HTTP (Englisch)	MOBOTIX HUB Mobiler Server	Abrufen von Video- und Audiostreams.
8082	HTTPS	MOBOTIX HUB Mobiler Server	Abrufen von Video- und Audiostreams.

Weitere Informationen

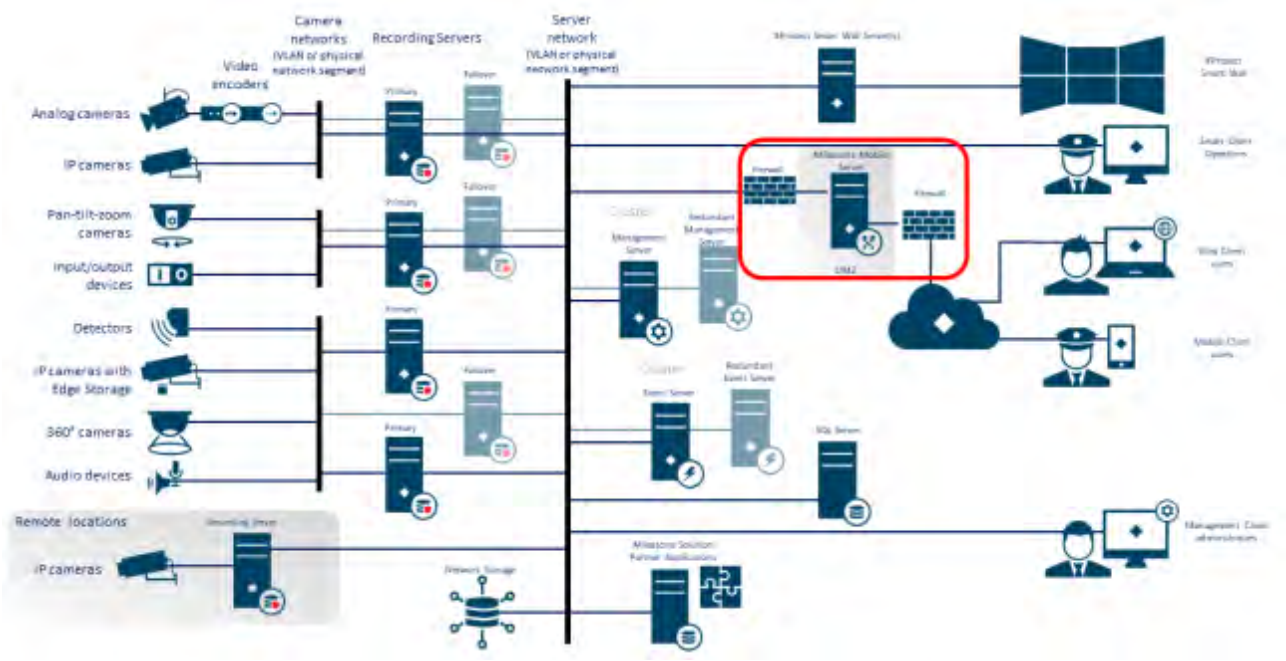
Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 CA-3 Systemverbindungen
- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 SC-7 Grenzschutz

5.2.3 Verwenden einer Firewall zwischen dem VMS und dem Internet

Das VMS sollte keine direkte Verbindung zum Internet herstellen. Wenn Sie Teile des VMS dem Internet zur Verfügung stellen, empfiehlt MOBOTIX, eine entsprechend konfigurierte Firewall zwischen dem VMS und dem Internet zu verwenden.

Wenn möglich, machen Sie nur die MOBOTIX Mobile-Serverkomponente für das Internet verfügbar und platzieren Sie sie in einer Demilitarisierungszone (DMZ) mit Firewalls auf beiden Seiten. Dies ist in der folgenden Abbildung dargestellt.



Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 CA-3 Systemverbindungen

5.2.4 Verbinden Sie das Kamera-Subnetz nur mit dem Subnetz des Aufzeichnungsservers

MOBOTIX empfiehlt, das Kamera-Subnetz nur mit dem Subnetz des Aufzeichnungsservers zu verbinden. Die Kameras und andere Geräte dürfen nur mit den Aufzeichnungsservern kommunizieren. Weitere Informationen finden Sie unter Aufzeichnungsserver auf der Seite 62.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 SC-7 Grenzschutz

5.3 Erweiterte Schritte – Geräte

5.3.1 Verwenden des Simple Network Management Protocol zum Überwachen von Ereignissen

MOBOTIX empfiehlt, die Verwendung von SNMP (Simple Network Management Protocol) zur Überwachung von Ereignissen auf den Geräten im Netzwerk zu verwenden. Sie können SNMP als Ergänzung für Syslog verwenden. SNMP funktioniert in Echtzeit mit vielen Arten von Ereignissen, die Warnungen auslösen können, z. B. wenn ein Gerät neu gestartet wird.

Damit dies funktioniert, müssen die Geräte die Protokollierung über SNMP unterstützen.

Es stehen mehrere Versionen von SNMP-Protokollen zur Verfügung. Die Versionen 2c und 3 sind die aktuellsten. Die Umsetzung umfasst eine Reihe von Standards. Eine gute Übersicht findet sich auf der SNMP-Referenzseite (http://www.snmp.com/protocol/snmp_rfcs.shtml).

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SI-4 Ereignisüberwachung

5.4 Erweiterte Schritte – Netzwerk

5.4.1 Verwenden Sie sichere drahtlose Protokolle

Wenn Sie drahtlose Netzwerke verwenden, empfiehlt MOBOTIX die Verwendung eines sicheren drahtlosen Protokolls, um unbefugten Zugriff auf Geräte und Computer zu verhindern. Verwenden Sie beispielsweise standardisierte Konfigurationen. Der NIST-Leitfaden zu drahtlosen lokalen Netzwerken enthält spezifische Details zur Netzwerkverwaltung und -konfiguration. Weitere Informationen finden Sie unter *SP 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks* (https://csrc.nist.gov/publications/detail/sp/800-48/rev-1/archive/2008-07-25).
Darüber hinaus empfiehlt MOBOTIX, drahtlose Kameras nicht an unternehmenskritischen Orten zu verwenden. Drahtlose Kameras sind leicht zu stören, was zum Verlust von Videos führen kann.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-18 Drahtloser Zugang
- NIST SP 800-53 SC-40 Schutz für drahtlose Verbindungen

5.4.2 Verwenden der portbasierten Zugriffskontrolle

Verwenden Sie die portbasierte Zugriffskontrolle, um unbefugten Zugriff auf das Kameranetzwerk zu verhindern. Wenn ein nicht autorisiertes Gerät eine Verbindung zu einem Switch- oder Router-Port herstellt, sollte der Port blockiert werden. Informationen zur Konfiguration von Switches und Routern erhalten Sie von den Herstellern. Weitere Informationen zum *Konfigurationsmanagement von Informationssystemen finden Sie in* SP 800-128, Guide for Security-Focused Configuration Management of Information Systems (https://csrc.nist.gov/publications/detail/sp/800-128/final).

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 CM-1 Richtlinie und Verfahren für das Konfigurationsmanagement
- NIST 800-53 CM-2 Baseline-Konfiguration
- NIST 800-53 AC-4 mit den geringsten Rechten
- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

5.4.3 Ausführen des VMS in einem dedizierten Netzwerk

MOBOTIX empfiehlt, dass Sie nach Möglichkeit das Netzwerk, in dem das VMS ausgeführt wird, von Netzwerken mit anderen Zwecken trennen. Beispielsweise sollte ein freigegebenes Netzwerk, wie z. B. das Druckernetzwerk, vom VMS-Netzwerk isoliert werden. Darüber hinaus sollten MOBOTIX HUB-VMS-Bereitstellungen eine Reihe allgemeiner Best Practices für Systemverbindungen befolgen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 CA-3 Systemverbindungen

6 MOBOTIX Server

6.1 Grundlegende Schritte – MOBOTIX Server

6.1.1 Verwenden Sie physische Zugangskontrollen und überwachen Sie den Serverraum

MOBOTIX empfiehlt, die Hardware mit den Servern in einem dafür vorgesehenen Serverraum zu platzieren und physische Zugangskontrollen zu verwenden. Darüber hinaus sollten Sie Zugriffsprotokolle führen, um zu dokumentieren, wer physischen Zugriff auf die Server hatte. Die Überwachung des Serverraums ist ebenfalls eine vorbeugende Vorsichtsmaßnahme.
MOBOTIX unterstützt die Integration von Zutrittskontrollsystemen und deren Informationen. So können Sie z.B. Zugriffsprotokolle im MOBOTIX HUB Smart Client einsehen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 PE-3 Physische Zugangskontrolle

6.1.2 Verschlüsselte Kommunikationskanäle nutzen

MOBOTIX empfiehlt die Verwendung eines VPN für Kommunikationskanäle für Installationen, bei denen Server über nicht vertrauenswürdige Netzwerke verteilt sind. Damit soll verhindert werden, dass Angreifer die Kommunikation zwischen den Servern abfangen. Auch für vertrauenswürdige Netzwerke empfiehlt MOBOTIX, HTTPS für die Konfiguration von Kameras und anderen Systemkomponenten zu verwenden.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-4 Durchsetzung des Informationsflusses
- NIST 800-53 AC-17 Fernzugriff

6.2 Erweiterte Schritte – MOBOTIX Server

6.2.1 Ausführen von Diensten mit Dienstkonten

MOBOTIX empfiehlt, dass Sie Dienstkonten für Dienste erstellen, die sich auf MOBOTIX HUB VMS beziehen, anstatt ein reguläres Benutzerkonto zu verwenden. Richten Sie die Dienstkonten als Domänenbenutzer ein, und erteilen Sie ihnen nur die Berechtigungen, die zum Ausführen der relevanten Dienste erforderlich sind. Siehe 4.1.11 Kerberos-Authentifizierung (erklärt). Das Dienstkonto sollte z. B. nicht in der Lage sein, sich am Windows-Desktop anzumelden.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-5 Aufgabentrennung
- NIST 800-53 AC-6 mit den geringsten Rechten

6.2.2 Ausführen von Komponenten auf dedizierten virtuellen oder physischen Servern

MOBOTIX empfiehlt, die Komponenten von MOBOTIX HUB VMS nur auf dedizierten virtuellen oder physischen Servern auszuführen, auf denen keine andere Software oder Dienste installiert sind.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 CM-9 Konfigurationsmanagementplan

6.2.3 Einschränken der Verwendung von Wechselmedien auf Computern und Servern

MOBOTIX empfiehlt, die Verwendung von Wechseldatenträgern, z. B. USB-Sticks, SD-Karten und Smartphones, auf Computern und Servern einzuschränken, auf denen Komponenten von MOBOTIX HUB VMS installiert sind. Dies hilft, das Eindringen von Malware in das Netzwerk zu verhindern. Erlauben Sie z. B. nur autorisierten Benutzern, Wechselmedien anzuschließen, wenn Sie Videobeweis übertragen müssen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 MP-7 Mediennutzung

6.2.4 Verwenden Sie einzelne Administratorkonten für eine bessere Überwachung

Im Gegensatz zu gemeinsam genutzten Administratorkonten empfiehlt MOBOTIX für Administratoren die Verwendung einzelner Konten. Auf diese Weise können Sie nachverfolgen, wer was in MOBOTIX HUB VMS tut. Dies hilft, das Eindringen von Malware in das Netzwerk zu verhindern. Sie können dann ein autorisierendes Verzeichnis wie Active Directory verwenden, um die Administratorkonten zu verwalten.
Administratorkonten weisen Sie Rollen im Management Client unter **Rollen** zu.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-5 Aufgabentrennung
- NIST 800-53 CM-9 Konfigurationsmanagementplan

6.2.5 Verwenden von Subnetzen oder VLANs zum Einschränken des Serverzugriffs

MOBOTIX empfiehlt, verschiedene Arten von Hosts und Benutzern logisch in separaten Subnetzen zu gruppieren. Dies kann Vorteile bei der Verwaltung von Berechtigungen für diese Hosts und Benutzer als Mitglieder einer Gruppe

mit einer bestimmten Funktion oder Rolle haben. Entwerfen Sie das Netzwerk so, dass für jede Funktion ein Subnetz oder VLAN vorhanden ist. Zum Beispiel ein Subnetz oder VLAN für Überwachungsoperatoren und eines für Administratoren. Auf diese Weise können Sie Firewall-Regeln nach Gruppe statt nach einzelnen Hosts definieren.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 CSC 11: Sichere Konfigurationen für Netzwerkgeräte wie Firewalls, Router und Switches
- NIST SP 800-53 SC-7 Grenzschutz

6.2.6 Aktivieren Sie nur die Ports, die vom Ereignisserver verwendet werden

MOBOTIX empfiehlt, nur die vom Ereignisserver verwendeten Ports zu aktivieren und alle anderen Ports, einschließlich der Windows-Standardports, zu blockieren.
Die in MOBOTIX HUB-VMS verwendeten Ereignisserver-Ports sind: 22331, 22333, 9090, 1234 und 1235.

Welche Ports verwendet werden, hängt von der Bereitstellung ab. Wenden Sie sich im Zweifelsfall an den MOBOTIX Support.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 CSC 11: Sichere Konfigurationen für Netzwerkgeräte wie Firewalls, Router und Switches

6.3 SQL Server

6.3.1 Anbindung an den SQL Server und die Datenbank

Es kann eine beliebige SQL-Verbindungszeichenfolge angegeben werden, einschließlich einer Zeichenfolge, bei der die SQL-Authentifizierung verwendet wird (Benutzername/Kennwort). Dies kann während des Testens nützlich sein, da kein Zugriff auf ein AD erforderlich ist. Es wird jedoch nicht empfohlen, die Authentifizierung mit Benutzername/Kennwort für Produktions-Setups zu verwenden, da sowohl der Benutzername als auch das Kennwort unverschlüsselt auf dem Computer gespeichert werden. Für Produktionsumgebungen empfehlen wir die Verwendung von integrierter Sicherheit.

Die Kommunikation zwischen den MOBOTIX MOBOTIX HUB-VMS und dem SQL Server und der Datenbank kann möglicherweise von einem Angreifer manipuliert werden, da das Zertifikat nicht überprüft wird.
Um dies zu beheben, müssen Sie zunächst überprüfbare Serverzertifikate einrichten. Nachdem die Zertifikate eingerichtet wurden, müssen Sie den ConnestionString in der Windows-Registrierung ändern, indem Sie trustServerCertificate=true wie folgt entfernen:
Registrierungsschlüssel:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\Common\ConnectionString

- Strömung
  Verbindungszeichenfolge: Datenquelle=localhost; initial catalog='Überwachung'; Integrierte Sicherheit = SSPI; encrypt=wahr; trustServerCertificate=wahr
- Gehärtet
  Verbindungszeichenfolge: Datenquelle=localhost; initial catalog='Überwachung'; Integrierte Sicherheit = SSPI; verschlüsseln=wahr

Dies führt dazu, dass die Verschlüsselung nur dann erfolgt, wenn ein überprüfbares Serverzertifikat vorhanden ist, andernfalls schlägt der Verbindungsversuch fehl.
Dieses Problem wird im Artikel Verwenden der Verschlüsselung ohne Überprüfung ausführlich beschrieben.

6.3.2 Ausführen von SQL Server und Datenbank auf einem separaten Server

MOBOTIX empfiehlt, den SQL Server und die Datenbank überflüssig zu machen. Dies reduziert das Risiko tatsächlicher oder vermeintlicher Ausfallzeiten.
Zur Unterstützung von Windows Server Failover Clustering (WSFC) empfiehlt MOBOTIX, dass Sie den SQL Server und die Datenbank auf einem separaten Server und nicht auf dem Verwaltungsserver ausführen.
SQL Server muss im WSFC-Setup ausgeführt werden, und die Verwaltungs- und Ereignisserver müssen in einem Microsoft-Clustersetup (oder einer ähnlichen Technologie) ausgeführt werden. Weitere Informationen zum WSFC finden Sie unter *Windows Server-Failoverclustering (WSFC) mit SQL Server* (https://msdn.microsoft.com/en-us/library/hh270278.aspx).

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 SC-7 Grenzschutz
- NIST 800-53 CM-9 Konfigurationsmanagementplan

6.4 Verwaltungsserver

6.4.1 Anpassen des Token-Timeouts

MOBOTIX HUB VMS verwendet Sitzungstoken, wenn es sich über die Protokolle SSL (Basisbenutzer) oder NTLM (Windows-Benutzer) beim Management-Server anmeldet. Ein Token wird vom Management-Server abgerufen und auf den sekundären Servern verwendet, z. B. auf dem Aufzeichnungsserver und manchmal auch auf dem Ereignisserver. Dadurch soll vermieden werden, dass die NTLM- und AD-Suche für jede Serverkomponente ausgeführt wird.
Standardmäßig ist ein Token 240 Minuten lang gültig. Sie können dies bis zu 1-Minuten-Intervallen anpassen. Dieser Wert kann auch im Laufe der Zeit angepasst werden. Kurze Intervalle erhöhen die Sicherheit, jedoch generiert das System zusätzliche Kommunikation, wenn es den Token erneuert.
Das beste Intervall hängt von der Bereitstellung ab. Diese Kommunikation erhöht die Systemlast und kann sich auf die Leistung auswirken.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- Verwaltung des NIST SP 800-53 IA-5 Authentifikators

6.4.2 Aktivieren Sie nur die Ports, die vom Management-Server verwendet werden

MOBOTIX empfiehlt, nur die Ports zu aktivieren, die vom Management-Server verwendet werden, und alle anderen Ports, einschließlich der Standard-Windows-Ports, zu blockieren. Diese Anleitung gilt für die Serverkomponenten von MOBOTIX HUB-VMS.
Die in MOBOTIX HUB-VMS verwendeten Management-Server-Ports sind: 80, 443, 1433, 7475, 8080, 8990, 9993, 12345.

Welche Ports verwendet werden, hängt von der Bereitstellung ab. Wenden Sie sich im Zweifelsfall an den MOBOTIX Support.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 SC-7 Grenzschutz

6.4.3 Deaktivieren Sie unsichere Protokolle

Wenn sich ein einfacher Benutzer über IIS beim Verwaltungsserver anmeldet, verwendet der Verwaltungsclient ein beliebiges verfügbares Protokoll. MOBOTIX empfiehlt, immer die neueste Version von Transport Layer Security (TLS, derzeit 1.2) (https://datatracker.ietf.org/wg/tls/charter/) zu implementieren und alle ungeeigneten Cipher Suites und veralteten Versionen von SSL/TLS-Protokollen zu deaktivieren. Ausführen von Aktionen zum Blockieren unsicherer Protokolle auf Betriebssystemebene. Dadurch wird verhindert, dass der Management-Client Protokolle verwendet, die nicht sicher sind. Das Betriebssystem bestimmt das zu verwendende Protokoll.

Welche Protokolle verwendet werden, hängt von der Bereitstellung ab. Wenden Sie sich im Zweifelsfall an den MOBOTIX Support.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-17 Fernzugriff (nicht verwendete Protokolle deaktivieren)
- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

6.4.4 Deaktivieren des Legacy-Remotingkanals

Die Kommunikation zwischen den Aufzeichnungsservern und dem Management-Server ist mit der im Jahr 2019 R2 implementierten Lösung sicherer geworden. Wenn Sie ein Upgrade von einer früheren MOBOTIX HUB VMS-Version durchführen, startet der Management-Server weiterhin die alte 3rd-Party-Technologie, um mit Aufzeichnungsservern in älteren Versionen kommunizieren zu können.
Wenn alle Aufzeichnungsserver in Ihrem System auf Version 2019 R2 oder höher aktualisiert werden, können Sie den Management-Server so konfigurieren, dass der Legacy-Remoting-Kanal nicht gestartet wird, um Ihr System weniger anfällig zu machen. MOBOTIX empfiehlt, **UseRemoting** in der Konfigurationsdatei des Management-Servers **auf** False zu setzen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-17 Fernzugriff (nicht verwendete Protokolle deaktivieren)
- Konfigurationseinstellungen für NIST 800-53 CM-6

6.4.5 Verwalten von IIS-Headerinformationen

Deaktivieren von IIS-Headerinformationen

Aus Sicherheitsgründen empfiehlt MOBOTIX, die Header X-Powered-By HTTP und X-AspNet-Version zu deaktivieren. Der HTTP-Header X-Powered-By zeigt die Version von IIS an, die auf dem Server verwendet wird. Deaktivieren Sie diesen Header, indem Sie wie folgt vorgehen:

1. Öffnen Sie den IIS-Manager.
2. Wählen Sie die Standardwebsite aus.
3. Wählen Sie HTTP-Antwortheader aus.
4. Wählen Sie den X-Powered-By-HTTP-Header aus, und klicken Sie auf Entfernen.

Der HTTP-Header X-AspNet-Version gibt die Version von ASP.NET an, die vom Verwaltungsserver-Anwendungspool verwendet wird. Deaktivieren Sie diesen Header, indem Sie wie folgt vorgehen:

1. Öffnen Sie die Datei web.config, die sich unter %windir%\Microsoft.NET\Framework\v4.0.30319\CONFIG befindet.
2. Fügen Sie nach dem <system.web>-Tag Folgendes hinzu: <httpRuntime enableVersionHeader="false" />
3. Speichern Sie die Datei.

Die Header-Variable SERVER sollte nicht entfernt werden, da sie dazu führt, dass die Funktionalität von Management Server nicht mehr funktioniert.

Festlegen von X-Frame-Optionen

Aus Sicherheitsgründen empfiehlt MOBOTIX, die X-Frame-Options auf **"deny" zu setzen**.
Wenn Sie den HTTP-Header X-Frame-Options auf deny setzen, wird das Laden der Seite in einem Frame deaktiviert, unabhängig davon, welche Website versucht, Zugriff zu erhalten.
Ändern Sie diese Kopfzeile, indem Sie wie folgt vorgehen:

1. Öffnen Sie den IIS-Manager.
2. Wählen Sie die Standardwebsite > Installation aus.
3. Wählen Sie HTTP-Antwortheader aus.
4. Klicken Sie mit der rechten Maustaste und wählen Sie Hinzufügen... aus der Speisekarte
5. Schreiben Sie in das Feld Name X-Frame-Options und in das Feld Wert deny.

6.4.6 Deaktivieren von IIS HTTP TRACE / TRACK-Verben

Aus Sicherheitsgründen empfiehlt MOBOTIX, das Verb HTTP TRACE in Ihrer IIS-Installation zu deaktivieren.
Deaktivieren Sie das HTTP TRACE-Verb, indem Sie wie folgt vorgehen:

1. Öffnen Sie den IIS-Manager.
2. Wählen Sie die Standardwebsite aus.
3. Doppelklicken Sie auf Anforderungsfilterung.

Wenn **die Anforderungsfilterung** nicht verfügbar ist, installieren Sie sie, indem Sie den Anweisungen hier folgen: https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/requestfiltering/

4. Wählen Sie die Registerkarte HTTP-Verben aus.
5. Wählen Sie im Menü "Aktionen" die Option "Verb verweigern" aus.
6. Geben Sie TRACE ein, und klicken Sie auf OK.
7. Wählen Sie im Menü "Aktionen" die Option "Verb verweigern" aus.
8. Geben Sie TRACK ein und klicken Sie auf OK.
9. Wählen Sie im Menü "Optionen" die Option "Verb verweigern" aus.
10. Geben Sie OPTIONS ein und klicken Sie auf OK.

6.4.7 Deaktivieren der IIS-Standardseite

Aus Sicherheitsgründen empfiehlt MOBOTIX, die IIS-Standardseite zu deaktivieren. Auf diese Weise entfernen Sie Informationen, die verwendet werden könnten, um zu ermitteln, welche Technologien in Ihrer Installation verwendet werden, und Sie richten sich an den von Microsoft definierten IIS-Best Practices aus. Deaktivieren Sie die Standardseite, indem Sie wie folgt vorgehen:

1. Öffnen Sie den IIS-Manager.
2. Wählen Sie die Standardwebsite aus.
3. Doppelklicken Sie auf Standarddokument.
4. Wählen Sie im Menü "Aktionen" die Option "Deaktivieren" aus.

6.5 Identitätsanbieter

6.5.1 Deaktivieren der IIS-Headerinformationen auf dem Identitätsanbieter

Aus Sicherheitsgründen empfiehlt MOBOTIX AG, den Server-Header in der Identity Provider-Anwendung zu deaktivieren .

Der Server-Header beschreibt die Software, die vom Server des Originals verwendet wird, der eine Anfrage verarbeitet. Deaktivieren Sie diesen Header, indem Sie wie folgt vorgehen.

Dies gilt nur für IIS 10 und höher.

1. Öffnen Sie den IIS-Manager.
2. Wählen Sie unter der Standardwebsite die Option **IDP aus**.
3. Öffnen Sie den **Konfigurationseditor**.
4. Wählen Sie den Abschnitt **system.webServer/security/requestFiltering**.
5. Legen Sie **removeServerHeader** auf **True fest**.

6.6 Aufzeichnungsserver

6.6.1 Eigenschaften der Speicher- und Aufzeichnungseinstellungen

Die verfügbaren Funktionen hängen vom verwendeten System ab. Weitere Informationen finden Sie unter https://www.mobotix.com/en/vms/mobotix-hub/levels .

Geben Sie im Dialogfeld Speicher- und Aufzeichnungseinstellungen Folgendes an:

Name	Beschreibung
Name	Benennen Sie den Speicher bei Bedarf um. Die Namen müssen eindeutig sein.
Pfad	Geben Sie den Pfad zu dem Verzeichnis an, in dem Sie Aufzeichnungen in diesem Speicher speichern. Der Speicher muss sich nicht zwingend auf dem Rechner des Aufnahmeservers befinden. Wenn das Verzeichnis nicht vorhanden ist, können Sie es erstellen. Netzlaufwerke müssen im UNC-Format (Universal Naming Convention) angegeben werden, z. B.: \\server\volume\directory\.
Verweildauer	Legen Sie fest, wie lange Aufzeichnungen im Archiv verbleiben sollen, bevor sie gelöscht oder in das nächste Archiv verschoben werden (abhängig von den Archiveinstellungen). Die Aufbewahrungszeit muss immer länger sein als die Aufbewahrungszeit des vorherigen Archivs oder der Standardaufzeichnungsdatenbank. Dies liegt daran, dass die für ein Archiv angegebene Anzahl von Aufbewahrungstagen alle zuvor im Prozess angegebenen Aufbewahrungszeiträume umfasst.
Maximale Größe	Wählen Sie die maximale Anzahl von Gigabyte an Aufzeichnungsdaten aus, die in der Aufzeichnungsdatenbank gespeichert werden sollen. Aufzeichnungsdaten, die die angegebene Anzahl von Gigabyte überschreiten, werden automatisch in das erste Archiv in der Liste verschoben - falls angegeben - oder gelöscht. Wenn weniger als 5 GB Speicherplatz frei sind, archiviert das System immer automatisch die ältesten Daten in einer Datenbank (oder löscht, wenn kein nächstes Archiv definiert ist). Wenn weniger als 1 GB Speicherplatz frei ist, werden die Daten gelöscht. Eine Datenbank benötigt immer 250 MB freien Speicherplatz. Wenn Sie diese Grenze erreichen (wenn die Daten nicht schnell genug gelöscht werden), werden keine Daten mehr auf die Datenbank geschrieben, bis Sie genügend Speicherplatz freigegeben haben. Die tatsächliche maximale Größe Ihrer Datenbank entspricht der von Ihnen angegebenen Anzahl von Gigabyte abzüglich 5 GB.
Unterzeichnung	Ermöglicht eine digitale Signatur für die Aufnahmen. Das bedeutet beispielsweise, dass das System bei der Wiedergabe bestätigt, dass das exportierte Video nicht verändert oder manipuliert wurde. Das System verwendet den SHA-2-Algorithmus für die digitale Signatur.
Verschlüsselung	Wählen Sie die Verschlüsselungsstufe der Aufzeichnungen aus: • Nichts • Leicht (weniger CPU-Auslastung) • Stark (mehr CPU-Auslastung) Das System verwendet den AES-256-Algorithmus für die Verschlüsselung. Wenn Sie **"Hell**" auswählen, wird ein Teil der Aufzeichnung verschlüsselt. Wenn Sie "Stark" auswählen, wird die gesamte Aufzeichnung verschlüsselt. Wenn Sie die Verschlüsselung aktivieren möchten, müssen Sie unten auch ein Kennwort angeben.
Passwort	Geben Sie ein Passwort für die Benutzer ein, die verschlüsselte Daten einsehen dürfen. MOBOTIX empfiehlt, sichere Passwörter zu verwenden. Sichere Passwörter enthalten keine Wörter, die in einem Wörterbuch zu finden sind oder Teil des Benutzernamens sind. Sie umfassen acht oder mehr alphanumerische Zeichen, Groß- und Kleinbuchstaben sowie Sonderzeichen.

6.6.2 Verwenden Sie separate Netzwerkkarten

MOBOTIX empfiehlt, mehrere Netzwerkkarten (NICs) zu verwenden, um die Kommunikation zwischen Aufzeichnungsservern und -geräten von der Kommunikation zwischen Aufzeichnungsservern und Client-Programmen zu trennen. Client-Programme müssen nicht direkt mit Geräten kommunizieren.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SC-7 Grenzschutz

6.6.3 Sichern Sie Network Attached Storage (NAS) zum Speichern aufgezeichneter Mediendaten

Der Aufzeichnungsserver kann Network Attached Storage (NAS) verwenden, um aufgezeichnete Mediendaten zu speichern.

Wenn Sie sich für die Verwendung von NAS entscheiden, kann es durch die Verwendung von SMB 3.0-Sicherheitsverbesserungen gehärtet werden, wie in diesem Dokument zu SMB-Sicherheitsverbesserungen beschrieben.

6.7 MOBOTIX Mobile Server-Komponente

6.7.1 Aktivieren Sie nur Ports, die der MOBOTIX Mobile Server verwendet

MOBOTIX empfiehlt, nur die Ports zu aktivieren, die vom MOBOTIX HUB Mobile-Server verwendet werden, und alle anderen Ports, einschließlich der Standard-Windows-Ports, zu blockieren.

Standardmäßig verwendet der mobile Server die Ports 8081 und 8082.

Welche Ports verwendet werden, hängt von der Bereitstellung ab. Wenden Sie sich im Zweifelsfall an den MOBOTIX Support.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 SC-7 Grenzschutz

6.7.2 Verwenden Sie eine "demilitarisierte Zone" (DMZ), um externen Zugriff zu ermöglichen

MOBOTIX empfiehlt, den MOBOTIX HUB Mobile-Server in einer DMZ und auf einem Computer mit zwei Netzwerkschnittstellen zu installieren:

- Einer für die interne Kommunikation
- Einer für den öffentlichen Internetzugang

Auf diese Weise können sich mobile Client-Benutzer mit einer öffentlichen IP-Adresse mit dem MOBOTIX Mobile-Server verbinden, ohne die Sicherheit oder Verfügbarkeit des VMS-Netzwerks zu beeinträchtigen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SC-7 Grenzschutz

6.7.3 Deaktivieren Sie unsichere Protokolle

MOBOTIX empfiehlt, nur die notwendigen Protokolle und nur die neuesten Versionen zu verwenden. Implementieren Sie beispielsweise die neueste Version von Transport Layer Security (TLS, derzeit 1.2) und deaktivieren Sie alle anderen Cipher Suites und veralteten Versionen von SSL/TLS-Protokollen. Dies erfordert die Konfiguration von Windows und anderen Systemkomponenten sowie die ordnungsgemäße Verwendung digitaler Zertifikate und Schlüssel.

Die gleiche Empfehlung wird für den Management-Server gegeben. Weitere Informationen finden Sie unter Deaktivieren Sie nicht sichere Protokolle auf der Seite 60.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-17 Fernzugriff (nicht verwendete Protokolle deaktivieren)
- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

6.7.4 Einrichten von Benutzern für die zweistufige Verifizierung per E-Mail

Die verfügbaren Funktionen hängen vom verwendeten System ab. Weitere Informationen finden Sie unter https://www.mobotix.com/en/vms/mobotix-hub/levels .

Um Benutzern des MOBOTIX HUB Mobile Clients oder MOBOTIX HUB Web Client einen zusätzlichen Anmeldeschritt aufzuerlegen, richten Sie die zweistufige Verifizierung auf dem MOBOTIX HUB Mobile Server ein. Zusätzlich zum Standardbenutzernamen und -kennwort muss der Benutzer einen Bestätigungscode eingeben, den er per E-Mail erhalten hat.

Die zweistufige Verifizierung erhöht das Schutzniveau Ihres Überwachungssystems.

Anforderungen

- Sie haben einen SMTP-Server installiert.
- Sie haben Ihrem MOBOTIX HUB-System im Management Client auf dem Knoten Rollen im Bereich Site-Navigation Benutzer und Gruppen hinzugefügt. Wählen Sie für die entsprechende Rolle die Registerkarte Benutzer und Gruppen aus.
- Wenn Sie Ihr System von einer früheren Version von MOBOTIX HUB aktualisiert haben, müssen Sie den mobilen Server neu starten, um die Funktion zur zweistufigen Verifizierung zu aktivieren.

Führen Sie im Verwaltungsclient oder in der Verwaltungsanwendung die folgenden Schritte aus:

1. Geben Sie Informationen zu Ihrem SMTP-Server ein.
2. Geben Sie die Einstellungen für den Überprüfungscode an, der an die Clientbenutzer gesendet wird.
3. Weisen Sie Benutzern und Domänengruppen die Anmeldemethode zu.

In diesem Thema werden die einzelnen Schritte beschrieben.

Geben Sie Informationen über Ihren SMTP-Server ein

Der Anbieter verwendet die Informationen über den SMTP-Server:

1. Wählen Sie im Navigationsbereich Mobile Server und dann den entsprechenden mobilen Server aus.
2. Aktivieren Sie auf der Registerkarte Zweistufige Überprüfung das Kontrollkästchen Zweistufige Überprüfung aktivieren.
3. Geben Sie unter Anbietereinstellungen auf der Registerkarte E-Mail Informationen zu Ihrem SMTP-Server ein, und geben Sie die E-Mail an, die das System an Clientbenutzer sendet, wenn sie sich anmelden und für eine sekundäre Anmeldung eingerichtet sind. Weitere Informationen zu den einzelnen Parametern finden Sie unter Registerkarte "Zweistufige Verifizierung" auf der Seite 66.

Geben Sie den Verifizierungscode an, der an die Benutzer gesendet wird

So geben Sie die Komplexität des Verifizierungscodes an:

1. Geben Sie auf der Registerkarte Zweistufige Verifizierung im Abschnitt Einstellungen für den Verifizierungscode den Zeitraum an, innerhalb dessen Benutzer des MOBOTIX Mobile Client oder des MOBOTIX HUB Web Client seine Anmeldung nicht erneut verifizieren müssen, z. B. wenn die Verbindung unterbrochen wird. Der Standardzeitraum beträgt 3 Minuten.
2. Geben Sie den Zeitraum an, innerhalb dessen der Benutzer den empfangenen Verifizierungscode verwenden kann. Nach Ablauf dieser Frist ist der Code ungültig und der Benutzer muss einen neuen Code anfordern. Der Standardzeitraum beträgt 5 Minuten.
3. Geben Sie die maximale Anzahl von Codeeingabeversuchen an, bevor der Benutzer blockiert wird. Die Standardnummer ist 3.
4. Geben Sie die Anzahl der Zeichen für den Code an. Die Standardlänge ist 6.
5. Geben Sie die Komplexität des Codes an, den das System erstellen soll.

Zuweisen der Anmeldemethode zu Benutzern und Active Directory-Gruppen

Auf der Registerkarte **Zweistufige Verifizierung** wird im Abschnitt **Benutzereinstellungen** die Liste der Benutzer und Gruppen angezeigt, die Ihrem MOBOTIX HUB-System hinzugefügt wurden.

1. Wählen Sie in der Spalte Anmeldemethode zwischen keine Anmeldung, keine zweistufige Überprüfung oder Übermittlungsmethode von Codes aus.
2. Fügen Sie im Feld Details die Versanddetails hinzu, z. B. die E-Mail-Adressen der einzelnen Benutzer. Wenn sich der Benutzer das nächste Mal am MOBOTIX HUB Web Client oder am MOBOTIX HUB Mobile Client anmeldet, wird er nach einer zweiten Anmeldung gefragt.
3. Wenn eine Gruppe in Active Directory konfiguriert ist, verwendet der Mobile-Server Details wie E-Mail-Adressen aus Active Directory.
4. Windows-Gruppen unterstützen die zweistufige Überprüfung nicht.
5. Speichern Sie Ihre Konfiguration.

Sie haben die Schritte zum Einrichten Ihrer Benutzer für die zweistufige Verifizierung per E-Mail abgeschlossen.

Registerkarte "Zweistufige Verifizierung"

Die verfügbaren Funktionen hängen vom verwendeten System ab. Weitere Informationen finden Sie unter https://www.mobotix.com/en/vms/mobotix-hub/levels .

Verwenden Sie die **Registerkarte Zweistufige Überprüfung**, um einen zusätzlichen Anmeldeschritt für Benutzer der folgenden Benutzer zu aktivieren und anzugeben:

- MOBOTIX HUB Mobile App auf ihren iOS- oder Android-Mobilgeräten
- MOBOTIX HUB Web-Client

Die erste Art der Verifizierung ist ein Passwort. Der zweite Typ ist ein Verifizierungscode, den Sie so konfigurieren können, dass er per E-Mail an den Benutzer gesendet wird.
Weitere Informationen finden Sie unter Einrichten von Benutzern für die zweistufige Verifizierung per E-Mail auf Seite 65.
In den folgenden Tabellen werden die Einstellungen auf dieser Registerkarte beschrieben.

Anbietereinstellungen > E-Mail

Name	Beschreibung
SMTP-Server	Geben Sie die IP-Adresse oder den Hostnamen des SMTP-Servers (Simple Mail Transfer Protocol) für zweistufige Verifizierungs-E-Mails ein.
Anschluss des SMTP-Servers	Geben Sie den Port des SMTP-Servers für den Versand von E-Mails an. Die Standardportnummer ist 25 ohne SSL und 465 mit SSL.
SSL verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Ihr SMTP-Server SSL-Verschlüsselung unterstützt.
Benutzername	Geben Sie den Benutzernamen für die Anmeldung am SMTP-Server an.
Passwort	Geben Sie das Kennwort für die Anmeldung am SMTP-Server an.
Verwenden der sicheren Kennwortauthentifizierung (SPA)	Aktivieren Sie dieses Kontrollkästchen, wenn Ihr SMTP-Server SPA unterstützt.
E-Mail-Adresse des Absenders	Geben Sie die E-Mail-Adresse für das Senden von Bestätigungscodes an.
Betreff der E-Mail	Geben Sie den Betrefftitel für die E-Mail an. Beispiel: Ihr Code für die zweistufige Verifizierung.
E-Mail-Text	Geben Sie die Nachricht ein, die Sie senden möchten. Beispiel: Ihr Code ist {0}. Wenn Sie vergessen, die Variable {0} einzuschließen, wird der Code standardmäßig am Ende des Textes hinzugefügt.

Einstellungen für den Verifizierungscode

Name	Beschreibung
Timeout für die Wiederherstellung der Verbindung (0-30 Minuten)	Geben Sie den Zeitraum an, innerhalb dessen Benutzer des MOBOTIX HUB Mobile-Clients ihre Anmeldung nicht erneut verifizieren müssen, wenn z. B. das Netzwerk unterbrochen wird. Der Standardzeitraum beträgt drei Minuten. Diese Einstellung gilt nicht für den MOBOTIX HUB Web Client.
Code läuft ab nach (1-10 Minuten)	Geben Sie den Zeitraum an, innerhalb dessen der Benutzer den empfangenen Verifizierungscode verwenden kann. Nach Ablauf dieser Frist ist der Code ungültig und der Benutzer muss einen neuen Code anfordern. Der Standardzeitraum beträgt fünf Minuten.
Eingabeversuche (1-10 Versuche)	Geben Sie die maximale Anzahl von Codeeingabeversuchen an, bevor der angegebene Code ungültig wird. Die Standardanzahl ist drei.

Name	Beschreibung
Codelänge (4-6 Zeichen)	Geben Sie die Anzahl der Zeichen für den Code an. Die Standardlänge beträgt sechs.
Zusammensetzung des Codes	Geben Sie die Komplexität des Codes an, den das System generieren soll. Sie können wählen zwischen: Lateinische Großbuchstaben (A-Z) Lateinischer Kleinbuchstabe (a-z) Ziffern (0-9) Sonderzeichen (!@#...)

Benutzereinstellungen

Name	Beschreibung
Benutzer und Gruppen	Listet die Benutzer und Gruppen auf, die dem MOBOTIX HUB-System hinzugefügt wurden. Wenn eine Gruppe in Active Directory konfiguriert ist, verwendet der mobile Server Details wie E-Mail-Adressen aus Active Directory. Windows-Gruppen unterstützen die zweistufige Überprüfung nicht.
Methode der Überprüfung	Wählen Sie für jeden Benutzer oder jede Gruppe eine Verifizierungseinstellung aus. Sie können wählen zwischen: Keine Anmeldung: Der Benutzer kann sich nicht anmelden Keine zweistufige Verifizierung: Der Benutzer muss den Benutzernamen und das Passwort eingeben E-Mail: Der Benutzer muss zusätzlich zu Benutzername und Passwort einen Verifizierungscode eingeben
Benutzerdetails	Geben Sie die E-Mail-Adresse ein, an die jeder Benutzer Codes erhält.

6.7.5 Konfigurieren der Content Security Policy (CSP)

WebSockets mit Platzhaltern sollten aus den CSP-Headern auf dem Mobile Server entfernt werden.
Derzeit können die ws://*:* und wss://*:* aufgrund von Einschränkungen des Safari-Browsers nicht aus dem CSP entfernt werden, der in der Mobile Server-Konfiguration beschrieben ist.
Um die Sicherheit auf Ihrem Mobile Server zu erhöhen, gehen Sie wie folgt vor:

1. Öffnen Sie die Datei VideoOS.MobileServer.Service.exe.config, die sich im Installationsordner des Mobile Servers befindet.
2. Ändern Sie den Abschnitt <HttpHeaders>, in dem der Wert von key="Content-Security-Policy" wie folgt angegeben ist:
   - Wenn die Unterstützung des Safari-Browsers nicht benötigt wird, entfernen Sie ws://*:* und wss://*:* aus der Kopfzeile.
   - Wenn die Unterstützung des Safari-Browsers erforderlich ist, ersetzen Sie ws://*:* und wss://*:* durch die entsprechenden Werte für "ws:// [Hostname]:[Port] und wss://[Hostname]:[Port]", wobei Hostname und Port die relevanten Werte sind, die für den Zugriff auf den Mobile Server verwendet werden.
3. Starten Sie den Mobile Server neu.

6.8 Protokollserver

6.8.1 Installieren des Protokollservers auf einem separaten Server mit SQL Server

Für sehr große Systeme mit vielen Transaktionen in und von der SQL-Datenbank des Protokollservers empfiehlt MOBOTIX, die Protokollserverkomponente auf einem separaten Server mit eigenem SQL Server zu installieren und die Protokolle in einer SQL-Datenbank auf diesem lokalen SQL Server zu speichern. Wenn der Protokollserver von Leistungsproblemen betroffen ist, z. B. aufgrund von Überflutung oder aus anderen Gründen, und denselben SQL Server wie der Verwaltungsserver verwendet, können beide Dienste betroffen sein.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SC-7 Grenzschutz
- NIST SP 800-53 CM-9 Konfigurationsmanagementplan

6.8.2 Beschränken des IP-Zugriffs auf den Protokollserver

MOBOTIX empfiehlt, dass nur VMS-Komponenten den Protokollserver kontaktieren können.Der Protokollserver verwendet Port 22337.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

7 Client-Programme

In diesem Abschnitt finden Sie eine Anleitung zum Schutz der MOBOTIX-Client-Programme.
Die Client-Programme sind:

- MOBOTIX HUB Smart Client
- MOBOTIX HUB Web-Client
- MOBOTIX HUB Management-Client
- MOBOTIX Mobile Client

7.1 Grundlegende Schritte (alle Client-Programme)

7.1.1 Verwenden von Windows-Benutzern mit AD

MOBOTIX empfiehlt, wenn immer möglich, Windows-Benutzer in Kombination mit Active Directory (AD) zu verwenden, um sich mit den Client-Programmen am VMS anzumelden. Auf diese Weise können Sie eine Kennwortrichtlinie erzwingen und Benutzereinstellungen konsistent auf die gesamte Domäne und das Netzwerk anwenden. Es bietet auch Schutz vor Brute-Force-Angriffen. Weitere Informationen finden Sie unter Verwenden von Windows-Benutzern mit Active Directory.

Weitere Informationen

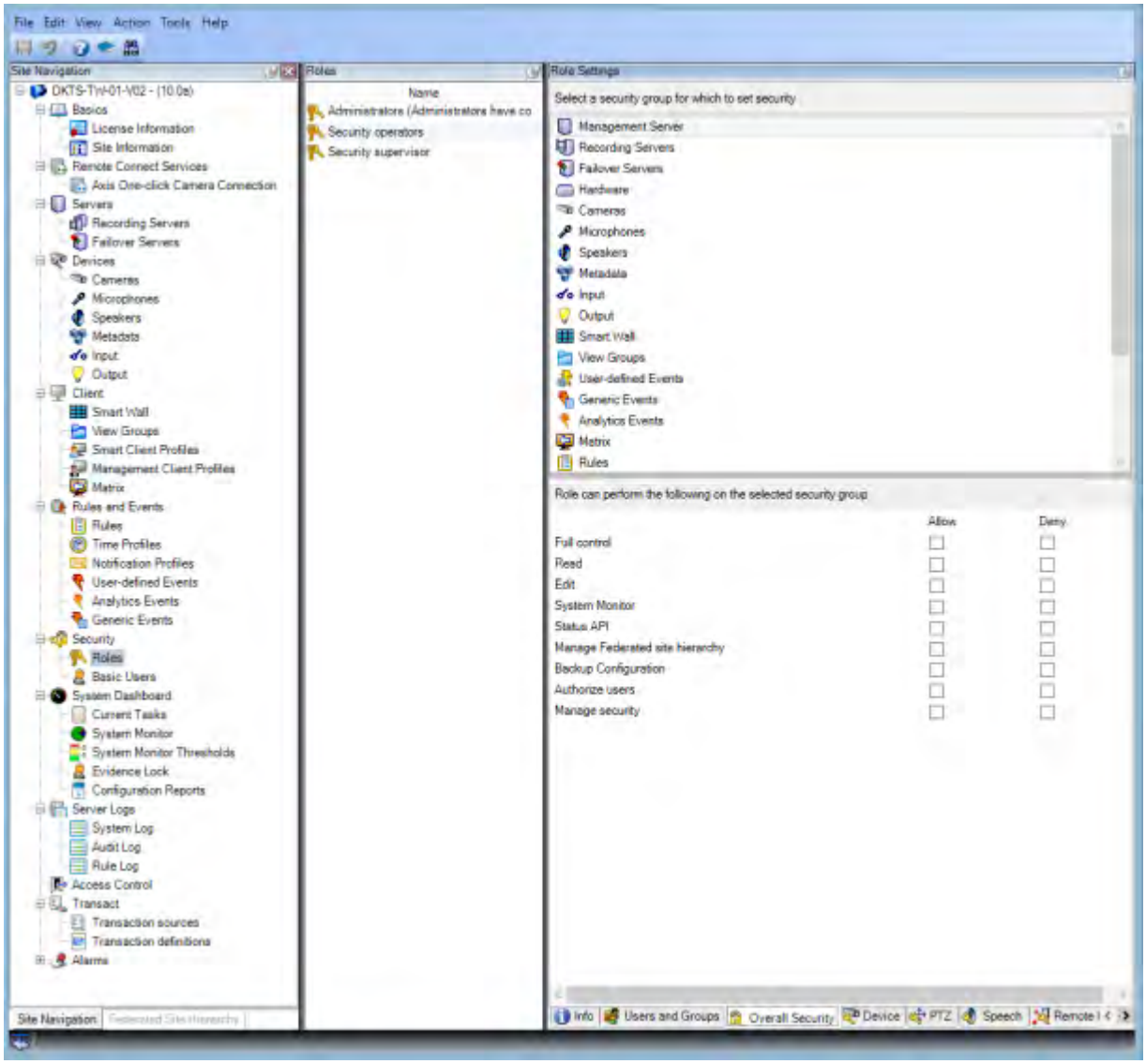
Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 SA-5 Dokumentation zum Informationssystem
- NIST 800-53 SA-13 Vertrauenswürdigkeit

7.1.2 Einschränken von Berechtigungen für Clientbenutzer

MOBOTIX empfiehlt, dass Administratoren festlegen, welche Aktionen Benutzer im Management Client oder MOBOTIX HUB Smart Client ausführen können.
In der folgenden Anleitung wird beschrieben, wie Sie dies tun können.
Gehen Sie folgendermaßen vor, um Clientbenutzerberechtigungen einzuschränken:

1. Öffnen Sie den Management-Client.
2. Erweitern Sie den Knoten Sicherheit, wählen Sie Rollen aus, und wählen Sie dann die Rolle aus, der der Benutzer zugeordnet ist.
3. Auf den Registerkarten unten können Sie Berechtigungen und Einschränkungen für die Rolle festlegen.



Standardmäßig haben alle Benutzer, die der Administratorrolle zugeordnet sind, uneingeschränkten Zugriff auf das System. Dazu gehören sowohl Benutzer, die der Administratorrolle in AD zugeordnet sind, als auch Benutzer mit der Rolle "Administrator" auf dem Management-Server.

Weitere Informationen

Die folgenden Dokumente enthalten zusätzliche Informationen:

- NIST 800-53 AC-4 mit den geringsten Rechten
- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

7.1.3 Führen Sie Clients immer auf vertrauenswürdiger Hardware in vertrauenswürdigen Netzwerken aus

MOBOTIX empfiehlt, MOBOTIX HUB-Clients immer auf Hardwaregeräten mit den richtigen Sicherheitseinstellungen auszuführen. Spezifische Anleitungen für mobile Geräte finden Sie in SP 800-124 (https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final). Diese Einstellungen sind gerätespezifisch.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SC-7 Grenzschutz
- Konfigurationseinstellungen für NIST SP800-53 CM-6

7.2 Erweiterte Schritte – MOBOTIX HUB Smart Client

7.2.1 Beschränken Sie den physischen Zugriff auf jeden Computer, auf dem MOBOTIX HUB Smart Client ausgeführt wird

MOBOTIX empfiehlt, den physischen Zugriff auf Computer zu beschränken, auf denen MOBOTIX HUB Smart Client ausgeführt wird. Erlauben Sie nur autorisiertem Personal den Zugriff auf die Computer. Halten Sie beispielsweise die Tür verschlossen und verwenden Sie Zugangskontrollen und Überwachung.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 PE-1 Richtlinien und Verfahren zum physischen und Umweltschutz
- NIST SP 800-53 PE-2 Physische Zugriffsberechtigungen
- NIST SP 800-53 PE-3 Physische Zugangskontrolle
- NIST SP 800-53 PE-6 Überwachen des physischen Zugriffs

7.2.2 Verwenden Sie standardmäßig immer eine sichere Verbindung, insbesondere über öffentliche Netzwerke

Wenn Sie mit dem MOBOTIX HUB Smart Client über ein öffentliches oder nicht vertrauenswürdiges Netzwerk auf das VMS zugreifen müssen, empfiehlt MOBOTIX die Verwendung einer sicheren Verbindung über VPN. Dadurch wird sichergestellt, dass die Kommunikation zwischen MOBOTIX HUB Smart Client und dem VMS-Server geschützt ist.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 AC-17 Fernzugriff
- Konfigurationseinstellungen für NIST SP 800-53 CM-6

7.2.3 Aktivieren der Login-Berechtigung

Die Anmeldeberechtigung erfordert, dass sich ein Benutzer am MOBOTIX HUB Smart Client oder Management Client anmeldet, und ein anderer Benutzer mit einem erhöhten Status, z. B. ein Supervisor, um die Genehmigung zu erteilen.

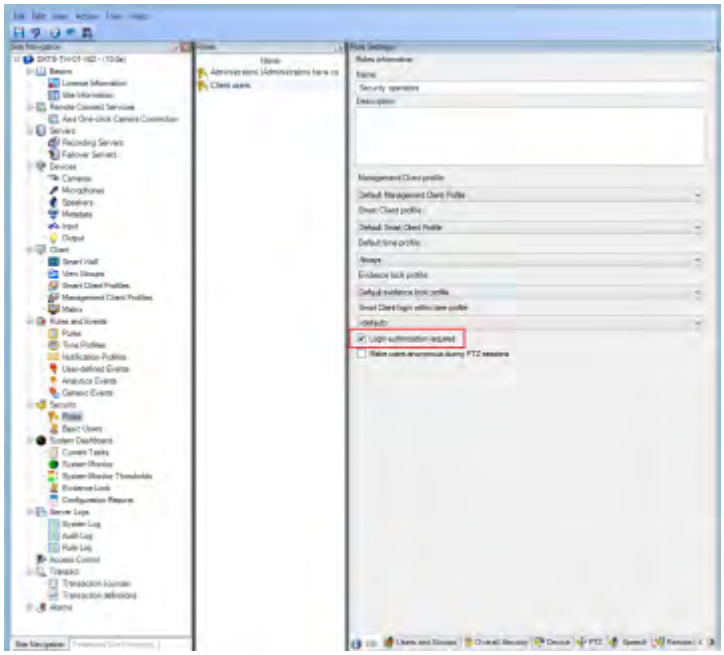
Sie richten die Anmeldeberechtigung für die Rollen ein. Benutzer, die der Rolle zugeordnet sind, werden aufgefordert, einen zweiten Benutzer (einen Supervisor) anzugeben, um ihren Zugriff auf das System zu autorisieren.

Die Anmeldeberechtigung wird derzeit vom mobilen Client, dem MOBOTIX HUB Web Client und allen MOBOTIX Integration Platform (MIP) SDK-Integrationen nicht unterstützt.

Gehen Sie folgendermaßen vor, um die Anmeldeberechtigung für eine Rolle zu aktivieren:

1. Öffnen Sie den Management-Client.
2. Erweitern Sie den Knoten Sicherheit, wählen Sie Rollen aus, und wählen Sie dann die entsprechende Rolle aus.

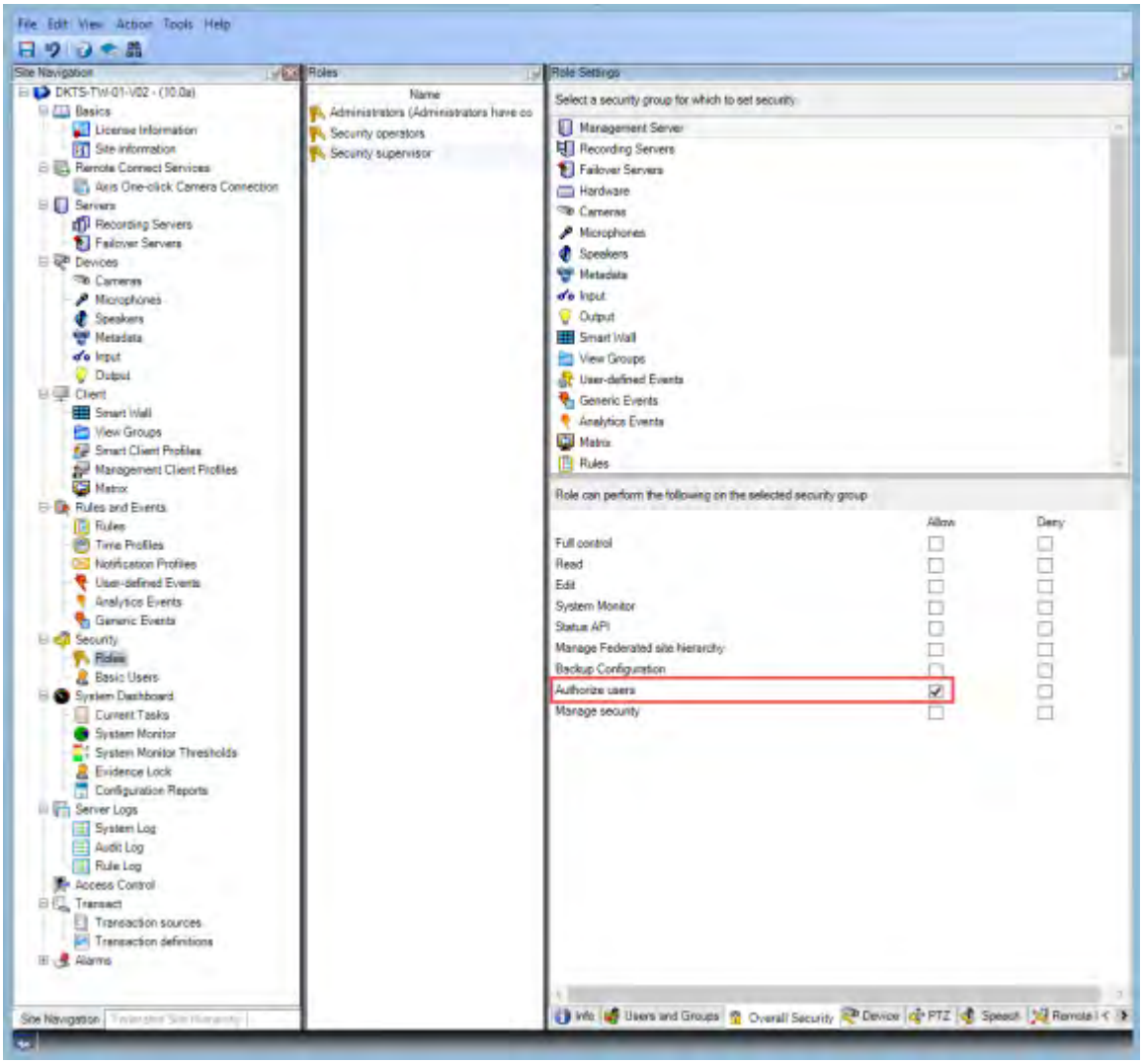
   Aktivieren Sie das **Kontrollkästchen Anmeldeberechtigung erforderlich**.



Gehen Sie folgendermaßen vor, um die Rollen zu konfigurieren, die den Zugriff autorisieren und gewähren:

1. Um eine neue Rolle zu erstellen, z. B. "Sicherheitsbeauftragter", erweitern Sie den Knoten Sicherheit, klicken Sie mit der rechten Maustaste auf Rollen, und erstellen Sie eine neue Rolle.
2. Klicken Sie auf die Registerkarte Gesamtsicherheit, und wählen Sie den Knoten Verwaltungsserver aus.

   Aktivieren Sie das **Kontrollkästchen Zulassen** neben dem Kontrollkästchen **Benutzer autorisieren**.



Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 AC-6 mit den geringsten Rechten
- NIST SP 800-53 AC-17 Fernzugriff
- Konfigurationseinstellungen für NIST SP 800-53 CM-6

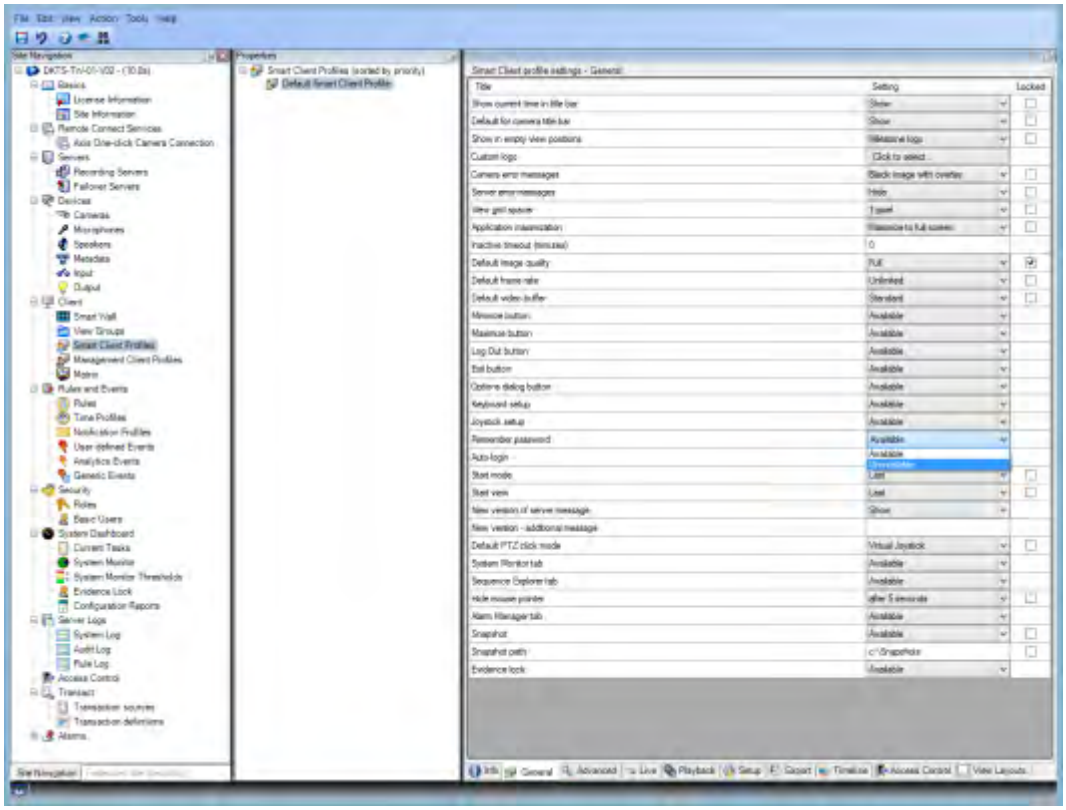
7.2.4 Speichern Sie keine Passwörter

MOBOTIX HUB Smart Client bietet die Möglichkeit, sich Passwörter für Benutzer zu merken. Um das Risiko eines unbefugten Zugriffs zu verringern, empfiehlt MOBOTIX, diese Funktion nicht zu verwenden.

Gehen Sie folgendermaßen vor, um die Funktion zum Speichern von Passwörtern zu deaktivieren:

1. Öffnen Sie den Management-Client.
2. Erweitern Sie den Knoten Client, wählen Sie Smart Client-Profile aus, und wählen Sie dann das entsprechende Smart Client-Profil aus.
3. Wählen Sie in der Liste Kennwort speichern die Option Nicht verfügbar aus.

Die Option **Kennwort speichern** ist nicht verfügbar, wenn sich ein Benutzer mit diesem Profil das nächste Mal beim MOBOTIX HUB Smart Client anmeldet.



Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 IA-1 Richtlinie und Verfahren zur Identifizierung und Authentifizierung

7.2.5 Aktivieren nur erforderlicher Clientfeatures

Aktivieren Sie nur erforderliche Funktionen und deaktivieren Sie Funktionen, die ein Überwachungsoperator nicht benötigt. Es geht darum, Möglichkeiten für Missbrauch oder Fehler zu begrenzen.

Sie können Funktionen im MOBOTIX HUB Smart Client und im MOBOTIX HUB Management Client ein- und ausschalten.

Konfigurieren Sie im Management-Client Smart-Client-Profile, um Berechtigungssätze für Benutzer anzugeben, die dem Profil zugewiesen sind. Smart Client-Profile ähneln den Management Client-Profilen, und jedem Profiltyp kann derselbe Benutzer zugewiesen werden.

Gehen Sie folgendermaßen vor, um ein Smart Client-Profil zu konfigurieren:

1. Öffnen Sie den Management-Client.
2. Erweitern Sie den Knoten Client, wählen Sie Smart Client-Profile aus, und wählen Sie dann das entsprechende Smart Client-Profil aus.
3. Verwenden Sie die Registerkarten, um Einstellungen für Funktionen im Smart Client festzulegen. Verwenden Sie z. B. die Einstellungen auf der Registerkarte Wiedergabe, um Funktionen zu steuern, die zum Untersuchen von aufgezeichneten Videos verwendet werden.

Bevor Sie einen Benutzer einem Smart Client-Profil zuweisen, stellen Sie sicher, dass die Berechtigungen für die Rolle des Benutzers für das Profil geeignet sind. Wenn Sie z. B. möchten, dass ein Benutzer in der Lage ist, Videos zu untersuchen, stellen Sie sicher, dass die Rolle es dem Benutzer ermöglicht, Videos von Kameras wiederzugeben, und dass die Registerkarte "Sequenz-Explorer" im Smart Client-Profil verfügbar ist.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 AC-6 mit den geringsten Rechten
- Konfigurationseinstellungen für NIST SP 800-53 CM-6

7.2.6 Verwenden Sie separate Namen für Benutzerkonten

MOBOTIX empfiehlt, für jeden Benutzer ein Benutzerkonto anzulegen und eine Namenskonvention zu verwenden, die es einfach macht, den Benutzer persönlich zu identifizieren, z. B. seinen Namen oder seine Initialen. Dies ist eine bewährte Methode, um den Zugriff auf das Notwendige zu beschränken, und reduziert auch die Verwirrung bei der Überwachung.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-4 mit den geringsten Rechten
- NIST 800-53 CM-1 Richtlinie und Verfahren für das Konfigurationsmanagement
- NIST 800-53 CM-2 Baseline-Konfiguration
- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

7.2.7 Verbieten Sie die Verwendung von Wechselmedien

Legen Sie für Videoexporte eine Kette von Verfahren fest, die spezifisch für Nachweise sind. MOBOTIX empfiehlt, dass die Sicherheitsrichtlinie nur autorisierten MOBOTIX HUB Smart Client-Betreibern erlaubt, Wechseldatenträger wie USB-Flash-Laufwerke, SD-Karten und Smartphones an den Computer anzuschließen, auf dem MOBOTIX HUB Smart Client installiert ist.

Wechseldatenträger können Malware in das Netzwerk übertragen und Videos einer nicht autorisierten Verbreitung aussetzen.

Alternativ kann die Sicherheitsrichtlinie angeben, dass Benutzer Beweise nur an einen bestimmten Speicherort im Netzwerk oder nur an einen Medienbrenner exportieren können. Sie können dies über das Smart Client-Profil steuern.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SO 800-53 MP-7 Mediennutzung
- NIST SP 800-53 SI-3 Schutz vor bösartigem Code

7.3 Erweiterte Schritte – MOBOTIX Mobile Client

SP 800-124 Revision 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) bietet eine Anleitung, die speziell für mobile Geräte entwickelt wurde. Die darin enthaltenen Informationen gelten für alle Themen in diesem Abschnitt.

7.3.1 Verwenden Sie den MOBOTIX Mobile Client immer auf sicheren Geräten

MOBOTIX empfiehlt, den MOBOTIX HUB Mobile Client immer auf sicheren Geräten zu verwenden, die gemäß einer Sicherheitsrichtlinie konfiguriert und gewartet werden. Stellen Sie beispielsweise sicher, dass mobile Geräte es Benutzern nicht erlauben, Software aus nicht autorisierten Quellen zu installieren. Ein Unternehmens-App-Store ist ein Beispiel für eine Möglichkeit, Geräteanwendungen als Teil der gesamten Verwaltung mobiler Geräte einzuschränken.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SC-7 Grenzschutz
- Konfigurationseinstellungen für NIST SP800-53 CM-6

7.3.2 Laden Sie den MOBOTIX Mobile Client von autorisierten Quellen herunter

MOBOTIX empfiehlt, den MOBOTIX HUB Mobile-Client von einer der folgenden Quellen herunterzuladen:

- Google Play Store
- Apple App Store
- Microsoft Windows Store.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 SC-7 Grenzschutz
- Konfigurationseinstellungen für NIST SP 800-53 CM-6

7.3.3 Mobile Geräte sollten gesichert werden

Wenn Sie mit einem mobilen Gerät über ein öffentliches oder nicht vertrauenswürdiges Netzwerk auf das VMS zugreifen möchten, empfiehlt MOBOTIX, dies mit einer sicheren Verbindung zu tun, eine ordnungsgemäße Authentifizierung und Transport Layer Security (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (oder eine Verbindung über VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) und HTTPS zu verwenden. Dies trägt zum Schutz der Kommunikation zwischen dem mobilen Gerät und dem VMS bei.
MOBOTIX empfiehlt, dass mobile Geräte die Bildschirmsperre verwenden. Dies hilft, unbefugten Zugriff auf das VMS zu verhindern, z. B. wenn das Smartphone verloren geht. Um maximale Sicherheit zu gewährleisten, implementieren Sie eine Sicherheitsrichtlinie, die es dem MOBOTIX HUB Mobile-Client verbietet, sich den Benutzernamen und das Kennwort zu merken.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- NIST SP 800-53 AC-17 Fernzugriff
- Konfigurationseinstellungen für NIST SP 800-53 CM-6

7.4 Erweiterte Schritte – MOBOTIX HUB Web Client

7.4.1 MOBOTIX HUB Web Client immer auf vertrauenswürdigen Client-Computern ausführen

Verbinden Sie alle Komponenten des VMS immer sicher. Server-zu-Server- und Client-zu-Server-Verbindungen sollten eine ordnungsgemäße Authentifizierung und Transport Layer Security (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (oder eine Verbindung über VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) und HTTPS verwenden. Führen Sie MOBOTIX HUB Web Client immer auf vertrauenswürdigen Computern aus, z. B. verwenden Sie einen Client-Computer nicht in einem öffentlichen Bereich. MOBOTIX empfiehlt, die Benutzer über die Sicherheitsmaßnahmen zu informieren, die bei der Verwendung browserbasierter Anwendungen, wie z. B. MOBOTIX HUB Web Client, zu beachten sind. Stellen Sie beispielsweise sicher, dass sie wissen, dass sie dem Browser nicht erlauben sollen, sich ihr Passwort zu merken.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 IA-2 Identifizierung und Authentifizierung

7.4.2 Verwenden von Zertifikaten zur Bestätigung der Identität eines MOBOTIX Mobile-Servers

In diesem Dokument wird die Verwendung des neuesten TLS betont. Damit einher geht die Notwendigkeit der ordnungsgemäßen Verwendung von Zertifikaten und der Implementierung der TLS-Cipher-Suite. MOBOTIX empfiehlt, ein Zertifikat auf dem MOBOTIX HUB Mobile-Server zu installieren, um die Identität des Servers zu bestätigen, wenn ein Benutzer versucht, eine Verbindung über den MOBOTIX HUB Web Client herzustellen. Weitere Informationen finden Sie im *Abschnitt Zertifikat bearbeiten* im *Handbuch MOBOTIX HUB VMS - Administrator*.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 IA-2 Identifizierung und Authentifizierung

7.4.3 Verwenden Sie nur unterstützte Browser mit den neuesten Sicherheitsupdates

MOBOTIX empfiehlt, nur einen der folgenden Browser auf Client-Rechnern zu installieren. Stellen Sie sicher, dass Sie die neuesten Sicherheitsupdates enthalten.

- Apfel-Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 CM-1 Richtlinie und Verfahren für das Konfigurationsmanagement
- NIST SP 800-53 CM-2 Baseline-Konfiguration

- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 PL-8 Architektur für Informationssicherheit
- NIST SP 800-53 SI-3 Schutz vor bösartigem Code

7.5 Erweiterte Schritte – Management Client

7.5.1 Verwenden Sie Management-Client-Profile, um einzuschränken, was Administratoren anzeigen können

MOBOTIX empfiehlt, die Verwendung von Management-Client-Profilen zu verwenden, um einzuschränken, was Administratoren im Management-Client anzeigen können.
Mit Management Client-Profilen können Systemadministratoren die Benutzeroberfläche des Management Clients ändern. Verknüpfen Sie Management-Client-Profile mit Rollen, um die Benutzeroberfläche so einzuschränken, dass sie die für jede Administratorrolle verfügbaren Funktionen darstellt.
Zeigen Sie nur die Teile des VMS an, die Administratoren zum Ausführen ihrer Aufgaben benötigen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST 800-53 AC-4 mit den geringsten Rechten
- NIST 800-53 CM-1 Richtlinie und Verfahren für das Konfigurationsmanagement
- NIST 800-53 CM-2 Baseline-Konfiguration
- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

7.5.2 Ermöglichen Sie Administratoren den Zugriff auf relevante Teile des VMS

Wenn Sie ein Setup haben, das mehrere Administratoren erfordert, empfiehlt MOBOTIX, dass Sie für Administratoren, die den Management Client verwenden, unterschiedliche Administratorrechte konfigurieren.
Gehen Sie folgendermaßen vor, um Administratorberechtigungen zu definieren:

1. Erweitern Sie im Verwaltungsclient den Knoten Sicherheit, wählen Sie Rollen aus, und wählen Sie dann die entsprechende Administratorrolle aus.
   Sie können die integrierte Administratorrolle nicht ändern, daher müssen Sie zusätzliche Administratorrollen erstellen.
2. Geben Sie auf der Registerkarte Gesamtsicherheit die Aktionen an, die der Administrator für jede Sicherheitsgruppe ausführen kann.
3. Geben Sie auf den anderen Registerkarten die Sicherheitseinstellungen für die Rolle im VMS an.
   Weitere Informationen finden Sie im Administratorhandbuch für MOBOTIX HUB VMS.
4. Verknüpfen Sie die Rolle auf der Registerkarte Info mit einem Management-Client-Profil.

Sie können Funktionen mithilfe des Management-Client-Profils aktivieren oder deaktivieren. Bevor Sie einem Management-Client-Profil einen Benutzer zuweisen, stellen Sie sicher, dass die Berechtigungen für die Rolle des Benutzers für das Profil geeignet sind. Wenn Sie z. B. möchten, dass ein Benutzer in der Lage ist, Kameras zu verwalten, stellen Sie sicher, dass die Rolle dies dem Benutzer ermöglicht und dass die Kameras im Profil des Verwaltungsclients aktiviert sind.

Weitere Informationen

- Die folgenden Steuerelemente bieten zusätzliche Anleitungen:
- NIST 800-53 AC-4 mit den geringsten Rechten
- NIST 800-53 CM-1 Richtlinie und Verfahren für das Konfigurationsmanagement
- NIST 800-53 CM-2 Baseline-Konfiguration
- Konfigurationseinstellungen für NIST 800-53 CM-6
- NIST 800-53 CM-7 Geringste Funktionalität

7.5.3 Führen Sie den Management-Client in vertrauenswürdigen und sicheren Netzwerken aus

Wenn Sie mit dem Management Client über HTTP auf den Management Server zugreifen, kann die Klartextkommunikation unverschlüsselte Systemdetails enthalten. MOBOTIX empfiehlt, den Management Client nur in vertrauenswürdigen und bekannten Netzwerken auszuführen. Verwenden Sie ein VPN, um den Fernzugriff zu ermöglichen.

Weitere Informationen

Die folgenden Steuerelemente bieten zusätzliche Anleitungen:

- NIST SP 800-53 AC-2 Kontoverwaltung
- Konfigurationseinstellungen für NIST SP 800-53 CM-6
- NIST SP 800-53 IA-2 Identifizierung und Authentifizierung

8 Beachtung

8.1 Konformität mit FIPS 140-2

In diesem Abschnitt wird FIPS 140-2 und die Konfiguration und Verwendung von MOBOTIX HUB VMS für den Betrieb im FIPS 140-2-konformen Modus erläutert.

Die Begriffe "FIPS 140-2-konform" und "FIPS 140-2-konformer Modus" sind rechtlich nicht bindend. Der Übersichtlichkeit halber werden hier die Begriffe verwendet.

FIPS 140-2-konform bedeutet, dass die Software FIPS 140-2-validierte Instanzen von Algorithmen und Hashing-Funktionen in allen Instanzen verwendet, in denen verschlüsselte oder gehashte Daten in die Software importiert oder aus der Software exportiert werden. Darüber hinaus bedeutet dies, dass die Software Schlüssel auf sichere Weise verwaltet, wie es für FIPS 140-2-validierte kryptografische Module erforderlich ist. Der Schlüsselverwaltungsprozess umfasst sowohl die Schlüsselgenerierung als auch die Schlüsselspeicherung.

Der FIPS 140-2-konforme Modus bezieht sich auf Software, die sowohl FIPS-zugelassene als auch nicht FIPS-zugelassene Sicherheitsmethoden enthält, wobei die Software über mindestens einen "FIPS-Betriebsmodus" verfügt. Dieser Betriebsmodus erlaubt nur den Betrieb von FIPS-zugelassenen Sicherheitsmethoden. Das bedeutet, dass im "FIPS-Modus" der Software keine nicht FIPS-zugelassene Methode anstelle der FIPS-zugelassenen Methode verwendet wird.

Die folgenden Themen werden behandelt.

8.1.1 Was ist FIPS?

Federal Information Processing Standards (FIPS) sind eine Familie von Standards, die von den folgenden zwei Regierungsbehörden entwickelt wurden:

- Das National Institute of Standards and Technology (NIST) in den Vereinigten Staaten
- Das Communications Security Establishment (CSE) in Kanada

Diese Standards zielen darauf ab, die Sicherheit und Interoperabilität von Computern zu gewährleisten.
Alle Softwarelösungen, die in staatlichen und stark regulierten Branchen in den Vereinigten Staaten und Kanada eingesetzt werden, müssen FIPS 140-2 erfüllen.

8.1.2 Was ist FIPS 140-2?

FIPS 140-2 mit dem Titel "Security Requirements for Cryptographic Modules" legt fest, welche Verschlüsselungsalgorithmen und welche Hashing-Algorithmen verwendet werden können und wie Verschlüsselungsschlüssel generiert und verwaltet werden sollen.
Die in dieser Norm spezifizierten Sicherheitsanforderungen sollen die Sicherheit eines kryptographischen Moduls aufrechterhalten, aber die Konformität mit dieser Norm reicht nicht aus, um sicherzustellen, dass ein bestimmtes Modul sicher ist. Der Betreiber eines kryptographischen Moduls ist dafür verantwortlich, dass die durch das Modul gebotene Sicherheit für den Eigentümer der zu schützenden Informationen ausreichend und akzeptabel ist und dass ein etwaiges Restrisiko anerkannt und akzeptiert wird.

8.1.3 Welche MOBOTIX HUB VMS-Anwendungen können in einem FIPS 140-2-konformen Modus betrieben werden?

Ab MOBOTIX HUB VMS 2020 R3 wurden alle Verschlüsselungsalgorithmen durch Microsofts Cryptography New Generation (CNG) ersetzt, das sich an die neuesten verfügbaren Sicherheitstechnologien hält und FIPS-konform ist. Das heißt, alle MOBOTIX HUB VMS 2020 R3-Anwendungen können im FIPS-konformen Modus betrieben werden. Aus Gründen der Abwärtskompatibilität bleiben einige nicht konforme Algorithmen und Prozesse in MOBOTIX HUB VMS auch nach Version 2020 R3 erhalten, dies hat jedoch keinen Einfluss auf die Fähigkeit, das System im FIPS-konformen Modus zu betreiben.

Ist MOBOTIX HUB VMS immer FIPS-konform?

Nein. Einige nicht konforme Algorithmen und Prozesse bleiben in MOBOTIX HUB VMS erhalten. MOBOTIX HUB VMS kann jedoch so konfiguriert und betrieben werden, dass es nur die FIPS 140-2-zertifizierten Algorithmusinstanzen verwendet und daher in einem FIPS-konformen Modus betrieben wird.

Sollten Sie den FIPS 140-2-Modus aktivieren?

Bevor Sie den FIPS 140-2-Modus aktivieren, müssen Sie verstehen, ob Sie ihn benötigen oder nicht. Wenn Sie beispielsweise mit einem Netzwerk und einer Infrastruktur der US-amerikanischen oder kanadischen Regierung arbeiten und verbunden sind, ist es zwingend erforderlich, FIPS 140-2 einzuhalten und es auf Ihrem Computer für die Kommunikation gemäß dem Standard zu aktivieren. Darüber hinaus schränkt die Aktivierung des FIPS 140-2-Modus auf Ihrem Windows-Betriebssystem die Ausführung vieler Programme und Dienste ein, da danach nur noch FIPS-genehmigte Algorithmen und Dienste unterstützt werden. Daher ist es ratsam zu prüfen, ob eine Notwendigkeit besteht oder nicht.

8.1.4 Wie kann sichergestellt werden, dass MOBOTIX HUB VMS im FIPS 140-2-konformen Modus betrieben werden kann?

Um MOBOTIX HUB VMS in einem FIPS 140-2-Betriebsmodus zu betreiben, müssen Sie:

- Stellen Sie sicher, dass Integrationen von Drittanbietern auf einem FIPS-fähigen Windows-Betriebssystem ausgeführt werden können (siehe Überprüfen von Integrationen von Drittanbietern auf der Seite 84)
- Verbinden Sie Geräte so, dass ein FIPS 140-2-konformer Betriebsmodus gewährleistet ist (siehe Verbinden von Geräten: Hintergrund auf der Seite 84)
- Stellen Sie sicher, dass die Daten in der Mediendatenbank mit FIPS 140-2-kompatiblen Algorithmen verschlüsselt werden (siehe Mediendatenbank: Überlegungen zur Abwärtskompatibilität auf der Seite 85)

- Führen Sie das Windows-Betriebssystem im von FIPS 140-2 genehmigten Betriebsmodus aus. Weitere Informationen zum Aktivieren von FIPS finden Sie auf der Microsoft-Website.

8.1.5 Überlegungen zum Upgrade

Für ein Upgrade auf MOBOTIX HUB VMS 2020 R3 für den Betrieb im FIPS-konformen Modus ist ein eindeutiger Upgrade-Prozess erforderlich. Dieser Upgrade-Vorgang ist nur für bestehende MOBOTIX HUB-VMS-Benutzer erforderlich, die in einem FIPS-konformen Modus arbeiten müssen.

Der Upgrade-Prozess hängt davon ab, von welcher Version von MOBOTIX HUB VMS Sie ein Upgrade durchführen.

Empfohlener Upgrade-Prozess für Kunden, die MOBOTIX HUB VMS ausführen

1. Starten Sie die Untersuchung, ob Integrationen von Drittanbietern FIPS 140-2-konform sind (siehe Überprüfen von Integrationen von Drittanbietern auf der Seite 84).
2. Bereiten Sie Geräteverbindungen so vor, dass sie FIPS 140-2-konform sind (siehe Verbinden von Geräten: Hintergrund auf der Seite 84).
3. Exportieren von Aufzeichnungen, die mit MOBOTIX HUB VMS-Versionen erstellt wurden, die älter als 2017 R2 sind (siehe Mediendatenbank: Überlegungen zur Abwärtskompatibilität auf der Seite 85).
   Dies gilt für Kunden, die Aufzeichnungen zu einem beliebigen Zeitpunkt verschlüsselt oder signiert haben.
4. Deaktivieren Sie FIPS auf dem Windows-Betriebssystem (siehe FIPS-Gruppenrichtlinie auf dem Windows-Betriebssystem auf der Seite 90).
5. Installieren Sie MOBOTIX HUB VMS2020 R3 (siehe Installieren von MOBOTIX HUB VMS2020 R3 auf der Seite 90).
6. Aktualisieren Sie die Aufzeichnungen in der Mediendatenbank, die mit MOBOTIX HUB VMS 2019 R3 oder früher erstellt wurden (siehe Mediendatenbank: Überlegungen zur Abwärtskompatibilität auf der Seite 85).
7. Aktualisieren Sie die Verschlüsselung von Kennwörtern für die Hardwareerkennung (siehe Verschlüsseln von Kennwörtern für die Hardwareerkennung auf der Seite 90).
8. Aktivieren Sie FIPS auf dem Windows-Betriebssystem und starten Sie alle Computer neu, auf denen MOBOTIX HUB VMS installiert ist.

Aktivieren Sie FIPS erst, wenn alle Computer im MOBOTIX HUB-VMS-Netzwerk, einschließlich der MOBOTIX HUB Smart Client-Workstations, für FIPS vorbereitet sind.

8.1.6 Überprüfen Sie Integrationen von Drittanbietern

Wenn eine Integration nicht FIPS 140-2-konform ist, kann sie nicht auf einem Windows-Betriebssystem ausgeführt werden, auf dem das FIPS-Gruppenrichtlinienflag aktiviert ist.
Darüber hinaus müssen Integrationen, die auf die Funktionsliste in der Lizenz zugreifen, aufgrund von Änderungen, die am MIP SDK in Bezug auf FIPS vorgenommen wurden, neu kompiliert werden.
Um sicherzustellen, dass die Integrationen nach dem Upgrade auf MOBOTIX HUB VMS 2020 R3 weiterhin funktionieren, müssen Sie folgende Schritte ausführen:

- Machen Sie eine Bestandsaufnahme aller Ihrer Integrationen zu MOBOTIX HUB VMS
- Wenden Sie sich an die Anbieter dieser Integrationen und fragen Sie, ob die Integrationen FIPS 140-2-konform sind und ob sie davon ausgehen, dass die Integrationen aufgrund der MIP SDK-Updates geändert werden müssen
- Bereitstellen der FIPS 140-2-konformen Integrationen auf MOBOTIX HUB-VMS, nachdem das VMS aktualisiert wurde

8.1.7 Geräte verbinden: Hintergrund

Wenn Sie MOBOTIX HUB VMS in einem FIPS-konformen Modus betreiben möchten, müssen Sie sicherstellen, dass die Treiber und damit die Kommunikation zu den Geräten ebenfalls FIPS-konform sind.
Die MOBOTIX MOBOTIX HUB VMS-Gerätetreiber können FIPS 140-2-konform sein, da sie so konfiguriert und betrieben werden können, dass sie nur FIPS 140-2-konforme Algorithmusinstanzen verwenden. Nur bestimmte Treiber in einer bestimmten Konfiguration sind FIPS 140-2-konform. In dieser speziellen FIPS 140-2-Konfiguration ist der Treiber in der Lage, auf konforme Weise mit Geräten zu kommunizieren. Die Geräte müssen mehrere Voraussetzungen erfüllen, um diese Kommunikation akzeptieren zu können. Darüber hinaus muss das FIPS-Gruppenrichtlinienflag in Windows auf dem Server aktiviert sein, auf dem der Aufzeichnungsserver installiert ist. Wenn das FIPS-Gruppenrichtlinienflag aktiviert ist, werden die FIPS 140-2-fähigen Treiber im konformen Modus ausgeführt und verwenden keine nicht genehmigten kryptografischen Primitive. Die Treiber verwenden die Algorithmen, die nur für gesicherte Kommunikationskanäle verwendet werden.

Anforderungen an die Gerätekonnektivität

MOBOTIX HUB VMS ist garantiert und kann den FIPS 140-2-konformen Betriebsmodus erzwingen, wenn die folgenden Kriterien erfüllt sind:

- Geräte verwenden nur Treiber aus der Liste (Unterstützte Treiber auf der Seite 91), um eine Verbindung zu MOBOTIX HUB VMS herzustellen
  Diese Liste zeigt Treiber, die die Einhaltung sicherstellen und erzwingen können.
- Geräte verwenden Device Pack Version 11.1 oder höher
  Treiber aus den älteren Treibergerätepaketen können keine FIPS 140-2-konforme Verbindung garantieren.
- Die Geräte werden über HTTPS und entweder über das Secure Real-Time Transport Protocol (SRTP) oder das Real Time Streaming Protocol (RTSP) über HTTPS für den Videostream verbunden

  Treibermodule können die FIPS 140-2-Konformität einer Verbindung über HTTP nicht garantieren. Die Verbindung kann konform sein, aber es gibt keine Garantie dafür, dass sie tatsächlich konform ist.

- Auf dem Computer, auf dem der Aufzeichnungsserver ausgeführt wird, muss das FIPS-Gruppenrichtlinienflag in Windows aktiviert sein

Auswirkungen des Betriebs im FIPS 140-2-konformen Modus

Beim Betrieb im FIPS 140-2-kompatiblen Modus sind einige Treiber nicht verfügbar. Treiber, die als FIPS 140-2 aufgeführt sind, können möglicherweise keine Verbindung zu Geräten herstellen, die die Geräteanforderungen nicht erfüllen.

Ein Treiber ist FIPS 140-2-konform und die Kommunikation mit dem Gerät ist FIPS 140-2-konform, wenn der FIPS 140-2-fähige Treiber:

- Arbeitet in einer Umgebung, in der die FIPS-Gruppenrichtlinie aktiviert ist
- Ist mit einem Gerät verbunden, das die Geräteanforderungen erfüllt (siehe Geräteanforderungen auf Seite 91)
- Ist ordnungsgemäß konfiguriert (siehe Konfigurieren des Geräts und des Treibers für FIPS 140-2 auf Seite 92)

Wenn eine der Anforderungen für den FIPS 140-2-kompatiblen Modus nicht erfüllt ist, gibt es keine Garantie für die FIPS 140-2-Konformität des Treibers oder der Kommunikation mit dem Gerät. Siehe Treiber und FIPS 140-2 auf Seite 91 für weitere Informationen.

Geräte, die über MOBOTIX Open Network Bridge laufen

Bei der Ausführung auf einem Computer, auf dem das FIPS-Gruppenrichtlinien-Flag in Windows aktiviert ist, verwendet die MOBOTIX Open Network Bridge SHA265 zum Verschlüsseln der Kommunikation. Auf einem Computer, auf dem FIPS nicht aktiviert ist, können Sie entweder MD5 oder SHA165 für die Verschlüsselung auswählen.

8.1.8 Mediendatenbank: Überlegungen zur Abwärtskompatibilität

Es ist möglich, Aufzeichnungen von mehreren verschiedenen Versionen von MOBOTIX HUB VMS gleichzeitig im selben Speicher zu haben.

Daten, die signiert oder verschlüsselt sind, müssen folgende Voraussetzungen erfüllen:

- Wird aus dem Speicher exportiert, wenn er mit MOBOTIX HUB VMS Version 2017 R1 oder älter aufgezeichnet wurde
  Der Datenexport erfolgt über den MOBOTIX HUB Smart Client.
- Upgrade, wenn es mit MOBOTIX HUB VMS Version 2017 R2 oder höher aufgezeichnet wurde
  Die Datenaktualisierung erfolgt in Zusammenarbeit mit dem MOBOTIX-Support unter Verwendung eines vom MOBOTIX-Support bereitgestellten Medienkonvertierungstools.

Das FIPS-Gruppenrichtlinienflag muss auf dem Windows-Betriebssystem deaktiviert sein, damit das Medienkonvertierungstool ausgeführt werden kann.

Der Aufzeichnungsserver muss auch gestoppt werden, während das Medienkonvertierungstool ausgeführt wird, und es werden keine Aufzeichnungen erstellt, während das Tool ausgeführt wird.

Medien-Upgrade abhängig von der MOBOTIX HUB VMS-Version

- Daten, die mit MOBOTIX HUB VMS Version 2017 R1 und früher aufgezeichnet wurden
  Verschlüsselte Mediendaten, die mit MOBOTIX HUB VMS 2017 R1 und früher aufgezeichnet wurden, sind bei Aktivierung von FIPS nicht verfügbar, selbst wenn das Medienkonvertierungstool ausgeführt wurde.
  Exportieren Sie die Mediendaten, die mit MOBOTIX HUB VMS 2017 R1 und früher aufgezeichnet wurden, um offline darauf zuzugreifen.
  Siehe Upgrade der Mediendatenbank-Daten: MOBOTIX HUB VMS 2017 R1 und früher auf der Seite 88.
- Datenaufzeichnung mit MOBOTIX HUB VMS Version 2017 R2 bis 2019 R3

Mediendaten, die mit den MOBOTIX HUB VMS-Versionen 2017 R2 bis 2019 R3 aufgezeichnet wurden, werden nicht automatisch erneut verschlüsselt. Eine Umrüstung kann zeitaufwendig sein und sollte im Vorfeld geplant werden.
Wenn Sie ältere Daten aktualisieren möchten, um FIPS-konforme Algorithmen zu verwenden, wenden Sie sich an den MOBOTIX-Support, um das Medienkonvertierungstool zu erhalten.
Weitere Hinweise finden Sie unter Upgrade der Mediendatenbank: MOBOTIX HUB VMS 2017 R2 zu MOBOTIX HUB VMS 2019 R3 auf Seite 88.

- Mit MOBOTIX HUB VMS Version 2020 R1 oder 2020 R2 aufgezeichnete Daten
  Mediendaten, die mit MOBOTIX HUB VMS 2020 R1 oder 2020 R2 aufgezeichnet wurden, werden automatisch mit FIPS 140-2-konformen Algorithmen erneut verschlüsselt, wenn der Aufzeichnungsserver nach einem Upgrade gestartet wird. Siehe Upgrade der Mediendatenbank: MOBOTIX HUB VMS 2020 R1 oder MOBOTIX HUB VMS 2020 R2 auf Seite 90.

Details zum Medien-Upgrade

Die erneute Verschlüsselung der Daten mit einem Aufzeichnungsserver mit FIPS-konformen Algorithmen ist ein zentraler Bestandteil des Upgrade-Prozesses. Daher variiert der Upgrade-Prozess je nach Version von MOBOTIX HUB VMS, die für die Aufzeichnung dieser Daten verwendet wird.

Daten, die mit				
	2017 R1 und früher	**2017 R2 - 2019 R3**	**2020 R1 - 2020 R2**	**2020 R3 und höher**
Änderungen	Mit DES verschlüsselte Daten Signieren mit MD5 Kennwörter: Cookie in der Speicherung CONFIG.XML Passwort _a & _b in der Tabelle CONFIG. XML-Dateien DES-verschlüsselt	Mit AES verschlüsselte Daten Signieren mit SHA	Passwortliste im Speicher CONFIG.XML Passwörter in der Passwortliste sind DES-verschlüsselt	Passwörter in der Passwortliste werden mit AES verschlüsselt Für die Aktualisierung der Tabelle CONFIG steht ein Medienkonvertierungstool zur Verfügung. XML's von Password _a & _b, um die aktualisierte Passwortliste zu verwenden
FIPS deaktiviert	Alle Funktionen funktionieren wie erwartet			
FIPS aktiviertSignierte Daten	Signierte Daten können wiedergegeben werden Überprüfen, ob das Signieren während des Exports fehlgeschlagen ist	Signierte Daten können wiedergegeben werden Überprüfen der Signierung während des Exports		

<table>
<tr><th colspan="5">Daten, die mit</th></tr>
<tr><th></th><th>2017 R1 und früher</th><th>2017 R2 - 2019 R3</th><th>2020 R1 - 2020 R2</th><th>2020 R3 und höher</th></tr>
<tr><td>FIPS aktiviertVerschlüsselte Daten Das Medienkonvertierungstool wird nicht ausgeführt</td><td colspan="3">Der Speicher bleibt offline
(Der Speicher kann offline bleiben, wenn die Verschlüsselung für den Speicher aktiviert wurde.)</td><td>Alle Funktionen funktionieren wie erwartet</td></tr>
<tr><td>FIPS aktiviertKeine Verschlüsselung Das Medienkonvertierungstool wird nicht ausgeführt</td><td colspan="4">Alle Funktionen funktionieren wie erwartet</td></tr>
<tr><td>Das Medienkonvertierungstool wurde ausgeführt</td><td colspan="2">Die Ausführung des Medienkonvertierungstools kann viel Zeit in Anspruch nehmen, da die Tabelle CONFIG aktualisiert wird. XML's für alle verschlüsselten Tabellen</td><td>Das Medienkonvertierungstool wird schnell ausgeführt, da es nur den Speicher aktualisieren muss CONFIG.XML</td><td>Das Medienkonvertierungstool läuft schnell, da kein Update erforderlich ist</td></tr>
<tr><td>FIPS aktiviertVerschlüsselte Daten Das Medienkonvertierungstool wurde ausgeführt</td><td>Verschlüsselte Daten sind nicht verfügbar Verbindung bei der Wiedergabe verloren Die Archivierung mit "Auf Keyframes reduzieren" archiviert die gesamte GoP</td><td colspan="3">Verschlüsselte Daten können wiedergegeben werden
Die Archivierung mit Auf Keyframes reduzieren funktioniert wie erwartet</td></tr>
<tr><td>FIPS aktiviertKeine</td><td colspan="4">Alle Funktionen funktionieren wie erwartet</td></tr>
</table>

Daten, die mit				
	2017 R1 und früher	**2017 R2 - 2019 R3**	**2020 R1 - 2020 R2**	**2020 R3 und höher**
Verschlüsselung Keine Unterschrift Das Medienkonvertierungstool wurde ausgeführt				

Upgrade der Mediendatenbank-Daten: MOBOTIX HUB VMS 2017 R1 und früher

Wenn Sie MOBOTIX HUB VMS Version 2017 R1 oder früher ausführen oder wenn Sie Daten signiert oder verschlüsselt haben, die mit diesen Versionen aufgezeichnet wurden, werden die Aufzeichnungen mit Algorithmen verschlüsselt, die nach dem FIPS 140-2-Standard nicht als sicher gelten.
Es ist nicht möglich, von einem Computer aus auf diese Aufzeichnungen zuzugreifen, auf dem das FIPS-Gruppenrichtlinienflag aktiviert ist.
Dies hat zur Folge, dass die Mediendatenbank an einen Ort exportiert werden muss, an dem sie noch erreichbar ist.

Upgrade der Mediendatenbank: MOBOTIX HUB VMS 2017 R2 auf MOBOTIX HUB VMS 2019 R3

Wenn Sie eine Version von MOBOTIX HUB VMS zwischen MOBOTIX HUB VMS 2017 R2 und MOBOTIX HUB VMS 2019 R3 ausführen und die Verschlüsselung zu einem beliebigen Zeitpunkt in der Mediendatenbank aktiviert wurde, müssen Sie eine der folgenden Optionen ausführen, um auf diese Aufzeichnungen zugreifen zu können.

Für beide Optionen ist die Verwendung des Medienkonvertierungstools erforderlich. Der Aufzeichnungsserver muss gestoppt werden, während das Medienkonvertierungstool ausgeführt wird, und es werden keine Aufzeichnungen erstellt, während das Tool ausgeführt wird. Siehe Was ist das Medienkonvertierungstool? auf Seite 89 für weitere Informationen.

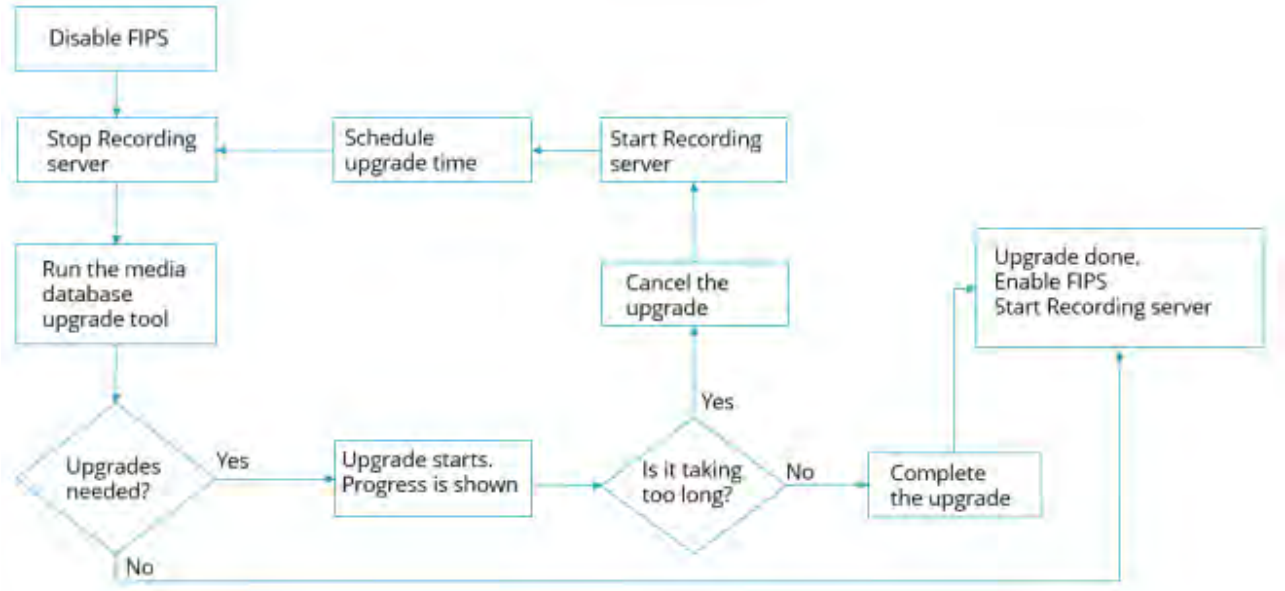
- Möglichkeit 1
  Verwenden Sie diese Option, um sofort in einer FIPS-Umgebung arbeiten zu können und wenn Sie eine lange Aufbewahrungszeit haben. Der Zeitaufwand, der zum Ausführen des Medienkonvertierungstools erforderlich ist, kann erheblich sein.
  1. Führen Sie ein Upgrade von MOBOTIX HUB VMS auf 2020 R3 durch.
  2. Wenn FIPS auf dem Windows-Betriebssystem deaktiviert ist, führen Sie das Medienkonvertierungstool aus, das vom MOBOTIX-Support bereitgestellt wird.
  3. Aktivieren Sie das FIPS-Gruppenrichtlinienflag auf dem Windows-Betriebssystem.
- Möglichkeit 2
  Verwenden Sie diese Option, wenn der Betrieb in einer FIPS-Umgebung warten kann, wenn Sie eine kurze Aufbewahrungszeit haben und wenn Sie das Medienkonvertierungstool mit weniger Daten ausführen.
  1. Führen Sie ein Upgrade von MOBOTIX HUB VMS auf 2020 R3 durch.

2. Führen Sie die MOBOTIX HUB-VMS während der Aufbewahrungszeit aus, ohne FIPS auf dem Windows-Betriebssystem zu aktivieren.
3. Führen Sie das Medienkonvertierungstool aus, um sicherzustellen, dass alle Daten FIPS-konform konvertiert werden.
4. Aktivieren Sie das FIPS-Gruppenrichtlinienflag auf dem Windows-Betriebssystem.

Was ist das Medienkonvertierungstool?

Das Medienkonvertierungstool ist ein eigenständiges PowerShell-Skript, das in der Quelle bereitgestellt wird. Es ist nicht Teil einer Installation.
Es darf nur über den MOBOTIX-Support an Kunden verteilt werden.
Es kann den gesamten Speicher in großen Mengen konvertieren oder auf einem bestimmten Speicher ausgeführt werden.
Fortschrittsindikatoren zeigen an, wie weit das Tool gekommen ist.
Wenn die Konvertierung zu lange dauert, können Sie den Auftrag abbrechen und ohne aktiviertes FIPS fortfahren.
Das Medienkonvertierungstool konvertiert verschlüsselte Anmeldeinformationen in vorhandenen Medientabellendateien in das neueste Format, das FIPS-kompatibel ist.
Das Medienkonvertierungstool ändert die Verschlüsselung der Videodaten selbst nicht. Wenn die Videodaten mit einem nicht konformen Algorithmus (DES) verschlüsselt sind, werden die aktualisierten Tabellen geladen, aber auf das Video kann im FIPS-kompatiblen Modus nicht zugegriffen werden.
Das Medienkonvertierungstool konvertiert und prüft, ob alle Tabellen FIPS-konforme Algorithmen verwenden. Genehmigte Tabellen werden markiert, um zu verhindern, dass sie erneut vom Medienkonvertierungstool überprüft werden.
Nach dem Ausführen des Medienkonvertierungstools kann der MOBOTIX HUB VMS 2020 R3 Tabellen im FIPS-konformen Modus laden.

Arbeitsablauf des Medienkonvertierungstools



Upgrade der Mediendatenbank: MOBOTIX HUB VMS 2020 R1 oder MOBOTIX HUB VMS 2020 R2

Wenn Sie MOBOTIX HUB VMS Version 2020 R1 oder MOBOTIX HUB VMS 2020 R2 ausführen, werden Mediendaten, die mit einer dieser Versionen aufgezeichnet wurden, während des Upgrades des Aufzeichnungsservers automatisch mit FIPS 140-2-konformen Algorithmen erneut verschlüsselt.

8.1.9 FIPS-Gruppenrichtlinie auf dem Windows-Betriebssystem

Der FIPS-Betriebsmodus wird mit dem FIPS-Gruppenrichtlinienflag auf dem Windows-Betriebssystem aktiviert und deaktiviert. Auf der Microsoft-Website finden Sie Informationen zum Aktivieren und Deaktivieren von FIPS.
Vor dem Upgrade müssen Sie das FIPS-Gruppenrichtlinienflag auf allen Computern deaktivieren, die Teil der MOBOTIX HUB-VMS sind, einschließlich des Computers, auf dem der SQL Server gehostet wird, und aller MOBOTIX HUB Smart Client-Arbeitsstationen.
Es gibt zwei Gründe, warum das FIPS-Gruppenrichtlinienflag auf allen Computern in den MOBOTIX HUB-VMS deaktiviert werden muss, bevor Sie ein Upgrade durchführen:

- Während des Upgrades werden Daten, die mit nicht genehmigten FIPS-Algorithmen verschlüsselt wurden, mit genehmigten Algorithmen erneut verschlüsselt. Um die Entschlüsselung auf dem Windows-Betriebssystem ausführen zu können, muss das Flag "FIPS-Gruppenrichtlinie" deaktiviert sein.
- Wenn das FIPS-Gruppenrichtlinien-Flag in Windows aktiviert ist, können Sie die MOBOTIX HUB-VMS erst verwenden, wenn alle Komponenten aktualisiert wurden. Beispielsweise kann ein 2020 R2 MOBOTIX HUB Smart Client nicht mit einem 2020 R3 Management Server kommunizieren, wenn sich der Management Server auf einem Computer befindet, auf dem das FIPS-Gruppenrichtlinienflag aktiviert ist.

FIPS-Gruppenrichtlinie und MOBOTIX Federated Architecture

Wenn eine Site in einer MOBOTIX-Verbundarchitektur mit dem in Windows aktivierten FIPS-Gruppenrichtlinien-Flag betrieben werden muss, müssen alle Sites auch mit dem in Windows aktivierten FIPS-Gruppenrichtlinien-Flag betrieben werden.
In der Konsequenz muss die gesamte MOBOTIX Federated Architecture-Installation auf die Version 2020 R3 aktualisiert werden.

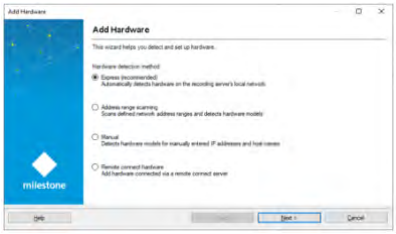
8.1.10 MOBOTIX HUB VMS2020 R3 installieren

Wenn Sie ein Upgrade durchführen, überprüft das MOBOTIX HUB VMS-Installationsprogramm die FIPS-Sicherheitsrichtlinie und verhindert, dass das Upgrade gestartet wird, wenn FIPS aktiviert ist.

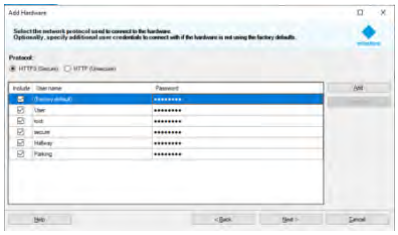
8.1.11 Verschlüsseln von Kennwörtern für die Hardwareerkennung

Die Kennwörter für die Hardwareerkennung müssen nach dem Upgrade auf MOBOTIX HUB VMS 2020 R3 aktualisiert werden.
Die Verschlüsselung der Hardware-Erkennungskennwörter wird während des Upgrades von einer früheren Version von MOBOTIX HUB VMS nicht aktualisiert. Diese Kennwörter können jedoch nicht gelesen werden, wenn das FIPS-Gruppenrichtlinienflag in Windows aktiviert ist.
Sie müssen eine Konvertierung dieser Kennwörter auslösen, bevor Sie FIPS aktivieren. Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass das FIPS-Gruppenrichtlinienflag in Windows deaktiviert ist.
2. Öffnen Sie im MOBOTIX HUB Management Client den Assistenten zum Hinzufügen von Hardware.



3. Wählen Sie die Erkennungsmethode aus, um die Hardwareerkennungsseite zu öffnen.



Dies löst die erneute Verschlüsselung der Hardware-Erkennungskennwörter mit FIPS-konformen Algorithmen aus.

Die Anmeldeinformationen werden jetzt mit FIPS-konformen Algorithmen verschlüsselt.

8.2 Treiber und FIPS 140-2

In diesem Abschnitt wird FIPS 140-2 und die Konfiguration und Verwendung der MOBOTIX-Treiber für den Betrieb im FIPS 140-2-kompatiblen Modus erläutert.

8.2.1 Anforderungen für den FIPS 140-2-konformen Modus

Die MOBOTIX MOBOTIX HUB VMS-Gerätetreiber können FIPS 140-2-konform sein, da sie so konfiguriert und betrieben werden können, dass sie nur FIPS 140-2-konforme Algorithmusinstanzen verwenden. Nur bestimmte Treiber in einer bestimmten Konfiguration sind FIPS 140-2-konform. In dieser speziellen FIPS 140-2-Konfiguration ist der Treiber in der Lage, auf konforme Weise mit Geräten zu kommunizieren. Die Geräte müssen mehrere Voraussetzungen erfüllen, um diese Kommunikation akzeptieren zu können. Darüber hinaus muss das FIPS-Gruppenrichtlinienflag in Windows auf dem Server aktiviert sein, auf dem der Aufzeichnungsserver installiert ist. Wenn das FIPS-Gruppenrichtlinienflag aktiviert ist, werden die FIPS 140-2-fähigen Treiber im konformen Modus ausgeführt und verwenden keine nicht genehmigten kryptografischen Primitive. Die Treiber verwenden die Algorithmen, die nur für gesicherte Kommunikationskanäle verwendet werden.

Anforderungen an das Gerät

Damit ein Gerät mit einem Treiber kommunizieren kann, der im FIPS 140-2-kompatiblen Modus ausgeführt wird, muss es alle folgenden Anforderungen erfüllen:

- Das Gerät muss die HTTPS-Kommunikation mit mindestens einer FIPS 140-2-kompatiblen Cipher Suite unterstützen (Beispiele finden Sie unter Beispiel für FIPS 140-2-konforme Cipher Suites auf Seite 96)
- Das Gerät muss RTSP über HTTPS (Tunneling RTSP und RTP over HTTP) mit HTTP Basic Authentication (RFC2068 Abschnitt 11.1) oder HTTP Digest Authentication (RFC2069, RFC7616) unterstützen
  oder
  Das Gerät muss Medien-Streaming mit SRTP und RTSPS (RFC3711) unterstützen.

Unterstützte Treiber

Derzeit ist nur eine Teilmenge der Treiber FIPS 140-2-konform. Diese Treiber unterstützen die Kommunikation über einen gesicherten Kanal für alle verfügbaren Funktionen.

Achse 1 Kanal	Achse 1 Kanal PTZ	Achse 2 Kanal	Achse 3 Kanal
Achse 4 Kanal	Achse 8 Kanal	Achse 11 Kanal	Achse 12 Kanal
Achsen-Audio	Bosch PTZ	Bosch 1 Kanal	Bosch 2 Kanal
Bosch 3 Kanal	Bosch 16 Kanal	Bosch X20XF	Bosch X40XF
Canon 1 Kanal	Canon 1-Kanal-PTZ	Canon VBM	Canon VBM 40

Canon VBS	Canon VBS ohne Ptz	TVI-Decoder für digitale Schranken	Hanwha Generika
ONVIF	ONVIF16	Universal	Universell 16 Kanäle
Universell 64 Kanäle	VideoPush (Englisch)		

Die Treiber in der Tabelle können bei ordnungsgemäßer Konfiguration im FIPS 140-2-kompatiblen Modus ausgeführt werden. Diese Liste ist nicht endgültig und kann in Zukunft erweitert werden. Einige Treiber sind FIPS 140-2-konform mit eingeschränkten Funktionen. In den folgenden Abschnitten finden Sie Informationen zur Konfiguration und zu den Einschränkungen.
Der FIPS 140-2-konforme Modus für Treiber ist seit Device Pack 11.1 verfügbar.

8.2.2 Auswirkungen der Ausführung im FIPS 140-2-kompatiblen Modus

Beim Betrieb im FIPS 140-2-kompatiblen Modus sind einige Treiber nicht verfügbar. Treiber, die als FIPS 140-2 aufgeführt sind, können möglicherweise keine Verbindung zu Geräten herstellen, die die Geräteanforderungen nicht erfüllen.
Ein Treiber ist FIPS 140-2-konform und die Kommunikation mit dem Gerät ist FIPS 140-2-konform, wenn der FIPS 140-2-fähige Treiber:

- Arbeitet in einer Umgebung, in der die FIPS-Gruppenrichtlinie aktiviert ist
- Ist mit einem Gerät verbunden, das die Geräteanforderungen erfüllt (siehe Geräteanforderungen auf der Seite 91)
- Ist ordnungsgemäß konfiguriert (siehe So konfigurieren Sie das Gerät und den Treiber für FIPS 140-2 auf Seite 92)

Wenn eine der Anforderungen für den FIPS 140-2-kompatiblen Modus nicht erfüllt ist, gibt es keine Garantie für die FIPS 140-2-Konformität des Treibers oder der Kommunikation mit dem Gerät.

8.2.3 Konfigurieren des Geräts und des Treibers für FIPS 140-2

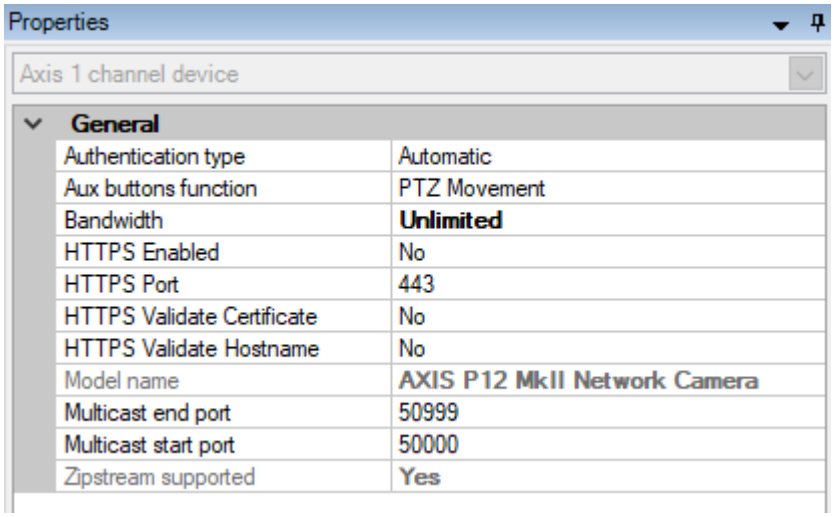
Die Konfiguration des Geräts und des Treibers für den FIPS 140-2-kompatiblen Modus ist geräte- und treiberspezifisch. Es gelten einige allgemeine Richtlinien:

- Die Kommunikationskanäle zwischen dem Treiber und dem Gerät müssen sicher und verschlüsselt sein (HTTPS, RTSP über HTTPS, SRTP).
- Das Gerät muss für den Betrieb über sichere Kanäle konfiguriert sein.
- Der Treiber und das Gerät müssen so konfiguriert sein, dass sie sichere Kanäle für die Kommunikation in MOBOTIX HUB VMS verwenden.

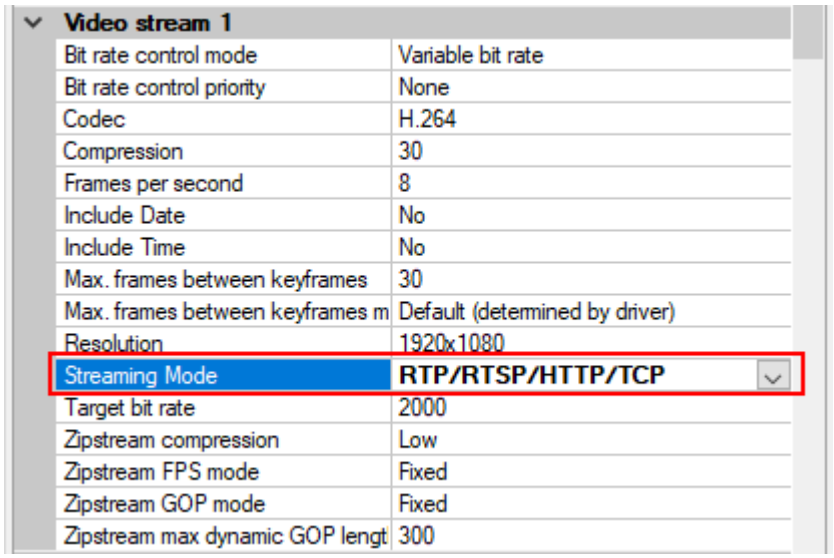
Treiber für Achsen

Gehen Sie wie folgt vor:

- Legen Sie HTTPS aktiviert auf Ja fest.
- Legen Sie HTTPS Validate Certificate auf Yes fest.
- Legen Sie HTTPS Validate Hostname auf Ja fest.

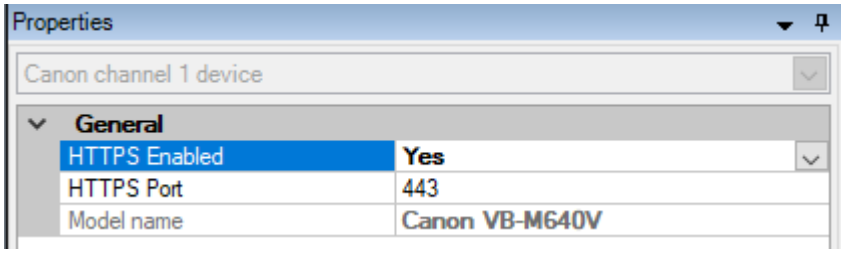


- Legen Sie für jeden aktivierten Medienkanal und Medienstream den Streamingmodus auf RTP/RTSP/HTTP/TCP fest.

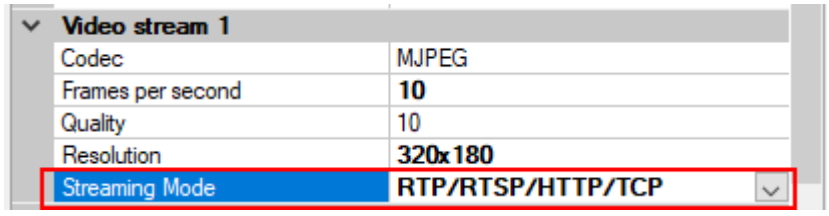


Canon-Treiber

- Legen Sie HTTPS aktiviert auf Ja fest.



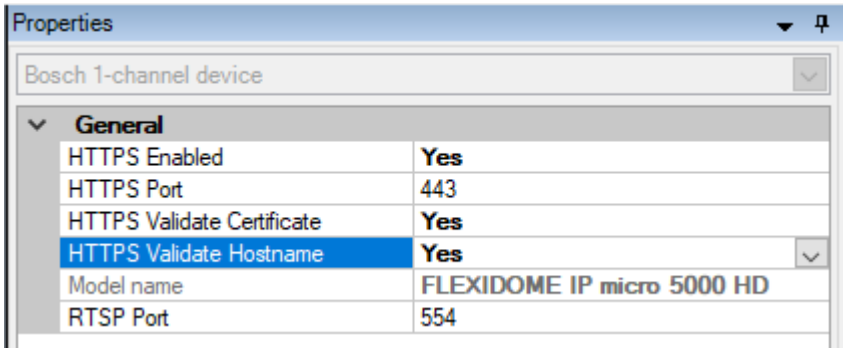
- Legen Sie für jeden aktivierten Medienkanal und Medienstream den Streamingmodus auf RTP/RTSP/HTTP/TCP fest.



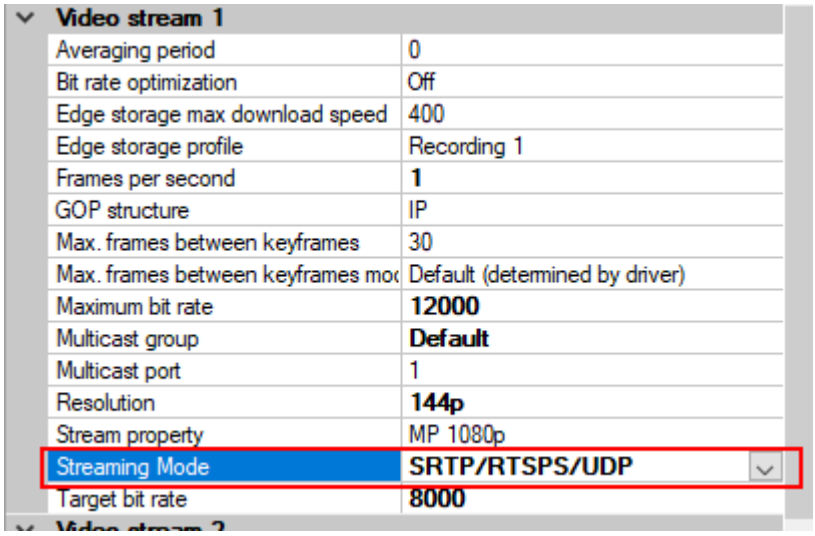
Bosch-Treiber

Gehen Sie wie folgt vor:

- Legen Sie HTTPS aktiviert auf Ja fest.
- Legen Sie HTTPS Validate Certificate auf Yes fest.
- Legen Sie HTTPS Validate Hostname auf Ja fest.

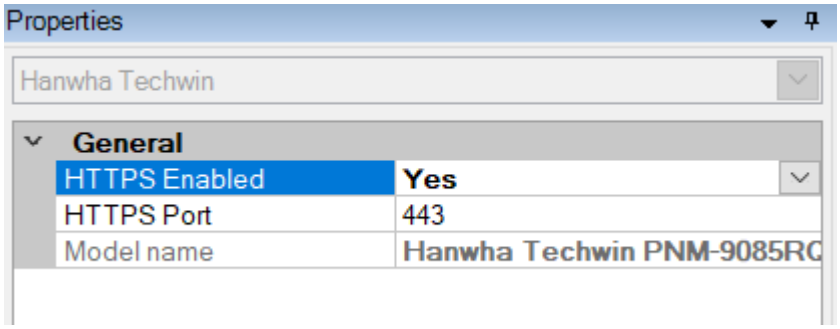


- Legen Sie für jeden aktivierten Medienkanal und Medienstream den Streamingmodus auf eine der folgenden Optionen fest:
  - RTP/RTSP/HTTP/TCP
  - SRTP/RTSPS/UDP
  - SRT/RTSPS/UDP Multicast

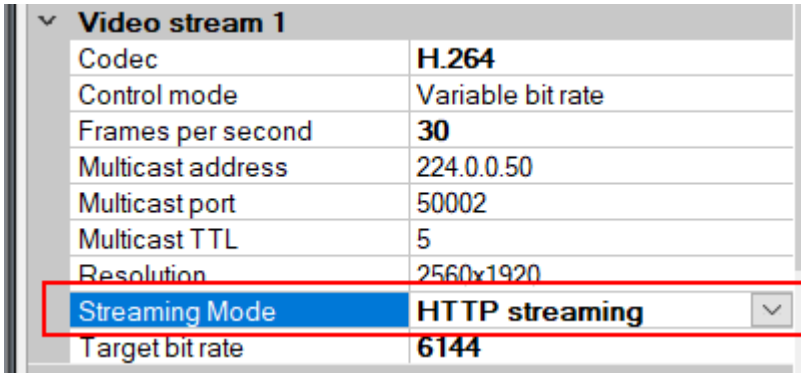


Hanwha Fahrer

- Legen Sie HTTPS aktiviert auf Ja fest.



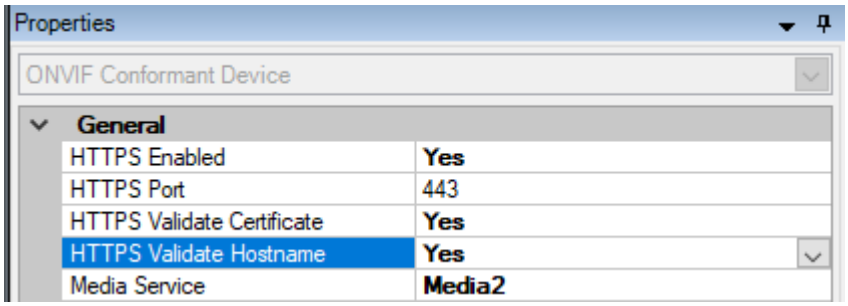
- Legen Sie für jeden aktivierten Medienkanal und Medienstream den Streamingmodus auf HTTP-Streaming fest.



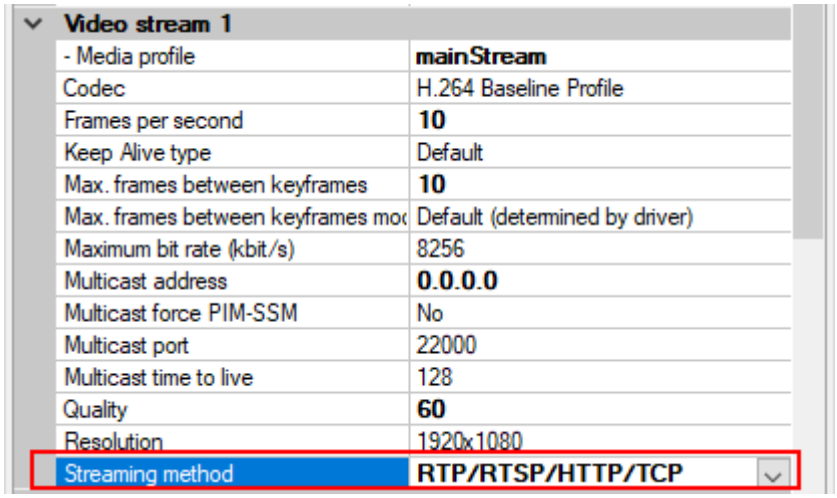
ONVIF-Treiber

Gehen Sie wie folgt vor:

- Legen Sie HTTPS aktiviert auf Ja fest.
- Legen Sie HTTPS Validate Certificate auf Yes fest.
- Legen Sie HTTPS Validate Hostname auf Ja fest.



- Legen Sie für jeden aktivierten Medienkanal und Medienstream die Streamingmethode auf RTP/RTSP/HTTP/TCP fest.

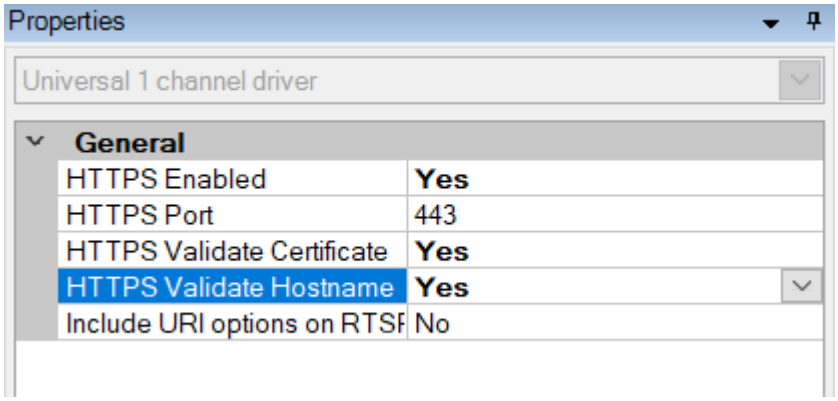


- Der Audio-Rückkanal (Audioausgang, Gerätelautsprecher) darf nicht verwendet werden, wenn der Treiber im FIPS 140-2-kompatiblen Modus ausgeführt wird.

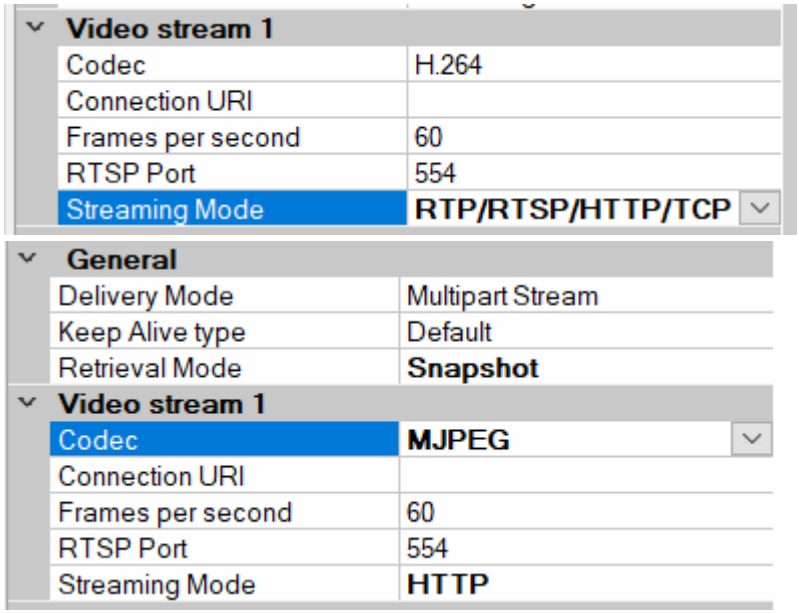
Universelle Treiber

Gehen Sie wie folgt vor:

- Legen Sie HTTPS aktiviert auf Ja fest.
- Legen Sie HTTPS Validate Certificate auf Yes fest.
- Legen Sie HTTPS Validate Hostname auf Ja fest.



- Legen Sie für jeden aktivierten Medienkanal und Medienstream den Streamingmodus auf RTP/RTSP/HTTP/TCP oder HTTP fest, je nachdem, ob der Streaming- oder der Snapshot-Abrufmodus verwendet wird.



VideoPush-Treiber

Es ist keine spezielle Konfiguration erforderlich. Durch Aktivieren der FIPS-Gruppenrichtlinie wird der Treiber gezwungen, mit dem MOBOTIX HUB Mobile Server auf FIPS 140-2-konforme Weise zu kommunizieren.

8.2.4 Beispiel für FIPS 140-2-konforme Cipher Suites

0x1302	TLS_AES_256_GCM_SHA384
0x1303	TLS_CHACHA20_POLY1305_SHA256
0x1301	TLS_AES_128_GCM_SHA256
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
0x00A3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
0x009F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
0x00A2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256

0x009E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
0xC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
0x006A	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
0x0040	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
0x00AD	TLS_RSA_PSK_WITH_AES_256_GCM_SHA384
0x00AB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384
0x009D	TLS_RSA_WITH_AES_256_GCM_SHA384
0x00A9	TLS_PSK_WITH_AES_256_GCM_SHA384
0x00AC	TLS_RSA_PSK_WITH_AES_128_GCM_SHA256
0x00AA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256
0x009C	TLS_RSA_WITH_AES_128_GCM_SHA256
0x00A8	TLS_PSK_WITH_AES_128_GCM_SHA256
0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256
0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x002F	TLS_RSA_WITH_AES_128_CBC_SHA

Diese Liste erhebt keinen Anspruch auf Vollständigkeit. Es gibt andere Cipher Suites, die FIPS 140-2-konform sind. Diese Liste dient nur als Beispiel für Cipher Suites, die mit FIPS 140-2 kompatibel sind.

8.3 FIPS-Ressourcen

1. FIPS 140-2 Sicherheitsanforderungen für kryptografische Module
   https://csrc.nist.gov/publications/detail/fips/140/2/final
2. Anhang A: Zugelassene Sicherheitsfunktionen für FIPS PUB 140-2
   https://csrc.nist.gov/CSRC/media/Publications/fips/140/2/final/documents/fips1402annexa.pdf
3. Richtlinien für die Auswahl, Konfiguration und Verwendung von TLS-Implementierungen (Transport Layer Security)
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
4. Implementierungsleitfaden für FIPS 140-2 und das Validierungsprogramm für kryptografische Module
   https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf
5. Microsofts Ansatz zur FIPS 140-2-Validierung
   https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation
6. Übersicht über TLS/SSL (Schannel SSP)
   https://docs.microsoft.com/en-us/windows-server/security/tls/tls-ssl-schannel-ssp-overview
7. Cipher Suites in TLS/SSL (Schannel SSP)
   https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

8. TLS-Verschlüsselungssammlungen in Windows 10 v1903, v1909 und v2004
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-cipher-suites-in-windows-10-v1903
9. TLS Elliptische Kurven in Windows 10 Version 1607 und höher
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-elliptic-curves-in-windows-10-1607-and-later

9 Tabelle zum Produktvergleich

9.1 Produktvergleichstabelle

MOBOTIX HUB VMS umfasst die folgenden Produkte:

- MOBOTIX NABE L1
- MOBOTIX NABE L2
- MOBOTIX NABE L3
- MOBOTIX NABE L4
- MOBOTIX NABE L5

Die vollständige Funktionsliste finden Sie auf der Produktübersichtsseite auf der MOBOTIX-Website https://www.mobotix.com/en/vms/mobotix-hub

Nachfolgend finden Sie eine Liste der Hauptunterschiede zwischen den Produkten:

Name	MOBOTIX NABE L1	MOBOTIX NABE L2	MOBOTIX NABE L3	MOBOTIX NABE L4	MOBOTIX NABE L5
Standorte pro SLC	1	1	Mehrere Standorte	Mehrere Standorte	Mehrere Standorte
Aufzeichnungsserver pro SLC	1	1	Frei	Frei	Frei
Hardware-Geräte pro Aufzeichnungsserver	8	48	Frei	Frei	Frei
MOBOTIX Verbindung™	-	Remote-Standort	Remote-Standort	Remote-Standort	Zentraler/entfernter Standort
MOBOTIX Verbundarchitektur™	-	-	-	Remote-Standort	Zentraler/entfernter Standort
Failover des Aufzeichnungsservers	-	-	-	Kalt- und Heiß-Standby	Kalt- und Heiß-Standby
Remoteverbindungsdienste	-	-	-	-	✓
Unterstützung von Edge-Speicher	-	-	✓	✓	✓
Mehrstufige Videospeicherung	Live-Datenbanken + 1 Archiv	Live-Datenbanken + 1 Archiv	Live-Datenbanken + 1 Archiv	Live-Datenbanken + uneingeschränkte Archive	Live-Datenbanken + uneingeschränkte Archive
SNMP-Benachrichtigung	-	-	-	✓	✓
Zeitgesteuerte Benutzerzugriffsrechte	-	-	-	-	✓
Reduzieren Sie die Bildrate (Grooming)	-	-	-	✓	✓
Verschlüsselung von Videodaten (Aufzeichnungsserver)	-	-	-	✓	✓
Signieren von Datenbanken (Aufzeichnungsserver)	-	-	-	✓	✓

Name	MOBOTIX NABE L1	MOBOTIX NABE L2	MOBOTIX NABE L3	MOBOTIX NABE L4	MOBOTIX NABE L5
PTZ-Prioritätsstufen	1	1	3	32000	32000
Erweitertes PTZ (PTZ-Sitzung reservieren und vom XProtect Smart Client aus patrouillieren)	-	-	-	✓	✓
Beweissicherung	-	-	-	-	✓
Lesezeichen-Funktion	-	-	Nur manuell	Manuell und regelbasiert	Manuell und regelbasiert
Live-Multi-Streaming oder Multicasting / Adaptives Streaming	-	-	-	✓	✓
Direktes Streaming	-	-	-	✓	✓
Allgemeine Sicherheit	Benutzerrechte des Clients	Benutzerrechte des Clients	Benutzerrechte des Clients	Benutzerrechte des Clients	Benutzerrechte des Kunden/ Benutzerrechte des Administrators
MOBOTIX HUB Management Client-Profile	-	-	-	-	✓
MOBOTIX HUB Smart Client-Profile	-	-	3	3	Frei
MOBOTIX HUB Smart Wall	-	-	-	wahlfrei	✓
Systemmonitor	-	-	-	✓	✓
Intelligente Karte	-	-	-	✓	✓
Zweistufige Verifizierung	-	-	-	-	✓
DLNA-Unterstützung	-	✓	✓	✓	✓
Maskierung von Privatsphären	-	✓	✓	✓	✓
Verwaltung von Geräte-Passwörtern			✓	✓	✓

10 Anhang

10.1 Anhang 1 – Ressourcen

Beschreibt die Mindestanforderungen an ein Videoüberwachungssystem. Siehe auch verwandte Normen.

1. Axis Communications: Leitfaden zum Sichern
2. Bosch Sicherheitssysteme: Bosch IP-Video- und Datensicherheitsleitfaden
3. Britische Norm BS EN 62676-1-1: Videoüberwachungssysteme für den Einsatz in Sicherheitsanwendungen, Teil 1-1: Systemanforderungen – Allgemeines
4. Beschreibt die Mindestanforderungen an ein Videoüberwachungssystem. Siehe auch verwandte Normen.
5. Center for Internet Security: Die CIS-kritischen Sicherheitskontrollen für eine effektive Cyber-Abwehr
6. Cloud Security Alliance (CSA) und die Cloud Controls Matrix
7. Defense Information Systems Agency (DISA): Security Technical Implementation Guides (STIGs)
8. Internet Engineering Task Force (IETF), mehrere Referenzen
9. ISO/IEC 15048 Informationstechnik - Sicherheitstechniken - Bewertungskriterien für die IT-Sicherheit
10. ISO/IEC 31000, Risikomanagement – Grundsätze und Richtlinien
11. ISO/IEC 31010, Risikomanagement – Risikobewertungstechniken
12. ISO 27001: Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Informationssicherheitsmanagementsysteme — Anforderungen
13. ISO 27002: Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Kontrollen der Informationssicherheit
14. Leitfaden für Microsoft-Sicherheitsupdates
15. Siehe u.a. Verwalten von Sicherheitsrichtlinieneinstellungen
16. Nationales Institut für Standards und Technologie: Abteilung für Computersicherheit Ressourcenzentrum für Computersicherheit
17. Nationales Institut für Standards und Technologie: Rahmenwerk für Cybersicherheit
18. Risikomanagement-Framework für Informationssysteme und Organisationen: Ein Systemlebenszyklus-Ansatz für Sicherheit und Datenschutz
19. National Institute of Standards and Technology: Management von Informationssicherheitsrisiken
20. Nationales Institut für Standards und Technologie: Sicherheits- und Datenschutzkontrollen für föderale Informationssysteme und -organisationen SP 800-53- Revision 5
21. NIST SP 800-100 Handbuch zur Informationssicherheit: Ein Leitfaden für Manager
22. NIST SP 800-124 Richtlinien für die Verwaltung der Sicherheit mobiler Geräte im Unternehmen
23. Website des SANS Institute und der SANS Critical Security Controls
24. XProtect® Corporate – Erweitertes Sicherheitsmanagement

10.2 Anlage 2 - Akronyme

AD – Aktives Verzeichnis
CSA – Allianz für Cloud-Sicherheit
CVE – Häufige Schwachstellen und Gefährdungen
HTTP – Hypertext Transfer Protocol
HTTPS – Hypertext Transfer Protocol Sicher
IEC – Internationale Elektrotechnische Kommission
IETF – Internet Engineering Task Force
IP – Internetprotokoll
ISO – Internationale Organisation für Normung
IT – Informationstechnologie
KB – Wissensdatenbank

NIST – Nationales Institut für Standards und Technologie
RSTP – Rapid Spanning Tree Protokoll
SMTP – Einfaches Mail-Transfer-Protokoll
SSL – Sichere Socket-Schicht
STIG – Leitfaden für technische Sicherheitsinformationen
TCP – Übertragungssteuerungsprotokoll
TLS - Sicherheit der Transportschicht
UDP – Benutzer-Datagramm-Protokoll
VMS – Videomanagement-Software
VPN – Virtuelles privates Netzwerk

MOBOTIX

BeyondHumanVision

EN_08/23

MOBOTIX AG • Kaiserstrasse • D-67722 Langmeil • Tel.: +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com