MOBOTIX HUB – Hardening guide

2023 R2 - 30/V2.01_8/2023

Inhaltsverzeichnis

1 Copyright, marchi e disclaimer

Marchi

MOBOTIX HUB è un marchio registrato di MOBOTIX AG.
Microsoft e Windows sono marchi registrati di Microsoft Corporation. App Store è un marchio di servizio di Apple Inc. Android è un marchio di Google Inc.
Tutti gli altri marchi citati in questo documento sono marchi dei rispettivi proprietari.

Disconoscimento

Il presente testo è destinato esclusivamente a scopi informativi generali e nella sua preparazione è stata prestata la dovuta cura.
Qualsiasi rischio derivante dall'uso di queste informazioni è a carico del destinatario e nulla di quanto contenuto nel presente documento deve essere interpretato come costituente alcun tipo di garanzia.
MOBOTIX AG si riserva il diritto di apportare modifiche senza preavviso.
Tutti i nomi di persone e organizzazioni usati negli esempi di questo testo sono fittizi. Qualsiasi somiglianza con un'organizzazione o una persona reale, viva o morta, è puramente casuale e non intenzionale.
Questo prodotto può utilizzare software di terze parti per i quali possono essere applicati termini e condizioni specifici. In questo caso, è possibile trovare ulteriori informazioni nel *file 3rd_party_software_terms_and_conditions.txt* si trova nella cartella di installazione del sistema MOBOTIX HUB.

2 Introduzione

Questa guida descrive le misure di sicurezza e di protezione fisica e le best practice che possono aiutare a proteggere il software di gestione video (VMS) XProtect dagli attacchi informatici. Ciò include considerazioni sulla sicurezza per l'hardware e il software di server, client e componenti dei dispositivi di rete di un sistema di videosorveglianza.

Questa guida adotta i controlli standard di sicurezza e privacy e li associa a ciascuna delle raccomandazioni. Ciò rende questa guida una risorsa per la conformità ai requisiti di sicurezza del settore e della pubblica amministrazione e della rete.

2.1 Che cos'è l'"Hardening"?

Lo sviluppo e l'implementazione di misure di sicurezza e best practice è noto come "hardening". L'hardening è un processo continuo di identificazione e comprensione dei rischi per la sicurezza e di adozione di misure appropriate per contrastarli. Il processo è dinamico perché le minacce e i sistemi che prendono di mira sono in continua evoluzione.

La maggior parte delle informazioni contenute in questa guida si concentra sulle impostazioni e sulle tecniche IT, ma è importante ricordare che anche la sicurezza fisica è una parte vitale della protezione avanzata. Ad esempio, è possibile utilizzare barriere fisiche per server e computer client e assicurarsi che elementi come gli involucri delle telecamere, le serrature, gli allarmi antimanomissione e i controlli di accesso siano sicuri.

Di seguito sono riportati i passaggi pratici per la protezione avanzata di un VMS:

1. Comprendere i componenti da proteggere
2. Rafforzare i componenti del sistema di sorveglianza:
    1. Rafforzamento dei server (fisici e virtuali) e dei computer e dispositivi client
    2. Rafforzare la rete6/2
    3. Rafforza le telecamere
3. Documenta e gestisci le impostazioni di sicurezza su ciascun sistema
4. Formare e investire in persone e competenze, compresa la supply chain

2.1.1 Target

Tutti in un'organizzazione devono comprendere almeno le nozioni di base sulla sicurezza della rete e del software. I tentativi di compromettere l'infrastruttura IT critica stanno diventando sempre più frequenti, quindi tutti devono prendere sul serio la protezione e la sicurezza.

Questa guida fornisce informazioni di base e avanzate per utenti finali, integratori di sistemi, consulenti e produttori di componenti.

- Le descrizioni di base forniscono informazioni generali sulla sicurezza
- Le descrizioni avanzate forniscono indicazioni specifiche per l'IT per la protezione avanzata dei prodotti VMS XProtect. Oltre al software, vengono descritte anche le considerazioni relative alla sicurezza dei componenti hardware e dei dispositivi del sistema.

2.1.2 Risorse e riferimenti

Le organizzazioni seguenti forniscono risorse e informazioni sulle procedure consigliate per la sicurezza:

- Organizzazione internazionale per la standardizzazione (ISO),
- Istituto nazionale di standard e tecnologia (NIST) degli Stati Uniti (USA)
- Linee guida per l'implementazione tecnica della sicurezza (STIGs) della Defense Information Systems Administration (DISA) degli Stati Uniti

- Centro per la sicurezza su Internet
- Istituto SANS
- Alleanza per la sicurezza del cloud (CSA)
- Task Force per l'ingegneria di Internet (IETF)
- Standard britannici

Inoltre, i produttori di fotocamere forniscono indicazioni per i loro dispositivi hardware.

Vedere Appendice 1 - Risorse a pagina 98 per un elenco di riferimenti e Appendice 2 - Acronimi a pagina 98 per un elenco di acronimi.

Questa guida sfrutta gli standard e le specifiche nazionali, internazionali e di settore. In particolare, si fa riferimento alla pubblicazione speciale 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) del National Institute of Standards and Technology del Dipartimento del Commercio degli Stati Uniti.

Il documento NIST è scritto per il governo federale degli Stati Uniti; Tuttavia, è generalmente accettato nel settore della sicurezza come l'attuale insieme di best practice.

Questa guida fa riferimento a ulteriori informazioni sui controlli di sicurezza. Le linee guida possono essere confrontate con i requisiti specifici del settore e con altri standard e quadri internazionali di sicurezza e gestione dei rischi. Ad esempio, l'attuale NIST Cybersecurity Framework utilizza SP 800-53 Rev4 come base per i controlli e le linee guida. Un altro esempio è l'Appendice H in SP 800-53 Rev 4, che contiene un riferimento ai requisiti ISO/IEC 15408, come i Common Criteria.

2.1.3 Componenti hardware e del dispositivo

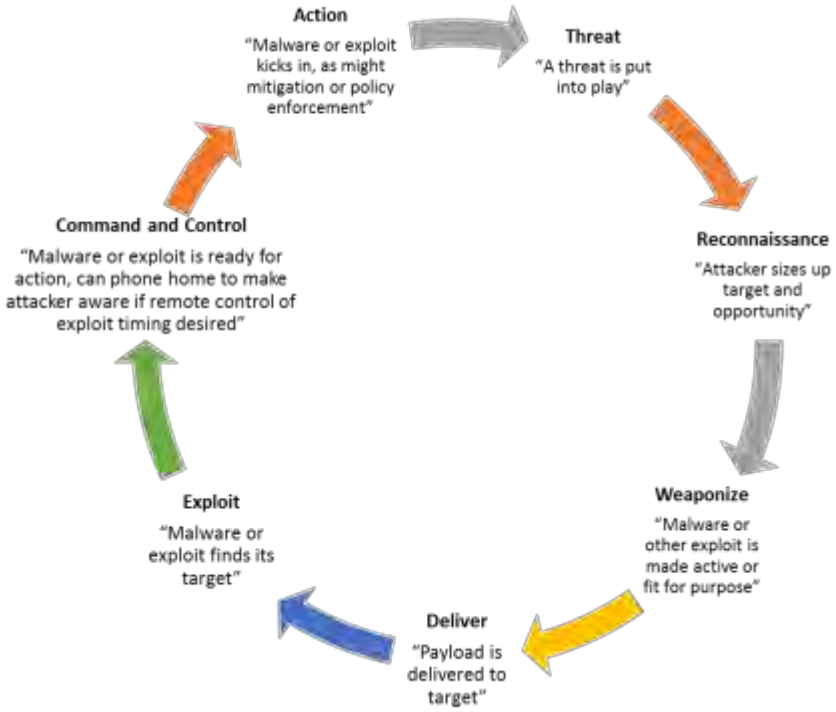
Oltre al software, i componenti di un'installazione di MOBOTIX HUB VMS includono in genere dispositivi hardware, quali:

- Telecamere
- Encoder
- Prodotti per il networking
- Sistemi di stoccaggio
- Server e computer client (macchine fisiche o virtuali)
- Dispositivi mobili, come gli smartphone

È importante includere i dispositivi hardware nei tuoi sforzi per rafforzare l'installazione di MOBOTIX HUB VMS. Ad esempio, le fotocamere hanno spesso password predefinite. Alcuni produttori pubblicano queste password online in modo che siano facili da trovare per i clienti. Sfortunatamente, ciò significa che le password sono disponibili anche per gli aggressori.
Questo documento fornisce raccomandazioni per i dispositivi hardware.

2.2 Minacce informatiche e rischi informatici

Esistono molte fonti di minacce per un VMS, tra cui attacchi o guasti aziendali, tecnologici, di processo e umani. Le minacce si verificano nell'arco di un ciclo di vita. Il ciclo di vita della minaccia, a volte chiamato "cyber kill" o "cyber threat chain", è stato sviluppato per descrivere le fasi delle minacce informatiche avanzate.
Ogni fase del ciclo di vita della minaccia richiede tempo. La quantità di tempo per ogni fase è specifica per la minaccia, o la combinazione di minacce, e i suoi attori e obiettivi.



Il ciclo di vita delle minacce è importante per la valutazione dei rischi perché mostra dove è possibile mitigare le minacce. L'obiettivo è ridurre il numero di vulnerabilità e affrontarle il prima possibile. Ad esempio, scoraggiare un utente malintenzionato che sta sondando un sistema alla ricerca di vulnerabilità può eliminare una minaccia.
La protezione avanzata mette in atto azioni che mitigano le minacce per ogni fase del ciclo di vita delle minacce. Ad esempio, durante la fase di ricognizione un utente malintenzionato esegue la scansione per trovare le porte aperte e determinare lo stato dei servizi correlati alla rete e al VMS. Per mitigare questo problema, le linee guida per la protezione avanzata consistono nel chiudere le porte di sistema non necessarie nelle macchine virtuali dell'hub MOBOTIX e nelle configurazioni di Windows.
Il processo di valutazione dei rischi e delle minacce comprende le seguenti fasi:

- Identificare i rischi per le informazioni e la sicurezza
- Valuta e assegna priorità ai rischi
- Implementare politiche, procedure e soluzioni tecniche per mitigare questi rischi

Il processo generale di valutazione dei rischi e delle minacce e l'implementazione dei controlli di sicurezza sono definiti framework di gestione dei rischi. Questo documento fa riferimento ai controlli di sicurezza e privacy del NIST e ad altre pubblicazioni sui framework di gestione del rischio.

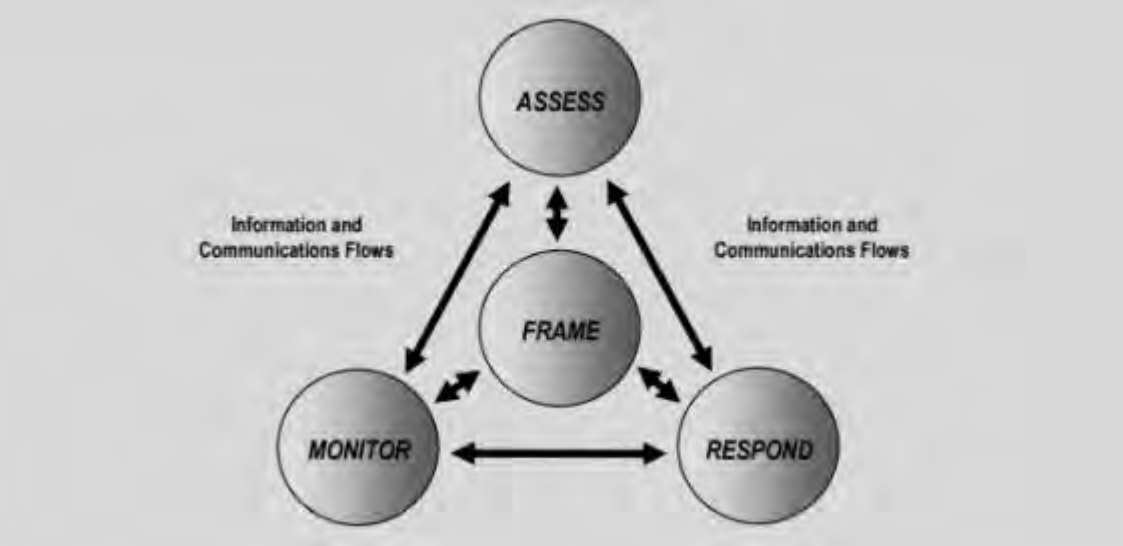
2.2.1 Framework di gestione del rischio informatico

I controlli di sicurezza e privacy in SP 800-53 Revisione 4 (http://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf) fanno parte di un quadro generale di gestione del rischio del NIST. Il documento NIST SP800-39 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf) è una guida all'applicazione di un framework di gestione del rischio. SP800-36 è un documento fondamentale per il NIST Cybersecurity Framework, descritto in Cybersecurity Framework (http://www.nist.gov/cyberframework/).
Le cifre qui riportate mostrano:

- Una panoramica del processo di gestione del rischio. Esso mostra un approccio globale di alto livello.
- Gestione del rischio a livello aziendale, tenendo conto di considerazioni strategiche e tattiche.

ciclo di vita di un framework di gestione dei rischi e i documenti NIST che forniscono dettagli per ciascuna delle fasi del ciclo di vita.

I controlli di sicurezza e privacy rappresentano azioni e raccomandazioni specifiche da implementare nell'ambito di un processo di gestione dei rischi. È importante che il processo includa la valutazione dell'organizzazione, i requisiti specifici di una determinata distribuzione e l'aggregazione di queste attività in un piano di sicurezza. SP 800-18 Revisione 1 (http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf) fornisce riferimenti per piani di sicurezza dettagliati.



Visione ad alto livello della gestione del rischio (SP 800-39, pagina 8 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

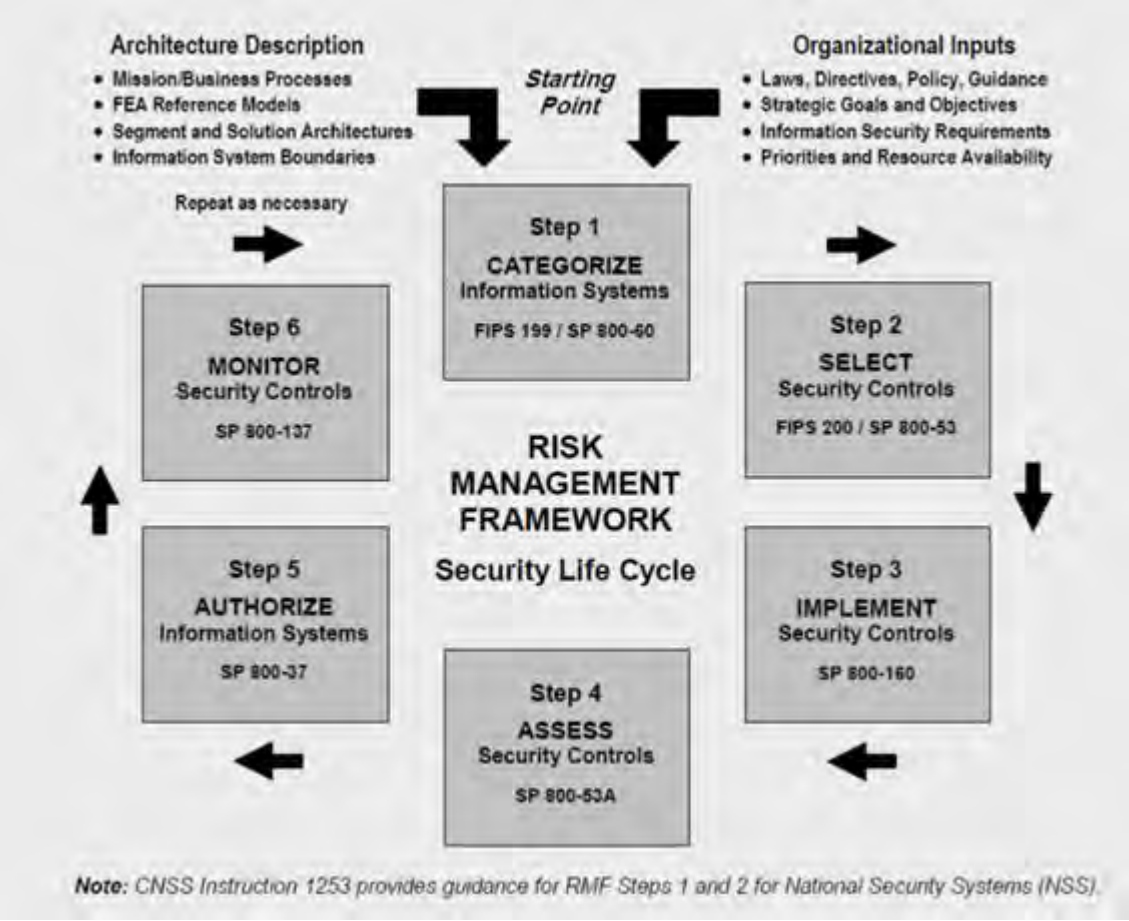
Il processo è interattivo e le risposte e i loro risultati sono iterativi. Le minacce alla sicurezza, i rischi, le risposte e i risultati sono dinamici e adattabili, e di conseguenza deve farlo anche un piano di sicurezza.

Questo diagramma mostra come un framework di gestione dei rischi considera i sistemi IT, i processi aziendali e l'organizzazione nel suo complesso per trovare un equilibrio per il piano di sicurezza.

Equilibrio tra sicurezza e obiettivi aziendali (SP 800-39, pagina 9 (http://csrc.nist.gov/publications/nistpubs/800-39/sp800-39-final.pdf))

Quando si rafforza un sistema, si bilancia l'impatto sulla produttività aziendale e sull'usabilità per motivi di sicurezza e, viceversa, nel contesto dei servizi forniti. Le linee guida sulla sicurezza non sono isolate da altre attività aziendali e IT.

Ad esempio, quando un utente immette la password in modo errato in tre tentativi consecutivi, la password viene bloccata e non può accedere al sistema. Il sistema è protetto da attacchi di forza bruta, ma l'utente sfortunato non può utilizzare il dispositivo per svolgere il proprio lavoro. Una politica di password complesse che richiede password di 30 caratteri e la modifica delle password ogni 30 giorni è una best practice, ma è anche difficile da usare.



Esempio di quadro di gestione dei rischi (SP 800-53 Rev 5, pagina 8 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final))

Per documentare il suo quadro di gestione del rischio, il NIST ha prodotto diverse pubblicazioni speciali. Include i seguenti componenti:

1. Categorizzazione (identificazione del livello di rischio)
2. Selezione dei controlli di sicurezza e privacy
3. Implementazione
4. Valutazione dell'efficacia dei controlli di sicurezza
5. Creazione di un profilo di sicurezza del sistema migliorato e della cosiddetta autorità di operare (ATO)
6. Monitoraggio e valutazione attraverso le iterazioni

framework di gestione dei rischi consente di inserire un piano di sicurezza e linee guida in un contesto di sicurezza.

2.3 Componenti del sistema di tempra

Per rafforzare i componenti del sistema, è necessario modificare le configurazioni per ridurre il rischio di un attacco riuscito. Gli aggressori cercano un modo per entrare e cercare vulnerabilità nelle parti esposte del sistema. I sistemi di sorveglianza possono coinvolgere 100 o addirittura 1000 componenti. Il mancato fissaggio di un componente può compromettere il sistema.

La necessità di mantenere le informazioni di configurazione viene talvolta trascurata. MOBOTIX HUB VMS offre funzionalità per la gestione delle configurazioni, ma le organizzazioni devono disporre di una policy e di un processo e impegnarsi a svolgere il lavoro.

La protezione avanzata richiede che le tue conoscenze sulla sicurezza siano aggiornate:

- Prestare attenzione ai problemi che interessano il software e l'hardware, inclusi sistemi operativi, dispositivi mobili, fotocamere, dispositivi di archiviazione e dispositivi di rete. Stabilire un punto di contatto per tutti i componenti del sistema. Idealmente, utilizzare le procedure di segnalazione per tenere traccia di bug e vulnerabilità per tutti i componenti.
- Tieniti aggiornato sulle vulnerabilità ed esposizioni comuni (CVE) (descritte in Vulnerabilità ed esposizioni comuni (https://cve.mitre.org/)) per tutti i componenti del sistema. Questi possono riguardare i sistemi operativi, i dispositivi che dispongono di password di manutenzione codificate e così via. Risolvi le vulnerabilità per ogni componente e avvisa i produttori delle vulnerabilità.
- Mantenere aggiornata la configurazione e la documentazione di sistema per il sistema. Utilizzare le procedure di controllo delle modifiche per il lavoro svolto e seguire le procedure consigliate per la gestione della configurazione, come descritto in SP 800-128 (https://csrc.nist.gov/publications/detail/sp/800-128/final).

Nelle sezioni seguenti vengono fornite raccomandazioni di base e avanzate per la protezione avanzata e la sicurezza per ogni componente del sistema. Le sezioni contengono anche esempi di come questi si riferiscono a specifici controlli di sicurezza descritti nella Pubblicazione Speciale NIST 800-53 Revisione 4, intitolata *Controlli di Sicurezza e Privacy per i Sistemi Informativi e le Organizzazioni Federali*.

Oltre al documento NIST, si fa riferimento alle seguenti fonti:

- Centro per la sicurezza su Internet
- SP 800-53
- Certificazione ISO 27001
- ISO/IEC 15408 (noto anche come Common Criteria, ISO/IEC 15408-1:2022 (https://www.iso.org/standard/72891.html)).

Appendice 1 - Risorse a pagina 98 in questo documento vengono forniti i consigli dei produttori di fotocamere. Questo è uno sforzo relativamente nuovo da parte dei produttori, quindi le risorse disponibili sono limitate. Per la maggior parte, le raccomandazioni possono essere generalizzate tra i produttori di fotocamere.

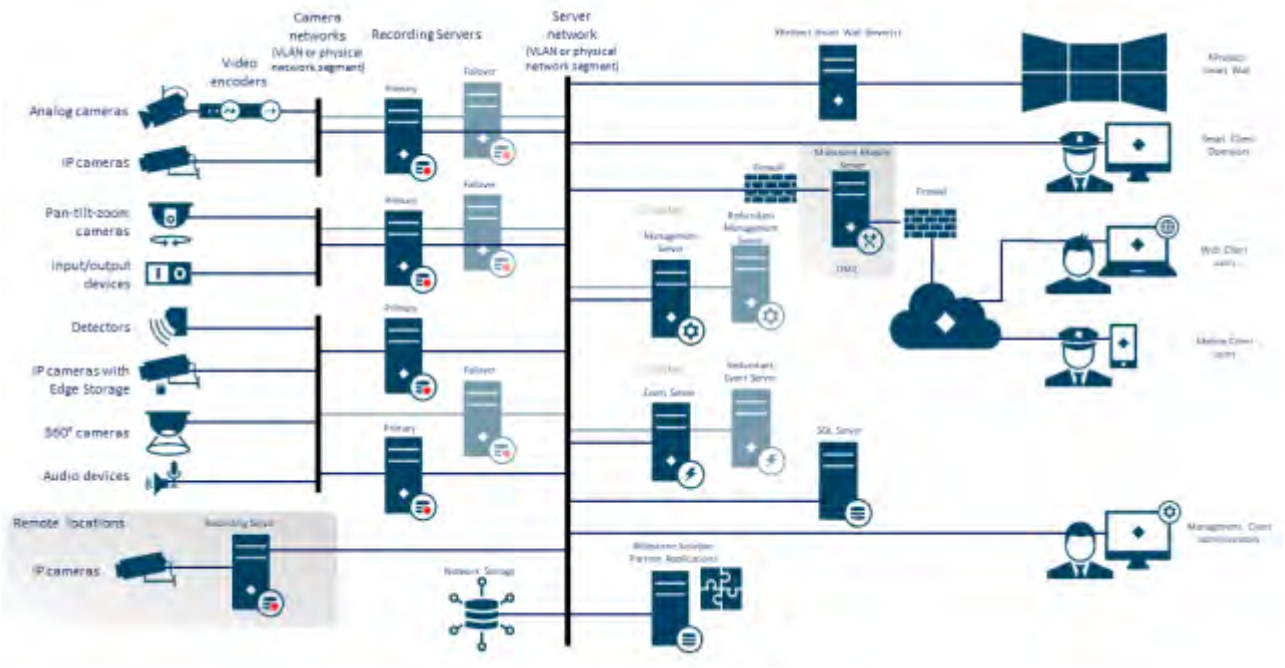
3 Configurazione generale

3.1 Panoramica

Per proteggere il sistema di sorveglianza, MOBOTIX consiglia quanto segue:

- Limitare l'accesso ai server. Conserva i server in stanze chiuse a chiave e rendi difficile l'accesso ai cavi di rete e di alimentazione da parte degli intrusi.
  (PE2 e PE3 nelle Appendici D e F in NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (PE Physical and Environment Protection).)
- Progetta un'infrastruttura di rete che utilizzi il più possibile la segmentazione della rete fisica o della VLAN.
  (SC3 nelle Appendici D e F in NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (SC System and Communication Protection).)
  - Separare la rete della telecamera dalla rete del server disponendo di due interfacce di rete in ciascun server di registrazione: una per la rete della telecamera e una per la rete del server.
  - Metti il server mobile in una "zona demilitarizzata" (DMZ) con un'interfaccia di rete per l'accesso pubblico e una per la comunicazione privata con altri server.
    (SC7 nelle Appendici D e F NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53 /rev-5/final).)
  - Si possono prendere molte precauzioni quando si tratta di una configurazione generale. Oltre ai firewall, questi includono tecniche per segmentare la rete e controllare l'accesso a server, client e applicazioni.
    (AC3, AC4, AC6, CA3, CM3, CM6, CM7, IR4, SA9, SC7, SC28, SI3, SI 8 nelle Appendici D e F in NIST SP 800-53 Rev5 (https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final) (Controlli di accesso CA), (Gestione della configurazione CM) (Risposta agli incidenti IR) (Acquisizione di sistemi e servizi SA) (Sistemi SI e integrità delle informazioni).)
- Configura il VMS con ruoli che controllano l'accesso al sistema e designano attività e responsabilità.
  (AC2, AC3, AC6, AC16, AC25, AU6, AU9, CM5, CM11, IA5, PL8, PS5, PS7, SC2, SI7, nelle Appendici D e 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).)

La figura mostra un esempio di configurazione generale.



3.1.1 Privacy fin dalla progettazione

I prodotti MOBOTIX sono progettati per fornire una comunicazione end-to-end sicura. I prodotti MOBOTIX sono progettati per proteggere la privacy e proteggere i dati. La protezione dei dati è sempre importante, ma soprattutto se si intende essere conformi al Regolamento generale sulla protezione dei dati (GDPR) nell'UE.

Ai sensi del GDPR, il titolare del trattamento dei dati personali, quando elabora tali dati, ha l'obbligo di attuare misure tecniche o organizzative volte ad attuare i principi di protezione dei dati stabiliti nel GDPR. Il GDPR si riferisce a questo come privacy by design.

Nel contesto di una telecamera di sorveglianza, un esempio rilevante di privacy by design sarebbe una funzione che consente digitalmente all'utente di limitare l'acquisizione di immagini a un determinato perimetro, impedendo alla telecamera di catturare immagini al di fuori di questo perimetro che altrimenti verrebbero catturate.

In MOBOTIX HUB, è disponibile il supporto per il mascheramento della privacy in due forme: maschere permanenti che non possono essere rimosse e maschere sollevabili che (con le giuste autorizzazioni) possono essere sollevate per rivelare l'immagine dietro la maschera.

Il titolare del trattamento ha inoltre l'obbligo di attuare misure tecniche o organizzative che, per impostazione predefinita, garantiscano il trattamento meno intrusivo della privacy dei dati personali in questione. Il GDPR si riferisce a questo come privacy per impostazione predefinita. Nel contesto di una telecamera, un esempio rilevante di privacy per impostazione predefinita potrebbe essere l'utilizzo del mascheramento della privacy per mantenere privata un'area sensibile all'interno della visuale della telecamera.

Cosa dovresti fare per garantire la privacy by design?

- Considera la risoluzione di diversi punti nella scena della fotocamera e documenta queste impostazioni Scopi diversi richiedono qualità dell'immagine diverse. Quando l'identificazione non è necessaria, è necessario scegliere la risoluzione della fotocamera e altri fattori modificabili per garantire che non vengano acquisite immagini facciali riconoscibili.
- Crittografa le tue registrazioni

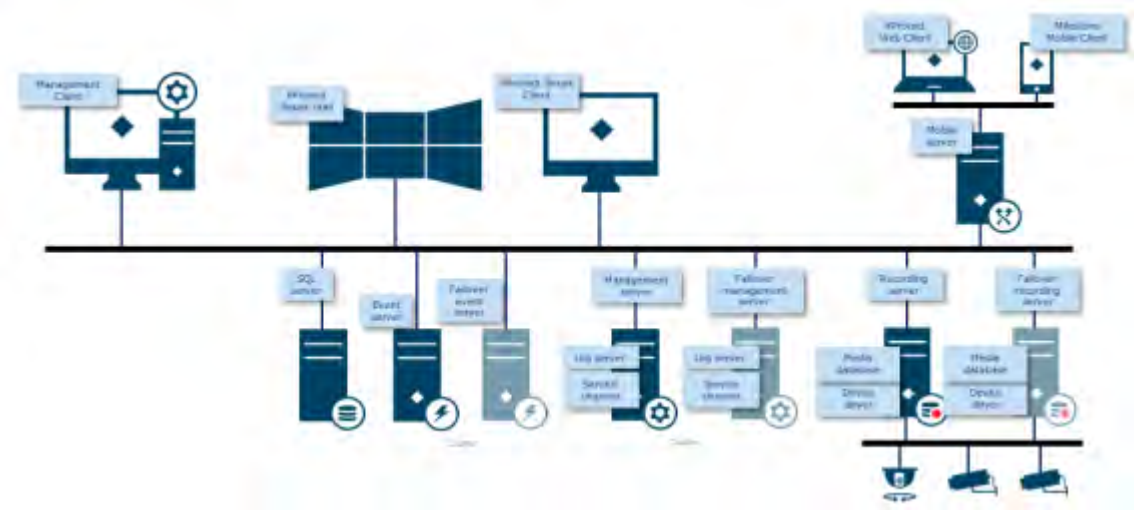
MOBOTIX consiglia di proteggere le registrazioni abilitando almeno la crittografia Light sulla memoria e sugli archivi dei server di registrazione. MOBOTIX utilizza l'algoritmo AES-256 per la crittografia. Quando si seleziona Crittografia leggera, viene crittografata solo una parte della registrazione. Quando si seleziona Crittografia avanzata, l'intera registrazione viene crittografata.

- Proteggi la rete
  MOBOTIX consiglia di selezionare telecamere che supportano HTTPS. Si consiglia di impostare le telecamere su VLAN separate e di utilizzare HTTPS per la comunicazione tra telecamera e server di registrazione.
  Si consiglia di utilizzare gli Smart Client MOBOTIX HUB e gli Smart Wall MOBOTIX HUB sulla stessa VLAN dei server.
  Utilizzare una rete crittografata VPN o simile se si utilizza Smart Client o Smart Wall da una postazione remota.
- Abilitare e documentare il tempo di conservazione previsto
  Ai sensi dell'articolo 4, paragrafo 1, lettera e), del GDPR, le registrazioni non devono essere conservate più a lungo del necessario per gli scopi specifici per i quali sono state effettuate. MOBOTIX consiglia di impostare il tempo di conservazione in base alle leggi e ai requisiti regionali e, in ogni caso, di impostare il tempo di conservazione a un massimo di 30 giorni.
- Esportazioni sicure
  MOBOTIX consiglia di consentire l'accesso alla funzionalità di esportazione solo a un gruppo selezionato di utenti che necessitano di questa autorizzazione.
  MOBOTIX consiglia inoltre di modificare il profilo Smart Client per consentire l'esportazione solo in formato MOBOTIX HUB con crittografia abilitata. Le esportazioni AVI e JPEG non dovrebbero essere consentite, perché non possono essere rese sicure. Ciò rende l'esportazione di qualsiasi materiale di prova protetta da password, crittografata e firmata digitalmente, assicurando che il materiale forense sia autentico, non manomesso e visualizzato solo dal destinatario autorizzato.
- Abilita il mascheramento della privacy: permanente o sollevabile
  Utilizza il mascheramento della privacy per eliminare la sorveglianza di aree irrilevanti per il tuo obiettivo di sorveglianza.
  MOBOTIX consiglia di impostare una maschera di sfocatura sollevabile per le aree sensibili e nei luoghi in cui l'identificazione delle persone non è consentita. Creare quindi un secondo ruolo che possa autorizzare il sollevamento della maschera.
- Limitare i diritti di accesso con i ruoli
  Applicare il principio del privilegio minimo (PoLP).
  MOBOTIX consiglia di consentire l'accesso alle funzionalità solo a un gruppo selezionato di utenti che necessitano di questa autorizzazione. Per impostazione predefinita, solo l'amministratore di sistema può accedere al sistema ed eseguire le attività. Tutti i nuovi ruoli e utenti creati non hanno accesso ad alcuna funzione fino a quando non vengono configurati deliberatamente da un amministratore.
  Imposta le autorizzazioni per tutte le funzionalità, tra cui: visualizzazione di video e registrazioni in diretta, ascolto dell'audio, accesso ai metadati, controllo delle telecamere PTZ, accesso e configurazione di Smart Wall, rimozione delle maschere per la privacy, utilizzo delle esportazioni, salvataggio di snapshot e così via.
  Concedere l'accesso solo alle telecamere a cui l'operatore specifico deve accedere e limitare completamente l'accesso ai video, all'audio e ai metadati registrati per gli operatori oppure concedere l'accesso solo al video, all'audio o ai metadati registrati nelle ultime ore o meno.

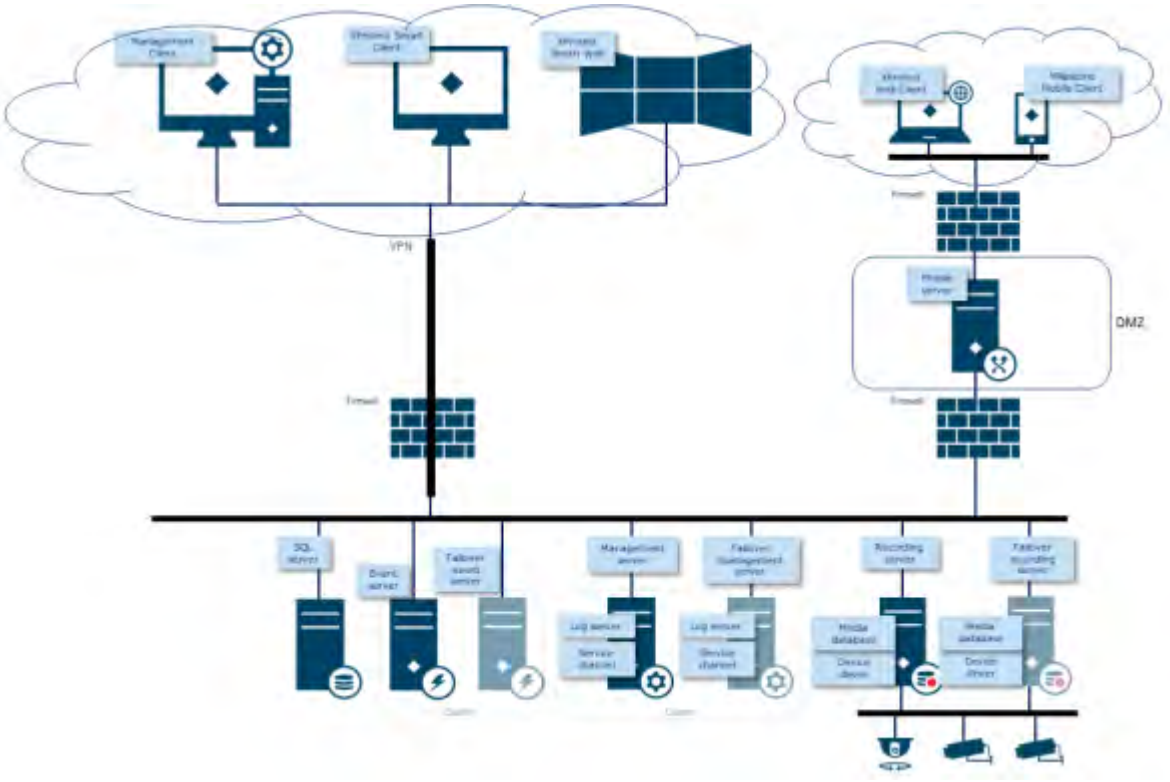
Valutare e rivedere regolarmente i ruoli e le responsabilità di operatori, investigatori, amministratori di sistema e altri soggetti con accesso al sistema. Il principio del privilegio minimo è ancora valido?

- Abilitare e utilizzare la verifica in due passaggi
  MOBOTIX consiglia di specificare un ulteriore passaggio di accesso per gli utenti di MOBOTIX HUB Mobile o MOBOTIX HUB Web Client abilitando la verifica in due passaggi.
- Limitare le autorizzazioni di amministratore
  MOBOTIX consiglia di limitare il numero di utenti che dispongono di un ruolo di amministratore. Se è necessario creare più ruoli di amministratore, è possibile limitarne l'accesso creando ruoli di amministratore in grado di gestire solo parti selezionate del sistema, ad esempio determinati dispositivi o funzioni.
  MOBOTIX raccomanda inoltre che l'amministratore del VMS non disponga di diritti di amministratore completi sullo storage che contiene il video registrato e che l'amministratore dello storage non abbia accesso al VMS o all'amministrazione del backup.

Per motivi di sicurezza, segmentare la rete in modo che vi sia una rete client/di gestione e reti di telecamere dietro i server di registrazione:



Per una maggiore sicurezza, posizionare il server mobile in una "zona demilitarizzata" (DMZ) con un'interfaccia di rete per l'accesso pubblico e una per la comunicazione privata con altri server e utilizzare reti crittografate VPN per le connessioni esterne o per aumentare la sicurezza per le reti interne meno sicure:


VPN
DMZ

4 Server, workstation, client e applicazioni

Questa sezione fornisce indicazioni per la protezione avanzata basate su Microsoft Windows e sui servizi utilizzati da MOBOTIX HUB VMS. Ciò include:

- Il prodotto MOBOTIX HUB VMS, ad esempio MOBOTIX HUB® Corporate o MOBOTIX HUB® Enterprise in esecuzione su server Windows
- Il pacchetto di dispositivi installato sui server di registrazione
- L'hardware del server o le piattaforme virtuali, i sistemi operativi e i servizi
- I computer client per MOBOTIX HUB® Smart Client e MOBOTIX HUB® Web Client
- Dispositivi mobili e relativi sistemi operativi e applicazioni

4.1 Passaggi di base

4.1.1 Stabilire obiettivi di sorveglianza e sicurezza

Prima di implementare il VMS, MOBOTIX consiglia di stabilire gli obiettivi di sorveglianza. Definisci gli obiettivi e le aspettative relative all'acquisizione e all'utilizzo dei dati video e dei metadati correlati. Tutte le parti interessate dovrebbero comprendere gli obiettivi della sorveglianza.

Le specifiche degli obiettivi di sorveglianza possono essere trovate in altri documenti, ad esempio BS EN 62676-1-1: *Sistemi di videosorveglianza per l'uso in applicazioni di sicurezza. Requisiti di sistema. Generale.*

Quando sono presenti obiettivi di sorveglianza, è possibile stabilire gli obiettivi di sicurezza. Gli obiettivi di sicurezza supportano gli obiettivi di sorveglianza indicando gli elementi da proteggere nel VMS. Una comprensione condivisa degli obiettivi di sicurezza semplifica la protezione del VMS e il mantenimento dell'integrità dei dati.
Con gli obiettivi di sorveglianza e sicurezza in atto, è possibile affrontare più facilmente gli aspetti operativi della protezione del VMS, ad esempio come:

- Evitare che i dati vengano compromessi
- Rispondi alle minacce e agli incidenti quando si verificano, inclusi ruoli e responsabilità.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Piano di sicurezza del sistema NIST SP 800-53 PL-2
- Processo di acquisizione NIST SP 800-53 SA-4

4.1.2 Stabilire una politica di sicurezza formale e un piano di risposta

In conformità con NIST SP 800-100 Information Security Handbook: A Guide for Managers (https://csrc.nist.gov/publications/detail/sp/800-100/final), MOBOTIX consiglia di stabilire una politica di sicurezza formale e un piano di risposta che descriva il modo in cui l'organizzazione affronta i problemi di sicurezza, in termini di procedure pratiche e linee guida. Ad esempio, un criterio di sicurezza può includere:

- Una politica delle password definita dal reparto IT interno
- Controllo accessi con badge identificativi
- Restrizioni per gli smartphone dalla connessione alla rete

Adotta le policy e i piani IT esistenti se aderiscono alle best practice di sicurezza.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Politica e procedure di risposta agli incidenti NIST SP 800-53 IR-1
- Piano del programma di sicurezza delle informazioni NIST SP 800-53 PM-1

4.1.3 Utilizzare gli utenti Windows con Active Directory

Esistono due tipi di utenti in MOBOTIX HUB VMS:

- Utente di base: un account utente VMS dedicato autenticato da una combinazione di nome utente e password utilizzando una politica di password. Gli utenti di base si connettono al VMS utilizzando un Secure Socket Layer (SSL) con la sessione del protocollo di sicurezza (https://datatracker.ietf.org/wg/tls/charter/) TLS (Transport Layer) corrente per l'accesso, crittografando il contenuto del traffico e il nome utente e la password.
- Utente Windows: l'account utente è specifico di una macchina o di un dominio e viene autenticato in base all'accesso di Windows. Gli utenti Windows che si connettono al VMS possono utilizzare Microsoft Windows Challenge/Response (NTML) per l'accesso, Kerberos (vedere Autenticazione Kerberos (spiegazione) a pagina 39) o altre opzioni SSP di Microsoft (https://msdn.microsoft.com/en-us /library/windows/desktop/aa380502(v=vs.85).aspx).

MOBOTIX consiglia, quando possibile, di utilizzare gli utenti Windows in combinazione con Active Directory (AD) per autorizzare l'accesso al VMS. Ciò consente di applicare:

- Un criterio password che richiede agli utenti di modificare regolarmente la password
- Protezione di forza bruta, in modo che l'account Windows AD venga bloccato dopo una serie di tentativi di autenticazione non riusciti, sempre in linea con i criteri password dell'organizzazione
- Autenticazione a più fattori nel VMS, in particolare per gli amministratori
- Autorizzazioni basate sui ruoli, in modo da poter applicare i controlli di accesso in tutto il dominio

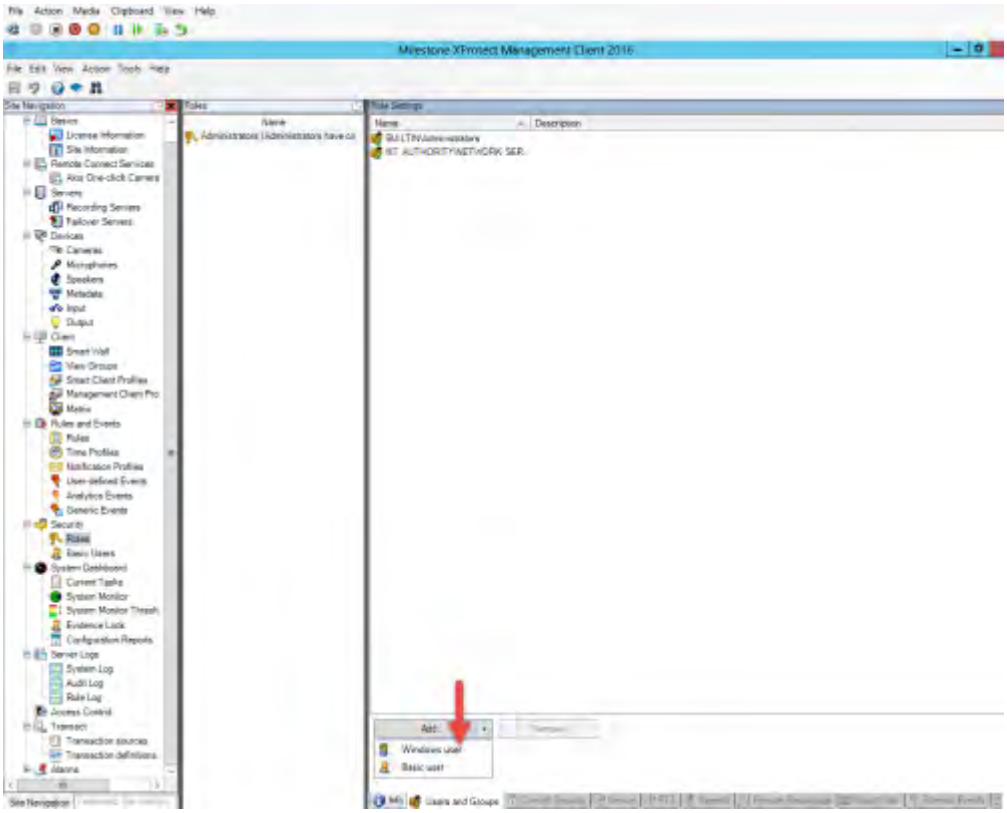
Se l'organizzazione non utilizza AD, è possibile aggiungere utenti Windows ai gruppi di lavoro sul server di gestione. I gruppi di lavoro offrono alcuni degli stessi vantaggi degli utenti Windows con AD. È possibile applicare una politica delle password, che aiuta a proteggere dagli attacchi di forza bruta, ma MOBOTIX consiglia di utilizzare un dominio Windows perché questo offre un controllo centralizzato sugli account utente.

Gli utenti Windows hanno il vantaggio di essere autenticati tramite la directory come singola fonte autorevole e servizio aziendale per la rete e non ad hoc per la loro macchina locale. In questo modo è possibile utilizzare i controlli degli accessi in base al ruolo per assegnare autorizzazioni a utenti e gruppi in modo coerente nel dominio e nei computer della rete.

Se si utilizzano utenti Windows locali, l'utente deve creare un nome utente e una password locali su ogni computer, il che è problematico dal punto di vista della sicurezza e dell'usabilità.

Per aggiungere utenti o gruppi Windows ai ruoli in Management Client, attenersi alla seguente procedura:

1. Aprire il client di gestione.
2. Espandere il nodo Sicurezza.



3. Selezionare il ruolo a cui si desidera aggiungere gli utenti Windows.
4. Nella scheda Utenti e gruppi fare clic su Aggiungi e selezionare Utente Windows. Viene visualizzata una finestra pop-up.
5. Se il nome di dominio non viene visualizzato nel campo Da questa posizione, fare clic su Località.

6. Specificare l'utente di Windows, quindi fare clic su OK.

Per verificare che l'utente Windows sia un utente AD, il nome di dominio deve essere visualizzato come prefisso, ad esempio "Domain\John".

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Impostazioni di configurazione NIST SP 800-53 CM-6
- Documentazione del sistema informativo NIST SP 800-53 SA-5
- Affidabilità NIST SP 800-53 SA-13

4.1.4 Comunicazione sicura (spiegazione)

HTTPS (Hypertext Transfer Protocol Secure) è un'estensione dell'Hypertext Transfer Protocol (HTTP) per la comunicazione sicura su una rete di computer. In HTTPS, il protocollo di comunicazione viene crittografato utilizzando Transport Layer Security (TLS) o il suo predecessore, Secure Sockets Layer (SSL).
In MOBOTIX HUB VMS, la comunicazione sicura si ottiene utilizzando SSL/TLS con crittografia asimmetrica (RSA). SSL/TLS utilizza una coppia di chiavi, una privata e una pubblica, per autenticare, proteggere e gestire le connessioni sicure.
Un'autorità di certificazione (CA) può emettere certificati per i servizi Web sui server utilizzando un certificato CA. Questo certificato contiene due chiavi, una chiave privata e una chiave pubblica. La chiave pubblica viene installata sui client di un servizio Web (client del servizio) installando un certificato pubblico. La chiave privata viene utilizzata per firmare i certificati del server che devono essere installati nel server. Ogni volta che un client del servizio chiama il servizio Web, il servizio Web invia al client il certificato del server che include la chiave pubblica. Il client del servizio può convalidare il certificato del server utilizzando il certificato CA pubblico già installato. Il client e il server possono ora utilizzare il certificato del server pubblico e privato per scambiarsi una chiave segreta e stabilire così una connessione SSL/TLS sicura.
Per ulteriori informazioni su TLS: https://en.wikipedia.org/wiki/Transport_Layer_Security

I certificati hanno una data di scadenza. MOBOTIX HUB VMS non ti avviserà quando un certificato sta per scadere. Se un certificato scade:- I client non considereranno più attendibile il server di registrazione con il certificato scaduto e quindi non potranno comunicare con esso
- I server di registrazione non considereranno più attendibile il server di gestione con il certificato scaduto e quindi non potranno comunicare con esso
- I dispositivi mobili non considereranno più attendibile il server mobile con il certificato scaduto e quindi non potranno comunicare con esso
Per rinnovare i certificati, segui i passaggi di questa guida come hai fatto quando hai creato i certificati.

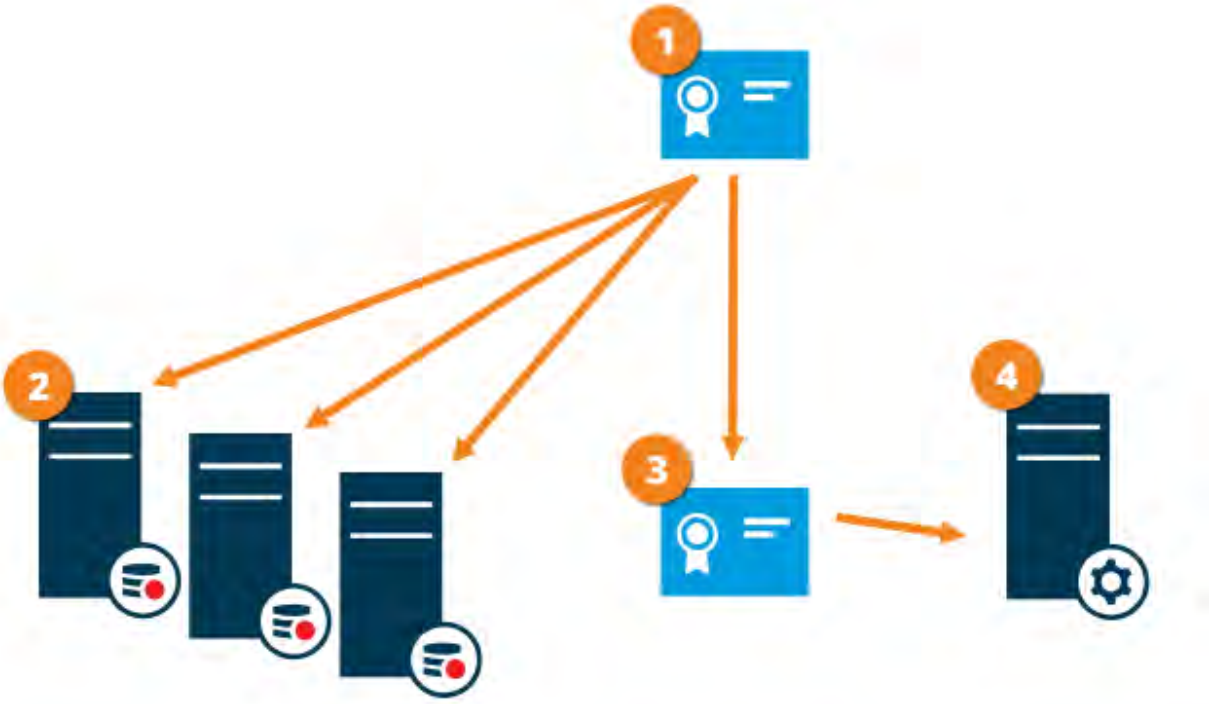
Per ulteriori informazioni, consultare la guida ai certificati su come proteggere le installazioni VMS di MOBOTIX Hub .

4.1.5 Crittografia del server di gestione (spiegazione)

È possibile crittografare la connessione bidirezionale tra il server di gestione e il server di registrazione. Quando si abilita la crittografia sul server di gestione, questa si applica alle connessioni da tutti i server di registrazione che si connettono al server di gestione. Se si abilita la crittografia sul server di gestione, è necessario abilitare anche la crittografia su tutti i server di registrazione. Prima di abilitare la crittografia, è necessario installare i certificati di sicurezza nel server di gestione e in tutti i server di registrazione.

Distribuzione dei certificati per i server di gestione

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti nelle macchine virtuali MOBOTIX HUB per proteggere la comunicazione con il server di gestione.



❶ Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server di gestione) che dalla parte che verifica il certificato (server di registrazione)
❷ Il certificato CA deve essere considerato attendibile su tutti i server di registrazione. In questo modo i server di registrazione possono verificare la validità dei certificati emessi dalla CA
❸ Il certificato CA viene utilizzato per stabilire una connessione sicura tra il server di gestione e i server di registrazione
❹ Il certificato CA deve essere installato nel computer in cui è in esecuzione il server di gestione
Requisiti per il certificato del server di gestione privato:

- Rilasciato al server di gestione in modo che il nome host del server di gestione sia incluso nel certificato, come soggetto (proprietario) o nell'elenco dei nomi DNS a cui viene rilasciato il certificato
- Attendibile nel server di gestione stesso, in quanto considera attendibile il certificato CA utilizzato per emettere il certificato del server di gestione
- Attendibile su tutti i server di registrazione connessi al server di gestione, in quanto considera attendibile il certificato CA utilizzato per emettere il certificato del server di gestione

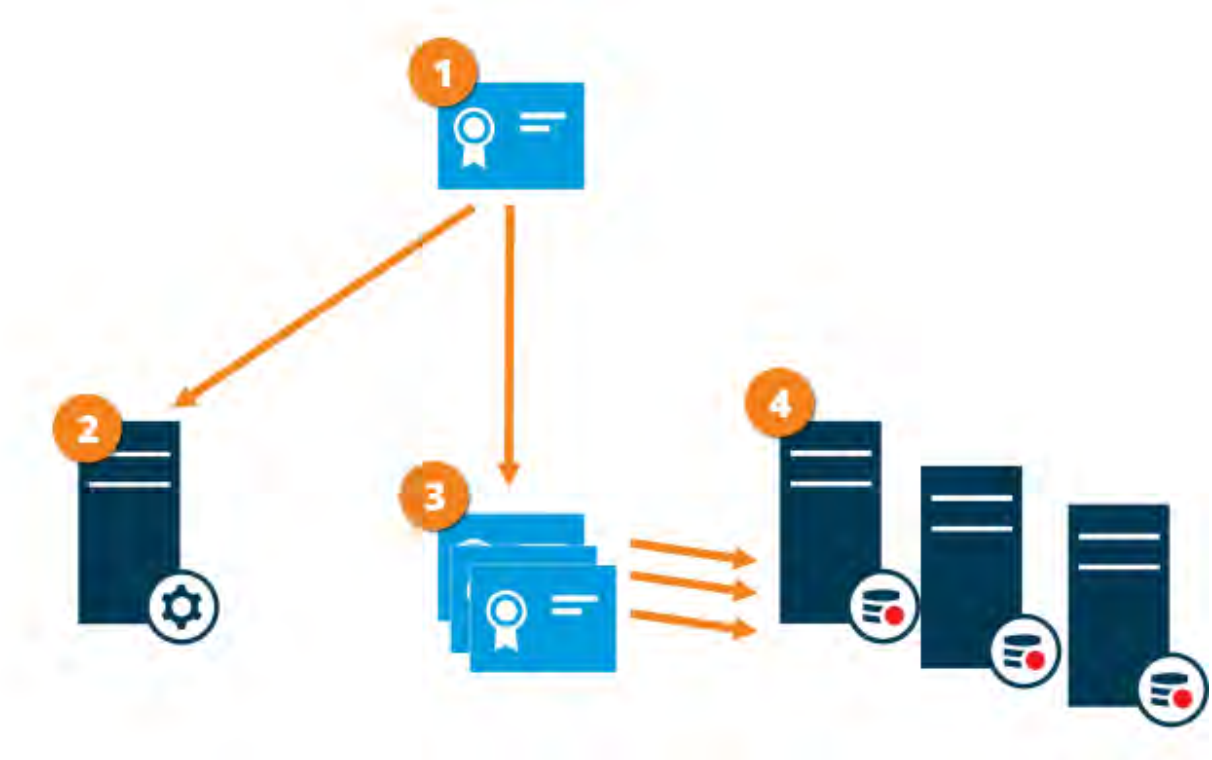
4.1.6 Crittografia dal server di gestione al server di registrazione (spiegazione)

È possibile crittografare la connessione bidirezionale tra il server di gestione e il server di registrazione. Quando si abilita la crittografia sul server di gestione, questa si applica alle connessioni da tutti i server di registrazione che si connettono al server di gestione. La crittografia di questa comunicazione deve seguire l'impostazione di crittografia sul server di gestione. Pertanto, se la crittografia del server di gestione è abilitata, questa deve essere

abilitata anche sui server di registrazione e viceversa. Prima di abilitare la crittografia, è necessario installare i certificati di protezione nel server di gestione e in tutti i server di registrazione, inclusi i server di registrazione di failover.

Distribuzione dei certificati

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti in MOBOTIX HUB VMS per proteggere la comunicazione dal server di gestione.



❶ Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server di registrazione) che dalla parte che verifica il certificato (server di gestione)

❷ Il certificato CA deve essere considerato attendibile sul server di gestione. In questo modo il server di gestione può verificare la validità dei certificati emessi dalla CA

❸ Il certificato CA viene utilizzato per stabilire una connessione sicura tra i server di registrazione e il server di gestione

❹ Il certificato CA deve essere installato nei computer in cui sono in esecuzione i server di registrazione

Requisiti per il certificato del server di registrazione privato:

- Rilasciato al server di registrazione in modo che il nome host del server di registrazione sia incluso nel certificato, come soggetto (proprietario) o nell'elenco dei nomi DNS a cui viene emesso il certificato
- Attendibile nel server di gestione, in quanto considera attendibile il certificato CA utilizzato per emettere il certificato del server di registrazione

4.1.7 Crittografia tra il server di gestione e il server dell'agente di raccolta dati (spiegazione)

È possibile crittografare la connessione bidirezionale tra il server di gestione e l'agente di raccolta dati affiliato quando si dispone di un server remoto del tipo seguente:

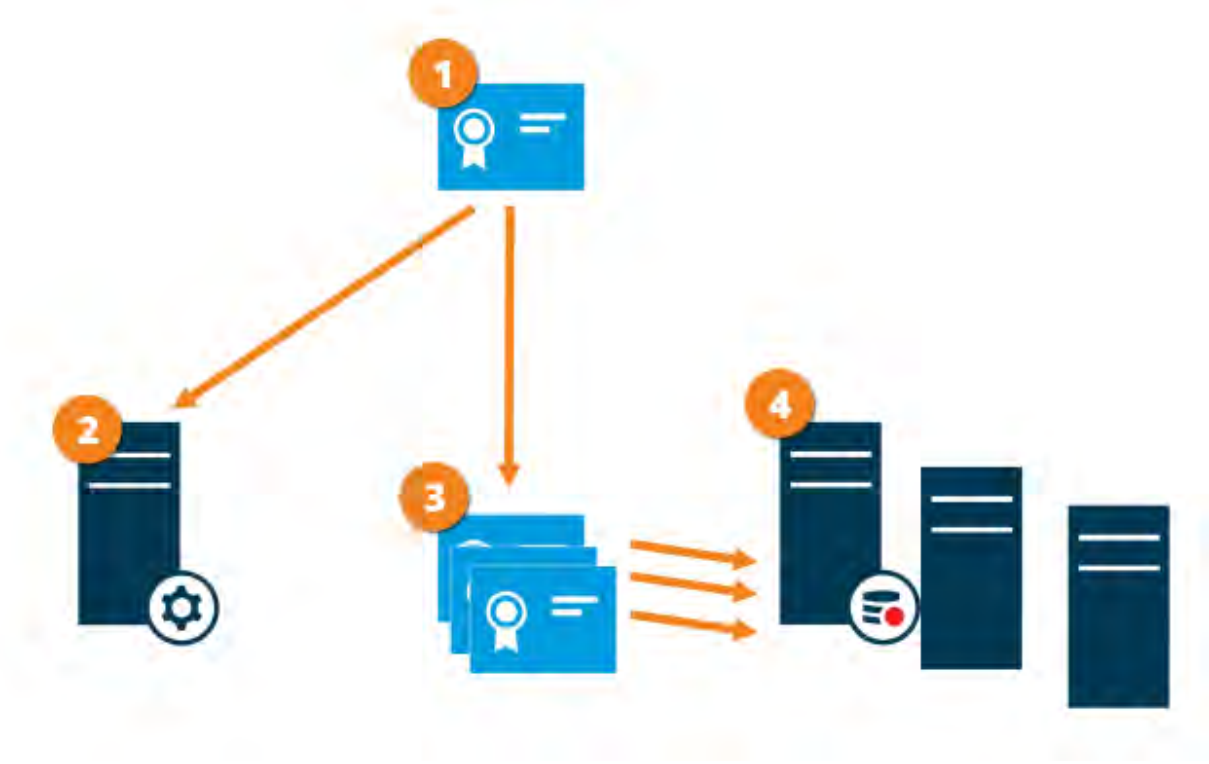
- Server di registrazione

- Server degli eventi
- Server di registro
- LPR Server
- Mobile Server

Quando si abilita la crittografia nel server di gestione, questa si applica alle connessioni da tutti i server dell'agente di raccolta dati che si connettono al server di gestione. La crittografia di questa comunicazione deve seguire l'impostazione di crittografia sul server di gestione. Pertanto, se la crittografia del server di gestione è abilitata, questa deve essere abilitata anche sui server dell'agente di raccolta dati affiliati a ciascun server remoto e viceversa. Prima di abilitare la crittografia, è necessario installare i certificati di sicurezza nel server di gestione e in tutti i server dell'agente di raccolta dati affiliati ai server remoti.

Distribuzione dei certificati

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti in MOBOTIX HUB VMS per proteggere la comunicazione dal server di gestione.



❶ Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server dell'agente di raccolta dati) che dalla parte che verifica il certificato (server di gestione)
❷ Il certificato CA deve essere considerato attendibile sul server di gestione. In questo modo il server di gestione può verificare la validità dei certificati emessi dalla CA
❸ Il certificato CA viene utilizzato per stabilire una connessione sicura tra i server dell'agente di raccolta dati e il server di gestione
❹ Il certificato CA deve essere installato nei computer in cui sono in esecuzione i server dell'agente di raccolta dati
Requisiti per il certificato del server dell'agente di raccolta dati privato:

- Rilasciato al server dell'agente di raccolta dati in modo che il nome host del server dell'agente di raccolta dati sia incluso nel certificato, come soggetto (proprietario) o nell'elenco dei nomi DNS a cui viene emesso il certificato
- Attendibile nel server di gestione, in quanto considera attendibile il certificato CA utilizzato per emettere il certificato del server dell'agente di raccolta dati

4.1.8 Crittografia per client e server che recuperano i dati dal server di registrazione (spiegazione)

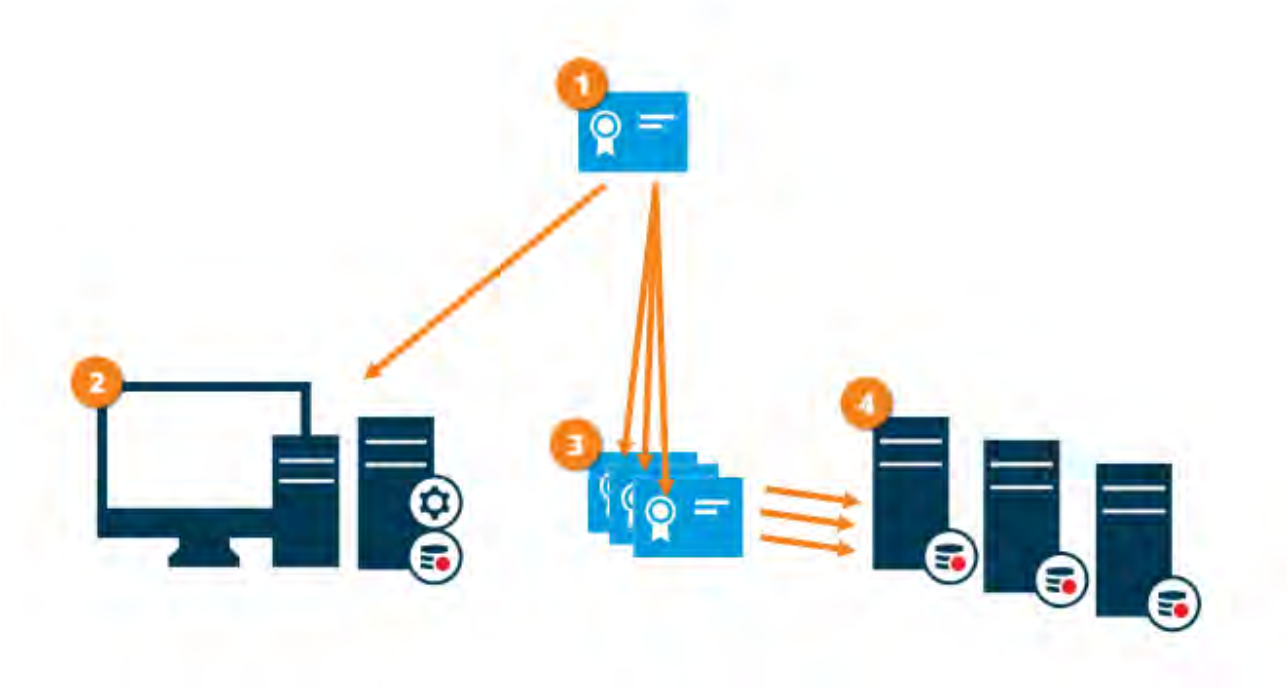
Quando si abilita la crittografia su un server di registrazione, la comunicazione con tutti i client, i server e le integrazioni che recuperano i flussi di dati dal server di registrazione viene crittografata. Nel presente documento denominati "clienti":

- MOBOTIX HUB Smart Client
- Client di gestione
- Server di gestione (per Monitor di sistema e per immagini e clip video AVI nelle notifiche e-mail)
- MOBOTIX HUB Mobile Server
- Server di eventi MOBOTIX HUB
- MOBOTIX HUB LPR
- Ponte di rete aperto MOBOTIX
- MOBOTIX HUB DLNA Server
- Siti che recuperano flussi di dati dal server di registrazione tramite MOBOTIX Interconnect
- Alcune integrazioni di MIP SDK di terze parti

Per le soluzioni compilate con MIP SDK 2018 R3 o versioni precedenti che accedono ai server di registrazione: se le integrazioni vengono effettuate usando le librerie MIP SDK, devono essere ricompilate con MIP SDK 2019 R1; se le integrazioni comunicano direttamente con le API del server di registrazione senza utilizzare le librerie MIP SDK, gli integratori devono aggiungere il supporto HTTPS.

Distribuzione dei certificati

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti in MOBOTIX HUB VMS per proteggere la comunicazione con il server di registrazione.



❶ Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server di registrazione) che dalla parte che verifica il certificato (tutti i client)

❷ Il certificato CA deve essere considerato attendibile in tutti i client. In questo modo i client possono verificare la validità dei certificati emessi dalla CA

❸ Il certificato CA viene utilizzato per stabilire una connessione sicura tra i server di registrazione e tutti i client e i servizi

❹ Il certificato CA deve essere installato nei computer in cui sono in esecuzione i server di registrazione

Requisiti per il certificato del server di registrazione privato:

- Rilasciato al server di registrazione in modo che il nome host del server di registrazione sia incluso nel certificato, come soggetto (proprietario) o nell'elenco dei nomi DNS a cui viene emesso il certificato
- Attendibile in tutti i computer che eseguono servizi che recuperano flussi di dati dai server di registrazione, considerando attendibile il certificato CA utilizzato per emettere il certificato del server di registrazione
- L'account del servizio che esegue il server di registrazione deve avere accesso alla chiave privata del certificato sul server di registrazione.

Se si abilita la crittografia sui server di registrazione e il sistema applica i server di registrazione failover, MOBOTIX consiglia di preparare anche i server di registrazione failover per la crittografia.

4.1.9 Crittografia della comunicazione con il server degli eventi

È possibile crittografare la connessione bidirezionale tra il server di eventi e i componenti che comunicano con il server di eventi, incluso il server LPR. Quando si abilita la crittografia nel server eventi, questa si applica alle connessioni da tutti i componenti che si connettono al server eventi. Prima di abilitare la crittografia, è necessario installare i certificati di sicurezza nel server eventi e in tutti i componenti di connessione.

Quando la comunicazione del server di eventi è crittografata, ciò si applica a tutte le comunicazioni con tale server di eventi. In altre parole, è supportata una sola modalità alla volta, http o https, ma non contemporaneamente.

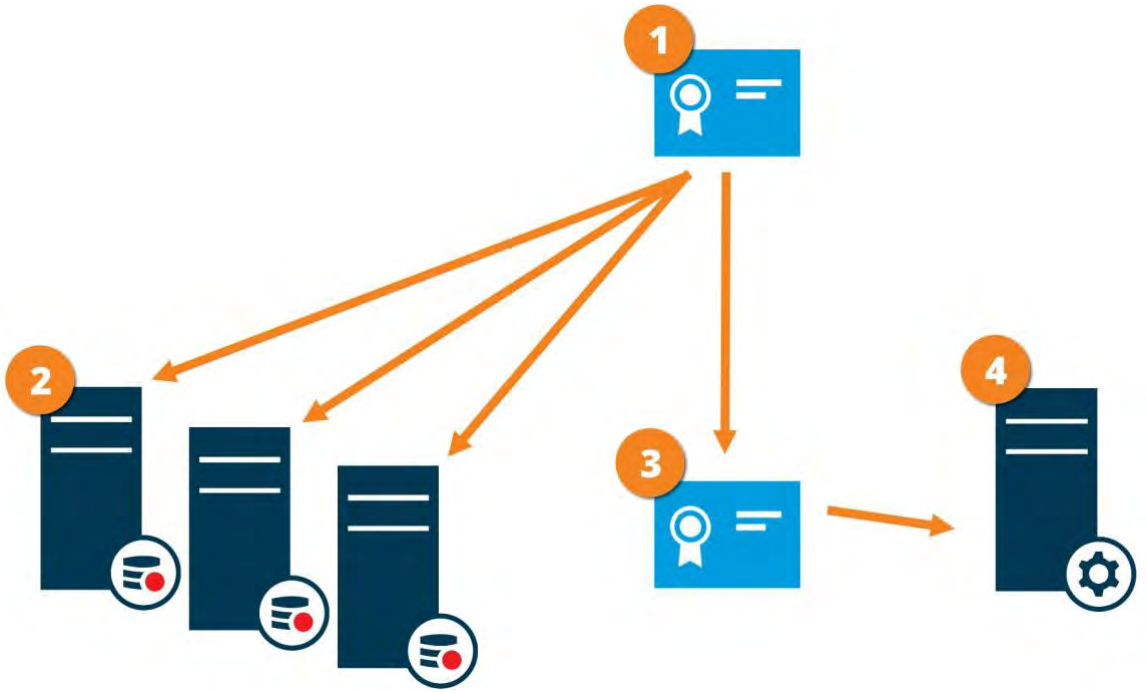
La crittografia si applica a tutti i servizi ospitati nel server eventi, inclusi Transact, Maps, GisMap e Intercommunication.

Prima di abilitare la crittografia nel server degli eventi, tutti i client (Smart Client e Management Client) e il plug-in XProtect LPR devono essere aggiornati almeno alla versione 2022 R1.

HTTPS è supportato solo se ogni componente viene aggiornato almeno alla versione 2022 R1.

Distribuzione dei certificati

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti in XProtect VMS per proteggere la comunicazione con il server degli eventi



❶ Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server eventi) che dalla parte che verifica il certificato

❷ Il certificato CA deve essere considerato attendibile in tutti i client. In questo modo, i client possono verificare la validità dei certificati emessi dalla CA

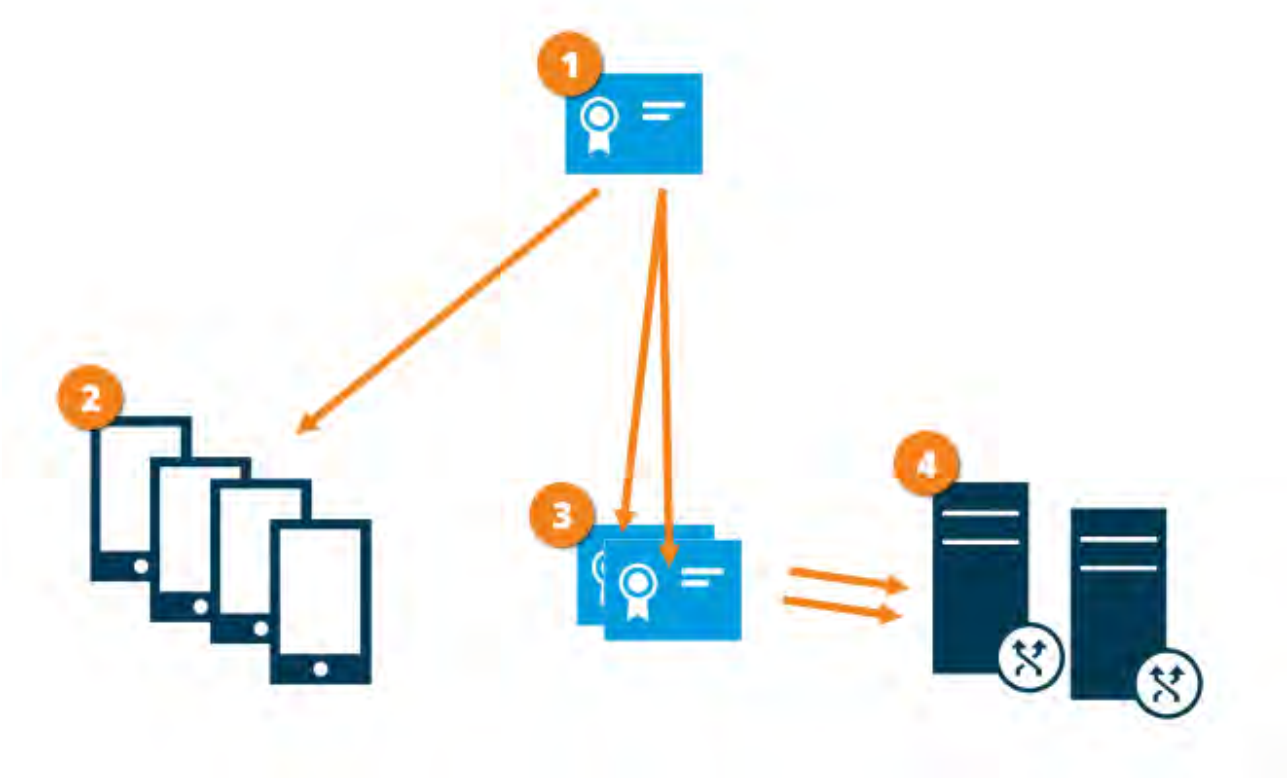
❸ Il certificato CA viene utilizzato per stabilire una connessione sicura tra il server di eventi e i client ❹ Il certificato CA deve essere installato nel computer in cui è in esecuzione il server di eventi

4.1.10 Crittografia dei dati dei server mobili (spiegazione)

In MOBOTIX HUB VMS, la crittografia è abilitata o disabilitata per ogni server mobile. Quando si abilita la crittografia su un server mobile, si avrà la possibilità di utilizzare la comunicazione crittografata con tutti i client, i servizi e le integrazioni che recuperano i flussi di dati.

Distribuzione dei certificati per i server mobili

L'immagine illustra il concetto di base di come i certificati vengono firmati, considerati attendibili e distribuiti in MOBOTIX HUB VMS per proteggere la comunicazione con il server mobile.



❶ Un certificato CA funge da terza parte attendibile, considerata attendibile sia dal soggetto/proprietario (server mobile) che dalla parte che verifica il certificato (tutti i client)
❷ Il certificato CA deve essere considerato attendibile in tutti i client. In questo modo i clienti possono verificare la validità dei certificati emessi dalla CA
❸ Il certificato CA viene utilizzato per stabilire una connessione sicura tra il server mobile e i client e i servizi
❹ Il certificato CA deve essere installato nel computer in cui è in esecuzione il server mobile

Requisiti per il certificato CA:

- Il nome host del server mobile deve essere incluso nel certificato, come soggetto/proprietario o nell'elenco dei nomi DNS a cui viene emesso il certificato
- Il certificato deve essere considerato attendibile su tutti i dispositivi che eseguono servizi che recuperano flussi di dati dal server mobile
- L'account del servizio che esegue il server mobile deve avere accesso alla chiave privata del certificato CA

Requisiti di crittografia dei server mobili per i client

Se non si abilita la crittografia e si utilizza una connessione HTTP, la funzione push-to-talk nel client Web MOBOTIX HUB non sarà disponibile.

4.1.11 Autenticazione Kerberos (spiegazione)

Kerberos è un protocollo di autenticazione di rete basato su ticket. È progettato per fornire un'autenticazione avanzata per applicazioni client/server o server/server.
Utilizzare l'autenticazione Kerberos come alternativa al protocollo di autenticazione Microsoft NTLM (NTLM) precedente.

L'autenticazione Kerberos richiede l'autenticazione reciproca, in cui il client esegue l'autenticazione al servizio e il servizio esegue l'autenticazione al client. In questo modo è possibile eseguire l'autenticazione in modo più sicuro dai client MOBOTIX HUB ai server MOBOTIX HUB senza esporre la password.

Per rendere possibile l'autenticazione reciproca nelle macchine virtuali MOBOTIX HUB, è necessario registrare i nomi principali del servizio (SPN) in Active Directory. Un SPN è un alias che identifica in modo univoco un'entità come un servizio server MOBOTIX HUB. Ogni servizio che utilizza l'autenticazione reciproca deve disporre di un SPN registrato in modo che i client possano identificare il servizio nella rete. Senza SPN registrati correttamente, l'autenticazione reciproca non è possibile.

La tabella seguente elenca i diversi servizi MOBOTIX con i numeri di porta corrispondenti necessari per la registrazione:

Servizio	Numero di porta
Server di gestione - IIS	80 - Configurabile
Server di gestione - Interno	8080
Server di registrazione - Agente di raccolta dati	7609
Failover Server	8990
Server degli eventi	22331
LPR Server	22334

Il numero di servizi necessari per la registrazione in Active Directory dipende dall'installazione corrente. Data Collector viene installato automaticamente durante l'installazione del server di gestione, del server di registrazione, del server eventi, del server LPR o del server di failover.

È necessario registrare due nomi SPN per l'utente che esegue il servizio: uno con il nome host e uno con il nome di dominio completo.

Se si esegue il servizio con un account del servizio utente di rete, è necessario registrare i due nomi SPN per ogni computer che esegue questo servizio.

Questo è lo schema di denominazione SPN MOBOTIX:

```
VideoOS/[Nome host DNS]:[Porta]
VideoOS/[Nome dominio completo]:[Porta]
```

Di seguito è riportato un esempio di nomi SPN per il servizio server di registrazione in esecuzione in un computer con i dettagli seguenti:

```
Nome host: Record-Server1
Dominio: Surveillance.com
```

SPN da registrare:

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

4.1.12 Utilizzare l'aggiornamento di Windows

MOBOTIX consiglia di utilizzare Windows Update per proteggere il VMS dalle vulnerabilità del sistema operativo, assicurandosi che siano installati gli aggiornamenti più recenti. MOBOTIX HUB VMS è basato su Windows, quindi gli aggiornamenti di sicurezza di Windows Update sono importanti.

Gli aggiornamenti possono richiedere una connessione a Internet, pertanto MOBOTIX consiglia di aprire questa connessione solo se necessario e di monitorare i modelli di traffico insoliti.

aggiornamenti di Windows spesso richiedono un riavvio. Questo può essere un problema se è richiesta un'elevata disponibilità, perché il server non è in grado di ricevere dati dai dispositivi durante il riavvio.
Esistono diversi modi per evitarlo o ridurre al minimo l'impatto. Ad esempio, è possibile scaricare gli aggiornamenti sul server e quindi applicarli in un momento in cui un riavvio interromperà il meno possibile la sorveglianza.
Se l'alta disponibilità è un problema, MOBOTIX consiglia di eseguire il server di gestione e i server di eventi in cluster che includono uno o più server di failover. Il server di failover subentrerà durante il riavvio del server di registrazione e la sorveglianza non verrà interrotta. Non includere i server di registrazione nel cluster. Per i server di registrazione, utilizzare un server di registrazione failover.

Prima di implementare gli aggiornamenti di Windows in tutta l'organizzazione, MOBOTIX consiglia di verificare gli aggiornamenti in un ambiente di test. Vedere NIST 800-53 CM-8 *Inventario dei componenti del sistema informativo e sandboxing e SC-44 Camere di detonazione*.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SI-2 Bonifica dei difetti

4.1.13 Mantieni aggiornati il software e il firmware del dispositivo

MOBOTIX consiglia di utilizzare l'ultima versione di MOBOTIX HUB VMS e il firmware per i dispositivi hardware, ad esempio le telecamere. Ciò garantirà che il tuo sistema includa le correzioni di sicurezza più recenti.
Per l'hardware, i componenti di rete e i sistemi operativi, controllare il database CVE e gli eventuali aggiornamenti inviati dai produttori.
Prima di aggiornare il firmware del dispositivo, verificare che MOBOTIX HUB VMS lo supporti. Inoltre, assicurarsi che il pacchetto di dispositivi installato sui server di registrazione supporti il firmware del dispositivo.
Eseguire questa operazione in un ambiente di test per la configurazione, l'integrazione e il test prima di inserirlo nell'ambiente di produzione.
Per verificare che il VMS supporti un dispositivo, attenersi alla seguente procedura:

1. Apri questo link (https://www.mobotix.com/mobotix_custom_table/hub_compatibility).
2. Seleziona il produttore del dispositivo, quindi fai clic su Filtro. La versione del firmware supportata dal pacchetto di dispositivi è elencata nella colonna Firmware testato.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SI-2 Bonifica dei difetti

4.1.14 Usa l'antivirus su tutti i server e computer

MOBOTIX consiglia di implementare il software antivirus su tutti i server e i computer che si connettono al VMS. Il malware che entra nel sistema può bloccare, crittografare o compromettere in altro modo i dati sui server e su altri dispositivi della rete.

Se i dispositivi mobili si connettono al VMS, ciò include la garanzia che i dispositivi dispongano dei sistemi operativi e delle patch più recenti (anche se non direttamente antivirus) installati.

Quando si esegue la scansione antivirus, non eseguire la scansione delle directory e delle sottodirectory del server di registrazione che contengono database di registrazione. Inoltre, non eseguire la scansione dei virus nelle directory di archiviazione degli archivi. La ricerca di virus in queste directory può influire sulle prestazioni del sistema.

Per informazioni sulle porte, le directory e le sottodirectory da escludere dalla scansione antivirus, vedere la sezione *Informazioni sulla scansione antivirus* in *MOBOTIX HUB VMS - Manuale dell'amministratore*.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Architettura di sicurezza delle informazioni NIST SP 800-53 PL-8
- NIST SP 800-53 SI-2 Bonifica dei difetti
- Protezione da codice dannoso NIST SP 800-53 SI-3
- NIST SP 800-53 SI Monitoraggio dei sistemi informativi

4.1.15 Monitorare i registri nel VMS per rilevare eventuali segni di attività sospette

MOBOTIX HUB VMS offre funzionalità per la generazione e la visualizzazione di registri che forniscono informazioni sui modelli di utilizzo, sulle prestazioni del sistema e su altri problemi. MOBOTIX consiglia di monitorare i registri alla ricerca di segni di attività sospette.

Esistono strumenti che sfruttano i log per scopi operativi e di sicurezza. Molte aziende utilizzano i server syslog per consolidare i registri. È possibile utilizzare syslog per annotare le attività a livello di Windows, tuttavia MOBOTIX HUB VMS non supporta syslog.

MOBOTIX consiglia di utilizzare il registro di controllo in MOBOTIX HUB VMS e di abilitare la registrazione dell'accesso utente in Management Client. Per impostazione predefinita, il registro di controllo annota solo gli accessi degli utenti. Tuttavia, è possibile attivare la registrazione degli accessi utente in modo che il registro di controllo annoti tutte le attività degli utenti in tutti i componenti client dei prodotti MOBOTIX HUB VMS. Ciò include gli orari delle attività e gli indirizzi IP di origine.

I componenti client sono MOBOTIX HUB Smart Client, Web Client, il componente MOBOTIX HUB Management Client e le integrazioni effettuate utilizzando MIP SDK. Esempi di attività sono le esportazioni, l'attivazione delle uscite, la visualizzazione delle telecamere dal vivo o in riproduzione e così via.

Il registro di controllo non rileva i tentativi di accesso non riusciti o quando l'utente si disconnette.

La registrazione di tutte le attività utente in tutti i client aumenta il carico sul sistema e può influire sulle prestazioni. È possibile regolare il carico specificando i seguenti criteri che controllano quando il sistema genererà una voce di registro:

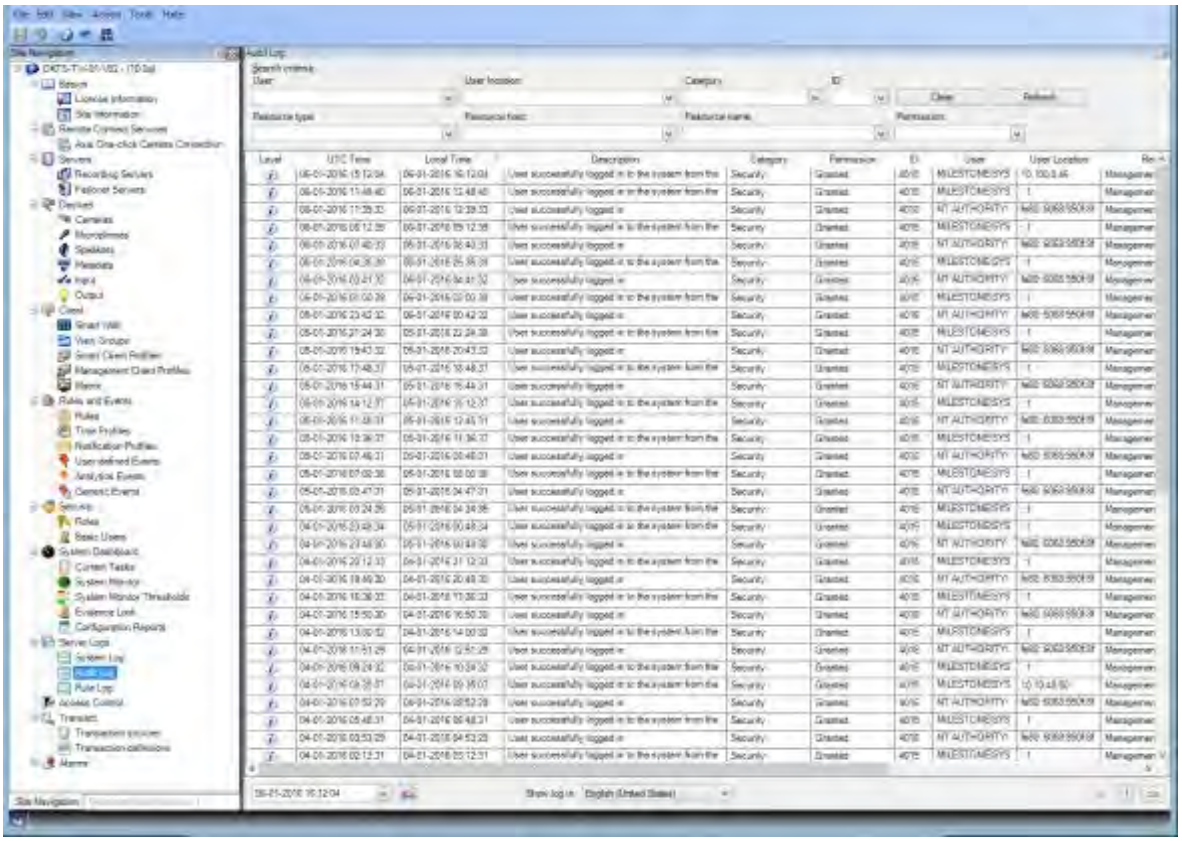
- Il numero di secondi che compongono una sequenza. Il VMS genera una voce di log quando un utente riproduce un video all'interno della sequenza.
- Il numero di fotogrammi che un utente deve visualizzare durante la riproduzione di un video prima che il VMS generi una voce di registro.

Per attivare e configurare la registrazione degli accessi utente estesi, attenersi alla seguente procedura:

1. In Management Client fare clic su Strumenti e selezionare Opzioni.
2. Nella scheda Registri server, in Impostazioni registro, selezionare Registro di controllo.
3. In Impostazioni selezionare la casella di controllo Abilita registrazione accesso utenti.
4. Facoltativo: per specificare le limitazioni per le informazioni annotate e ridurre l'impatto sulle prestazioni, effettuare le selezioni nei campi Lunghezza registrazione sequenza di riproduzione e Record visualizzati prima della registrazione.

Per visualizzare il registro di controllo in MOBOTIX HUB VMS, attenersi alla seguente procedura:

1. Aprire il client di gestione.
2. Espandere il nodo Registri server.
3. Fare clic su Log di controllo.



Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 AU-3 Contenuto dei registri di audit

- Scansione delle vulnerabilità NIST SP 800-53 RA-5
- NIST SP 800-53 AU-6 Revisione, analisi e reportistica dell'audit

4.2 Passaggi avanzati

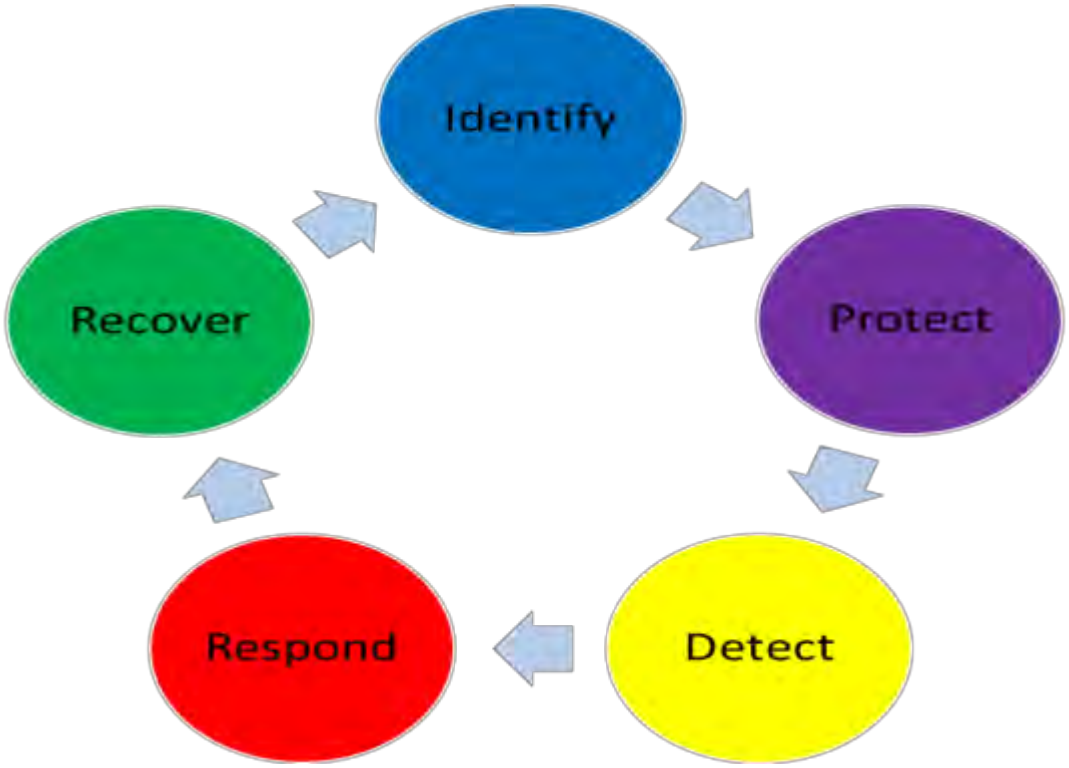
4.2.1 Adotta standard per implementazioni sicure di rete e VMS

MOBOTIX consiglia di adottare gli standard per le implementazioni di reti sicure e MOBOTIX HUB VMS. L'uso di standard è una componente fondamentale dell'ingegneria di Internet e delle reti e la base dell'interoperabilità e della conformità del sistema. Ciò vale anche per l'uso di soluzioni crittografiche, in cui la crittografia basata su standard è l'approccio più comunemente accettato.

4.2.2 Stabilire un piano di risposta agli incidenti

MOBOTIX consiglia di iniziare con una serie di politiche e procedure e di stabilire un piano di risposta agli incidenti. Designare il personale per monitorare lo stato del sistema e rispondere a eventi sospetti. Ad esempio, attività che si svolgono in orari insoliti. Stabilisci un punto di contatto (POC) di sicurezza con ciascuno dei tuoi fornitori, incluso MOBOTIX.

L'immagine seguente è adattata dal NIST Cybersecurity Framework (http://www.nist.gov/cyberframework/). Mostra il ciclo di vita che deve essere considerato quando si crea un piano. Il materiale di supporto nel framework fornisce dettagli sul ciclo di vita e sui controlli di sicurezza per i piani di risposta agli incidenti.



Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 IR 1-13 Risposta agli incidenti

4.2.3 Proteggi i componenti VMS sensibili

MOBOTIX consiglia di utilizzare il controllo dell'accesso fisico e di utilizzare il VMS per monitorare e proteggere i componenti VMS sensibili. La restrizione fisica e il controllo degli accessi fisici basato sui ruoli sono contromisure che mantengono sicuri server e workstation.

Gli amministratori e gli utenti devono avere accesso solo alle informazioni di cui hanno bisogno per adempiere alle loro responsabilità. Se tutti gli utenti interni hanno lo stesso livello di accesso ai dati critici, è più facile per gli aggressori accedere alla rete.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 PE-1 Politica e procedure per la protezione fisica e ambientale
- NIST SP 800-53 PE-2 Autorizzazioni di accesso fisico
- NIST SP 800-53 PE-3 Controllo degli accessi fisici
- NIST SP 800-53 AC-4 Privilegio minimo

4.2.4 Segui le best practice per la sicurezza del sistema operativo Microsoft

MOBOTIX consiglia di seguire le best practice di sicurezza per i sistemi operativi Microsoft per mitigare i rischi del sistema operativo e mantenere la sicurezza. In questo modo è possibile proteggere i server e i computer client Microsoft.

Per ulteriori informazioni, vedere *la Guida all'aggiornamento della protezione Microsoft* (https://msrc.microsoft.com/update-guide).

4.2.5 Utilizzare gli strumenti per automatizzare o implementare i criteri di sicurezza

MOBOTIX consiglia di trovare uno o più strumenti che aiutino ad automatizzare e implementare la politica di sicurezza. L'automazione riduce il rischio di errore umano e semplifica la gestione della policy. Ad esempio, è possibile automatizzare l'installazione di patch e aggiornamenti di sicurezza su server e computer client.
Un modo per implementare questa raccomandazione consiste nel combinare Microsoft Security Configuration Manager (SCCM) con il protocollo SCAP (Security Content Automation Protocol). (Vedi ad esempio, *Esperto a tutto tondo: automatizza le impostazioni di sicurezza di base* (https://technet.microsoft.com/en-us/magazine/ff721825.aspx) e il *programma di convalida SCAP (Security Content Automation Protocol)* (https://csrc.nist.gov/projects/scap-validation-program).) In questo modo si ottiene un framework per creare, distribuire e convalidare le impostazioni di protezione nei computer della rete.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Politica e procedure di gestione della configurazione NIST SP 800-53 CM-1
- Configurazione di base NIST SP 800-53 CM-2
- Controllo della modifica della configurazione NIST SP 800-53 CM-3

4.2.6 Segui le best practice consolidate per la sicurezza della rete

MOBOTIX consiglia di seguire le best practice IT e dei fornitori per garantire che i dispositivi sulla rete siano configurati in modo sicuro. Chiedi ai tuoi fornitori di fornire queste informazioni. È importante aprire e mantenere un dialogo sulla sicurezza e una discussione sulle migliori pratiche è un buon punto di partenza.
È importante negare l'accesso al VMS non utilizzando impostazioni di rete vulnerabili. Per ulteriori informazioni, vedere *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) (specifico per i firewall) e *ICS-CERT Standards and References* (https://www.cisa.gov/ics) (elenco generale).

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Impostazioni di configurazione NIST 800-53 CM-6
- Strumenti di manutenzione NIST 800-53 MA-3

5 Dispositivi e rete

Questa sezione fornisce indicazioni per la protezione avanzata dei dispositivi e dei componenti di rete correlati alle VM MOBOTIX HUB. Ciò include parti chiave del sistema come le telecamere, l'archiviazione e la rete.
I sistemi di sorveglianza spesso includono telecamere ai margini della rete. Le telecamere e le loro connessioni di rete, se non protette, rappresentano un rischio significativo di compromissione, consentendo potenzialmente agli intrusi un ulteriore accesso al sistema.

5.1 Passaggi di base – Dispositivi

5.1.1 Usa password complesse invece di password predefinite

MOBOTIX consiglia di modificare le password predefinite sui dispositivi, ad esempio su una telecamera. Non utilizzare password predefinite perché vengono spesso pubblicate su Internet e sono facilmente disponibili. Utilizza invece password complesse per i dispositivi. Le password complesse includono otto o più caratteri alfanumerici, utilizzano lettere maiuscole e minuscole e caratteri speciali.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'autenticatore NIST 800-53 IA-4
- Feedback sull'autenticatore NIST 800-53 IA-8
- Gestione degli errori NIST 800-53 SI-11

5.1.2 Arrestare i servizi e i protocolli inutilizzati

Per evitare l'accesso non autorizzato o la divulgazione di informazioni, MOBOTIX consiglia di interrompere i servizi e i protocolli inutilizzati sui dispositivi. Ad esempio, Telnet, SSH, FTP, UPnP, Ipv6 e Bonjour.
È inoltre importante utilizzare l'autenticazione avanzata su tutti i servizi che accedono al VMS, alla rete o ai dispositivi. Ad esempio, utilizzare le chiavi SSH anziché i nomi utente e le password e utilizzare i certificati di un'autorità di certificazione per HTTPS. Per ulteriori informazioni, vedere le guide alla protezione avanzata e altre indicazioni fornite dal produttore del dispositivo.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Accesso remoto NIST SP 800-53 AC-17 (disabilita i protocolli inutilizzati)
- Impostazioni di configurazione NIST SP 800-53 CM-6
- NIST SP 800-53 CM-7 Funzionalità minima
- Identificazione e autenticazione NIST SP 800-53 IA-2

- NIST SP 800-53 SA-9 Servizi di informazione esterna

5.1.3 Crea account utente dedicati su ogni dispositivo

Tutte le telecamere dispongono di un account utente predefinito con un nome utente e una password che il VMS utilizza per accedere al dispositivo. A scopo di controllo, MOBOTIX consiglia di modificare il nome utente e la password predefiniti.

Creare un account utente specifico per l'uso da parte del VMS e utilizzare questo account utente e la password quando si aggiunge la telecamera al VMS. Quando un server di registrazione si connette alla telecamera, utilizza il nome utente e la password creati. Se la telecamera dispone di un registro, questo registro mostra che il server di registrazione si è connesso alla telecamera.

Con un nome utente e una password dedicati, i registri del dispositivo possono aiutarti a determinare se un server di registrazione o una persona ha effettuato l'accesso alla telecamera. Ciò è rilevante quando si esaminano potenziali problemi di sicurezza che interessano i dispositivi.

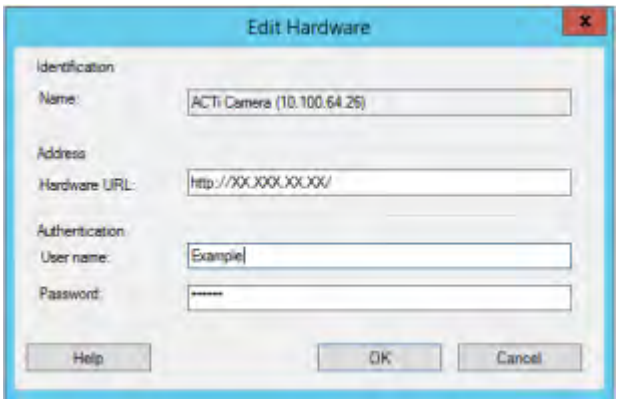
È possibile modificare il nome utente e la password di un dispositivo prima o dopo averlo aggiunto nel client di gestione.

Per modificare il nome utente e la password prima di aggiungere il dispositivo, attenersi alla seguente procedura:

1. Vai all'interfaccia web del dispositivo e modifica il nome utente e la password predefiniti.
2. In Client di gestione aggiungere il dispositivo e specificare il nome utente e la password.

Per modificare il nome utente e le password dei dispositivi già aggiunti, attenersi alla seguente procedura:

1. Nel riquadro Spostamento siti del client di gestione espandere il nodo Server e selezionare Server di registrazione.
2. Nel riquadro Server di registrazione espandere il server di registrazione che contiene il dispositivo, quindi fare clic con il pulsante destro del mouse sul dispositivo e scegliere Modifica hardware.



3. In Autenticazione immettere il nuovo nome utente e la nuova password.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- NIST SP 800-53 AC-4 Privilegio minimo

5.1.4 Scansione dei dispositivi

La scansione dei dispositivi (ad esempio, **la scansione rapida** o la **scansione dell'intervallo di indirizzi** quando si aggiunge l'hardware) viene eseguita utilizzando trasmissioni che possono contenere nomi utente e password in testo normale.

meno che non si tratti di una configurazione iniziale, questa funzionalità non deve essere utilizzata per aggiungere dispositivi al sistema. Utilizzare invece l' **opzione Manuale** e selezionare manualmente il driver.
Sui sistemi sensibili, la funzionalità di **rilevamento automatico dei dispositivi** deve essere disabilitata su MOBOTIX HUB Professional VMS (che si trova in Impostazioni > **Collegamento di dispositivi hardware**), perché invierà periodicamente trasmissioni che possono contenere nomi utente e password.

5.2 Passaggi di base – Rete

5.2.1 Utilizza una connessione di rete sicura e affidabile

Le comunicazioni di rete devono essere sicure, indipendentemente dal fatto che ci si trovi o meno su una rete chiusa. Per impostazione predefinita, è necessario utilizzare comunicazioni sicure quando si accede al VMS. Per esempio:

- Tunnel VPN o HTTPS per impostazione predefinita
- Versione più recente di Transport Layer Security (https://datatracker.ietf.org/wg/tls/charter/) (TLS, attualmente 1.2) con certificati validi che soddisfano le procedure consigliate del settore, ad esempio da Public-Key Infrastructure (X.509) (https://datatracker.ietf.org/wg/ipsec/documents/) e CA/Browser Forum (https://cabforum.org/).

In caso contrario, le credenziali potrebbero essere compromesse e gli intrusi potrebbero utilizzarle per accedere al VMS.
Configurare la rete per consentire ai computer client di stabilire sessioni HTTPS sicure o tunnel VPN tra i dispositivi client e i server VMS.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SI-2 Bonifica dei difetti
- Impostazioni di configurazione NIST SP 800-53 CM-6
- Autenticità della sessione NIST SP 800-53 SC-23

5.2.2 Utilizzare i firewall per limitare l'accesso IP a server e computer

MOBOTIX consiglia di utilizzare connessioni sicure e di seguire i seguenti passaggi aggiuntivi:

- Usa l'autenticazione sicura del dispositivo
- Usa TLS
- Utilizzare la whitelist dei dispositivi per autenticare i dispositivi
- Utilizzare i firewall per limitare la comunicazione di rete tra server e computer client e programmi.

Tutti i componenti MOBOTIX HUB e le porte necessarie sono elencati nelle singole sezioni seguenti. Per garantire, ad esempio, che il firewall blocchi solo il traffico indesiderato, è necessario specificare le porte utilizzate da

MOBOTIX HUB VMS. È consigliabile abilitare solo queste porte. Gli elenchi includono anche le porte utilizzate per i processi locali.

Sono organizzati in due gruppi:

- Componenti server (servizi): offrono il loro servizio su porte specifiche, motivo per cui devono ascoltare le richieste dei client su queste porte. Pertanto, queste porte devono essere aperte in Windows Firewall per le connessioni in entrata.
- Componenti client (client): consente di avviare connessioni a porte specifiche sui componenti del server. Pertanto, queste porte devono essere aperte per le connessioni in uscita. Le connessioni in uscita sono in genere aperte per impostazione predefinita in Windows Firewall.

Se non viene menzionato nient'altro, le porte per i componenti server devono essere aperte per le connessioni in ingresso e le porte per i componenti client devono essere aperte per le connessioni in uscita.

Tenere presente che i componenti server possono fungere da client anche per altri componenti server.

I numeri di porta sono i numeri predefiniti, ma possono essere modificati. Contattare l'assistenza MOBOTIX se è necessario modificare le porte che non sono configurabili tramite il client di gestione.

Componenti del server (connessioni in entrata)

Ciascuna delle sezioni seguenti elenca le porte che devono essere aperte per un determinato servizio. Per capire quali porte devono essere aperte su un determinato computer, è necessario considerare tutti i servizi in esecuzione su questo computer.

Limitare l'accesso remoto al server di gestione aggiungendo regole del firewall per consentire solo ai server di registrazione di connettersi alla porta TCP 9993.

Servizio Server di gestione e processi correlati

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
80	Protocollo HTTP	IIS	Tutti i server e lo Smart Client MOBOTIX HUB e il client di gestione	Lo scopo della porta 80 e della porta 443 è lo stesso. Tuttavia, la porta utilizzata dal VMS dipende dal fatto che siano stati utilizzati certificati per proteggere la comunicazione. • Quando la comunicazione con i certificati non è stata protetta , il VMS utilizza la porta 80. • Dopo aver protetto la comunicazione con i certificati, il VMS utilizza la porta 443, ad eccezione della comunicazione dal
443	HTTPS	IIS		

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
				server degli eventi al server di gestione. La comunicazione tra il server di eventi e il server di gestione utilizza Windows Secured Framework (WCF) e l'autenticazione di Windows sulla porta 80.
6473	TCP	Servizio Server di gestione	Icona della barra delle applicazioni di Management Server Manager, solo connessione locale.	Visualizzazione dello stato e gestione del servizio.
8080	TCP	Server di gestione	Solo connessione locale.	Comunicazione tra i processi interni sul server.
9000	Protocollo HTTP	Server di gestione	Servizi del server di registrazione	Servizio web per la comunicazione interna tra server.
12345	TCP	Servizio Server di gestione	MOBOTIX HUB Smart Client	Comunicazione tra il sistema e i destinatari di Matrix. È possibile modificare il numero di porta nel client di gestione.
12974	TCP	Servizio Server di gestione	Servizio SNMP di Windows	Comunicazione con l'agente di estensione SNMP. Non utilizzare la porta per altri scopi, anche se il sistema non applica SNMP. Nei sistemi MOBOTIX HUB 2014 o precedenti, il numero di porta era 6475. Nei sistemi MOBOTIX HUB 2019 R2 e precedenti, il numero di porta era 7475.

Servizio SQL Server

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
1433	TCP	SQL Server	Servizio Server di gestione	Memorizzazione e recupero delle configurazioni.
1433	TCP	SQL Server	Servizio Event Server	Archiviazione e recupero di eventi.
1433	TCP	SQL Server	Servizio server di registro	Archiviazione e recupero delle voci di registro.

Servizio di raccolta dati

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
7609	Protocollo HTTP	IIS	Nel computer del server di gestione: servizi dell'agente di raccolta dati in tutti gli altri server. Su altri computer: servizio di raccolta dati sul server di gestione.	Monitor di sistema.

Servizio Event Server

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
1234	TCP/UDP	Servizio server eventi	Qualsiasi server che invia eventi generici al sistema MOBOTIX HUB.	Ascolto di eventi generici da sistemi o dispositivi esterni. Solo se l'origine dati pertinente è abilitata.
1235	TCP	Servizio Event Server	Qualsiasi server che invia eventi generici al sistema MOBOTIX HUB.	Ascolto di eventi generici da sistemi o dispositivi esterni. Solo se l'origine dati pertinente è abilitata.
9090	TCP	Servizio Event Server	Qualsiasi sistema o dispositivo che invia eventi di analisi al sistema MOBOTIX HUB.	Ascolto di eventi di analisi da sistemi o dispositivi esterni. Rilevante solo se la funzione Eventi di analisi è abilitata.
22331	TCP	Servizio Event Server	MOBOTIX HUB Smart Client e il client di gestione	Configurazione, eventi, allarmi e dati delle mappe.
22333	TCP	Servizio Event Server	Plug-in MIP e applicazioni.	Messaggistica MIP.

Servizio server di registrazione

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
25	SMTP	Servizio server di registrazione	Telecamere, codificatori e dispositivi I/O.	Ascolto dei messaggi di evento dai dispositivi. La porta è disabilitata per impostazione predefinita. (Obsoleto) L'abilitazione di questa opzione aprirà una porta per le connessioni non crittografate e non è consigliato.
5210	TCP	Servizio server di registrazione	Server di registrazione di failover.	Unione di database dopo l'esecuzione di un server di registrazione di failover.
5432	TCP	Servizio server di registrazione	Telecamere, codificatori e dispositivi I/O.	Ascolto dei messaggi di evento dai dispositivi. La porta è disabilitata per impostazione predefinita.
7563	TCP	Servizio server di registrazione	MOBOTIX HUB Smart Client, client di gestione	Recupero di flussi video e audio, comandi PTZ.
8966	TCP	Servizio server di registrazione	Icona della barra delle applicazioni di Recording Server Manager, solo connessione locale.	Visualizzazione dello stato e gestione del servizio.
9001	Protocollo HTTP	Servizio server di registrazione	Server di gestione	Servizio web per la comunicazione interna tra server. Se sono in uso più istanze del server di registrazione, ogni istanza necessita di una propria porta. Le porte aggiuntive saranno 9002, 9003, ecc.
11000	TCP	Servizio server di registrazione	Server di registrazione di failover	Polling dello stato dei server di registrazione.
12975	TCP	Servizio server di registrazione	Servizio SNMP di Windows	Comunicazione con l'agente di estensione SNMP. Non utilizzare la porta per altri scopi, anche se il sistema non applica SNMP. Nei sistemi MOBOTIX HUB 2014 o precedenti, il numero di porta era 6474. Nei sistemi MOBOTIX HUB 2019 R2 e precedenti, il numero di porta era 7474.

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
65101	UDP	Servizio server di registrazione	Solo connessione locale	Ascolto delle notifiche degli eventi da parte dei conducenti.

Oltre alle connessioni in entrata al servizio Recording Server sopra elencate, il servizio Recording Server stabilisce connessioni in uscita a telecamere, NVR e siti interconnessi remoti (MOBOTIX Interconnect ICP).

Servizio server di failover e servizio server di registrazione di failover

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
25	SMTP	Servizio server di registrazione di failover	Telecamere, codificatori e dispositivi I/O.	Ascolto dei messaggi di evento dai dispositivi. La porta è disabilitata per impostazione predefinita. (Obsoleto) L'abilitazione di questa opzione aprirà una porta per le connessioni non crittografate e non è consigliato.
5210	TCP	Servizio server di registrazione di failover	Server di registrazione di failover	Unione di database dopo l'esecuzione di un server di registrazione di failover.
5432	TCP	Servizio server di registrazione di failover	Telecamere, codificatori e dispositivi I/O.	Ascolto dei messaggi di evento dai dispositivi. La porta è disabilitata per impostazione predefinita.
7474	TCP	Servizio server di registrazione di failover	Servizio SNMP di Windows	Comunicazione con l'agente di estensione SNMP. Non utilizzare la porta per altri scopi, anche se il sistema non applica SNMP.
7563	TCP	Servizio server di registrazione di failover	MOBOTIX HUB Smart Client	Recupero di flussi video e audio, comandi PTZ.
8844	UDP	Servizio server di registrazione di failover	Solo connessione locale.	Comunicazione tra i server.

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
8966	TCP	Servizio server di registrazione di failover	Icona della barra delle applicazioni di Failover Recording Server Manager, solo connessione locale.	Visualizzazione dello stato e gestione del servizio.
8967	TCP	Servizio server di failover	Icona della barra delle applicazioni di Failover Server Manager, solo connessione locale.	Visualizzazione dello stato e gestione del servizio.
8990	TCP	Servizio server di failover	Servizio Server di gestione	Monitoraggio dello stato del servizio Server di failover.
9001	Protocollo HTTP	Servizio server di failover	Server di gestione	Servizio web per la comunicazione interna tra server.

Oltre alle connessioni in entrata al servizio Server di failover/Server di registrazione di failover elencati in precedenza, il servizio Server di failover/Server di registrazione di failover stabilisce connessioni in uscita ai normali registratori, telecamere e per il push video.

Servizio server di registro

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
22337	Protocollo HTTP	Servizio server di registro	Tutti i componenti di MOBOTIX HUB, ad eccezione del client di gestione e del server di registrazione.	Scrivere, leggere e configurare il server di log.

Servizio server mobile

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
8000	TCP	Servizio server mobile	Icona della barra delle applicazioni di Mobile Server Manager, solo connessione locale.	Applicazione SysTray.
8081	Protocollo HTTP	Servizio server mobile	Client mobili, client Web e client di gestione.	Invio di flussi di dati; video e audio.
8082	HTTPS	Servizio server mobile	Client mobili e client Web.	Invio di flussi di dati; video e audio.

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
40001 - 40099	Protocollo HTTP	Servizio server mobile	Servizio server di registrazione	Push video del server mobile. Questo intervallo di porte è disabilitato per impostazione predefinita.

Servizio server LPR

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
22334	TCP	Servizio server LPR	Server degli eventi	Recupero delle targhe riconosciute e dello stato del server. Per connettersi, sul server degli eventi deve essere installato il plug-in LPR.
22334	TCP	Servizio server LPR	Icona LPR Server Manager nella barra delle applicazioni, solo connessione locale.	Applicazione SysTray

Servizio MOBOTIX Open Network Bridge

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
580	TCP	Servizio bridge di rete aperto MOBOTIX	Clienti ONVIF	Autenticazione e richieste di configurazione del flusso video.
554	RTSP	Servizio RTSP	Clienti ONVIF	Streaming del video richiesto ai client ONVIF.

Servizio server DLNA di MOBOTIX HUB

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
9100	Protocollo HTTP	Servizio server DLNA	Dispositivo DLNA	Rilevamento dei dispositivi e configurazione dei canali DLNA. Richieste di flussi video.
9200	Protocollo HTTP	Servizio server DLNA	Dispositivo DLNA	Streaming del video richiesto ai dispositivi DLNA.

Servizio di registrazione dello schermo MOBOTIX HUB

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
52111	TCP	Registratore dello schermo MOBOTIX HUB	Servizio server di registrazione	Fornisce video da un monitor. Appare e agisce allo stesso modo di una telecamera sul server di registrazione. È possibile modificare il numero di porta nel client di gestione.

Servizio XProtect Incident Manager

Numero di porta	Protocollo	Processo	Collegamenti da...	Scopo
80	Protocollo HTTP	IIS	XProtect Smart Client e il client di gestione	Lo scopo della porta 80 e della porta 443 è lo stesso. Tuttavia, la porta utilizzata dal VMS dipende dal fatto che siano stati utilizzati certificati per proteggere la comunicazione. • Quando la comunicazione con i certificati non è stata protetta, il VMS utilizza la porta 80. • Dopo aver protetto la comunicazione con i certificati, il VMS utilizza la porta 443
443	HTTPS			

Componenti del server (connessioni in uscita)

Servizio Server di gestione

Numero di porta	Protocollo	Collegamenti con...	Scopo
443	HTTPS	Il server licenze che ospita il servizio di gestione delle licenze.	Attivazione delle licenze.

Servizio server di registrazione

Numero di porta	Protocollo	Collegamenti con...	Scopo
80	Protocollo HTTP	Telecamere, NVR, codificatori Siti interconnessi	Autenticazione, configurazione, flussi di dati, video e audio. Accesso
443	HTTPS	Telecamere, NVR, codificatori	Autenticazione, configurazione, flussi di dati, video e audio.
554	RTSP	Telecamere, NVR, codificatori	Flussi di dati, video e audio.
7563	TCP	Siti interconnessi	Flussi di dati ed eventi.
11000	TCP	Server di registrazione di failover	Polling dello stato dei server di registrazione.
40001 – 40099	Protocollo HTTP	Servizio server mobile	Push video del server mobile. Questo intervallo di porte è disabilitato per impostazione predefinita.

Servizio server di failover e servizio server di registrazione di failover

Numero di porta	Protocollo	Collegamenti con...	Scopo
11000	TCP	Server di registrazione di failover	Polling dello stato dei server di registrazione.

Servizio server di registro

Numero di porta	Protocollo	Collegamenti con...	Scopo
443	HTTPS	Server di registro	Inoltro dei messaggi al server di log.

API Gateway

Numero di porta	Protocollo	Collegamenti con...	Scopo
80	Protocollo HTTP	Server di gestione	RESTful API

Numero di porta	Protocollo	Collegamenti con...	Scopo
443	HTTPS	Server di gestione	RESTful API

Telecamere, codificatori e dispositivi I/O (connessioni in entrata)

Numero di porta	Protocollo	Collegamenti da...	Scopo
80	TCP	Server di registrazione e server di registrazione failover	Autenticazione, configurazione e flussi di dati; video e audio.
443	HTTPS	Server di registrazione e server di registrazione failover	Autenticazione, configurazione e flussi di dati; video e audio.
554	RTSP	Server di registrazione e server di registrazione failover	Flussi di dati; video e audio.

Telecamere, codificatori e dispositivi I/O (connessioni in uscita)

Numero di porta	Protocollo	Collegamenti con...	Scopo
25	SMTP	Server di registrazione e server di registrazione failover	Invio di notifiche degli eventi (obsoleto).
5432	TCP	Server di registrazione e server di registrazione failover	Invio di notifiche di eventi. La porta è disabilitata per impostazione predefinita.
22337	Protocollo HTTP	Server di registro	Inoltro dei messaggi al server di log.

Solo pochi modelli di fotocamera sono in grado di stabilire connessioni in uscita.

Componenti client (connessioni in uscita)

Smart Client MOBOTIX HUB, Client di gestione MOBOTIX HUB, Server mobile MOBOTIX HUB

Numero di porta	Protocollo	Collegamenti con...	Scopo
80	Protocollo HTTP	Servizio Server di gestione	Autenticazione
443	HTTPS	Servizio Server di gestione	Autenticazione degli utenti di base.
7563	TCP	Servizio server di registrazione	Recupero di flussi video e audio, comandi PTZ.

Numero di porta	Protocollo	Collegamenti con...	Scopo
22331	TCP	Servizio Event Server	Allarmi.

Client Web MOBOTIX HUB, client mobile MOBOTIX HUB

Numero di porta	Protocollo	Collegamenti con...	Scopo
8081	Protocollo HTTP	MOBOTIX HUB Server mobile	Recupero di flussi video e audio.
8082	HTTPS	MOBOTIX HUB Server mobile	Recupero di flussi video e audio.

Ulteriori informazioni

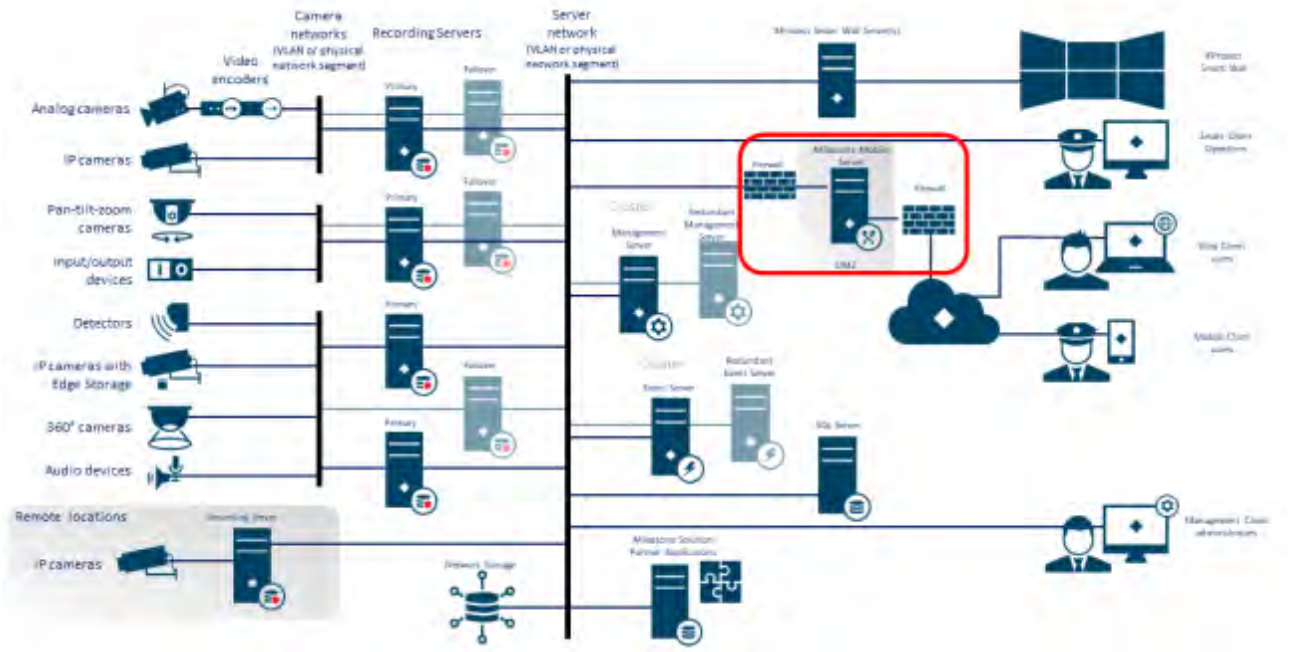
I controlli seguenti forniscono ulteriori indicazioni:

- Connessioni di sistema NIST SP 800-53 CA-3
- Impostazioni di configurazione NIST SP 800-53 CM-6
- NIST SP 800-53 SC-7 Protezione dei confini

5.2.3 Utilizzare un firewall tra il VMS e Internet

Il VMS non deve connettersi direttamente a Internet. Se si espongono parti del VMS a Internet, MOBOTIX consiglia di utilizzare un firewall configurato in modo appropriato tra il VMS e Internet.

Se possibile, esporre a Internet solo il componente del server MOBOTIX Mobile e posizionarlo in una zona demilitarizzata (DMZ) con firewall su entrambi i lati. Questa operazione è illustrata nella figura seguente.



Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Connessioni di sistema NIST SP 800-53 CA-3

5.2.4 Collegare la subnet della telecamera solo alla subnet del server di registrazione

MOBOTIX consiglia di collegare la subnet della telecamera solo alla subnet del server di registrazione. Le telecamere e gli altri dispositivi devono comunicare solo con i server di registrazione. Per ulteriori informazioni, vedere Server di registrazione a pagina 59.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 SC-7 Protezione dei confini

5.3 Passaggi avanzati – Dispositivi

5.3.1 Usa Simple Network Management Protocol per monitorare gli eventi

MOBOTIX consiglia di utilizzare il protocollo SNMP (Simple Network Management Protocol) per monitorare gli eventi sui dispositivi della rete. È possibile utilizzare SNMP come supplemento per syslog. SNMP funziona in tempo reale con molti tipi di eventi che possono attivare avvisi, ad esempio se un dispositivo viene riavviato.

Affinché ciò funzioni, i dispositivi devono supportare la registrazione tramite SNMP.

Sono disponibili diverse versioni dei protocolli SNMP. Le versioni 2c e 3 sono le più recenti. L'implementazione coinvolge una serie di standard. Una buona panoramica è disponibile sul sito di riferimento SNMP (http://www.snmp.com/protocol/snmp_rfcs.shtml).

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Monitoraggio degli eventi NIST SP 800-53 SI-4

5.4 Passaggi avanzati – Rete

5.4.1 Utilizza protocolli wireless sicuri

Se si utilizzano reti wireless, MOBOTIX consiglia di utilizzare un protocollo wireless sicuro per impedire l'accesso non autorizzato a dispositivi e computer. Ad esempio, utilizzare configurazioni standardizzate. Le linee guida NIST sulle reti locali wireless forniscono dettagli specifici sulla gestione e la configurazione della rete. Per ulteriori informazioni, vedere *SP 800-48 revisione 1, Guida alla protezione delle reti wireless IEEE 802.11 legacy* (https://csrc.nist.gov/publications/detail/sp/800-48/rev-1/archive/2008-07-25).
Inoltre, MOBOTIX consiglia di non utilizzare telecamere wireless in luoghi mission-critical. Le videocamere wireless sono facili da inceppare, il che può portare alla perdita del video.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Accesso wireless NIST SP 800-53 AC-18

- Protezione del collegamento wireless NIST SP 800-53 SC-40

5.4.2 Utilizzare il controllo degli accessi basato sulle porte

Utilizzare il controllo degli accessi basato sulle porte per impedire l'accesso non autorizzato alla rete della telecamera. Se un dispositivo non autorizzato si connette a una porta dello switch o del router, la porta dovrebbe essere bloccata. Le informazioni su come configurare switch e router sono disponibili presso i produttori. Per *informazioni sulla gestione della configurazione dei sistemi informativi, vedere* SP 800-128, Guida per la gestione della configurazione dei sistemi informativi (https://csrc.nist.gov/publications/detail/sp/800-128/final incentrata sulla sicurezza).

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Politica e procedure di gestione della configurazione NIST 800-53 CM-1
- Configurazione di base NIST 800-53 CM-2
- NIST 800-53 AC-4 Privilegio minimo
- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

5.4.3 Esegui il VMS su una rete dedicata

MOBOTIX consiglia, quando possibile, di separare la rete in cui è in esecuzione il VMS dalle reti con altri scopi. Ad esempio, una rete condivisa, ad esempio la rete della stampante, deve essere isolata dalla rete VMS. Inoltre, le implementazioni di MOBOTIX HUB VMS devono seguire una serie generale di best practice per le interconnessioni di sistema.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Connessioni di sistema NIST SP 800-53 CA-3

6 Server MOBOTIX

6.1 Procedura di base – Server MOBOTIX

6.1.1 Utilizza i controlli di accesso fisici e monitora la sala server

MOBOTIX consiglia di posizionare l'hardware con i server installati in una sala server designata e di utilizzare i controlli di accesso fisici. Inoltre, è necessario mantenere i registri di accesso per documentare chi ha avuto accesso fisico ai server. Anche la sorveglianza della sala server è una precauzione preventiva.
MOBOTIX supporta l'integrazione dei sistemi di controllo degli accessi e delle relative informazioni. Ad esempio, è possibile visualizzare i registri di accesso in MOBOTIX HUB Smart Client.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 PE-3 Controllo degli accessi fisici

6.1.2 Utilizzare canali di comunicazione crittografati

MOBOTIX consiglia di utilizzare una VPN per i canali di comunicazione per le installazioni in cui i server sono distribuiti su reti non attendibili. Questo per impedire agli aggressori di intercettare le comunicazioni tra i server. Anche per le reti affidabili, MOBOTIX consiglia di utilizzare HTTPS per la configurazione delle telecamere e di altri componenti del sistema.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 AC-4 Applicazione del flusso di informazioni
- Accesso remoto NIST 800-53 AC-17

6.2 Procedura avanzata – Server MOBOTIX

6.2.1 Eseguire servizi con account di servizio

MOBOTIX consiglia di creare account di servizio per i servizi relativi a MOBOTIX HUB VMS, invece di utilizzare un normale account utente. Configurare gli account del servizio come utenti del dominio e concedere loro solo le

autorizzazioni necessarie per eseguire i servizi pertinenti. Vedere 4.1.11 Autenticazione Kerberos (spiegazione). Ad esempio, l'account del servizio non deve essere in grado di accedere al desktop di Windows.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 AC-5 Separazione dei compiti
- NIST 800-53 AC-6 Privilegio minimo

6.2.2 Esegui i componenti su server virtuali o fisici dedicati

MOBOTIX consiglia di eseguire i componenti di MOBOTIX HUB VMS solo su server virtuali o fisici dedicati senza altri software o servizi installati.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Piano di gestione della configurazione NIST 800-53 CM-9

6.2.3 Limitare l'uso di supporti rimovibili su computer e server

MOBOTIX consiglia di limitare l'uso di supporti rimovibili, ad esempio chiavi USB, schede SD e smartphone, su computer e server in cui sono installati i componenti di MOBOTIX HUB VMS. Questo aiuta a prevenire l'ingresso di malware nella rete. Ad esempio, consentire solo agli utenti autorizzati di collegare supporti rimovibili quando è necessario trasferire prove video.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 MP-7 Uso dei media

6.2.4 Utilizza account amministratore individuali per un controllo migliore

A differenza degli account amministratore condivisi, MOBOTIX consiglia di utilizzare account individuali per gli amministratori. In questo modo è possibile tenere traccia di chi fa cosa in MOBOTIX HUB VMS. Questo aiuta a prevenire l'ingresso di malware nella rete. È quindi possibile utilizzare una directory autorevole, ad esempio Active Directory, per gestire gli account amministratore.
Gli account amministratore vengono assegnati ai ruoli in Management Client in **Ruoli**.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 AC-5 Separazione dei compiti
- Piano di gestione della configurazione NIST 800-53 CM-9

6.2.5 Utilizzare subnet o VLAN per limitare l'accesso al server

MOBOTIX consiglia di raggruppare logicamente diversi tipi di host e utenti in subnet separate. Ciò può comportare vantaggi nella gestione dei privilegi per questi host e utenti come membri di un gruppo con una determinata funzione o ruolo. Progettare la rete in modo che vi sia una subnet o una VLAN per ogni funzione. Ad esempio, una subnet o una VLAN per gli operatori di sorveglianza e una per gli amministratori. In questo modo è possibile definire le regole del firewall per gruppo anziché per singoli host.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- NIST SP 800-53 CSC 11: configurazioni sicure per dispositivi di rete come firewall, router e switch
- NIST SP 800-53 SC-7 Protezione dei confini

6.2.6 Abilita solo le porte utilizzate dal server eventi

MOBOTIX consiglia di abilitare solo le porte utilizzate dal server degli eventi e di bloccare tutte le altre porte, incluse le porte predefinite di Windows.
Le porte del server di eventi utilizzate nelle macchine virtuali hub MOBOTIX sono: 22331, 22333, 9090, 1234 e 1235.

Le porte utilizzate dipendono dalla distribuzione. In caso di dubbi, contattare l'assistenza MOBOTIX.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 CSC 11: configurazioni sicure per dispositivi di rete come firewall, router e switch

6.3 SQL Server

6.3.1 Connessione al server SQL e al database

È possibile specificare qualsiasi stringa di connessione SQL, inclusa quella in cui viene utilizzata l'autenticazione SQL (nome utente/password). Questo può essere utile durante i test perché non richiede l'accesso a un AD. Tuttavia, non è consigliabile utilizzare l'autenticazione con nome utente/password per le impostazioni di produzione, poiché sia il nome utente che la password vengono mantenuti non crittografati nel computer. Per le configurazioni di produzione si consiglia di utilizzare la sicurezza integrata.

La comunicazione tra le macchine virtuali MOBOTIX MOBOTIX HUB e il server SQL e il database può essere potenzialmente manomessa da un utente malintenzionato perché il certificato non è convalidato.
Per mitigare questo problema, è necessario prima configurare certificati server verificabili. Dopo aver configurato i certificati, è necessario modificare ConnestionString nel registro di Windows rimuovendo trustServerCertificate=true, come indicato di seguito:
Chiave del Registro di sistema:
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\Common\ConnectionString

- Corrente
  stringa di connessione: Data Source=localhost; catalogo iniziale='Sorveglianza'; Sicurezza Integrata = SSPI; crittografare=vero; trustServerCertificate=vero
- Temprato
  stringa di connessione: Data Source=localhost; catalogo iniziale='Sorveglianza'; Sicurezza Integrata = SSPI; encrypt=vero

In questo modo, la crittografia viene eseguita solo se è presente un certificato server verificabile, altrimenti il tentativo di connessione non riesce.
Questo problema è descritto in dettaglio nell'articolo Utilizzo della crittografia senza convalida.

6.3.2 Eseguire SQL Server e il database in un server separato

MOBOTIX consiglia di rendere ridondanti SQL Server e il database. Ciò riduce il rischio di tempi di inattività reali o percepiti.

Per supportare Windows Server Failover Clustering (WSFC), MOBOTIX consiglia di eseguire SQL Server e il database su un server separato e non sul server di gestione.
SQL Server deve essere eseguito nell'installazione WSFC e i server di gestione e di eventi devono essere eseguiti in un'installazione di Microsoft Cluster (o tecnologia simile). Per altre informazioni su WSFC, vedere *Windows Server Failover Clustering (WSFC) con SQL Server* (https://msdn.microsoft.com/en-us/library/hh270278.aspx).

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 SC-7 Protezione dei confini
- Piano di gestione della configurazione NIST 800-53 CM-9

6.4 Server di gestione

6.4.1 Regolare il timeout del token

MOBOTIX HUB VMS utilizza i token di sessione quando accede al server di gestione utilizzando i protocolli SSL (utenti di base) o NTLM (utenti Windows). Un token viene recuperato dal server di gestione e utilizzato sui server secondari, ad esempio il server di registrazione e talvolta anche il server degli eventi. In questo modo si evita che la ricerca NTLM e AD venga eseguita su ogni componente del server.
Per impostazione predefinita, un token è valido per 240 minuti. È possibile regolarlo fino a intervalli di 1 minuto. Questo valore può anche essere regolato nel tempo. Brevi intervalli aumentano la sicurezza, tuttavia, il sistema genera una comunicazione aggiuntiva quando rinnova il token.
L'intervallo migliore da utilizzare dipende dalla distribuzione. Questa comunicazione aumenta il carico del sistema e può influire sulle prestazioni.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'autenticatore NIST SP 800-53 IA-5

6.4.2 Abilitare solo le porte utilizzate dal server di gestione

MOBOTIX consiglia di abilitare solo le porte utilizzate dal server di gestione e di bloccare tutte le altre porte, incluse le porte predefinite di Windows. Queste linee guida sono coerenti per i componenti server di MOBOTIX HUB VMS.
Le porte del server di gestione utilizzate nelle VMS HUB MOBOTIX sono: 80, 443, 1433, 7475, 8080, 8990, 9993, 12345.

Le porte utilizzate dipendono dalla distribuzione. In caso di dubbi, contattare l'assistenza MOBOTIX.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- NIST SP 800-53 SC-7 Protezione dei confini

6.4.3 Disabilita i protocolli non sicuri

Quando un utente di base accede al server di gestione tramite IIS, il client di gestione utilizzerà qualsiasi protocollo disponibile. MOBOTIX consiglia di implementare sempre l'ultima versione di Transport Layer Security (TLS, attualmente 1.2) (https://datatracker.ietf.org/wg/tls/charter/) e di disabilitare tutte le suite di crittografia improprie e le versioni obsolete dei protocolli SSL/TLS. Eseguire azioni per bloccare i protocolli non sicuri a livello di sistema operativo. In questo modo si evita che il client di gestione utilizzi protocolli non sicuri. Il sistema operativo determina il protocollo da utilizzare.

I protocolli utilizzati dipendono dalla distribuzione. In caso di dubbi, contattare l'assistenza MOBOTIX.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Accesso remoto NIST 800-53 AC-17 (disabilita i protocolli inutilizzati)
- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

6.4.4 Disabilitare il canale di comunicazione remota legacy

La comunicazione tra i server di registrazione e il server di gestione è diventata più sicura con la soluzione implementata nel 2019 R2. Se si esegue l'aggiornamento da una versione precedente di MOBOTIX HUB VMS, il server di gestione avvia comunque la tecnologia legacy di terze parti per poter comunicare con i server di registrazione nelle versioni precedenti.
Quando tutti i server di registrazione del sistema vengono aggiornati alla versione 2019 R2 o successiva, è possibile configurare il server di gestione in modo che non avvii il canale di comunicazione remota legacy, per rendere il sistema meno vulnerabile, MOBOTIX consiglia di impostare **UseRemoting** su **False** nel file di configurazione del server di gestione.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Accesso remoto NIST 800-53 AC-17 (disabilita i protocolli inutilizzati)
- Impostazioni di configurazione NIST 800-53 CM-6

6.4.5 Gestire le informazioni dell'intestazione IIS

Disabilitare le informazioni dell'intestazione IIS

Per motivi di sicurezza, MOBOTIX consiglia di disabilitare le intestazioni X-Powered-By HTTP e X-AspNet-Version. L'intestazione HTTP X-Powered-By rivela la versione di IIS utilizzata nel server. Disabilitare questa intestazione effettuando le seguenti operazioni:

1. Aprire Gestione IIS.
2. Seleziona il sito Web predefinito.
3. Selezionare Intestazioni risposta HTTP.
4. Selezionare l'intestazione HTTP X-Powered-By e selezionare Rimuovi.

L'intestazione HTTP X-AspNet-Version rivela la versione di ASP.NET utilizzata dal pool di applicazioni del server di gestione. Disabilitare questa intestazione effettuando le seguenti operazioni:

1. Aprire il file web.config che si trova in %windir%\Microsoft.NET\Framework\v4.0.30319\CONFIG.
2. Dopo il tag <system.web> aggiungere questo: <httpRuntime enableVersionHeader="false" />
3. Salva il file.

La variabile di intestazione SERVER non deve essere rimossa, poiché causerà l'interruzione della funzionalità all'interno del server di gestione.

Impostazione delle opzioni del fotogramma X

Per motivi di sicurezza, MOBOTIX consiglia di impostare le opzioni X-Frame su **Nega**.
Quando si imposta l'intestazione HTTP X-Frame-Options su deny, questo disabilita il caricamento della pagina in un frame, indipendentemente dal sito che sta tentando di accedere.
Modificare questa intestazione effettuando le seguenti operazioni:

1. Aprire Gestione IIS.
2. Seleziona il sito Web predefinito > l'installazione.
3. Selezionare Intestazioni risposta HTTP.
4. Fare clic con il pulsante destro del mouse e selezionare Aggiungi... dal menu
5. Nel campo Nome scrivere X-Frame-Options e nel campo Valore scrivere negare.

6.4.6 Disabilita i verbi HTTP TRACE / TRACK IIS

Per motivi di sicurezza, MOBOTIX consiglia di disabilitare il verbo HTTP TRACE nell'installazione di IIS. Disabilitare il verbo HTTP TRACE eseguendo le operazioni seguenti:

1. Aprire Gestione IIS.
2. Seleziona il sito Web predefinito.
3. Fare doppio clic su Filtro richieste.

Se **il filtro delle richieste** non è disponibile, installarlo seguendo le istruzioni riportate di seguito: https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/requestfiltering/

4. Selezionare la scheda Verbi HTTP.
5. Selezionare Nega verbo dal menu Azioni.
6. Digitare TRACE e fare clic su OK.
7. Selezionare Nega verbo dal menu Azioni.
8. Digita TRACK e fai clic su OK.
9. Selezionare Nega verbo dal menu Opzioni.

10. Digita OPTIONS e fai clic su OK.

6.4.7 Disabilita la pagina predefinita di IIS

Per motivi di sicurezza, MOBOTIX consiglia di disabilitare la pagina predefinita di IIS. In questo modo, si rimuovono le informazioni che potrebbero essere utilizzate per individuare le tecnologie utilizzate nell'installazione e ci si allinea alle procedure consigliate di IIS definite da Microsoft. Disabilita la pagina predefinita effettuando le seguenti operazioni:

1. Aprire Gestione IIS.
2. Seleziona il sito Web predefinito.
3. Fare doppio clic su Documento predefinito.
4. Seleziona Disabilita nel menu Azioni.

6.5 Provider di identità

6.5.1 Disabilitare le informazioni dell'intestazione IIS sul provider di identità

Per motivi di sicurezza, MOBOTIX AG consiglia di disabilitare l'intestazione del server nell'applicazione del provider di identità .

L'intestazione del server descrive il software utilizzato dal server di original che gestisce una richiesta. Disabilitare questa intestazione effettuando le seguenti operazioni.

Questa opzione è applicabile solo a IIS 10 e versioni successive.

1. Aprire Gestione IIS.
2. Nel sito Web predefinito, seleziona **IDP**.
3. Aprire l' **editor di configurazione**.
4. Seleziona la sezione **system.webServer/security/requestFiltering**.
5. Impostare **removeServerHeader** su **True**.

6.6 Server di registrazione

6.6.1 Proprietà delle impostazioni di archiviazione e registrazione

Le funzionalità disponibili dipendono dal sistema in uso. Per ulteriori informazioni, vedere https://www.mobotix.com/en/vms/mobotix-hub/levels.

Nella finestra di dialogo **Impostazioni di archiviazione e registrazione**, specificare quanto segue:

Nome	Descrizione
Nome	Se necessario, rinominare lo spazio di archiviazione. I nomi devono essere univoci.
Sentiero	Specificare il percorso della directory in cui salvare le registrazioni in questa memoria. L'archiviazione non deve necessariamente trovarsi sul computer del server di registrazione.

Nome	Descrizione
	Se la directory non esiste, è possibile crearla. Le unità di rete devono essere specificate utilizzando il formato UNC (Universal Naming Convention), ad esempio: \\server\volume\directory\.
Tempo di ritenzione	Specificare per quanto tempo le registrazioni devono rimanere nell'archivio prima di essere eliminate o spostate nell'archivio successivo (a seconda delle impostazioni dell'archivio). Il tempo di conservazione deve essere sempre superiore al tempo di conservazione dell'archivio precedente o del database di registrazione predefinito. Ciò è dovuto al fatto che il numero di giorni di conservazione specificato per un archivio include tutti i periodi di conservazione indicati in precedenza nel processo.
Dimensione massima	Selezionare il numero massimo di gigabyte di dati di registrazione da salvare nel database di registrazione. La registrazione di dati in eccesso rispetto al numero di gigabyte specificato viene spostata automaticamente nel primo archivio dell'elenco, se specificato, o eliminata. Quando sono disponibili meno di 5 GB di spazio libero, il sistema archivia automaticamente (o elimina sempre se non è definito un archivio successivo) i dati più vecchi in un database. Se lo spazio libero è inferiore a 1 GB, i dati vengono eliminati. Un database richiede sempre 250 MB di spazio libero. Se si raggiunge questo limite (se i dati non vengono eliminati abbastanza velocemente), non vengono scritti altri dati nel database fino a quando non si libera spazio sufficiente. La dimensione massima effettiva del database è la quantità di gigabyte specificata, meno 5 GB.
Firma	Abilita una firma digitale per le registrazioni. Ciò significa, ad esempio, che il sistema conferma che il video esportato non è stato modificato o manomesso durante la riproduzione. Il sistema utilizza l'algoritmo SHA-2 per la firma digitale.
Codifica	Seleziona il livello di crittografia delle registrazioni: • Nessuno • Leggero (minore utilizzo della CPU) • Forte (maggiore utilizzo della CPU) Il sistema utilizza l'algoritmo AES-256 per la crittografia. Se si seleziona **Chiaro**, una parte della registrazione viene crittografata. Se si seleziona Forte, l'intera registrazione viene crittografata. Se si sceglie di abilitare la crittografia, è necessario specificare anche una password di seguito.
Parola d'ordine	Immettere una password per gli utenti autorizzati a visualizzare i dati crittografati. MOBOTIX consiglia di utilizzare password complesse. Le password complesse non contengono parole che possono essere trovate in un dizionario o che fanno parte del nome dell'utente. Includono otto o più caratteri alfanumerici, lettere maiuscole e minuscole e caratteri speciali.

6.6.2 Utilizzare schede di interfaccia di rete separate

MOBOTIX consiglia di utilizzare più schede di interfaccia di rete (NIC) per separare la comunicazione tra i server di registrazione e i dispositivi dalla comunicazione tra i server di registrazione e i programmi client. I programmi client non devono comunicare direttamente con i dispositivi.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SC-7 Protezione dei confini

6.6.3 Harden Network Attached Storage (NAS) per archiviare i dati multimediali registrati

Il server di registrazione può utilizzare NAS (Network Attached Storage) per archiviare i dati multimediali registrati. Se si sceglie di utilizzare il NAS, è possibile rafforzarlo utilizzando i miglioramenti della sicurezza SMB 3.0, come descritto in questo documento sui miglioramenti della sicurezza SMB.

6.7 Componente server mobile MOBOTIX

6.7.1 Abilita solo le porte utilizzate dal server MOBOTIX Mobile

MOBOTIX consiglia di abilitare solo le porte utilizzate dal server MOBOTIX HUB Mobile e di bloccare tutte le altre porte, incluse le porte predefinite di Windows.
Per impostazione predefinita, il server mobile utilizza le porte 8081 e 8082.

Le porte utilizzate dipendono dalla distribuzione. In caso di dubbi, contattare l'assistenza MOBOTIX.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- NIST SP 800-53 SC-7 Protezione dei confini

6.7.2 Utilizzare una "zona demilitarizzata" (DMZ) per fornire l'accesso esterno

MOBOTIX consiglia di installare il server MOBOTIX HUB Mobile in una DMZ e su un computer con due interfacce di rete:

- Uno per la comunicazione interna
- Uno per l'accesso pubblico a Internet

Ciò consente agli utenti di client mobili di connettersi al server MOBOTIX Mobile con un indirizzo IP pubblico, senza compromettere la sicurezza o la disponibilità della rete VMS.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SC-7 Protezione dei confini

6.7.3 Disabilita i protocolli non sicuri

MOBOTIX consiglia di utilizzare solo i protocolli necessari e solo le versioni più recenti. Ad esempio, implementare l'ultima versione di Transport Layer Security (TLS, attualmente 1.2) e disabilitare tutte le altre suite di crittografia e

le versioni obsolete dei protocolli SSL/TLS. Ciò richiede la configurazione di Windows e di altri componenti del sistema e l'uso corretto di certificati e chiavi digitali.

La stessa raccomandazione viene fornita per il server di gestione. Per ulteriori informazioni, vedere Disabilita i protocolli non sicuri nella pagina 57.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Accesso remoto NIST 800-53 AC-17 (disabilita i protocolli inutilizzati)
- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

6.7.4 Configurare gli utenti per la verifica in due passaggi tramite e-mail

Le funzionalità disponibili dipendono dal sistema in uso. Per ulteriori informazioni, vedere https://www.mobotix.com/en/vms/mobotix-hub/levels.

Per imporre un ulteriore passaggio di accesso agli utenti del client MOBOTIX HUB Mobile o del client Web MOBOTIX HUB, impostare la verifica in due passaggi sul server MOBOTIX HUB Mobile. Oltre al nome utente e alla password standard, l'utente deve inserire un codice di verifica ricevuto via e-mail.

La verifica in due passaggi aumenta il livello di protezione del sistema di sorveglianza.

Fabbisogno

- È stato installato un server SMTP.
- Sono stati aggiunti utenti e gruppi al sistema MOBOTIX HUB nel client di gestione nel nodo Ruoli nel riquadro di navigazione del sito. Nel ruolo pertinente, selezionare la scheda Utenti e gruppi.
- Se il sistema è stato aggiornato da una versione precedente di MOBOTIX HUB, è necessario riavviare il server mobile per abilitare la funzione di verifica in due passaggi.

In Client di gestione o Applicazione di gestione eseguire la procedura seguente:

1. Inserisci le informazioni sul tuo server SMTP.
2. Specificare le impostazioni per il codice di verifica che verrà inviato agli utenti client.
3. Assegna il metodo di accesso a utenti e gruppi di dominio.

In questo argomento viene descritto ognuno di questi passaggi.

Inserisci le informazioni sul tuo server SMTP

Il provider utilizza le informazioni sul server SMTP:

1. Nel riquadro di navigazione, selezionare Server mobili, quindi selezionare il server mobile pertinente.
2. Nella scheda Verifica in due passaggi selezionare la casella di controllo Abilita verifica in due passaggi.
3. In Impostazioni provider, nella scheda E-mail, inserisci le informazioni sul tuo server SMTP e specifica l'e-mail che il sistema invierà agli utenti client quando accedono e sono configurati per un accesso secondario. Per informazioni dettagliate su ciascun parametro, vedere la scheda Verifica in due passaggi a pagina 63.

Specificare il codice di verifica che verrà inviato agli utenti

Per specificare la complessità del codice di verifica:

1. Nella scheda Verifica in due passaggi, nella sezione Impostazioni codice di verifica, specificare il periodo entro il quale gli utenti di MOBOTIX Mobile Client o MOBOTIX HUB Web Client non devono verificare nuovamente l'accesso in caso, ad esempio, di una rete disconnessa. Il periodo predefinito è di 3 minuti.
2. Specificare il periodo entro il quale l'utente può utilizzare il codice di verifica ricevuto. Trascorso questo periodo, il codice non è più valido e l'utente deve richiederne uno nuovo. Il periodo predefinito è di 5 minuti.
3. Specificare il numero massimo di tentativi di immissione del codice, prima che l'utente venga bloccato. Il numero predefinito è 3.
4. Specificare il numero di caratteri per il codice. La lunghezza predefinita è 6.
5. Specificare la complessità del codice che si desidera venga composto dal sistema.

Assegnare il metodo di accesso a utenti e gruppi di Active Directory

Nella scheda **Verifica in due passaggi**, nella sezione **Impostazioni utente**, viene visualizzato l'elenco degli utenti e dei gruppi aggiunti al sistema MOBOTIX HUB.

1. Nella colonna Metodo di accesso, selezionare tra nessun accesso, nessuna verifica in due passaggi o metodo di consegna dei codici.
2. Nel campo Dettagli, aggiungi i dettagli di consegna, ad esempio gli indirizzi e-mail dei singoli utenti. La prossima volta che l'utente accede al client Web MOBOTIX HUB o al client MOBOTIX HUB Mobile, gli viene chiesto di effettuare un accesso secondario.
3. Se un gruppo è configurato in Active Directory, il server Mobile utilizza i dettagli, ad esempio gli indirizzi di posta elettronica, di Active Directory.
4. I gruppi di Windows non supportano la verifica in due passaggi.
5. Salvare la configurazione.

Hai completato i passaggi per configurare gli utenti per la verifica in due passaggi tramite email.

Scheda Verifica in due passaggi

Le funzionalità disponibili dipendono dal sistema in uso. Per ulteriori informazioni, vedere https://www.mobotix.com/en/vms/mobotix-hub/levels.

Utilizzare la **scheda Verifica in due passaggi** per abilitare e specificare un passaggio di accesso aggiuntivo per gli utenti di:

- App mobile MOBOTIX HUB sui dispositivi mobili iOS o Android
- MOBOTIX HUB Web Client

Il primo tipo di verifica è una password. Il secondo tipo è un codice di verifica, che è possibile configurare per essere inviato all'utente via e-mail.

Per ulteriori informazioni, vedere Configurare gli utenti per la verifica in due passaggi tramite e-mail a pagina 62.

Nelle tabelle seguenti vengono descritte le impostazioni di questa scheda.

Impostazioni del provider > Email

Nome	Descrizione
Server SMTP	Inserisci l'indirizzo IP o il nome host del server SMTP (Simple Mail Transfer Protocol) per le e-mail di verifica in due passaggi.
Porta del server SMTP	Specificare la porta del server SMTP per l'invio di e-mail. Il numero di porta predefinito è 25 senza SSL e 465 con SSL.

Nome	Descrizione
Usa SSL	Selezionare questa casella di controllo se il server SMTP supporta la crittografia SSL.
Nome utente	Specificare il nome utente per l'accesso al server SMTP.
Parola d'ordine	Specificare la password per l'accesso al server SMTP.
Utilizzare l'autenticazione con password sicura (SPA)	Selezionare questa casella di controllo se il server SMTP supporta SPA.
Indirizzo email del mittente	Specifica l'indirizzo e-mail per l'invio dei codici di verifica.
Oggetto dell'e-mail	Specifica il titolo dell'oggetto dell'e-mail. Esempio: il codice di verifica in due passaggi.
Testo dell'e-mail	Inserisci il messaggio che desideri inviare. Esempio: il tuo codice è {0}. Se si dimentica di includere la variabile {0}, il codice viene aggiunto alla fine del testo per impostazione predefinita.

Impostazioni del codice di verifica

Nome	Descrizione
Timeout di riconnessione (0-30 minuti)	Specificare il periodo entro il quale gli utenti del client MOBOTIX HUB Mobile non devono verificare nuovamente il proprio accesso in caso, ad esempio, di rete disconnessa. Il periodo predefinito è di tre minuti. Questa impostazione non si applica al client Web MOBOTIX HUB.
Il codice scade dopo (1-10 minuti)	Specificare il periodo entro il quale l'utente può utilizzare il codice di verifica ricevuto. Trascorso questo periodo, il codice non è più valido e l'utente deve richiederne uno nuovo. Il periodo predefinito è di cinque minuti.
Tentativi di immissione del codice (1-10 tentativi)	Specificare il numero massimo di tentativi di immissione del codice prima che il codice fornito non sia più valido. Il numero predefinito è tre.
Lunghezza del codice (4-6 caratteri)	Specificare il numero di caratteri per il codice. La lunghezza predefinita è sei.
Composizione del codice	Specificare la complessità del codice che si desidera venga generato dal sistema. Puoi scegliere tra: Latino maiuscolo (A-Z) Latino minuscolo (a-z) Cifre (0-9) Caratteri speciali (!@#...)

Impostazioni utente

Nome	Descrizione
Utenti e gruppi	Elenca gli utenti e i gruppi aggiunti al sistema MOBOTIX HUB.

Nome	Descrizione
	Se un gruppo è configurato in Active Directory, il server mobile utilizza i dettagli, ad esempio gli indirizzi di posta elettronica, di Active Directory. I gruppi di Windows non supportano la verifica in due passaggi.
Metodo di verifica	Seleziona un'impostazione di verifica per ogni utente o gruppo. Puoi scegliere tra: Nessun accesso: l'utente non può effettuare l'accesso Nessuna verifica in due passaggi: l'utente deve inserire nome utente e password Email: l'utente deve inserire un codice di verifica oltre al nome utente e alla password
Dettagli utente	Inserisci l'indirizzo email al quale ogni utente riceverà i codici.

6.7.5 Configurazione dei criteri di sicurezza dei contenuti (CSP)

I WebSocket con caratteri jolly devono essere rimossi dalle intestazioni CSP sul server mobile.

Attualmente ws://*:* e wss://*:* non possono essere rimossi dal CSP descritto nella configurazione del server mobile a causa delle limitazioni del browser Safari.

Per aumentare la sicurezza del server mobile, effettuare le seguenti operazioni:

1. Aprire il file VideoOS.MobileServer.Service.exe.config, che si trova nella cartella di installazione del server mobile.
2. Modificare la sezione <HttpHeaders>, dove il valore di key="Content-Security-Policy" è il seguente:
   - Se il supporto del browser Safari non è necessario, rimuovi ws://*:* e wss://*:* dall'intestazione.
   - Se è necessario il supporto del browser Safari, sostituisci ws://*:* e wss://*:* con i valori pertinenti "ws:// [nome host]:[porta] e wss://[nome host]:[porta]", dove nome host e porta sono quelli pertinenti utilizzati per accedere al server mobile.
3. Riavvia il server mobile.

6.8 Server di registro

6.8.1 Installare Log Server in un server separato con SQL Server

Per sistemi molto grandi con molte transazioni da e verso il database SQL del server di registro, MOBOTIX consiglia di installare il componente Server di registro su un server separato con il proprio SQL Server e di archiviare i registri in un database SQL su tale SQL Server locale. Se il server di log è interessato da problemi di prestazioni, ad esempio a causa di flooding o altri motivi, e utilizza lo stesso SQL Server del server di gestione, entrambi i servizi possono essere interessati.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SC-7 Protezione dei confini
- Piano di gestione della configurazione NIST SP 800-53 CM-9

6.8.2 Limitare l'accesso IP al server di log

MOBOTIX consiglia che solo i componenti VMS possano contattare il server di registro.Il server di registro utilizza la porta 22337.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

7 Programmi client

In questa sezione vengono fornite indicazioni su come proteggere i programmi client MOBOTIX.

I programmi client sono:

- MOBOTIX HUB Smart Client
- MOBOTIX HUB Web Client
- Client di gestione MOBOTIX HUB
- Cliente mobile MOBOTIX

7.1 Passaggi di base (tutti i programmi client)

7.1.1 Utilizzare gli utenti Windows con AD

MOBOTIX consiglia, quando possibile, di utilizzare gli utenti Windows in combinazione con Active Directory (AD) per accedere al VMS con i programmi client. In questo modo è possibile applicare un criterio password e applicare le impostazioni utente in modo coerente nel dominio e nella rete. Fornisce inoltre protezione contro gli attacchi di forza bruta. Per ulteriori informazioni, vedere Utilizzare gli utenti Windows con Active Directory.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Impostazioni di configurazione NIST 800-53 CM-6
- Documentazione del sistema informativo NIST 800-53 SA-5
- Affidabilità NIST 800-53 SA-13

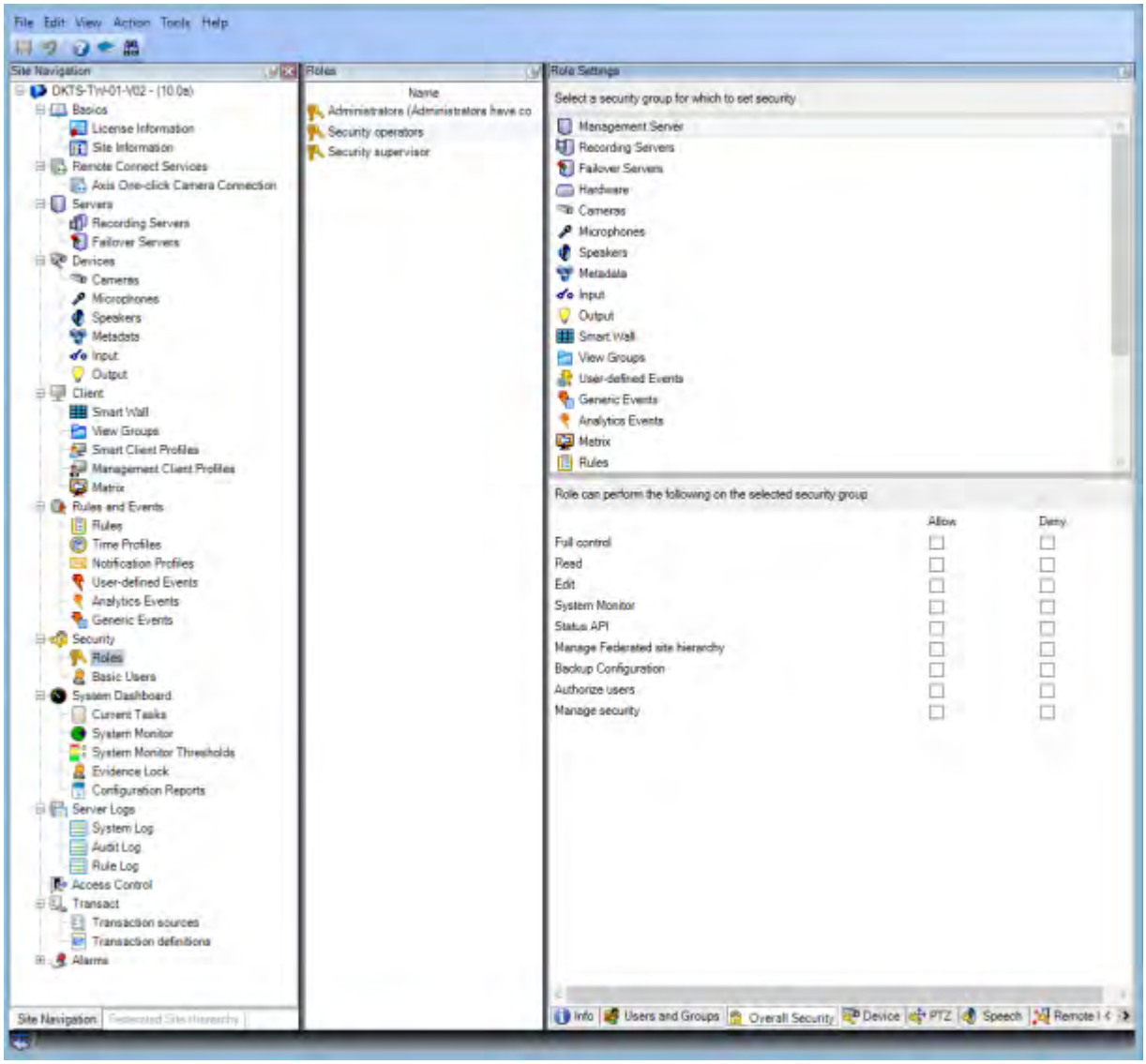
7.1.2 Limitare le autorizzazioni per gli utenti client

MOBOTIX consiglia agli amministratori di specificare le operazioni che gli utenti possono eseguire in Management Client o MOBOTIX HUB Smart Client.

Le istruzioni seguenti descrivono come eseguire questa operazione.

Per limitare le autorizzazioni degli utenti client, attenersi alla seguente procedura:

1. Aprire il client di gestione.
2. Espandere il nodo Sicurezza, selezionare Ruoli e quindi selezionare il ruolo a cui è associato l'utente.
3. Nelle schede in basso, puoi impostare autorizzazioni e restrizioni per il ruolo.



Per impostazione predefinita, tutti gli utenti associati al ruolo di amministratore hanno accesso illimitato al sistema. Sono inclusi gli utenti associati al ruolo di amministratore in Active Directory e quelli con il ruolo di amministratore nel server di gestione.

Ulteriori informazioni

I seguenti documenti forniscono ulteriori informazioni:

- NIST 800-53 AC-4 Privilegio minimo
- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

7.1.3 Esegui sempre i client su hardware attendibile su reti affidabili

MOBOTIX consiglia di eseguire sempre i client MOBOTIX HUB su dispositivi hardware con le impostazioni di sicurezza appropriate. Le linee guida specifiche per i dispositivi mobili sono disponibili in SP 800-124 (https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final). Queste impostazioni sono specifiche per il dispositivo.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SC-7 Protezione dei confini
- Impostazioni di configurazione NIST SP800-53 CM-6

7.2 Passaggi avanzati – MOBOTIX HUB Smart Client

7.2.1 Limita l'accesso fisico a qualsiasi computer che esegue MOBOTIX HUB Smart Client

MOBOTIX consiglia di limitare l'accesso fisico ai computer che eseguono MOBOTIX HUB Smart Client. Consentire l'accesso ai computer solo al personale autorizzato. Ad esempio, tieni la porta chiusa a chiave e usa i controlli di accesso e la sorveglianza.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 PE-1 Politica e procedure per la protezione fisica e ambientale
- NIST SP 800-53 PE-2 Autorizzazioni di accesso fisico
- NIST SP 800-53 PE-3 Controllo degli accessi fisici
- NIST SP 800-53 PE-6 Monitoraggio dell'accesso fisico

7.2.2 Utilizzare sempre una connessione sicura per impostazione predefinita, in particolare su reti pubbliche

Se è necessario accedere al VMS con MOBOTIX HUB Smart Client su una rete pubblica o non attendibile, MOBOTIX consiglia di utilizzare una connessione sicura tramite VPN. In questo modo è possibile garantire che la comunicazione tra MOBOTIX HUB Smart Client e il server VMS sia protetta.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- Accesso remoto NIST SP 800-53 AC-17
- Impostazioni di configurazione NIST SP 800-53 CM-6

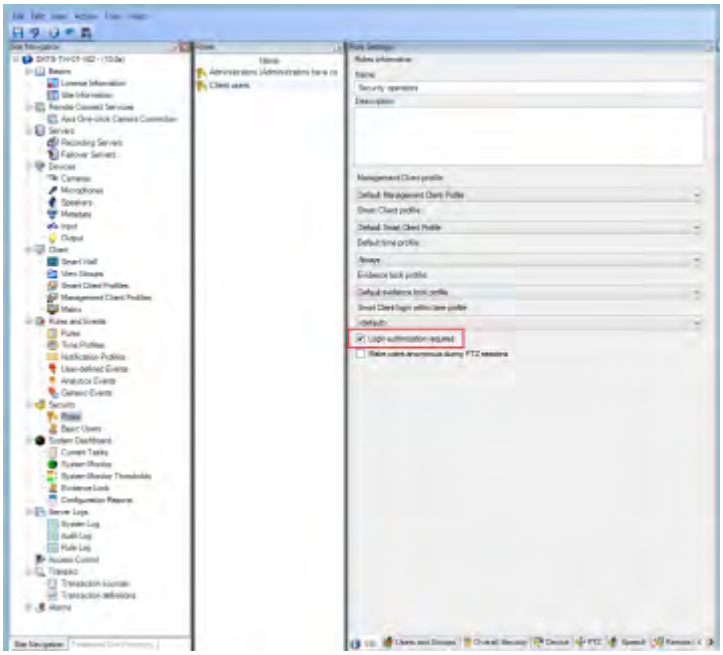
7.2.3 Attiva l'autorizzazione all'accesso

L'autorizzazione all'accesso richiede che un utente effettui l'accesso a MOBOTIX HUB Smart Client o Management Client e che un altro utente con uno stato elevato, ad esempio un supervisore, fornisca l'approvazione.
È possibile impostare l'autorizzazione di accesso per i ruoli. Agli utenti associati al ruolo viene richiesto a un secondo utente (un supervisore) di autorizzare il loro accesso al sistema.

L'autorizzazione all'accesso non è attualmente supportata dal client mobile, dal client Web MOBOTIX HUB e da qualsiasi integrazione SDK MOBOTIX Integration Platform (MIP).

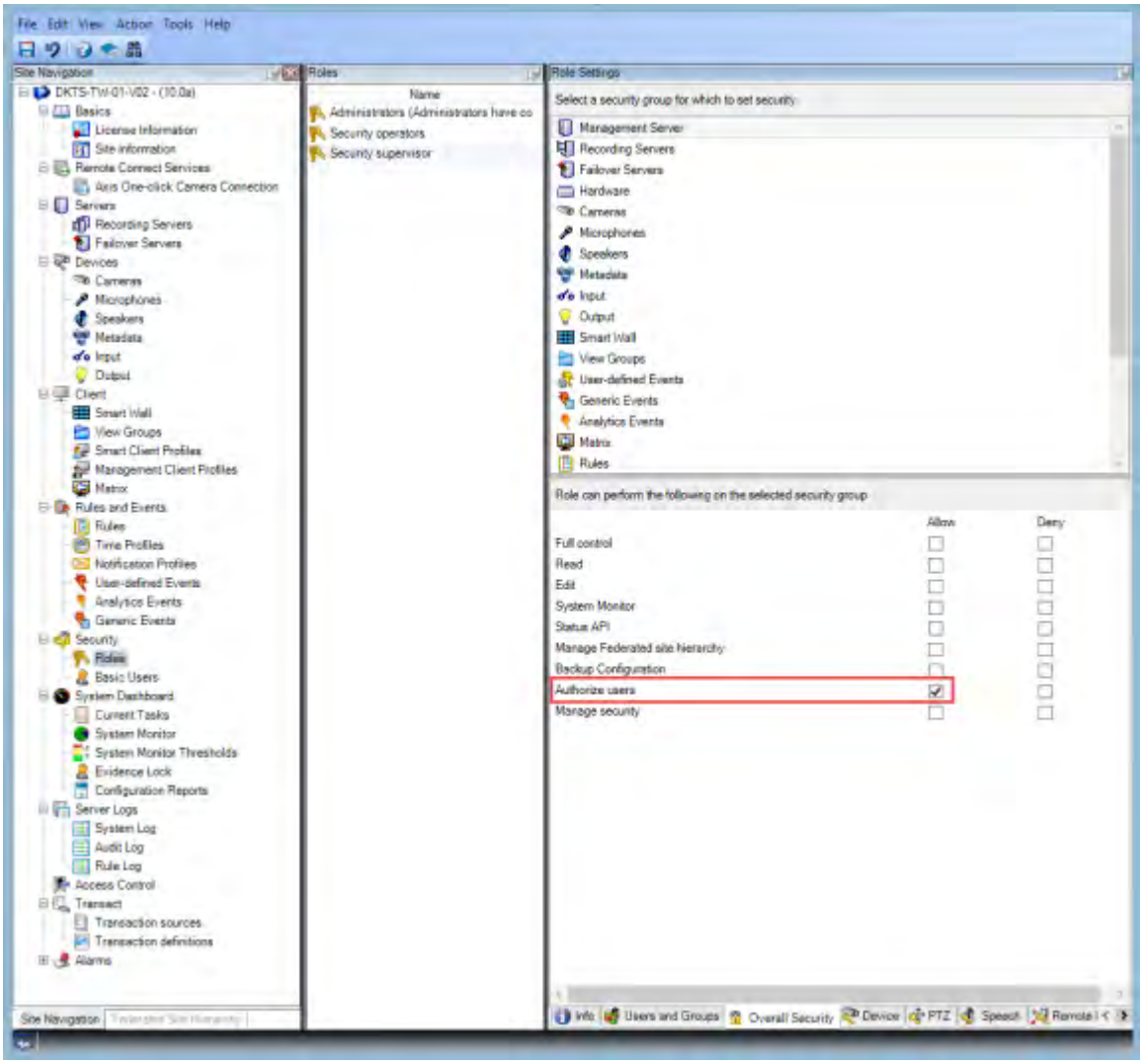
Per attivare l'autorizzazione all'accesso per un ruolo, procedi nel seguente modo:

1. Aprire il client di gestione.
2. Espandere il nodo Sicurezza, selezionare Ruoli e quindi selezionare il ruolo pertinente.
   Selezionare la **casella di controllo** Autorizzazione di accesso richiesta.



Per configurare i ruoli che autorizzano e concedono l'accesso, attenersi alla seguente procedura:

1. Per creare un nuovo ruolo, ad esempio "Supervisore della sicurezza", espandere il nodo Sicurezza, fare clic con il pulsante destro del mouse su Ruoli e creare un nuovo ruolo.
2. Fare clic sulla scheda Sicurezza generale e selezionare il nodo Server di gestione.
   Selezionare la casella di controllo Consenti accanto alla casella di **controllo Autorizza utenti**.



Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- NIST SP 800-53 AC-6 Privilegio minimo
- Accesso remoto NIST SP 800-53 AC-17
- Impostazioni di configurazione NIST SP 800-53 CM-6

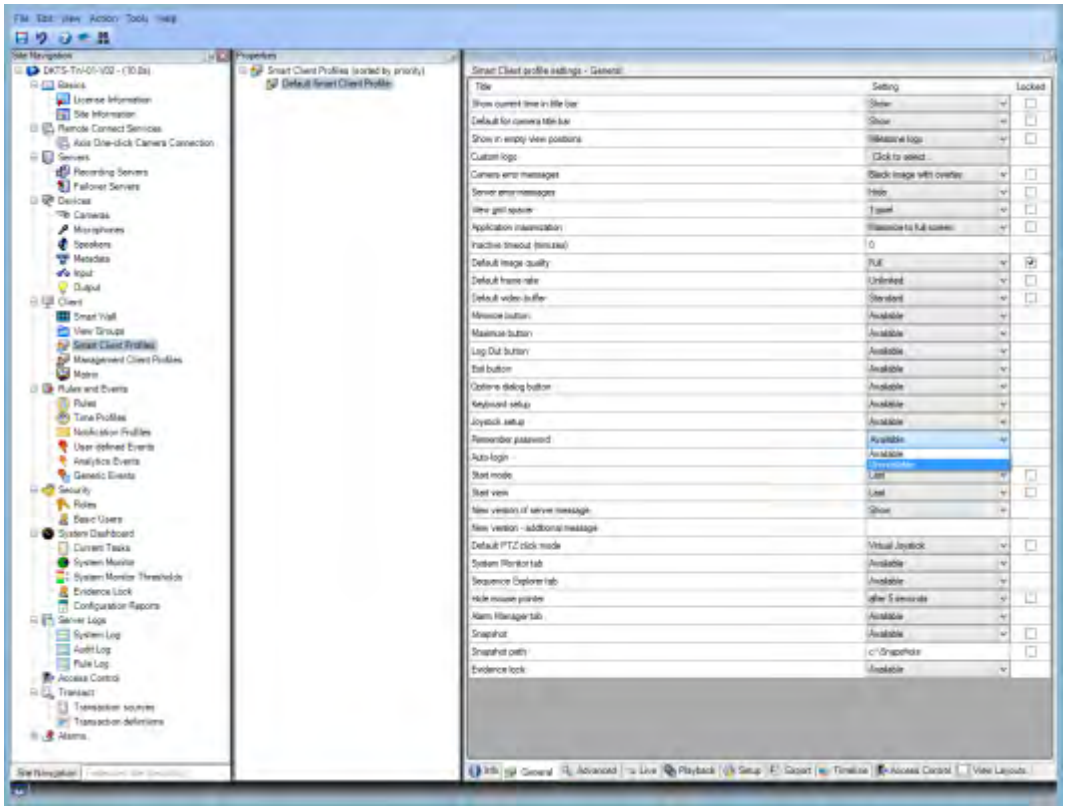
7.2.4 Non memorizzare le password

MOBOTIX HUB Smart Client offre agli utenti la possibilità di ricordare le password. Per ridurre il rischio di accesso non autorizzato, MOBOTIX consiglia di non utilizzare questa funzione.

Per disattivare la funzione Ricorda password, procedi nel seguente modo:

1. Aprire il client di gestione.
2. Espandere il nodo Client, selezionare Profili Smart Client e quindi selezionare il profilo Smart Client pertinente.
3. Nell'elenco Memorizza password selezionare Non disponibile.

L' opzione **Memorizza password** non è disponibile la prossima volta che un utente con questo profilo accede a MOBOTIX HUB Smart Client.



Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- Impostazioni di configurazione NIST SP 800-53 CM-6
- Politica e procedure di identificazione e autenticazione NIST SP 800-53 IA-1

7.2.5 Attivare solo le funzionalità client necessarie

Attiva solo le funzioni necessarie e disattiva le funzioni che non sono necessarie a un operatore di sorveglianza. Il punto è limitare le opportunità di uso improprio o errori.

È possibile attivare e disattivare le funzioni in MOBOTIX HUB Smart Client e in MOBOTIX HUB Management Client. In Management Client, configurare i profili Smart Client per specificare i set di autorizzazioni per gli utenti assegnati al profilo. I profili Smart Client sono simili ai profili Management Client e lo stesso utente può essere assegnato a ciascun tipo di profilo.

Per configurare un profilo Smart Client, attenersi alla seguente procedura:

1. Aprire il client di gestione.
2. Espandere il nodo Client, selezionare Profili Smart Client e quindi selezionare il profilo Smart Client pertinente.
3. Utilizzare le schede per specificare le impostazioni per le funzioni in Smart Client. Ad esempio, utilizzare le impostazioni della scheda Riproduzione per controllare le funzioni utilizzate per analizzare i video registrati.

Prima di assegnare un utente a un profilo Smart Client, assicurarsi che le autorizzazioni per il ruolo dell'utente siano appropriate per il profilo. Ad esempio, se si desidera che un utente sia in grado di analizzare il video, assicurarsi che il ruolo consenta all'utente di riprodurre video dalle videocamere e che la scheda Esplora sequenze sia disponibile nel profilo Smart Client.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- NIST SP 800-53 AC-6 Privilegio minimo
- Impostazioni di configurazione NIST SP 800-53 CM-6

7.2.6 Utilizzare nomi separati per gli account utente

MOBOTIX consiglia di creare un account utente per ogni utente e di utilizzare una convenzione di denominazione che semplifichi l'identificazione personale dell'utente, come il nome o le iniziali. Si tratta di una procedura consigliata per limitare l'accesso solo a ciò che è necessario e riduce anche la confusione durante l'auditing.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 AC-4 Privilegio minimo
- Politica e procedure di gestione della configurazione NIST 800-53 CM-1
- Configurazione di base NIST 800-53 CM-2
- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

7.2.7 Vietare l'uso di supporti rimovibili

Per le esportazioni video, stabilire una catena di procedure specifiche per le prove. MOBOTIX raccomanda che la politica di sicurezza consenta solo agli operatori autorizzati di MOBOTIX HUB Smart Client di collegare dispositivi di archiviazione rimovibili come unità flash USB, schede SD e smartphone al computer su cui è installato MOBOTIX HUB Smart Client.

I supporti rimovibili possono trasferire malware nella rete e sottoporre i video a una distribuzione non autorizzata. In alternativa, i criteri di sicurezza possono specificare che gli utenti possono esportare le prove solo in una posizione specifica della rete o solo in un masterizzatore multimediale. È possibile controllare questa operazione tramite il profilo Smart Client.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SO 800-53 MP-7 Uso dei media
- Protezione da codice dannoso NIST SP 800-53 SI-3

7.3 Passaggi avanzati – Client mobile MOBOTIX

SP 800-124 revisione 1 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf) fornisce indicazioni specifiche per i dispositivi mobili. Le informazioni in esso contenute si applicano a tutti gli argomenti di questa sezione.

7.3.1 Utilizzare sempre il client MOBOTIX Mobile su dispositivi sicuri

MOBOTIX consiglia di utilizzare sempre il client MOBOTIX HUB Mobile su dispositivi sicuri, configurati e mantenuti in base a una politica di sicurezza. Ad esempio, assicurarsi che i dispositivi mobili non consentano agli utenti di installare software da fonti non autorizzate. Un app store aziendale è un esempio di un modo per limitare le applicazioni dei dispositivi come parte della gestione complessiva dei dispositivi mobili.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SC-7 Protezione dei confini
- Impostazioni di configurazione NIST SP800-53 CM-6

7.3.2 Scarica il client MOBOTIX Mobile da fonti autorizzate

MOBOTIX consiglia di scaricare il client MOBOTIX HUB Mobile da una delle seguenti fonti:

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

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST SP 800-53 SC-7 Protezione dei confini
- Impostazioni di configurazione NIST SP 800-53 CM-6

7.3.3 I dispositivi mobili devono essere protetti

Se si desidera accedere al VMS con un dispositivo mobile su una rete pubblica o non attendibile, MOBOTIX consiglia di farlo con una connessione sicura, utilizzare l'autenticazione appropriata e Transport Layer Security (TLS) (https://datatracker.ietf.org/wg/tls/charter/) (o connettersi tramite VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) e HTTPS. Ciò consente di proteggere le comunicazioni tra il dispositivo mobile e il VMS.

MOBOTIX consiglia ai dispositivi mobili di utilizzare il blocco schermo. In questo modo è possibile impedire l'accesso non autorizzato al VMS, ad esempio in caso di smarrimento dello smartphone. Per la massima sicurezza, implementare una politica di sicurezza che impedisca al client MOBOTIX HUB Mobile di ricordare il nome utente e la password.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- Accesso remoto NIST SP 800-53 AC-17
- Impostazioni di configurazione NIST SP 800-53 CM-6

7.4 Procedura avanzata – MOBOTIX HUB Web Client

7.4.1 Esegui sempre MOBOTIX HUB Web Client su computer client attendibili

Collegare sempre in modo sicuro tutti i componenti del VMS. Le connessioni da server a server e da client a server devono utilizzare l'autenticazione appropriata e la https://datatracker.ietf.org/wg/tls/charter/ (Transport Layer Security) (o connettersi tramite VPN (https://datatracker.ietf.org/wg/ipsec/documents/)) e HTTPS. Eseguire sempre MOBOTIX HUB Web Client su computer affidabili, ad esempio, non utilizzare un computer client in uno spazio pubblico. MOBOTIX consiglia di informare gli utenti sulle misure di sicurezza da ricordare quando si utilizzano applicazioni basate su browser, come MOBOTIX HUB Web Client. Ad esempio, assicurati che sappiano di non consentire al browser di ricordare la loro password.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- Impostazioni di configurazione NIST SP 800-53 CM-6
- Identificazione e autenticazione NIST SP 800-53 IA-2

7.4.2 Utilizzo dei certificati per confermare l'identità di un server MOBOTIX Mobile

Questo documento sottolinea l'uso della versione più recente di TLS. Da qui la necessità di un uso corretto dei certificati e dell'implementazione della suite di crittografia TLS. MOBOTIX consiglia di installare un certificato sul server MOBOTIX HUB Mobile per confermare l'identità del server quando un utente tenta di connettersi tramite il client Web MOBOTIX HUB.

Per ulteriori informazioni, vedere la *sezione Modifica certificato* nel *manuale MOBOTIX HUB VMS - Administrator*.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- Impostazioni di configurazione NIST SP 800-53 CM-6
- Identificazione e autenticazione NIST SP 800-53 IA-2

7.4.3 Utilizza solo i browser supportati con gli aggiornamenti di sicurezza più recenti

MOBOTIX consiglia di installare solo uno dei seguenti browser sui computer client. Assicurati di includere gli aggiornamenti di sicurezza più recenti.

- Safari delle mele
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Politica e procedure di gestione della configurazione NIST SP 800-53 CM-1
- Configurazione di base NIST SP 800-53 CM-2
- Impostazioni di configurazione NIST SP 800-53 CM-6
- Architettura di sicurezza delle informazioni NIST SP 800-53 PL-8
- Protezione da codice dannoso NIST SP 800-53 SI-3

7.5 Passaggi avanzati - Client di gestione

7.5.1 Utilizzare i profili client di gestione per limitare la visualizzazione consentita dagli amministratori

MOBOTIX consiglia di utilizzare i profili del client di gestione per limitare ciò che gli amministratori possono visualizzare nel client di gestione.

I profili del client di gestione consentono agli amministratori di sistema di modificare l'interfaccia utente del client di gestione. Associare i profili client di gestione ai ruoli per limitare l'interfaccia utente in modo da rappresentare le funzionalità disponibili per ogni ruolo di amministratore.

Visualizzare solo le parti del VMS necessarie agli amministratori per svolgere le proprie attività.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- NIST 800-53 AC-4 Privilegio minimo
- Politica e procedure di gestione della configurazione NIST 800-53 CM-1
- Configurazione di base NIST 800-53 CM-2
- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

7.5.2 Consenti agli amministratori di accedere alle parti pertinenti del VMS

Se si dispone di una configurazione che richiede più amministratori, MOBOTIX consiglia di configurare diritti di amministratore diversi per gli amministratori che utilizzano il client di gestione.

Per definire le autorizzazioni di amministratore, attenersi alla seguente procedura:

1. In Client di gestione espandere il nodo Sicurezza, selezionare Ruoli e quindi selezionare il ruolo di amministratore pertinente.
   Non è possibile modificare il ruolo di amministratore predefinito, pertanto è necessario creare ruoli di amministratore aggiuntivi.
2. Nella scheda Sicurezza generale specificare le azioni che l'amministratore può eseguire per ogni gruppo di sicurezza.
3. Nelle altre schede, specificare le impostazioni di sicurezza per il ruolo nel VMS.
   Per ulteriori informazioni, consultare il manuale dell'amministratore di MOBOTIX HUB VMS.
4. Nella scheda Info, associare il ruolo a un profilo client di gestione.

È possibile attivare o disattivare le funzionalità utilizzando il profilo del client di gestione. Prima di assegnare un utente a un profilo client di gestione, assicurarsi che le autorizzazioni per il ruolo dell'utente siano appropriate per il profilo. Ad esempio, se si desidera che un utente sia in grado di gestire le telecamere, assicurarsi che il ruolo consenta all'utente di eseguire questa operazione e che le telecamere siano abilitate nel profilo del client di gestione.

Ulteriori informazioni

- I controlli seguenti forniscono ulteriori indicazioni:
- NIST 800-53 AC-4 Privilegio minimo
- Politica e procedure di gestione della configurazione NIST 800-53 CM-1
- Configurazione di base NIST 800-53 CM-2
- Impostazioni di configurazione NIST 800-53 CM-6
- NIST 800-53 CM-7 Funzionalità minima

7.5.3 Esegui il client di gestione su reti affidabili e sicure

Se si accede al server di gestione con il client di gestione tramite HTTP, la comunicazione in testo normale può contenere dettagli di sistema non crittografati. MOBOTIX consiglia di eseguire il client di gestione solo su reti affidabili e conosciute. Usa una VPN per fornire l'accesso remoto.

Ulteriori informazioni

I controlli seguenti forniscono ulteriori indicazioni:

- Gestione dell'account NIST SP 800-53 AC-2
- Impostazioni di configurazione NIST SP 800-53 CM-6
- Identificazione e autenticazione NIST SP 800-53 IA-2

8 Conformità

8.1 Conformità FIPS 140-2

In questa sezione viene illustrato FIPS 140-2 e come configurare e utilizzare MOBOTIX HUB VMS per operare in modalità conforme a FIPS 140-2.

I termini "conforme a FIPS 140-2" e "modalità conforme a FIPS 140-2" non sono giuridicamente vincolanti. I termini sono utilizzati qui per chiarezza.

Conforme a FIPS 140-2 significa che il software utilizza istanze di algoritmi e funzioni di hashing convalidate da FIPS 140-2 in tutti i casi in cui i dati crittografati o con hash vengono importati o esportati dal software. Inoltre, ciò significa che il software gestirà le chiavi in modo sicuro, come richiesto dai moduli crittografici convalidati FIPS 140-2. Il processo di gestione delle chiavi include anche la generazione e l'archiviazione delle chiavi.

La modalità conforme a FIPS 140-2 si riferisce al software che contiene metodi di sicurezza approvati da FIPS e non approvati da FIPS, in cui il software dispone di almeno una "modalità di funzionamento FIPS". Questa modalità di funzionamento consente solo il funzionamento di metodi di sicurezza approvati dalla FIPS. Ciò significa che quando il software è in "modalità FIPS", non viene utilizzato un metodo non approvato da FIPS al posto del metodo approvato da FIPS.

Vengono trattati i seguenti argomenti.

8.1.1 Che cos'è FIPS?

Gli standard federali per l'elaborazione delle informazioni (FIPS) sono una famiglia di standard sviluppati dai seguenti due enti governativi:

- Il National Institute of Standards and Technology (NIST) negli Stati Uniti
- L'Istituzione per la Sicurezza delle Comunicazioni (CSE) in Canada

Tali norme mirano a garantire la sicurezza e l'interoperabilità informatica.

Tutte le soluzioni software implementate nella pubblica amministrazione e nei settori altamente regolamentati negli Stati Uniti e in Canada devono essere conformi allo standard FIPS 140-2.

8.1.2 Che cos'è FIPS 140-2?

FIPS 140-2, intitolato "Security Requirements for Cryptographic Modules", specifica quali algoritmi di crittografia e quali algoritmi di hashing possono essere utilizzati e come devono essere generate e gestite le chiavi di crittografia. I requisiti di sicurezza specificati in questo standard hanno lo scopo di mantenere la sicurezza fornita da un modulo crittografico, ma la conformità a questo standard non è sufficiente per garantire che un particolare modulo sia sicuro. L'operatore di un modulo crittografico è responsabile di garantire che la sicurezza fornita dal modulo sia sufficiente e accettabile per il proprietario delle informazioni che vengono protette e che qualsiasi rischio residuo sia riconosciuto e accettato.

8.1.3 Quali applicazioni MOBOTIX HUB VMS possono funzionare in modalità conforme a FIPS 140-2?

A partire da MOBOTIX HUB VMS 2020 R3, tutti gli algoritmi di crittografia sono stati sostituiti con Cryptography New Generation (CNG) di Microsoft, che aderisce alle più recenti tecnologie di sicurezza disponibili ed è conforme a FIPS. In altre parole, tutte le applicazioni MOBOTIX HUB VMS 2020 R3 possono funzionare in modalità conforme a FIPS. Per motivi di compatibilità con le versioni precedenti, alcuni algoritmi e processi non conformi persistono in MOBOTIX HUB VMS, anche dopo la versione 2020 R3, ma ciò non pregiudica la capacità di far funzionare il sistema in modalità conforme a FIPS.

MOBOTIX HUB VMS è sempre conforme a FIPS?

No. Alcuni algoritmi e processi non conformi persistono nelle VMS MOBOTIX HUB. Tuttavia, MOBOTIX HUB VMS può essere configurato e funzionare in modo da utilizzare solo le istanze dell'algoritmo certificato FIPS 140-2 e quindi operare in una modalità conforme a FIPS.

È necessario abilitare la modalità FIPS 140-2?

Prima di abilitare la modalità FIPS 140–2 è necessario capire se ne hai bisogno o meno. Ad esempio, se si lavora ed è connessi a una rete e a un'infrastruttura governativa statunitense o canadese, è obbligatorio rispettare lo standard FIPS 140-2 e abilitarlo sul computer per la comunicazione secondo lo standard. Inoltre, l'abilitazione della modalità FIPS 140-2 nel sistema operativo Windows limita l'esecuzione di molti programmi e servizi, poiché in seguito saranno supportati solo algoritmi e servizi approvati da FIPS. Pertanto, si consiglia di verificare se c'è una necessità o meno.

8.1.4 Come garantire che le VMS MOBOTIX HUB possano funzionare in modalità conforme a FIPS 140-2?

Per utilizzare MOBOTIX HUB VMS in modalità FIPS 140-2, è necessario:

- Assicurarsi che le integrazioni di terze parti possano funzionare su un sistema operativo Windows abilitato per FIPS (vedere Verifica delle integrazioni di terze parti a pagina 80)
- Connettersi ai dispositivi in modo da garantire una modalità di funzionamento conforme a FIPS 140-2 (vedere Connessione di dispositivi: informazioni di base a pagina 81)
- Assicurarsi che i dati nel database multimediale siano crittografati con algoritmi conformi a FIPS 140-2 (vedere Database multimediale: considerazioni relative alla compatibilità con le versioni precedenti nella pagina 82)
- Esegui il sistema operativo Windows in modalità di funzionamento approvata FIPS 140-2. Per informazioni sull'abilitazione di FIPS, vedere il sito Microsoft.

8.1.5 Considerazioni relative all'aggiornamento

L'aggiornamento a MOBOTIX HUB VMS 2020 R3 per funzionare in modalità conforme a FIPS richiede un processo di aggiornamento univoco. Questo processo di aggiornamento è richiesto solo dagli utenti esistenti di MOBOTIX HUB VMS che devono operare in modalità conforme a FIPS.

Il processo di aggiornamento dipende dalla versione di MOBOTIX HUB VMS da cui si sta eseguendo l'aggiornamento.

Processo di aggiornamento consigliato per i clienti che eseguono MOBOTIX HUB VMS

1. Avviare un'indagine per verificare se le integrazioni di terze parti sono conformi a FIPS 140-2 (vedere Verificare le integrazioni di terze parti a pagina 80).
2. Preparare le connessioni dei dispositivi in modo che siano conformi a FIPS 140-2 (vedere Connessione dei dispositivi: informazioni di base a pagina 81).
3. Esportare le registrazioni effettuate con le versioni di MOBOTIX HUB VMS precedenti alla 2017 R2 (vedere Database multimediale: Considerazioni sulla compatibilità con le versioni precedenti a pagina 82).
   Questo vale per i clienti che hanno crittografato o firmato registrazioni in qualsiasi momento.
4. Disabilitare FIPS nel sistema operativo Windows (vedere Criteri di gruppo FIPS nel sistema operativo Windows a pagina 87).
5. Installare MOBOTIX HUB VMS2020 R3 (vedere Installazione di MOBOTIX HUB VMS2020 R3 a pagina 87).
6. Aggiornare le registrazioni nel database multimediale effettuate con MOBOTIX HUB VMS 2019 R3 o versioni precedenti (vedere Database multimediale: Considerazioni sulla compatibilità con le versioni precedenti a pagina 82).
7. Aggiornare la crittografia delle password di rilevamento hardware (vedere Crittografare le password di rilevamento hardware a pagina 87).
8. Abilita FIPS sul sistema operativo Windows e riavvia tutti i computer su cui è installato MOBOTIX HUB VMS.

Non abilitare FIPS fino a quando tutti i computer nella rete MOBOTIX HUB VMS, incluse le workstation MOBOTIX HUB Smart Client, non sono pronti per FIPS.

8.1.6 Verificare le integrazioni di terze parti

Se un'integrazione non è conforme a FIPS 140-2, non può essere eseguita in un sistema operativo Windows con il flag Criteri di gruppo FIPS abilitato.

Inoltre, a causa delle modifiche apportate all'SDK MIP in relazione a FIPS, le integrazioni che accedono all'elenco delle funzionalità nella licenza devono essere ricompilate.

Per garantire che le integrazioni continuino a funzionare dopo l'aggiornamento a MOBOTIX HUB VMS 2020 R3, è necessario:

- Fai un inventario di tutte le tue integrazioni con MOBOTIX HUB VMS
- Contatta i fornitori di queste integrazioni e chiedi se le integrazioni sono conformi a FIPS 140-2 e se prevedono che le integrazioni debbano essere modificate a causa degli aggiornamenti dell'SDK MIP
- Distribuisci le integrazioni conformi a FIPS 140-2 su MOBOTIX HUB VMS dopo l'aggiornamento del VMS

8.1.7 Connettere dispositivi: sfondo

Se si desidera utilizzare MOBOTIX HUB VMS in modalità conforme a FIPS, è necessario assicurarsi che anche i driver, e quindi la comunicazione con i dispositivi, siano conformi alla conformità FIPS.
I driver di dispositivo MOBOTIX HUB VMS MOBOTIX possono essere conformi a FIPS 140-2 perché possono essere configurati e funzionare in modo da utilizzare solo istanze di algoritmo conformi a FIPS 140-2. Solo i driver specifici in una configurazione specifica sono conformi a FIPS 140-2. In questa specifica configurazione FIPS 140-2 il conducente sarà in grado di comunicare con i dispositivi in modo conforme. I dispositivi devono soddisfare diversi requisiti per poter accettare questa comunicazione. Inoltre, il flag Criteri di gruppo FIPS deve essere abilitato in Windows nel server in cui è installato il server di registrazione. Quando il flag Criteri di gruppo FIPS è abilitato, i driver compatibili con FIPS 140-2 funzioneranno in modalità conforme e non utilizzeranno primitive crittografiche non approvate. I driver utilizzeranno gli algoritmi utilizzati solo per i canali di comunicazione sicuri.

Requisiti di connettività del dispositivo

MOBOTIX HUB VMS è garantito e può applicare la modalità di funzionamento conforme a FIPS 140-2 se vengono soddisfatti i seguenti criteri:

- I dispositivi utilizzano solo i driver dell'elenco (Driver supportati nella pagina 88) per connettersi a MOBOTIX HUB VMS
  Questo elenco mostra i driver in grado di garantire e far rispettare la conformità.
- I dispositivi utilizzano la versione 11.1 o successiva del Device Pack
  I driver dei pacchetti di dispositivi driver legacy non possono garantire una connessione conforme a FIPS 140-2.
- I dispositivi sono connessi tramite HTTPS e tramite Secure Real-Time Transport Protocol (SRTP) o Real Time Streaming Protocol (RTSP) su HTTPS per il flusso video

  I moduli driver non possono garantire la conformità FIPS 140-2 di una connessione tramite HTTP. La connessione può essere conforme, ma non vi è alcuna garanzia che sia effettivamente conforme.

- Nel computer che esegue il server di registrazione deve essere abilitato il flag Criteri di gruppo FIPS in Windows

Effetti del funzionamento in modalità conforme a FIPS 140-2

Quando si opera in modalità conforme a FIPS 140-2, alcuni driver non saranno disponibili per l'uso. I driver elencati come FIPS 140-2 potrebbero non essere in grado di connettersi a dispositivi che non soddisfano i requisiti del dispositivo.
Un driver è conforme a FIPS 140-2 e la comunicazione con il dispositivo è conforme a FIPS 140-2 se il driver compatibile con FIPS 140-2:

- Funziona in un ambiente in cui sono abilitati i Criteri di gruppo FIPS
- È collegato a un dispositivo che soddisfa i requisiti del dispositivo (vedere Requisiti del dispositivo a pagina 88)

- È configurato correttamente (vedere Come configurare il dispositivo e il driver per FIPS 140-2 a pagina 89)

Se uno qualsiasi dei requisiti per la modalità conforme a FIPS 140-2 non è soddisfatto, non vi è alcuna garanzia sulla conformità FIPS 140-2 del conducente o sulla comunicazione con il dispositivo. Vedere Driver e FIPS 140-2 a pagina 88 per maggiori informazioni.

Dispositivi in esecuzione su MOBOTIX Open Network Bridge

Quando viene eseguito su un computer con il flag Criteri di gruppo FIPS abilitato in Windows, MOBOTIX Open Network Bridge utilizza SHA265 per crittografare la comunicazione. Su un computer in cui non è abilitato FIPS, è possibile selezionare MD5 o SHA165 per la crittografia.

8.1.8 Database multimediale: Considerazioni sulla compatibilità con le versioni precedenti

È possibile avere registrazioni nello stesso storage da diverse versioni di MOBOTIX HUB VMS contemporaneamente. I dati firmati o crittografati devono essere:

- Esportato dallo storage se è stato registrato con MOBOTIX HUB VMS versione 2017 R1 o precedente
  L'esportazione dei dati viene eseguita utilizzando MOBOTIX HUB Smart Client.
- Aggiornato, se è stato registrato con MOBOTIX HUB VMS versione 2017 R2 o successiva
  L'aggiornamento dei dati viene eseguito in collaborazione con l'assistenza MOBOTIX, utilizzando uno strumento di conversione multimediale fornito dall'assistenza MOBOTIX.

  Per l'esecuzione dello strumento di conversione multimediale, è necessario disabilitare il flag Criteri di gruppo FIPS nel sistema operativo Windows.

  Il server di registrazione deve essere arrestato anche mentre lo strumento di conversione multimediale è in esecuzione e non vengono effettuate registrazioni mentre lo strumento è in esecuzione.

Aggiornamento dei supporti in base alla versione di MOBOTIX HUB VMS

- Dati registrati con MOBOTIX HUB VMS versione 2017 R1 e precedenti
  I dati multimediali crittografati registrati con MOBOTIX HUB VMS 2017 R1 e versioni precedenti non sono disponibili se si abilita FIPS, anche se è stato eseguito lo strumento di conversione multimediale.
  Esporta i dati multimediali registrati con MOBOTIX HUB VMS 2017 R1 e versioni precedenti per accedervi offline.
  Vedere Aggiornamento dei dati del database multimediale: MOBOTIX HUB VMS 2017 R1 e versioni precedenti nella pagina 85.
- Dati registrati con MOBOTIX HUB VMS versione da 2017 R2 a 2019 R3
  I dati multimediali registrati con MOBOTIX HUB VMS versioni da 2017 R2 a 2019 R3 non verranno crittografati nuovamente. La conversione può richiedere molto tempo e deve essere pianificata in anticipo. Per aggiornare i dati più vecchi per utilizzare algoritmi conformi a FIPS, contatta l'assistenza MOBOTIX per ottenere lo strumento di conversione multimediale.
  Vedere Aggiornamento del database multimediale: DA MOBOTIX HUB VMS 2017 R2 a MOBOTIX HUB VMS 2019 R3 a pagina 85.
- Dati registrati con MOBOTIX HUB VMS versione 2020 R1 o 2020 R2
  I dati multimediali registrati con MOBOTIX HUB VMS 2020 R1 o 2020 R2 verranno automaticamente crittografati nuovamente con algoritmi conformi a FIPS 140-2 all'avvio del server di registrazione dopo un aggiornamento. Vedere Aggiornamento del database multimediale: MOBOTIX HUB VMS 2020 R1 o MOBOTIX HUB VMS 2020 R2 a pagina 86.

Dettagli sull'aggiornamento dei supporti

La nuova crittografia dei dati con un server di registrazione con algoritmi conformi a FIPS è una parte centrale del processo di aggiornamento. Pertanto, il processo di aggiornamento varia in base alla versione di MOBOTIX HUB VMS utilizzata per la registrazione di tali dati.

<table>
<tr><th colspan="5">Dati registrati con</th></tr>
<tr><th></th><th>2017 R1 e versioni precedenti</th><th>2017 R2 - 2019 R3</th><th>2020 R1 - 2020 R2</th><th>2020 R3 e versioni successive</th></tr>
<tr><td>Cambiamenti</td><td>Dati crittografati con DES
Firma con MD5
Password: Cookie in CONFIG.XML di archiviazione
Password _a & _b nella tabella CONFIG. XML
DES crittografato</td><td>Dati crittografati con AES
Firma tramite SHA</td><td>Elenco delle password nella CONFIG.XML di archiviazione
Le password nell'elenco delle password sono crittografate DES</td><td>Le password nell'elenco delle password sono crittografate utilizzando AES
È disponibile uno strumento di conversione multimediale per l'aggiornamento della tabella CONFIG. XML dall'avere _a password e _b, per utilizzare l'elenco delle password aggiornato</td></tr>
<tr><td>FIPS disabilitato</td><td colspan="4">Tutte le funzionalità funzionano come previsto</td></tr>
<tr><td>FIPS abilitatoDati firmati</td><td>I dati firmati possono essere riprodotti
Verificare che la firma durante l'esportazione non riesca</td><td colspan="3">I dati firmati possono essere riprodotti
Verificare la firma durante i lavori di esportazione</td></tr>
<tr><td>FIPS abilitatoDati crittografati
Lo strumento di conversione multimediale non viene eseguito</td><td colspan="2">Lo storage rimane offline
L'archiviazione potrebbe rimanere offline se la crittografia è stata abilitata per l'archiviazione.</td><td colspan="2">Tutte le funzionalità funzionano come previsto</td></tr>
<tr><td>FIPS abilitatoN</td><td colspan="4">Tutte le funzionalità funzionano come previsto</td></tr>
</table>

<table>
<tr><th colspan="5">Dati registrati con</th></tr>
<tr><th></th><th>2017 R1 e versioni precedenti</th><th>2017 R2 - 2019 R3</th><th>2020 R1 - 2020 R2</th><th>2020 R3 e versioni successive</th></tr>
<tr><td>essuna crittografia
Lo strumento di conversione multimediale non viene eseguito</td><td colspan="4"></td></tr>
<tr><td>Lo strumento di conversione multimediale è stato eseguito</td><td colspan="2">Lo strumento di conversione multimediale potrebbe richiedere molto tempo per l'esecuzione perché aggiorna la tabella CONFIG.XML per tutte le tabelle crittografate</td><td>Lo strumento di conversione multimediale funziona velocemente perché deve solo aggiornare lo spazio di archiviazione CONFIG.XML</td><td>Lo strumento di conversione multimediale funziona velocemente perché non è necessario alcun aggiornamento</td></tr>
<tr><td>FIPS abilitatoDati crittografati
Lo strumento di conversione multimediale è stato eseguito</td><td>I dati crittografati non sono disponibili
Connessione persa durante la riproduzione
L'archiviazione con Riduci a fotogrammi chiave archivia l'intero GoP</td><td colspan="3">I dati crittografati possono essere riprodotti
L'archiviazione con Riduci a fotogrammi chiave funziona come previsto</td></tr>
<tr><td>FIPS abilitatoNessuna crittografia
Nessuna firma</td><td colspan="4">Tutte le funzionalità funzionano come previsto</td></tr>
</table>

Dati registrati con				
	2017 R1 e versioni precedenti	**2017 R2 - 2019 R3**	**2020 R1 - 2020 R2**	**2020 R3 e versioni successive**
Lo strumento di conversione multimediale è stato eseguito				

Aggiornamento dei dati del database multimediale: MOBOTIX HUB VMS 2017 R1 e versioni precedenti

Se si esegue MOBOTIX HUB VMS versione 2017 R1 o precedente o se sono stati registrati dati firmati o crittografati con queste versioni, le registrazioni vengono crittografate con algoritmi che non sono considerati sicuri dallo standard FIPS 140-2.
Non è possibile accedere a queste registrazioni da un computer in cui è abilitato il flag Criteri di gruppo FIPS.
Di conseguenza, è necessario esportare il database multimediale in una posizione in cui è ancora possibile accedervi.

Aggiornamento del database multimediale: da MOBOTIX HUB VMS 2017 R2 a MOBOTIX HUB VMS 2019 R3

Se si esegue una versione di MOBOTIX HUB VMS tra MOBOTIX HUB VMS 2017 R2 e MOBOTIX HUB VMS 2019 R3 e se in qualsiasi momento è stata abilitata la crittografia nel database multimediale, per accedere a queste registrazioni è necessario eseguire una delle seguenti opzioni.

Entrambe le opzioni richiedono l'uso dello strumento di conversione multimediale. Il server di registrazione deve essere arrestato mentre lo strumento di conversione multimediale è in esecuzione e non vengono effettuate registrazioni mentre lo strumento è in esecuzione. Vedere Che cos'è lo strumento di conversione multimediale? a pagina 86 per maggiori informazioni.

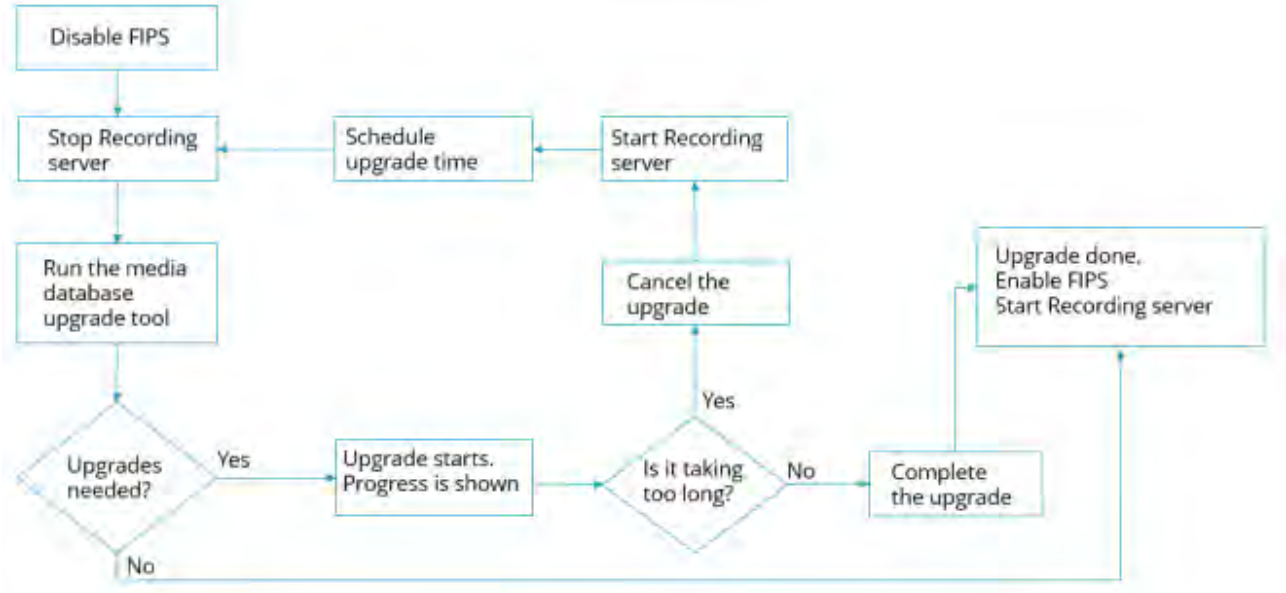
- Opzione 1
  Utilizzare questa opzione per poter operare immediatamente in un ambiente FIPS e se si dispone di un lungo periodo di conservazione. Il tempo necessario per eseguire lo strumento di conversione multimediale potrebbe essere significativo.
  1. Aggiorna MOBOTIX HUB VMS alla versione 2020 R3.
  2. Con FIPS disabilitato sul sistema operativo Windows, eseguire lo strumento di conversione multimediale fornito dal supporto MOBOTIX.
  3. Abilitare il flag Criteri di gruppo FIPS nel sistema operativo Windows.
- Opzione 2
  Utilizzare questa opzione se l'operatività in un ambiente FIPS può attendere l'attesa, se si dispone di un tempo di conservazione breve e se si esegue lo strumento di conversione multimediale su meno dati.
  1. Aggiorna MOBOTIX HUB VMS alla versione 2020 R3.
  2. Esegui le VMS MOBOTIX HUB durante il tempo di conservazione senza abilitare FIPS sul sistema operativo Windows.

3. Esegui lo strumento di conversione multimediale per assicurarti che tutti i dati vengano convertiti in modo che siano conformi a FIPS.
4. Abilitare il flag Criteri di gruppo FIPS nel sistema operativo Windows.

Che cos'è lo strumento di conversione multimediale?

Lo strumento di conversione multimediale è uno script di PowerShell autonomo, che viene recapitato nell'origine. Non fa parte di alcuna installazione.
Deve essere distribuito ai clienti solo tramite l'assistenza MOBOTIX.
Può convertire tutto lo spazio di archiviazione in blocco oppure può essere eseguito in uno spazio di archiviazione specifico.
Gli indicatori di avanzamento mostrano fino a che punto è arrivato lo strumento.
Se la conversione richiede troppo tempo, è possibile annullare il processo e continuare senza FIPS abilitato.
Lo strumento di conversione multimediale converte le credenziali crittografate all'interno dei file della tabella multimediale esistenti nel formato più recente compatibile con FIPS.
Lo strumento di conversione multimediale non modifica la crittografia dei dati video stessi. Se i dati video vengono crittografati con un algoritmo non conforme (DES), le tabelle aggiornate verranno caricate, ma il video non sarà accessibile in modalità conforme a FIPS.
Lo strumento di conversione multimediale converte e controlla se tutte le tabelle utilizzano algoritmi conformi a FIPS.
Le tabelle approvate verranno contrassegnate per evitarne il controllo da parte dello strumento di conversione multimediale.
Dopo aver eseguito lo strumento di conversione multimediale, MOBOTIX HUB VMS 2020 R3 sarà in grado di caricare le tabelle in modalità conforme a FIPS.

Flusso di lavoro dello strumento di conversione multimediale



Aggiornamento del database multimediale: MOBOTIX HUB VMS 2020 R1 o MOBOTIX HUB VMS 2020 R2

Se si esegue MOBOTIX HUB VMS versione 2020 R1 o MOBOTIX HUB VMS 2020 R2, i dati multimediali registrati con una di queste versioni verranno automaticamente crittografati nuovamente con algoritmi conformi a FIPS 140-2 durante l'aggiornamento del server di registrazione.

8.1.9 Criteri di gruppo FIPS nel sistema operativo Windows

La modalità di funzionamento FIPS è abilitata e disabilitata con il flag Criteri di gruppo FIPS nel sistema operativo Windows. Per informazioni sull'abilitazione e la disabilitazione di FIPS, vedere il sito Microsoft.
Prima di eseguire l'aggiornamento, è necessario disabilitare il flag Criteri di gruppo FIPS su tutti i computer che fanno parte di MOBOTIX HUB VMS, incluso il computer che ospita SQL Server e tutte le workstation Smart Client MOBOTIX HUB.
Esistono due motivi per cui il flag Criteri di gruppo FIPS deve essere disabilitato su tutti i computer nelle macchine virtuali MOBOTIX HUB prima di eseguire l'aggiornamento:

- Durante l'aggiornamento, i dati crittografati con algoritmi FIPS non approvati vengono nuovamente crittografati con algoritmi approvati. Per eseguire la decrittografia sul sistema operativo Windows, il flag Criteri di gruppo FIPS deve essere disabilitato.
- Se il flag Criteri di gruppo FIPS è abilitato in Windows, non sarà possibile utilizzare le VMS HUB MOBOTIX fino a quando tutti i componenti non saranno aggiornati. Ad esempio, uno Smart Client MOBOTIX HUB 2020 R2 non sarà in grado di comunicare con un server di gestione R3 2020 se il server di gestione si trova su un computer in cui è abilitato il flag Criteri di gruppo FIPS.

Criteri di gruppo FIPS e architettura federata MOBOTIX

Se un sito in un'architettura federata MOBOTIX deve funzionare con il flag Criteri di gruppo FIPS abilitato in Windows, tutti i siti devono funzionare anche con il flag Criteri di gruppo FIPS abilitato in Windows.
Di conseguenza, l'intera installazione di MOBOTIX Federated Architecture deve essere aggiornata alla versione 2020 R3.

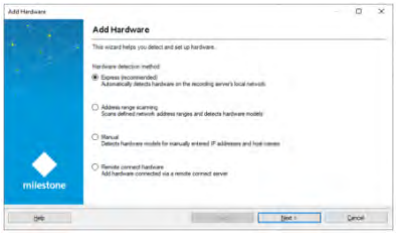
8.1.10 Installazione di MOBOTIX HUB VMS2020 R3

Quando si esegue l'aggiornamento, il programma di installazione delle macchine virtuali dell'hub MOBOTIX controllerà la politica di sicurezza FIPS e impedirà l'avvio dell'aggiornamento se FIPS è abilitato.

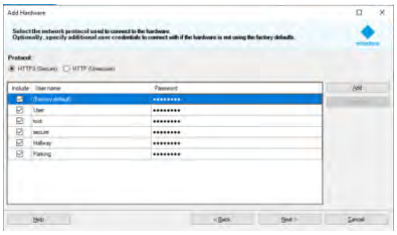
8.1.11 Crittografa le password di rilevamento hardware

Le password di rilevamento hardware devono essere aggiornate dopo l'aggiornamento a MOBOTIX HUB VMS 2020 R3.
La crittografia delle password di rilevamento hardware non viene aggiornata durante l'aggiornamento da una versione precedente di MOBOTIX HUB VMS. Tuttavia, queste password non possono essere lette se il flag Criteri di gruppo FIPS è abilitato in Windows.
È necessario attivare una conversione di queste password prima di abilitare FIPS. Procedere come indicato di seguito:

1. Assicurati che il flag Criteri di gruppo FIPS sia disabilitato in Windows.
2. Nel client di gestione MOBOTIX HUB, aprire la procedura guidata Aggiungi hardware.



3. Selezionare il metodo di rilevamento per aprire la pagina di rilevamento hardware.



In questo modo viene attivata la ricrittografia delle password di rilevamento hardware con algoritmi conformi a FIPS.

Le credenziali sono ora crittografate con algoritmi conformi a FIPS.

8.2 Driver e FIPS 140-2

In questa sezione viene descritto FIPS 140-2 e come configurare e utilizzare i driver MOBOTIX per funzionare in modalità conforme a FIPS 140-2.

8.2.1 Requisiti per la modalità conforme a FIPS 140-2

I driver di dispositivo MOBOTIX HUB VMS MOBOTIX possono essere conformi a FIPS 140-2 perché possono essere configurati e funzionare in modo da utilizzare solo istanze di algoritmo conformi a FIPS 140-2. Solo i driver specifici in una configurazione specifica sono conformi a FIPS 140-2. In questa specifica configurazione FIPS 140-2 il conducente sarà in grado di comunicare con i dispositivi in modo conforme. I dispositivi devono soddisfare diversi requisiti per poter accettare questa comunicazione. Inoltre, il flag Criteri di gruppo FIPS deve essere abilitato in Windows nel server in cui è installato il server di registrazione. Quando il flag Criteri di gruppo FIPS è abilitato, i driver compatibili con FIPS 140-2 funzioneranno in modalità conforme e non utilizzeranno primitive crittografiche non approvate. I driver utilizzeranno gli algoritmi utilizzati solo per i canali di comunicazione sicuri.

Requisiti del dispositivo

Affinché un dispositivo sia in grado di comunicare con un driver in esecuzione in modalità conforme a FIPS 140-2, deve soddisfare tutti i requisiti:

- Il dispositivo deve supportare la comunicazione HTTPS con almeno un pacchetto di crittografia conforme a FIPS 140-2 (per esempi, vedere Esempio di pacchetti di crittografia conformi a FIPS 140-2 a pagina 93)
- Il dispositivo deve supportare RTSP su HTTPS (tunneling RTSP e RTP su HTTP) utilizzando l'autenticazione di base HTTP (RFC2068 Sezione 11.1) o l'autenticazione digest HTTP (RFC2069, RFC7616)

  o

  Il dispositivo deve supportare lo streaming multimediale tramite SRTP e RTSPS (RFC3711)

Driver supportati

Attualmente solo un sottoinsieme di driver è conforme a FIPS 140-2. Questi driver supportano la comunicazione tramite un canale protetto per tutte le funzionalità disponibili.

Asse 1 canale	PTZ a 1 canale dell'asse	Asse 2 canali	Asse 3 canali
Asse 4 canali	Asse 8 canali	Asse 11 canali	Asse 12 canali
Asse Audio	Bosch PTZ	Bosch 1 canale	Bosch 2 canali
Bosch 3 canali	Bosch 16 canali	Bosch X20XF	Bosch X40XF
Canon 1 canale	Canon PTZ a 1 canale	Canon VBM	Canon VBM 40
Canon VBS	Canon VBS No Ptz	Barriere digitali Decoder TVI	Hanwha Generico
ONVIF	ONVIF16	Universale	Universale a 16 canali

Universale a 64 canali	VideoPush		

I driver nella tabella sono in grado di essere eseguiti in modalità conforme a FIPS 140-2 se configurati correttamente. Questo elenco non è definitivo e potrebbe espandersi in futuro. Alcuni driver sono conformi a FIPS 140-2 con funzionalità limitate. Fare riferimento alle sezioni specifiche dei driver di seguito per informazioni su come configurarli ed eventuali limitazioni.
La modalità conforme a FIPS 140-2 per i driver è disponibile a partire dal Device Pack 11.1.

8.2.2 Effetti dell'esecuzione in modalità conforme a FIPS 140-2

Quando si opera in modalità conforme a FIPS 140-2, alcuni driver non saranno disponibili per l'uso. I driver elencati come FIPS 140-2 potrebbero non essere in grado di connettersi a dispositivi che non soddisfano i requisiti del dispositivo.
Un driver è conforme a FIPS 140-2 e la comunicazione con il dispositivo è conforme a FIPS 140-2 se il driver compatibile con FIPS 140-2:

- Funziona in un ambiente in cui sono abilitati i Criteri di gruppo FIPS
- È collegato a un dispositivo che soddisfa i requisiti del dispositivo (vedere Requisiti del dispositivo nella pagina 88)
- È configurato correttamente (vedere Come configurare il dispositivo e il driver per FIPS 140-2 a pagina 89)

Se uno qualsiasi dei requisiti per la modalità conforme a FIPS 140-2 non è soddisfatto, non vi è alcuna garanzia sulla conformità FIPS 140-2 del conducente o sulla comunicazione con il dispositivo.

8.2.3 Come configurare il dispositivo e il driver per FIPS 140-2

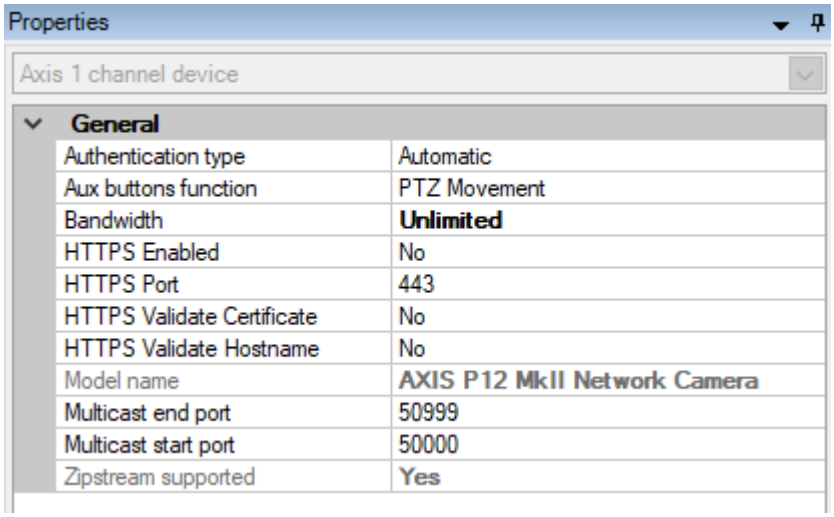
La configurazione del dispositivo e del driver per la modalità conforme a FIPS 140-2 è specifica del dispositivo e del driver. Si applicano alcune linee guida generali:

- I canali di comunicazione tra il driver e il dispositivo devono essere sicuri e crittografati (HTTPS, RTSP su HTTPS, SRTP).
- Il dispositivo deve essere configurato per il funzionamento tramite canali sicuri.
- Il driver e il dispositivo devono essere configurati per l'utilizzo di canali sicuri per la comunicazione nelle VMS MOBOTIX HUB.

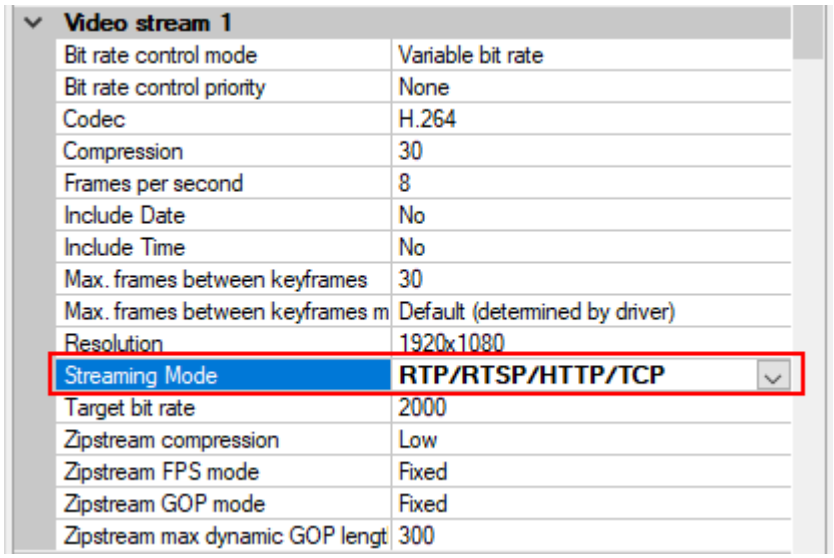
Driver degli assi

Procedere come indicato di seguito:

- Impostare HTTPS abilitato su Sì.
- Impostare Convalida certificato HTTPS su Sì.
- Impostare HTTPS Convalida nome host su Sì.

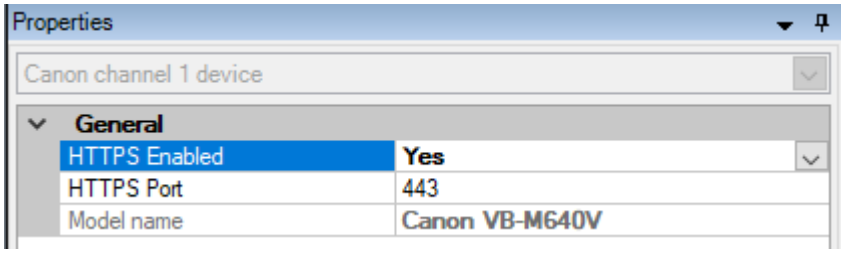


- Per ogni canale multimediale e flusso multimediale abilitato, impostare la modalità di streaming su RTP/RTSP/HTTP/TCP.

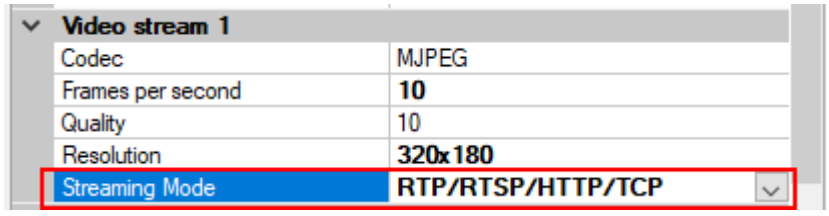


Driver Canon

- Impostare HTTPS abilitato su Sì.



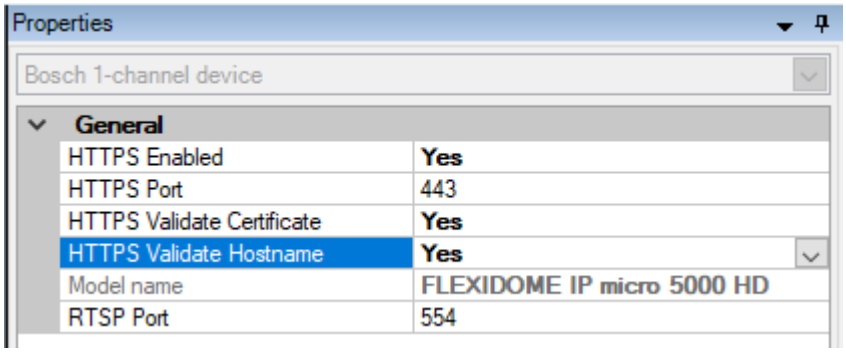
- Per ogni canale multimediale e flusso multimediale abilitato, impostare la modalità di streaming su RTP/RTSP/HTTP/TCP.



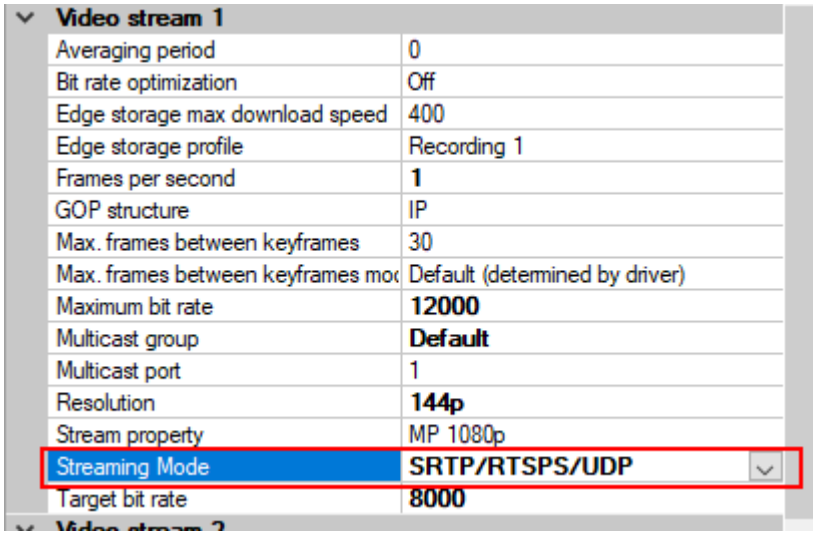
Driver Bosch

Procedere come indicato di seguito:

- Impostare HTTPS abilitato su Sì.
- Impostare Convalida certificato HTTPS su Sì.
- Impostare HTTPS Convalida nome host su Sì.

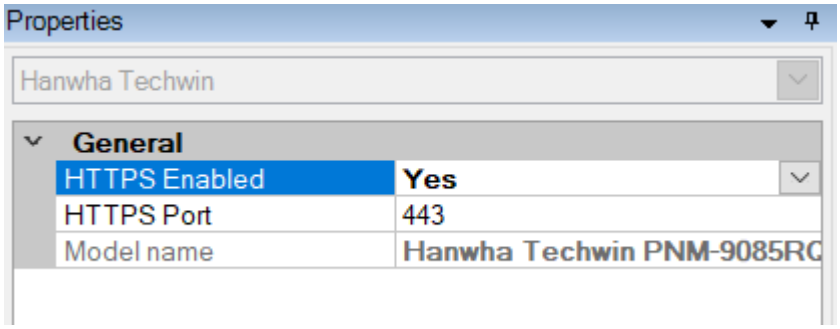


- Per ogni canale multimediale e flusso multimediale abilitato, impostare la modalità di streaming su una delle seguenti opzioni:
  - RTP/RTSP/HTTP/TCP
  - SRTP/RTSPS/UDP
  - Multicast SRT/RTSPS/UDP

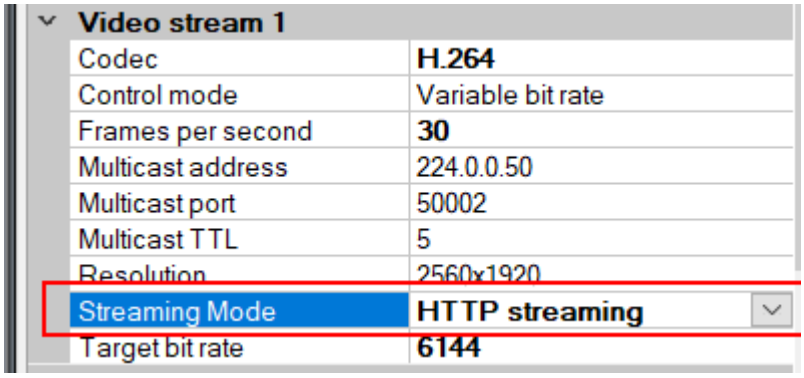


Autisti Hanwha

- Impostare HTTPS abilitato su Sì.



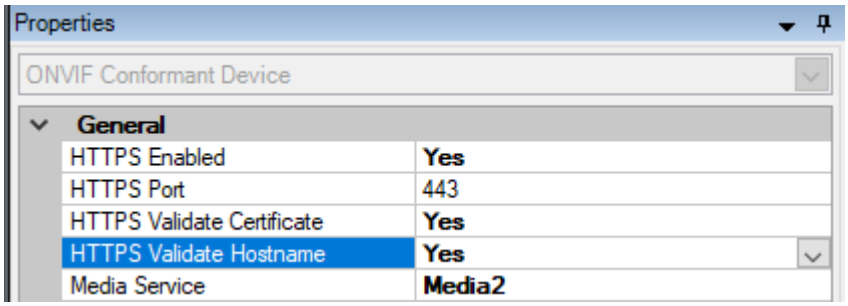
- Per ogni canale multimediale e flusso multimediale abilitato, impostare Modalità streaming su Streaming HTTP.



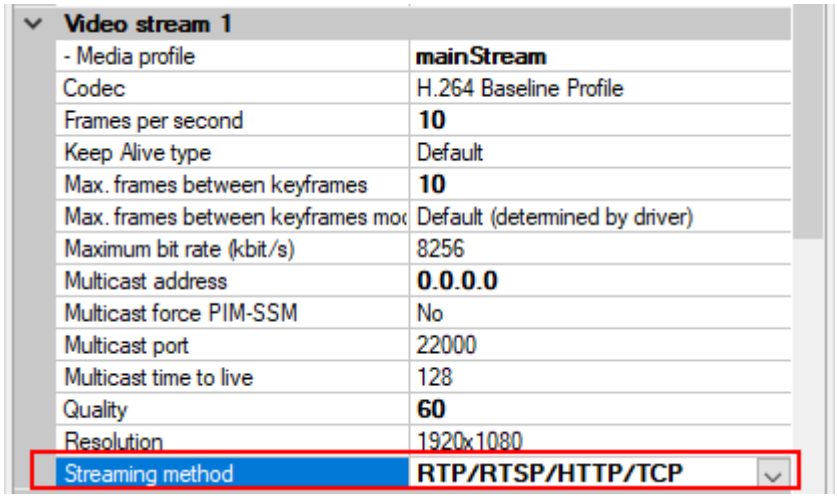
Driver ONVIF

Procedere come indicato di seguito:

- Impostare HTTPS abilitato su Sì.
- Impostare Convalida certificato HTTPS su Sì.
- Impostare HTTPS Convalida nome host su Sì.



- Per ogni canale multimediale e flusso multimediale abilitato, impostare Metodo di streaming su RTP/RTSP/HTTP/TCP.

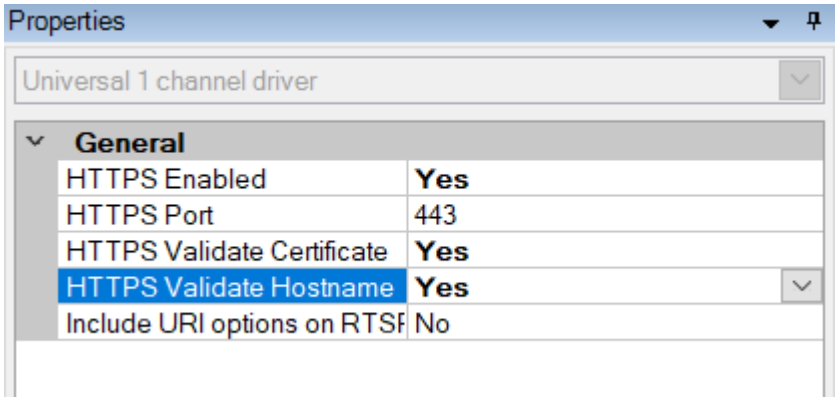


- Il canale posteriore audio (uscita audio, altoparlante dispositivo) non deve essere utilizzato quando il driver è in esecuzione in modalità conforme a FIPS 140-2.

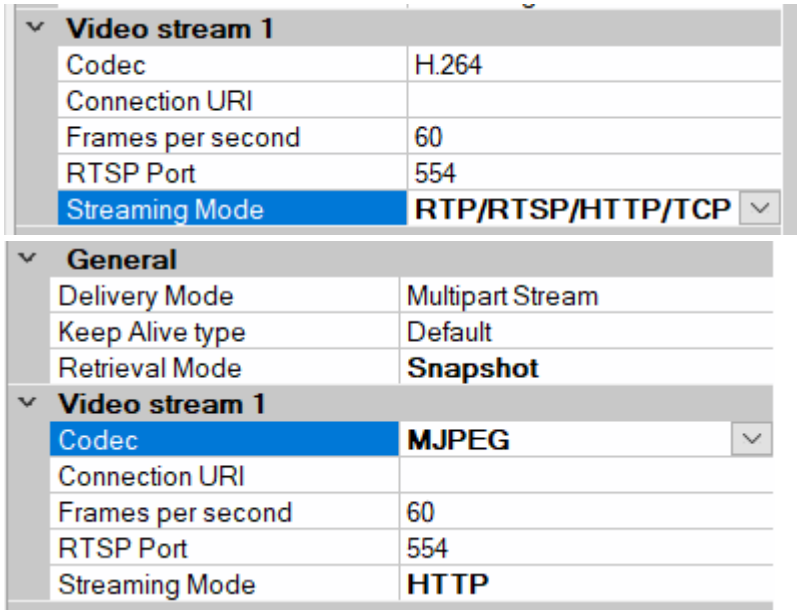
Driver universali

Procedere come indicato di seguito:

- Impostare HTTPS abilitato su Sì.
- Impostare Convalida certificato HTTPS su Sì.
- Impostare HTTPS Convalida nome host su Sì.



- Per ogni canale multimediale e flusso multimediale abilitato, impostare la modalità di streaming su RTP/RTSP/HTTP/TCP o HTTP, a seconda che venga utilizzata la modalità di streaming o di recupero delle istantanee.



Driver VideoPush

Non è necessaria alcuna configurazione specifica. L'abilitazione dei criteri di gruppo FIPS costringerà il driver a comunicare con il server mobile MOBOTIX HUB in modo conforme a FIPS 140-2.

8.2.4 Esempio di suite di crittografia conformi a FIPS 140-2

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

L'elenco non è esaustivo. Esistono altri pacchetti di crittografia conformi a FIPS 140-2. Questo elenco viene fornito solo come esempio di pacchetti di crittografia conformi a FIPS 140-2.

8.3 Risorse FIPS

1. Requisiti di sicurezza FIPS 140-2 per i moduli crittografici
   https://csrc.nist.gov/publications/detail/fips/140/2/final
2. Allegato A: Funzioni di sicurezza approvate per FIPS PUB 140-2
   https://csrc.nist.gov/CSRC/media/Publications/fips/140/2/final/documents/fips1402annexa.pdf
3. Linee guida per la selezione, la configurazione e l'utilizzo delle implementazioni TLS (Transport Layer Security)
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf
4. Linee guida per l'implementazione di FIPS 140-2 e del programma di convalida del modulo crittografico
   https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/fips140-2/fips1402ig.pdf
5. L'approccio di Microsoft alla convalida FIPS 140-2
   https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation
6. Panoramica di TLS/SSL (SSP Schannel)
   https://docs.microsoft.com/en-us/windows-server/security/tls/tls-ssl-schannel-ssp-overview
7. Suite di crittografia in TLS/SSL (SSP Schannel)
   https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

8. Suite di crittografia TLS in Windows 10 v1903, v1909 e v2004
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-cipher-suites-in-windows-10-v1903
9. Curve ellittiche TLS in Windows 10 versione 1607 e successive
   https://docs.microsoft.com/en-us/windows/win32/secauthn/tls-elliptic-curves-in-windows-10-1607-and-later

9 Tabella di confronto dei prodotti

9.1 Tabella di confronto dei prodotti

MOBOTIX HUB VMS include i seguenti prodotti:

- MOBOTIX HUB L1
- MOBOTIX HUB L2
- MOBOTIX HUB L3
- MOBOTIX HUB L4
- MOBOTIX HUB L5

L'elenco completo delle funzioni è disponibile nella pagina di panoramica dei prodotti sul sito Web MOBOTIX https://www.mobotix.com/en/vms/mobotix-hub

Di seguito un elenco delle principali differenze tra i prodotti:

Nome	MOBOTIX HUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
Siti per SLC	1	1	Multisito	Multisito	Multisito
Server di registrazione per SLC	1	1	Illimitato	Illimitato	Illimitato
Dispositivi hardware per server di registrazione	8	48	Illimitato	Illimitato	Illimitato
Interconnessione™ MOBOTIX	-	Sito remoto	Sito remoto	Sito remoto	Sito centrale/remoto
Architettura™ federata MOBOTIX	-	-	-	Sito remoto	Sito centrale/remoto
Registrazione del failover del server	-	-	-	Standby a freddo e a caldo	Standby a freddo e a caldo
Servizi di connessione remota	-	-	-	-	✓
Supporto per l'archiviazione edge	-	-	✓	✓	✓
Archiviazione video multistadio	Banche dati live + 1 archivio	Banche dati live + 1 archivio	Banche dati live + 1 archivio	Database live + archivi illimitati	Database live + archivi illimitati
Notifica SNMP	-	-	-	✓	✓
Diritti di accesso degli utenti a tempo controllato	-	-	-	-	✓
Riduci frame rate (toelettatura)	-	-	-	✓	✓
Crittografia dei dati video (server di registrazione)	-	-	-	✓	✓
Firma del database (server di registrazione)	-	-	-	✓	✓
Livelli di priorità PTZ	1	1	3	32000	32000

Nome	MOBOTIX HUB L1	MOBOTIX HUB L2	MOBOTIX HUB L3	MOBOTIX HUB L4	MOBOTIX HUB L5
PTZ esteso (riserva sessione PTZ e pattugliamento da XProtect Smart Client)	-	-	-	✓	✓
Blocco delle prove	-	-	-	-	✓
Funzione segnalibro	-	-	Solo manuale	Manuale e basato su regole	Manuale e basato su regole
Multi-streaming live o multicasting/Streaming adattivo	-	-	-	✓	✓
Streaming diretto	-	-	-	✓	✓
Sicurezza generale	Diritti utente client	Diritti utente client	Diritti utente client	Diritti utente client	Diritti utente del cliente/ Diritti utente amministratore
Gestione MOBOTIX HUB Profili client	-	-	-	-	✓
Profili Smart Client di MOBOTIX HUB	-	-	3	3	Illimitato
MOBOTIX HUB Smart Wall	-	-	-	opzionale	✓
Monitor di sistema	-	-	-	✓	✓
Mappa intelligente	-	-	-	✓	✓
Verifica in due passaggi	-	-	-	-	✓
Supporto DLNA	-	✓	✓	✓	✓
Mascheramento della privacy	-	✓	✓	✓	✓
Gestione delle password dei dispositivi			✓	✓	✓

10 Appendice

10.1 Appendice 1 – Risorse

Descrive i requisiti minimi per un sistema di videosorveglianza. Vedere anche le norme correlate.

1. Axis Communications: Guida alla protezione avanzata
2. Bosch Security Systems: Guida alla sicurezza dei dati e dei video IP Bosch
3. Standard britannico BS EN 62676-1-1: Sistemi di videosorveglianza per l'uso in applicazioni di sicurezza, Parte 1-1: Requisiti di sistema - Generale
4. Descrive i requisiti minimi per un sistema di videosorveglianza. Vedere anche le norme correlate.
5. Center for Internet Security: i controlli di sicurezza critici della CSI per un'efficace difesa informatica
6. Cloud Security Alliance (CSA) e la matrice dei controlli cloud
7. Defense Information Systems Agency (DISA): Guide all'implementazione tecnica della sicurezza (STIGs)
8. Internet Engineering Task Force (IETF), riferimenti multipli
9. ISO/IEC 15048 Tecniche di sicurezza - Tecniche di valutazione per la sicurezza informatica
10. ISO/IEC 31000, Gestione del rischio – Principi e linee guida
11. ISO/IEC 31010, Gestione del rischio – Tecniche di valutazione del rischio
12. ISO 27001: Sicurezza delle informazioni, cibersicurezza e protezione della vita privata — Sistemi di gestione della sicurezza delle informazioni — Requisiti
13. ISO 27002: Sicurezza delle informazioni, sicurezza informatica e protezione della vita privata — Controlli della sicurezza delle informazioni
14. Guida all'aggiornamento della sicurezza Microsoft
15. Vedere anche, tra gli altri, Amministrare le impostazioni dei criteri di sicurezza
16. Istituto Nazionale di Standard e Tecnologia: Divisione Sicurezza Informatica Centro Risorse per la Sicurezza Informatica
17. Istituto nazionale di standard e tecnologia: Quadro di sicurezza informatica
18. Quadro di riferimento per la gestione del rischio per i sistemi informativi e le organizzazioni: un approccio al ciclo di vita del sistema per la sicurezza e la privacy
19. National Institute of Standards and Technology: Gestione dei rischi per la sicurezza delle informazioni
20. National Institute of Standards and Technology: Controlli di sicurezza e privacy per i sistemi informativi e le organizzazioni federali SP 800-53- Revisione 5
21. Manuale sulla sicurezza delle informazioni NIST SP 800-100: una guida per i manager
22. Linee guida NIST SP 800-124 per la gestione della sicurezza dei dispositivi mobili nell'azienda
23. Sito web del SANS Institute e SANS Critical Security Controls
24. XProtect® Corporate – Gestione avanzata della sicurezza

10.2 Appendice 2 - Acronimi

AD - Active Directory

CSA – Alleanza per la sicurezza del cloud

CVE – Vulnerabilità ed esposizioni comuni

HTTP – Protocollo di trasferimento ipertestuale

HTTPS – Protocollo di trasferimento ipertestuale sicuro

IEC – Commissione elettrotecnica internazionale

IETF – Task Force per l'ingegneria di Internet

IP – Protocollo Internet

ISO – Organizzazione internazionale per la standardizzazione

IT - Tecnologia dell'informazione

KB – Base di conoscenza

NIST – Istituto Nazionale di Standard e Tecnologia
RSTP – Protocollo Rapid Spanning Tree
SMTP – Protocollo di trasferimento della posta semplice
SSL – Livello di presa sicuro
STIG – Guida alle informazioni tecniche sulla sicurezza
TCP – Protocollo di controllo della trasmissione
TLS - Sicurezza del livello di trasporto
UDP – Protocollo datagramma utente
VMS – Software di gestione video
VPN – Rete privata virtuale

MOBOTIX

BeyondHumanVision

EN_08/23

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