AXIS OS Hardening Guide

Portale AXIS OS | Note sul rilascio di AXIS OS | Knowledge Base di AXIS OS | Avvisi di sicurezza di AXIS OS| Playlist YouTube AXIS OS

Introduzione

Introduzione

Axis Communications si impegna ad applicare le migliori pratiche di cybersecurity nella progettazione, nello sviluppo e nel collaudo dei suoi dispositivi per ridurre al minimo il rischio di vulnerabilità che potrebbero essere sfruttate da hacker in un attacco. Ciononostante, l'intera catena di fornitura e l'organizzazione dell'utente finale devono partecipare alla protezione di una rete, dei suoi dispositivi e dei servizi che supporta. Un ambiente protetto dipende dagli utenti, dai processi e dalla tecnologia. Il fine di tale guida è contribuire alla protezione della rete, dei dispositivi e dei servizi.

Le minacce più evidenti che possono interessare un dispositivo Axis sono il sabotaggio fisico, atti vandalici e le manomissioni. Per tutelare un dispositivo da tali minacce, è importante scegliere un modello o un alloggiamento che sia resistente agli atti vandalici, montarlo nella maniera consigliata e proteggere i cavi.

I dispositivi Axis sono endpoint di rete, proprio come i computer e i cellulari. Molti di essi hanno un'interfaccia Web che potrebbe esporre vulnerabilità a sistemi connessi. In questa guida, illustriamo in che modo si possono ridurre tali rischi.

La guida fornisce consigli tecnici per chiunque sia coinvolto nell'implementazione delle soluzioni Axis. Comprende una configurazione di base consigliata e una guida alla protezione che tiene a mente l'evoluzione del panorama delle minacce. Potrebbe rendersi necessario consultare il manuale per l'utente del dispositivo per saperne di più su come si configurano impostazioni specifiche. Tenere conto che i dispositivi Axis hanno ricevuto un aggiornamento dell'interfaccia Web in AXIS OS 7.10 e 10.9 che ha modificato il percorso di configurazione.

Configurazione dell'interfaccia Web
La guida si riferisce alla configurazione delle impostazioni del dispositivo nell'interfaccia Web del dispositivo Axis. Il percorso di configurazione differisce sulla base della versione di AXIS OS installata nel dispositivo:

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Impostazione > Opzioni di sistema > Sicurezza > IEEE 802.1X
≥ 7.10	Impostazioni > Sistema > Sicurezza
≥ 10.9	Sistema > Sicurezza

Ambito

Questa guida è applicabile a tutti i dispositivi basati su AXIS OS che eseguono AXIS OS (LTS o traccia attiva) nonché ai dispositivi legacy che eseguono 4.xx e 5.xx.

Introduzione

Architettura di sicurezza del sistema operativo AXIS

Il diagramma dell'architettura di sicurezza del sistema operativo AXIS delinea le funzionalità di sicurezza informatica del sistema operativo AXIS su vari livelli offrendo una visione completa delle basi della sicurezza, della sicurezza assistita da silicone, del sistema operativo AXIS OS e del livello di controllo dell'applicazione e dell'accesso.

Fare clic con il tasto destro e aprire l'immagine in una nuova scheda per una migliore esperienza visiva.

Notifiche di sicurezza

Consigliamo l'abbonamento al *servizio di notifiche di sicurezza Axis* per la ricezione di informazioni su vulnerabilità appena scoperte nei dispositivi, soluzioni e servizi Axis e su come tutelare i dispositivi Axis.

Livelli di protezione CIS

Ci atteniamo ai metodi delineati nella versione 8 di Center for Internet Safety (CIS) Controls per strutturare le nostre raccomandazioni in merito al framework di cybersecurity. I CIS Controls, precedentemente conosciuti come SANS Top 20 Critical Security Controls, mettono a disposizione 18 categorie di controlli di sicurezza critici (CSC) incentrati sulle categorie di rischio di cybersecurity più diffuse in un'organizzazione.

Questa guida fa riferimento ai controlli di sicurezza critici aggiungendo il numero di CSC (**CSC #**) per ogni argomento relativo alla protezione. Per saperne di più sulle categorie CSC, consultare *18 CIS Critical Security Controls* presso cisecurity.org.

Protezione predefinita

I dispositivi Axis vengono forniti con impostazioni di protezione predefinite. Ci sono vari controlli di sicurezza che non c'è bisogno di configurare. Questi controlli mettono a disposizione un livello di base di protezione del dispositivo e fungono da fondamenta per una protezione più ampia.

Disabilitato per impostazione predefinita

CSC #4: Configurazione sicura delle risorse e del software aziendali

Il dispositivo Axis non funzionerà finché non sarà avvenuta l'impostazione della password amministratore.

Per saperne di più su come si configura l'accesso al dispositivo, consultare *Accesso ai dispositivi* nella Knowledge Base di AXIS OS.

Edge storage

CSC #4: Configurazione sicura delle risorse e del software aziendali

A partire da Axis OS 12.0, l'opzione di montaggio noexec è stata aggiunta come opzione predefinita per le condivisioni di rete montate. Ciò disabiliterà l'esecuzione diretta di binari dalla condivisione di rete montata. Per le schede di memoria questa opzione era già stata aggiunta nelle versioni precedenti di AXIS OS.

Accesso con credenziali

Dopo l'impostazione della password amministratore, l'accesso alle funzioni di amministratore e/o ai flussi video può avvenire unicamente attraverso l'autenticazione di credenziali di nome utente e password valide. Non consigliamo l'uso di funzionalità che rendono possibile l'accesso non autenticato, ad esempio la visualizzazione anonima e la modalità sempre multicast.

Protocolli di rete

CSC #4: Configurazione sicura delle risorse e del software aziendali

Solo una quantità minima di protocolli e servizi di rete sono abilitati per impostazione predefinita nei dispositivi Axis. Questa tabella illustra quali sono.

Protocollo	Porta	Trasporto	Commenti
HTTP	80	TCP	Traffico HTTP generale, ad esempio accesso all'interfaccia web, VAPIX e l'interfaccia API ONVIF o comunicazione edge-to-edge.*
HTTPS	443	TCP	Traffico HTTPS generale, ad esempio accesso all'interfaccia Web, VAPIX e l'interfaccia API ONVIF o comunicazione edge-to-edge.*
RTSP	554	TCP	Usato dal dispositivo Axis per lo streaming video/audio.
RTP	Intervallo porte effimere*	UDP	Usato dal dispositivo Axis per lo streaming video/audio.

Protezione predefinita

Protocollo	Porta	Trasporto	Commenti
UPnP®	49152	TCP	Usato da applicazioni di terzi per trovare il dispositivo Axis tramite il protocollo di rilevamento UPnP®. **NOTA:** Disabilitato per impostazione predefinita a partire da AXIS OS 12.0.
Bonjour	5353	UDP	Usato da applicazioni di terzi per trovare il dispositivo Axis tramite il protocollo di rilevamento mDNS (Bonjour).
SSDP	1900	UDP	Usato da applicazioni di terzi per trovare il dispositivo Axis attraverso SSDP (UPnP®). **NOTA:** Disabilitato per impostazione predefinita a partire da AXIS OS 12.0.
WS-Discovery	3702	UDP	Usato da applicazioni di terzi per trovare il dispositivo Axis tramite il protocollo di rilevamento WS-Discovery (ONVIF).

** Per saperne di più sulla tecnologia edge-to-edge, consulta il white paper in merito alla tecnologia edge-to-edge.*

***Allocato in automatico in un intervallo predefinito di numeri di porta secondo RFC 6056. Per saperne di più, consultare l'articolo Wikipedia Ephemeral port.*

Consigliamo di disabilitare i protocolli e i servizi di rete non usati quando possibile. Per un elenco totale dei servizi usati per impostazione predefinita o abilitabili in base alla configurazione, consultare *Porte di rete usate comunemente* nella Knowledge Base di AXIS OS.

Ad esempio, c'è la possibilità di abilitare in modo manuale l'ingresso/uscita audio e la funzionalità microfono nei dispositivi di videosorveglianza Axis come le telecamere di rete, invece negli interfono e negli altoparlanti di rete, l'ingresso/uscita audio e la funzionalità microfono sono funzionalità principali e di conseguenza sono abilitate per impostazione predefinita.

Interfaccia UART/debug

CSC #4: Configurazione sicura delle risorse e del software aziendali

Ciascun dispositivo Axis è dotato di una cosiddetta interfaccia UART (Universal Receiver Receiver) fisica, a volte chiamata "porta di debug" o "console seriale". Si può accedere all'interfaccia in sé solo fisicamente smontando in modo esaustivo il dispositivo Axis. L'interfaccia UART/debug è usata unicamente per sviluppare prodotti e ai fini di debug nell'ambito di progetti di ricerca e sviluppo interni all'interno di Axis.

L'interfaccia UART/debug è abilitata per impostazione predefinita nei dispositivi Axis dotati di AXIS OS 10.10 e versioni precedenti, ma necessita dell'accesso autenticato e non mostra informazioni riservate se non viene eseguita l'autenticazione. A partire da AXIS OS 10.11, l'interfaccia UART/debug è disabilitata per impostazione predefinita. L'interfaccia si può abilitare solo sbloccandola attraverso un certificato fornito da Axis personalizzato e unico per il dispositivo.

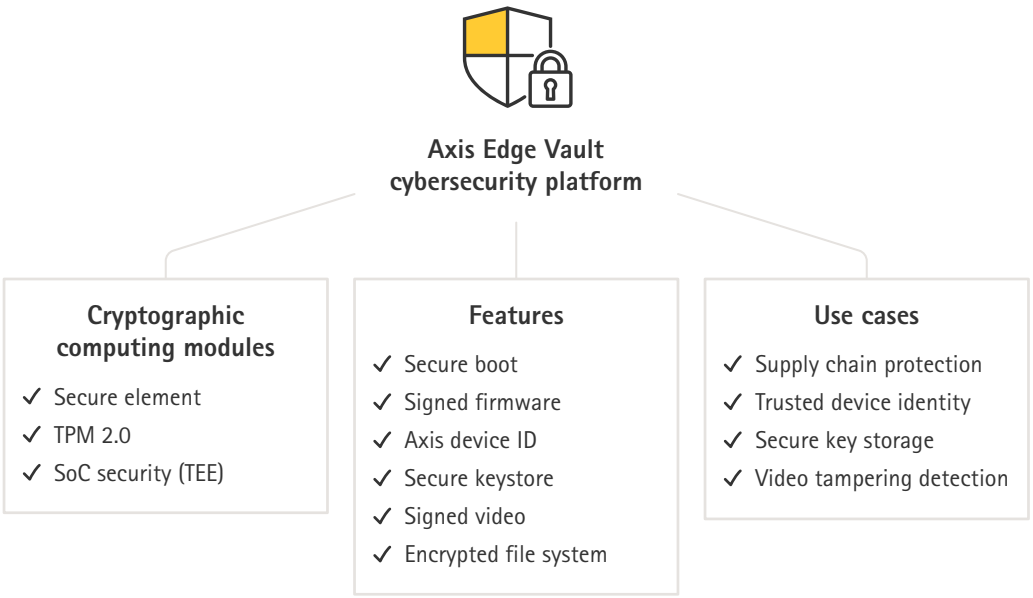
Axis Edge Vault

Axis Edge Vault offre una piattaforma di cybersecurity basata sull'hardware che protegge i dispositivi Axis. Poggia sulle solide fondamenta di moduli di elaborazione crittografica (secure element e TPM) e di sicurezza SoC (TEE e secure boot), uniti alle competenze nella sicurezza dei dispositivi edge. Axis Edge Vault gode di solide radici di attendibilità stabilite dall'avvio sicuro e dal

Protezione predefinita

firmware firmato. Queste caratteristiche rendono possibile una catena ininterrotta di software convalidati crittograficamente per la catena di attendibilità da cui dipendono tutte le operazioni sicure.

I dispositivi Axis dotati di Axis Edge Vault riducono al minimo l'esposizione dei clienti ai rischi di cybersecurity impedendo le intercettazioni e l'estrazione da parte di malintenzionati delle informazioni sensibili. Axis Edge Vault assicura in più che il dispositivo Axis sia un'unità affidabile nella rete del cliente.

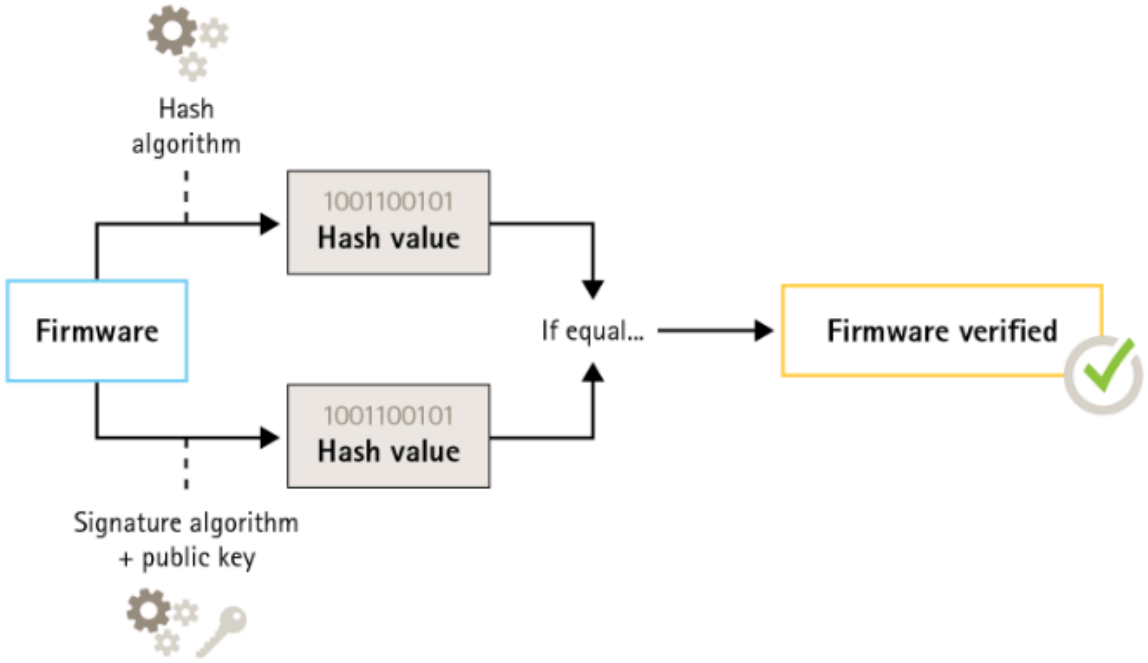


Firmware firmato

CSC #2: Inventario e controllo delle risorse software

AXIS OS è firmato dalla versione 9.20.1. Ogni volta che si esegue l'aggiornamento della versione di AXIS OS sul dispositivo, il dispositivo verificherà l'integrità dei file di aggiornamento attraverso la verifica della firma crittografica e rifiuterà i file manomessi. Ciò impedisce ai malintenzionati di indurre gli utenti all'installazione di file compromessi.

Protezione predefinita

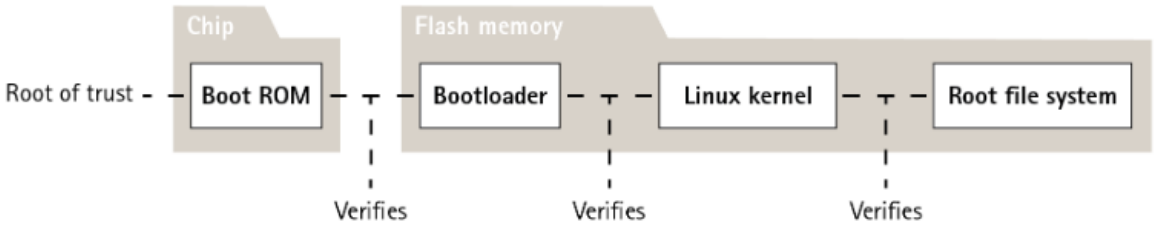


Per ulteriori informazioni, visitare il white paper su *Axis Edge Vault*.

Avvio sicuro

CSC #2: Inventario e controllo delle risorse software

La maggioranza dei dispositivi Axis dispone di una sequenza di avvio sicura per salvaguardare l'integrità del dispositivo. L'avvio sicuro impedisce di implementare i dispositivi Axis che sono stati manomessi.



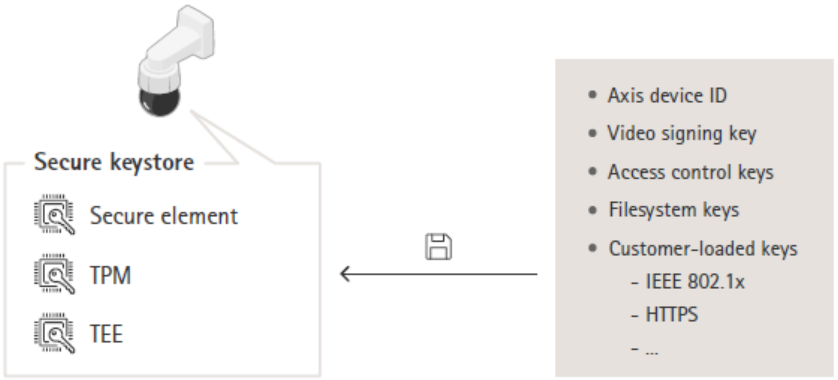
Per ulteriori informazioni, visitare il white paper su *Axis Edge Vault*.

Archivio chiavi sicuro

CSC #6: Gestione del controllo degli accessi

L'archivio chiavi sicuro mette a disposizione l'archiviazione su base hardware e protetta da manomissioni delle informazioni di crittografia. Protegge l'ID del dispositivo Axis e le informazioni di crittografia caricate dal cliente, impedendo al tempo stesso l'accesso non autorizzato e l'estrazione da parte di malintenzionati in caso di violazione della sicurezza. A seconda dei requisiti di sicurezza, un dispositivo Axis può avere uno o più moduli di questo tipo, come un TPM 2.0 (Trusted Platform Module), un elemento sicuro e/o un Trusted Execution Environment (TEE).

Protezione predefinita



Per ulteriori informazioni, visitare il white paper su *Axis Edge Vault*.

File system criptato

CSC #3: Protezione dati

È possibile che un malintenzionato tenti di estrarre le informazioni dal file system smontando la memoria flash e accedendovi attraverso un dispositivo flash reader. Tuttavia, il dispositivo Axis è in grado di tutelare il file system dall'esfiltrazione malintenzionata di dati e dalla manomissione della configurazione nel caso qualcuno riesca ad accedervi fisicamente o lo rubi. Quando il dispositivo Axis è spento, le informazioni nel file system sono crittografate con AES-XTS-Plain64256bit. Nel corso del processo di avvio sicuro, il file system lettura/scrittura è decrittografato ed è montabile e utilizzabile dal dispositivo Axis.

Per ulteriori informazioni, visitare il white paper su *Axis Edge Vault*.

HTTPS abilitato

CSC #3: Protezione dati

A partire da AXIS OS 7.20, HTTPS è stato abilitato per impostazione predefinita con un certificato autofirmato che consente di impostare la password del dispositivo in modo sicuro. A partire da AXIS OS 10.10, il certificato autofirmato è stato sostituito dal certificato ID dispositivo sicuro IEEE 802.1AR.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Sicurezza > HTTPS
≥ 7.10	Impostazioni > Sistema > Sicurezza > HTTP e HTTPS
≥ 10.9	Sistema > Rete > HTTP e HTTPS

Intestazioni HTTP(S) predefinite

AXIS OS ha le intestazioni HTTP(S) correlate alla sicurezza più comuni abilitate per impostazione predefinita al fine di migliorare il livello di base di cybersecurity nelle condizioni di fabbrica. A partire da AXIS OS 9.80, puoi usare l'intestazione HTTP VAPIX API personalizzata per la configurazione di intestazioni HTTP(S) aggiuntive.

Per saperne di più sull'intestazione HTTP API VAPIX, consultare la *libreria VAPIX*.

Per saperne di più sulle intestazioni HTTP(S) predefinite, consultare *Intestazioni HTTP(S) predefinite* nella Knowledge Base di AXIS OS.

Autenticazione digest

CSC #3: Protezione dati

Protezione predefinita

I client che accedono al dispositivo eseguono l'autenticazione con una password che deve essere crittografata quando inviata in rete. Raccomandiamo pertanto di utilizzare solo l'autenticazione digest anziché Base o sia Base che Digest. Questo riduce il rischio che gli sniffer di rete acquisiscano la password.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Avanzato > Configurazione normale > Rete > Criteri autenticazione rete HTTP
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Rete > Criteri autenticazione rete HTTP
≥ 10.9	Sistema > Configurazione normale > Rete > Criteri autenticazione rete HTTP

Protezione da replay-attack ONVIF

CSC #3: Protezione dati

La protezione da replay-attack è una funzione di sicurezza standard abilitata per impostazione predefinita nei dispositivi Axis. Il suo fine è l'ottenimento dell'autenticazione utente adeguata basata su ONVIF aggiungendo un'intestazione di sicurezza aggiuntiva, che comprende UsernameToken, timestamp valido, nonce e digest password. Il digest della password è calcolato sulla base della password (già archiviata nel sistema), del nonce e del timestamp. Il fine del digest della password è la convalida dell'utente e la prevenzione dei replay attack, ecco perché i digest vengono memorizzati nella cache. Raccomandiamo di mantenere abilitata questa impostazione.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Avanzate > Configurazione normale > Sistema > Abilitare protezione da replay-attack
≥ 7.10	Impostazioni > Sistema > Configurazione normale > ServizioWeb > Abilitare la protezione da replay-attack
≥ 10.9	Sistema > Configurazione normale > ServizioWeb > Abilitare la protezione da replay-attack

Prevenire gli attacchi di forza bruta

CSC #4: Configurazione sicura delle risorse e del software aziendali
CSC #13: Monitoraggio e difesa rete

I dispositivi Axis sono dotati di un meccanismo di prevenzione per l'identificazione e il blocco di attacchi di forza bruta provenienti dalla rete, che comportano ad esempio indovinare la password. La funzione, chiamata *protezione ritardo forza bruta,* è disponibile in AXIS OS 7.30 e versioni successive.

Per impostazione predefinita, la protezione ritardo forza bruta è abilitata a partire da AXIS OS 11.5. Per vedere esempi di configurazione e raccomandazioni approfonditi, consultare *Protezione ritardo forza bruta* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Sistema > Prevenire attacco DOS
≥ 10.9	Sistema > Sicurezza > Prevenire attacchi forza bruta

Protezione predefinita

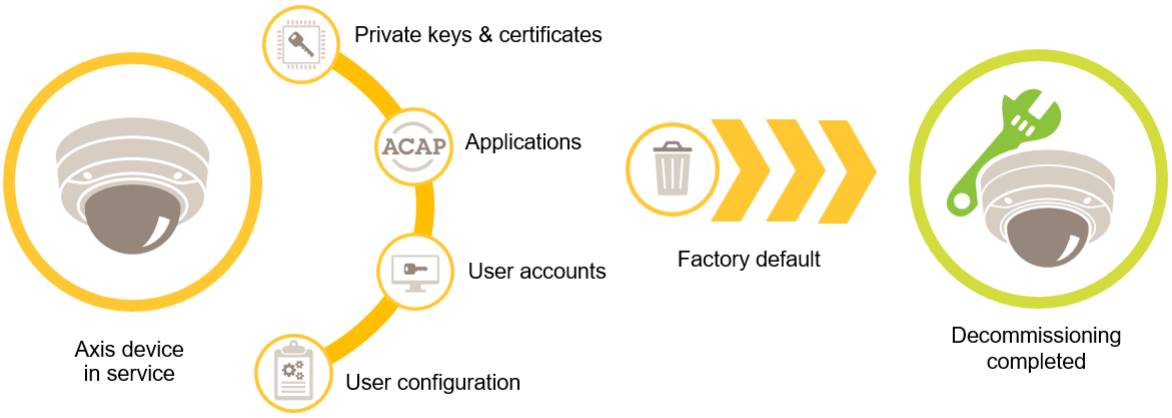
Smantellamento

CSC #3: Protezione dati

I dispositivi Axis usano sia una memoria volatile che non volatile e, mentre la memoria volatile viene cancellata ogni volta che si scollega il dispositivo dalla fonte di alimentazione, le informazioni memorizzate nella memoria non volatile restano e vengono rese nuovamente disponibili all'avvio. Evitiamo la pratica comune di rimuovere semplicemente i puntatori per rendere i dati memorizzati invisibili al file system, ecco perché è necessario un ripristino di fabbrica. Per la memoria flash NAND viene utilizzata la funzione UBI Rimuovi volume, la funzione equivalente viene utilizzata per la memoria flash eMMC, che indica che i blocchi di archiviazione non vengono più utilizzati. Il dispositivo di controllo dell'archiviazione ripulirà quindi i blocchi di archiviazione di conseguenza.

Quando si smantella un dispositivo Axis, consigliamo di eseguirne il ripristino delle impostazioni predefinite di fabbrica. Questa operazione comporterà la cancellazione di tutti i dati archiviati nella memoria non volatile del dispositivo.

L'emissione di un comando predefinito di fabbrica non cancellerà immediatamente i dati, ma il dispositivo si riavvierà e la cancellazione dei dati si verificherà durante l'avvio del sistema. Pertanto, non è sufficiente emettere il comando predefinito di fabbrica; al dispositivo deve essere consentito anche di riavviarsi e completare l'avvio prima di essere spento per garantire che la cancellazione dei dati venga completata.



Versione di AXIS OS	Percorso configurazione interfaccia web
< 7.10	Configurazione > Opzioni di sistema > Manutenzione > Impostazione predefinita
≥ 7.10	Impostazioni > Sistema > Manutenzione > Impostazione predefinita
≥ 10.9	Manutenzione > Impostazione predefinita

Questa tabella contiene maggiori informazioni sui dati archiviati nella memoria non volatile.

Informazioni e dati	Cancellati dopo il ripristino dei valori predefiniti di fabbrica
Nomi utente e password VAPIX e ONVIF	Sì
Certificati e chiavi private	Sì
Certificato autofirmato	Sì
Informazioni memorizzate su TPM e Axis Edge Vault	Sì

Protezione predefinita

Impostazioni WLAN e utenti/password	Sì
Certificati personalizzati*	No
Chiave crittografia della scheda di memoria	Sì
Dati della scheda di memoria**	No
Impostazioni e utenti/password della condivisione di rete	Sì
Dati condivisione di rete**	No
Configurazione utente***	Sì
Applicazioni caricate (ACAP)****	Sì
Dati di produzione e statistiche sulla durata****	No
Grafici e sovrapposizioni caricati	Sì
Dati orologio RTC	Sì

** Il processo firmware firmato usa certificati personalizzati che permettono agli utenti di caricare (tra le altre cose) AXIS OS.*
*** Le registrazioni e le immagini archiviate su edge storage (scheda di memoria, condivisione di rete) vanno eliminate separatamente dall'utente. Per saperne di più, consultare Formattazione delle schede di memoria* nella Knowledge Base di AXIS OS.
**** Tutte le configurazioni create dall'utente, dalla creazione di account alle configurazioni di rete, O3C, eventi, immagini, PTZ e di sistema.*
***** Il dispositivo conserva tutte le applicazioni preinstallate ma ne elimina tutte le configurazioni effettuate dall'utente*
****** Dati di produzione (calibrazione, certificati di produzione 802.1AR) e le statistiche sulla durata includono informazioni non sensibili e non relative all'utente.*

Protezione di base

Protezione di base

La protezione di base è il livello di protezione minimo raccomandato per i dispositivi Axis. Gli argomenti in merito alla protezione di base sono "configurabili su edge". Ciò significa che possono essere configurati direttamente nel dispositivo Axis senza ulteriori dipendenze da infrastrutture di rete, video management system o sistemi di gestione delle prove (VMS, EMS), apparecchiature o applicazioni di terze parti.

Impostazioni dei valori predefiniti di fabbrica

CSC #4: Configurazione sicura delle risorse e del software aziendali

Prima di configurare il dispositivo, accertarsi che sia nello stato di impostazione di fabbrica. Inoltre, è importante eseguire il ripristino delle impostazioni predefinite di fabbrica del dispositivo quando si devono cancellare i dati utente o smantellare il dispositivo. Per ulteriori informazioni, consultare .

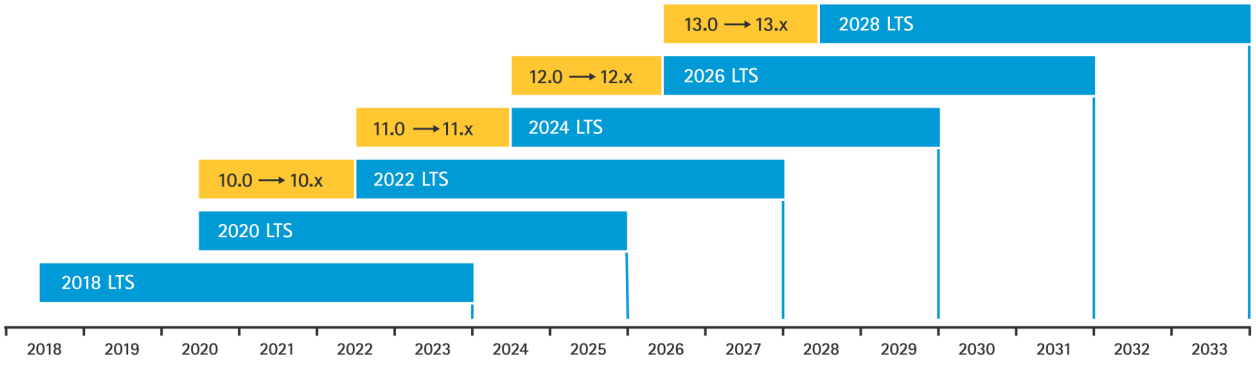
Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Manutenzione > Impostazione predefinita
≥ 7.10	Impostazioni > Sistema > Manutenzione > Impostazione predefinita
≥ 10.9	Manutenzione > Impostazione predefinita

Aggiornare all'AXIS OS più recente

CSC #2: Inventario e controllo delle risorse software

L'installazione di patch per il software è un aspetto importante della cybersecurity. I malintenzionati tentano spesso di sfruttare vulnerabilità conosciute e possono riuscire nel loro intento se ottengono l'accesso di rete a un servizio al quale non è stata applicata la patch. Accertarsi di usare sempre l'AXIS OS più recente dal momento che può comprendere patch di sicurezza per vulnerabilità note. È possibile che le note di rilascio per una versione specifica menzionino esplicitamente una correzione di sicurezza critica, ma non tutte le correzioni generali.

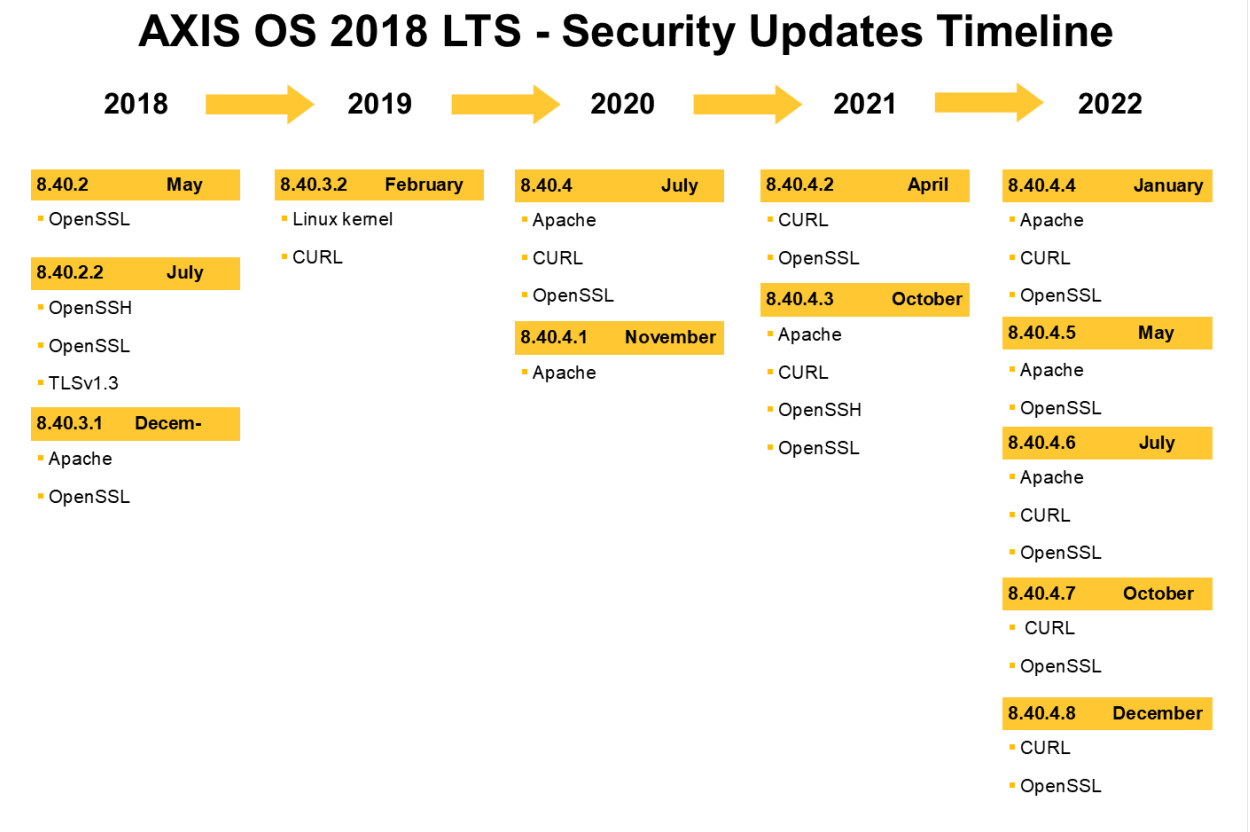
Axis gestisce due tipi di tracce AXIS OS: la traccia attiva o le tracce di supporto a lungo termine (LTS). Benché entrambi i tipi comprendano le ultime patch per le vulnerabilità critiche, nelle tracce LTS non sono comprese nuove funzionalità perché il loro fine è la riduzione al minimo del rischio di problemi di compatibilità. Per saperne di più, consultare *ciclo di vita di AXIS OS* nelle informazioni di AXIS OS.



Axis mette a disposizione le previsioni per le versioni future con informazioni in merito a nuove funzionalità importanti, correzioni di bug e patch di sicurezza. Per saperne di più, consultare *Prossime versioni* nelle informazioni su AXIS OS. Visitare *Firmware* presso axis.com per eseguire il download di AXIS OS per il tuo dispositivo.

Protezione di base

Questo grafico illustra quanto è importante mantenere aggiornati i dispositivi Axis.



Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Manutenzione > Server di aggiornamento
≥ 7.10	Impostazioni > Sistema > Manutenzione > Aggiornamento firmware
≥ 10.9	Manutenzione > Aggiornamento firmware

Imposta password root dispositivo

CSC #4: Configurazione sicura delle risorse e del software aziendali
CSC #5: Gestione account

L'account root del dispositivo è l'account di amministrazione principale del dispositivo. Per usare l'account root, prima bisogna impostare una password del dispositivo. Accertarsi di usare una password complessa e limitare l'uso dell'account root unicamente alle attività di amministrazione. Non consigliamo di usare l'account root nella produzione giornaliera.

Quando si usano i dispositivi Axis, impiegare la stessa password rende più semplice la gestione ma incrementa la vulnerabilità alle violazioni e alle perdite di dati. Impiegare password univoche per ogni dispositivo Axis assicura un'elevata sicurezza, ma rende più complesso gestire i dispositivi. Consigliamo di modificare regolarmente la password sui propri dispositivi.

Consigliamo l'implementazione di linee guida che richiedano che le nuove password siano abbastanza lunghe e complesse, come le *raccomandazioni sulle password NIST*. I dispositivi Axis supportano password fino a 64 caratteri. Le password al di sotto di **8 caratteri** sono considerate deboli.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Configurazione di base > Utenti
≥ 7.10	Impostazioni > Sistema > Utenti
≥ 10.9	Sistema > Utenti
≥ 11.6	Sistema > Account

Creare account dedicati

CSC #4: Configurazione sicura delle risorse e del software aziendali
CSC #5: Gestione account

L'account root predefinito dispone di tutti i privilegi e deve essere riservato per le attività amministrative. Consigliamo la creazione di un account utente client con privilegi limitati per le attività quotidiane. Ciò riduce il rischio di compromissione della password dell'amministratore dispositivo.

Per ulteriori informazioni, vedere la *sezione relativa all'identità e alla gestione degli accessi nella Knowledge Base di AXIS OS*.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Configurazione di base > Utenti
≥ 7.10	Impostazioni > Sistema > Utenti
≥ 10.9	Sistema > Utenti
≥ 11.6	Sistema > Account

Limita l'accesso all'interfaccia Web

CSC #5: Gestione account

I dispositivi Axis hanno un server Web che permette agli utenti di eseguire l'accesso al dispositivo con un browser Web standard. L'interfaccia Web è pensata per la configurazione, la manutenzione e la risoluzione dei problemi. Non è pensata per le operazioni quotidiane, ad esempio in qualità di client per visualizzare video.

Gli unici client a cui dovrebbe essere permessa l'interazione con i dispositivi Axis nel corso delle operazioni quotidiane sono i video management system (VMS) o gli strumenti di amministrazione e gestione dei dispositivi come AXIS Device Manager. Agli utenti di sistema non dovrebbe mai essere permesso l'accesso diretto ai dispositivi Axis. Per ulteriori informazioni, consultare .

Disabilitare l'accesso all'interfaccia Web

CSC #4: Configurazione sicura delle risorse e del software aziendali

A partire da AXIS OS 9.50, si può disabilitare l'interfaccia Web di un dispositivo Axis. Una volta implementato un dispositivo Axis in un sistema (o aggiunto ad AXIS Device Manager), consigliamo di rimuovere l'opzione di accesso al dispositivo da parte di persone nell'organizzazione tramite un browser Web. Ciò crea un livello di sicurezza in più se la password dell'account del dispositivo viene condivisa nell'organizzazione. L'opzione più sicura è impostare l'accesso ai dispositivi Axis esclusivamente tramite applicazioni dedicate che mettono a disposizione un'architettura IAM (Identity Access Management) avanzata, maggiore tracciabilità e tutele per evitare perdite di account.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Sistema > Interfaccia Web disabilitata
≥ 10.9	Sistema > Configurazione normale > Sistema > Interfaccia Web disabilitata

Configurazione delle impostazioni di rete

CSC #12: Gestione dell'infrastruttura di rete

La configurazione IP del dispositivo dipende dalla configurazione di rete, come IPv4/IPv6, indirizzo di rete statico o dinamico (DHCP), subnet mask e router predefinito. Consigliamo di rivedere la propria topologia di rete ogni qualvolta che si aggiungono nuovi tipi di componenti.

Consigliamo anche di usare la configurazione dell'indirizzo IP statico sui dispositivi Axis per assicurare la raggiungibilità di rete e districare la questione della dipendenza dai server in rete (ad esempio i server DHCP) che potrebbero essere presi di mira da attacchi.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Configurazione di base > TCP/IP
≥ 7.10	Impostazioni > Sistema > TCP/IP
≥ 10.9	Sistema > Rete

Configurare impostazioni Data e ora

CSC #8: Gestione registro di controllo

Dalla prospettiva della sicurezza, è importante impostare la data e l'ora esatte. Ciò assicura, ad esempio, che i registri di sistema siano contrassegnati con l'ora esatta e che si possano convalidare e usare i certificati digitali durante l'esecuzione. Senza una corretta sincronizzazione dell'ora, i servizi che si affidano a certificati digitali come HTTPS, IEEE e 802.1x potrebbero non funzionare in modo esatto.

Consigliamo di mantenere l'orologio del dispositivo Axis sincronizzato con i server NTP (Network Time Protocol, non crittografati) o, preferibilmente, con i server Network Time Security (NTS, crittografati). Network Time Security (NTS), una variante crittografata e sicura del protocollo NTP (Network Time Protocol), è stata aggiunta in AXIS OS 11.1. Consigliamo la configurazione di più server ora per una maggiore precisione di sincronizzazione dell'ora, ma anche in previsione di uno scenario di failover in cui uno dei server ora configurati potrebbe non essere disponibile.

Usare server NTP o NTS pubblici può essere un'alternativa per individui e piccole organizzazioni che non possono semplificare da sole le istanze del server dell'ora locale. Per saperne di più su NTP/NTS nei dispositivi Axis, consultare *NTP e NTS* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Configurazione di base > Data e ora
≥ 7.10	Impostazioni > Sistema > Data e ora
≥ 10.9	Sistema > Data e ora
≥ 11.6	Sistema > Ora e ubicazione

Crittografia edge storage

CSC #3: Protezione dati

Scheda di memoria
Se il dispositivo Axis supporta e usa schede Secure Digital (SD) per archiviare le registrazioni video, consigliamo di applicare la crittografia. Ciò impedirà a persone non autorizzate di riprodurre il video memorizzato da una scheda di memoria rimossa.

Per saperne di più sulla crittografia della scheda di memoria nei dispositivi Axis, consultare *Supporto per schede di memoria* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Archiviazione
≥ 7.10	Impostazioni > Sistema > Archiviazione
≥ 10.9	Sistema > Archiviazione

Condivisione di rete (NAS)
Se si usa un dispositivo NAS (Network Attached Storage) come dispositivo di registrazione, consigliamo di tenerlo in un'area protetta con accesso limitato e di abilitarvi la codifica su disco rigido. I dispositivi Axis usano SMB come protocollo di rete per la connessione a un NAS per l'archiviazione delle registrazioni video. Benché le versioni precedenti di SMB (1.0 e 2.0) non forniscano alcuna sicurezza o crittografia, le versioni successive (2.1 e successive) lo fanno, ecco perché consigliamo di usare versioni successive durante la produzione.

Per saperne di più sulla corretta configurazione SMB quando si connette un dispositivo Axis a una condivisione di rete, consultare *Condivisione di rete* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Archiviazione
≥ 7.10	Impostazioni > Sistema > Archiviazione
≥ 10.9	Sistema > Archiviazione

Esportare codifica delle registrazioni

CSC #3: Protezione dati

A partire da AXIS OS 10.10, i dispositivi Axis supportano l'esportazione crittografata di registrazioni edge. Consigliamo di usare questa funzione in quanto impedisce a persone non autorizzate di riprodurre materiale video esportato.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	N/D
≥ 10.9	Registrazioni

Applicazioni (ACAP)

CSC #4: Configurazione sicura delle risorse e del software aziendali

Puoi caricare le applicazioni sul dispositivo Axis per l'ampliamento della sua funzionalità. Molte di esse hanno la propria interfaccia utente ai fini dell'interazione con una determinata funzionalità. Le applicazioni potrebbero usare la funzionalità di sicurezza messa a disposizione da AXIS OS.

Nei dispositivi Axis sono precaricate varie applicazioni sviluppate da Axis in base al *Modello di sviluppo della sicurezza Axis (ASDM)*. Per saperne di più in merito alle applicazioni Axis, consultare *Analisi* presso axis.com.

Per le applicazioni di terzi, consigliamo di contattare il fornitore per quanto riguarda punti di prova in merito alla sicurezza dell'applicazione in termini di funzionamento e verifica e per accertare se sono state sviluppate secondo modelli di sviluppo di

sicurezza basati sulle migliori prassi comuni. Le vulnerabilità trovate in applicazioni di terzi vanno segnalate direttamente al fornitore terzo.

Consigliamo di usare solo applicazioni attendibili e rimuovere quelle inutilizzate dai dispositivi Axis.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Applicazione
≥ 7.10	Impostazioni > App
≥ 10.9	App

Disabilita funzioni/servizi inutilizzati

CSC #4: Configurazione sicura delle risorse e del software aziendali

Benché le funzioni e i servizi non usati non rappresentino un pericolo immediato per la sicurezza, si consiglia di disabilitare le funzioni e i servizi inutilizzati per ridurre i rischi non necessari. Continuare a leggere per saperne di più sui servizi e le funzioni che si possono disabilitare se non sono in uso.

Porte di rete fisiche non usate

A cominciare da AXIS OS 11.2, i dispositivi con molteplici porte di rete, come AXIS S3008, presentano la possibilità di eseguire la disabilitazione sia di PoE che del traffico di rete delle loro porte di rete. Lasciare incustodite le porte di rete non in uso e attive rappresenta un grave rischio per la sicurezza.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	N/D
≥ 11.2	Sistema > Power over Ethernet:

Protocolli di rilevamento della rete

I protocolli di rilevamento, quali Bonjour, UPnP®, ZeroConf, WS-Discovery e LLDP/CDP sono servizi di supporto che rendono più facile individuare il dispositivo Axis e i relativi servizi in rete. Dopo l'implementazione del dispositivo e l'aggiunta al VMS, consigliamo la disabilitazione del protocollo di rilevamento affinché il dispositivo Axis non annunci la sua presenza nella rete.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Avanzate > Configurazione normale > Rete > Bonjour rete abilitato, UPnP® rete abilitato, ZeroConf rete abilitato, UPnP® NATTraversal rete abilitato*
	N/D
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Rete > Bonjour rete abilitato, UPnP® rete abilitato, ZeroConf rete abilitato, UPnP® NATTraversal rete abilitato*
	Impostazioni > Sistema > Configurazione normale > WebService > Modalità rilevamento

Versione di AXIS OS	Percorso configurazione Interfaccia Web
≥ 10.9	Impostazioni > Configurazione normale > Rete > Bonjour abilitato, UPnP® abilitato, ZeroConf abilitato
	Sistema > Configurazione normale > WebService > Modalità rilevamento > Abilita modalità rilevabile WS-Discovery
≥ 11.11	Sistema > Rete > Protocolli di rilevamento della rete > LLDP and CDP**

** La funzionalità è stata rimossa da AXIS 10.12 e non è disponibile in versioni successive.*
*** La disabilitazione di LLDP e CDP potrebbe influire sulla negoziazione dell'alimentazione PoE.*

Versioni TLS obsolete

Consigliamo la disabilitazione di versioni TLS obsolete e non sicure prima di inserire il proprio dispositivo Axis nella produzione. Le versioni TLS obsolete sono normalmente disabilitate per impostazione predefinita, ma si possono abilitare nei dispositivi Axis per assicurare la compatibilità retroattiva con applicazioni di terze parti che non hanno ancora implementato TLS 1.2 e TLS 1.3.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Avanzato > Configurazione normale > HTTPS > Consentire TLSv1.0 *e/o* Consentire TLSv1.1
≥ 7.10	Impostazioni > Sistema > Configurazione normale > HTTPS > Consenti TLSv1.0 *e/o* Consenti TLSv1.1
≥ 10.9	Sistema > Configurazione normale > HTTPS > Consenti TLSv1.0 *e/o* Consenti TLSv1.1

Ambiente editor di script

Consigliamo la disabilitazione dell'accesso all'ambiente dell'editor di script. L'editor di script è impiegato unicamente ai fini della risoluzione di problemi e di debug.

L'editor di script è stato rimosso da AXIS OS 10.11 e non è disponibile in versioni successive.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Sistema > Abilita l'editor di script (editcgi)
≥ 10.9	Sistema > Configurazione normale > Sistema > Abilita l'editor di script (editcgi)

Intestazioni server HTTP(S)

Per impostazione predefinita, i dispositivi Axis annunciano le versioni Apache e OpenSSL attuali nel corso delle connessioni HTTP(S) con i client nella rete. Queste informazioni risultano utili quando si usano regolarmente scanner di sicurezza di rete poiché forniscono un report più dettagliato delle vulnerabilità presenti in una particolare versione del sistema operativo AXIS.

Si possono disabilitare le intestazioni server HTTP(S) ai fini della riduzione dell'esposizione delle informazioni durante le connessioni HTTP(S). Ciononostante, consigliamo la disabilitazione delle intestazioni solo se si usa il dispositivo secondo le nostre raccomandazioni e viene mantenuto sempre aggiornato.

L'opzione per la disabilitazione delle intestazioni server HTTP(S) è disponibile a partire da AXIS OS 10.6.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Sistema > Commenti intestazione server HTTP
≥ 10.9	Sistema > Configurazione normale > Sistema > Commenti intestazione server HTTP

Audio

Nei dispositivi Axis orientati alla videosorveglianza, come le telecamere di rete, l'ingresso/uscita audio e la funzionalità microfono sono disattivati per impostazione predefinita. Se servono funzionalità audio, bisogna abilitarle prima dell'uso. Nei dispositivi Axis nei quali le funzioni audio di ingresso/uscita e microfono sono caratteristiche chiave, come gli interfoni Axis e gli altoparlanti di rete, le funzionalità audio sono abilitate per impostazione predefinita.

Consigliamo la disabilitazione delle funzionalità audio se non sono usate.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Avanzate > Configurazione normale > Audio > Audio A* > Abilitato
≥ 7.10	Impostazioni > Audio > Consenti audio
≥ 10.9	Audio > Impostazioni dispositivo

Slot per schede di memoria

I dispositivi Axis supportano solitamente almeno una scheda di memoria per mettere a disposizione l'archiviazione su dispositivi edge locale delle registrazioni video. Consigliamo la disabilitazione totale dello slot per schede di memoria se non se ne usano. L'opzione di disabilitazione dello slot per schede di memoria è disponibile in AXIS OS 9.80

Per saperne di più, consultare *Disabilitare scheda di memoria* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Archiviazione > SD disk abilitato
≥ 10.9	Sistema > Configurazione normale > Archiviazione > SD disk abilitato

Accesso FTP

FTP è un protocollo di comunicazione non sicuro impiegato unicamente ai fini della risoluzione di problemi e di debug. L'accesso FTP è stato rimosso da AXIS OS 11.1 e non è a disposizione nelle versioni successive. Consigliamo la disabilitazione dell'accesso FTP e l'uso dell'accesso SSH sicuro ai fini di risoluzione di problemi.

Per saperne di più su SSH, consultare *Accesso SSH* nel portale AXIS OS. Per saperne di più sulle opzioni di uso di FTP, consultare *Accesso FTP* nel portale AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Configurazione normale > Rete > FTP abilitato
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Rete > FTP abilitato
≥ 10.9	Sistema > Configurazione normale > Rete > FTP abilitato

Accesso SSH

SSH è un protocollo di comunicazione sicuro impiegato unicamente ai fini della risoluzione di problemi e di debug. È supportato dai dispositivi Axis a partire da AXIS OS 5.50. Consigliamo la disabilitazione dell'accesso SSH.

Per saperne di più sulle opzioni di uso di SSH, consultare *Accesso SSH* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Configurazione normale > Rete > SSH abilitato
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Rete > SSH abilitato
≥ 10.9	Sistema > Configurazione normale > Rete > SSH abilitato

Accesso Telnet

Telnet è un protocollo di comunicazione non sicuro impiegato unicamente ai fini della risoluzione di problemi e di debug. Viene supportato dai dispositivi Axis con versioni precedenti ad AXIS OS 5.50. Consigliamo di disabilitare l'accesso Telnet.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 5,50	Per trovare istruzioni, consultare *Accesso ai dispositivi* nella Knowledge Base di AXIS OS.
< 7,10	N/D
≥ 7.10	N/D
≥ 10.9	N/D

ARP/Ping

ARP/Ping era un metodo di impostazione dell'indirizzo IP del dispositivo Axis usando strumenti come AXIS IP Utility. La funzionalità è stata rimossa da AXIS OS 7.10 e non è disponibile in versioni successive. Consigliamo la disabilitazione della funzione nei dispositivi Axis con AXIS OS 7.10 e versioni precedenti.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Avanzate > Configurazione normale > Rete > ARP/Ping
≥ 7.10	N/D
≥ 10.9	N/D

Filtro indirizzi IP

CSC #1: Inventario e controllo delle risorse aziendali
CSC #4: Configurazione sicura delle risorse e del software aziendali
CSC #13: Monitoraggio e difesa rete

Il filtro indirizzi IP impedisce a client non autorizzati di accedere al dispositivo Axis. Consigliamo di eseguire la configurazione del proprio dispositivo in modo da permettere gli indirizzi IP di host di rete autorizzati o negare gli indirizzi IP di host di rete non autorizzati.

Se si sceglie di permettere gli indirizzi IP, accertarsi di aggiungere al proprio elenco tutti i client autorizzati (server VMS e client amministrativi).

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Impostazione > Opzioni di sistema > Sicurezza > Filtro indirizzi IP
≥ 7.10	Impostazioni > Sistema > TCP/IP > Filtro indirizzi IP
≥ 10.9*	Impostazioni > Sicurezza > Filtro indirizzi IP

** In AXIS OS 11.9 e versioni successive, il filtro per indirizzi IP è stato sostituito dal nuovo firewall basato su host.*

Firewall basato su host

CSC #1: Inventario e controllo delle risorse aziendali
CSC #4: Configurazione sicura delle risorse e del software aziendali
CSC #13: Monitoraggio e difesa rete

Gli utenti possono utilizzare il firewall per creare regole per gestire il traffico in ingresso verso i dispositivi in base all'indirizzo IP e/o ai numeri di porta TCP/UDP. Questo può impedire ai client non autorizzati di accedere al dispositivo Axis o a determinati servizi sul dispositivo.

Se il criterio predefinito è impostato su "Nega", assicurarsi di aggiungere all'elenco tutte le porte e/o i client autorizzati (VMS e client amministrativi).

Versione di AXIS OS	**Percorso configurazione interfaccia web**
≥ 11.9	Impostazione > Sicurezza > Firewall

HTTPS

CSC #3: Protezione dati

HTTP e HTTPS sono abilitati per impostazione predefinita nei dispositivi Axis a partire da AXIS OS 7.20. Mentre l'accesso HTTP non risulti sicuro senza alcuna crittografia, HTTPS crittografa il traffico tra il client e il dispositivo Axis. Consigliamo l'uso di HTTPS per tutte le attività amministrative sul dispositivo Axis.

Per istruzioni di configurazione, consultare e .

Solo HTTPS

Consigliamo la configurazione del dispositivo Axis affinché usi unicamente HTTPS (senza accesso HTTP possibile). Ciò risulterà nell'abilitazione automatica di HSTS (HTTP Strict Transport Security), che comporterà un ulteriore miglioramento della sicurezza del dispositivo.

A partire da AXIS OS 7.20, i dispositivi Axis sono dotati di certificato autofirmato. Benché un certificato autofirmato non sia di per sé attendibile, è sufficiente per accedere con sicurezza al dispositivo Axis nel corso della configurazione iniziale e quando non c'è alcuna public key infrastructure (PKI). Se c'è, bisognerebbe rimuovere il certificato autofirmato e sostituirlo con adeguati

certificati client firmati emessi da un'autorità PKI scelta. A partire da AXIS OS 10.10, il certificato autofirmato è stato sostituito dal certificato ID dispositivo sicuro IEEE 802.1AR.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Sicurezza > HTTPS
≥ 7.10	Impostazioni > Sistema > Sicurezza > HTTP e HTTPS
≥ 10.9	Sistema > Rete > HTTP e HTTPS

Crittografia HTTPS

I dispositivi Axis supportano e usano cipher suite TLS 1.2 e TLS 1.3 per crittografare con sicurezza le connessioni HTTPS. La versione TLS e la cipher suite specifiche usate dipendono dal client che si collega al dispositivo Axis e saranno negoziate di conseguenza. Con gli aggiornamenti regolari AXIS OS, l'elenco di crittografia disponibile del dispositivo Axis può ricevere aggiornamenti senza che la configurazione effettiva della crittografia venga modificata. Una modifica di configurazioni di crittografia deve essere avviata dall'utente, eseguendo un reset alle impostazioni predefinite di fabbrica del dispositivo Axis o tramite la configurazione manuale dell'utente. A partire da AXIS OS 10.8 e versioni successive, l'elenco di crittografia viene aggiornato automaticamente quando l'utente esegue un aggiornamento di AXIS OS.

TLS 1.2 e versione inferiore

Quando si utilizza TLS 1.2 o versione inferiore, è possibile specificare la crittografia HTTPS che deve essere utilizzata dal dispositivo Axis dopo il riavvio. Non ci sono restrizioni relativamente alla crittografia che è possibile scegliere, ma consigliamo di scegliere una o tutte le seguenti crittografie forti:

```
ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
POLY1305
```

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Avanzate > Configurazione normale > HTTPS > Crittografia
≥ 7.10	Impostazioni > Sistema > Configurazione normale > HTTPS > Crittografia
≥ 10.9	Sistema > Configurazione normale > HTTPS > Crittografia

TLS 1.3

Per impostazione predefinita, sono a disposizione solo cipher suite forti secondo le specifiche TLS 1.3:

```
TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384
```

Queste suite non possono essere configurate dall'utente.

Registro degli accessi

CSC #1: Inventario e controllo delle risorse aziendali
CSC #8: Gestione registro di controllo

Il registro di accessi mette a disposizione registri dettagliati degli utenti che eseguono l'accesso al dispositivo Axis, rendendo così più facili i controlli e la gestione del controllo degli accessi. Consigliamo l'abilitazione di questa funzione in congiunzione con un server syslog remoto affinché il dispositivo Axis sia in grado di inviare i registri ad un ambiente di registrazione centrale. Ciò semplifica l'archiviazione dei messaggi di registro e il tempo di conservazione.

Per maggiori informazioni, consultare *Registrazione degli accessi ai dispositivi* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Avanzate > Configurazione normale > Sistema > Registro accessi
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Sistema > Controllo degli accessi
≥ 10.9	Sistema > Configurazione normale > Sistema > Controllo degli accessi

Accessori anti-manomissione fisica

CSC #1: Inventario e controllo delle risorse aziendali
CSC #12: Gestione dell'infrastruttura di rete

Axis mette a disposizione switch contro intrusioni fisiche e/o manomissioni come accessori facoltativi per migliorare la protezione fisica dei dispositivi Axis. Questi switch sono in grado di attivare un allarme che permette ai dispositivi Axis di inviare una notifica o un allarme ai client selezionati.

Per saperne di più riguardo agli accessori anti-manomissione disponibili, consultare:

- *AXIS TA8501 Physical Tampering Switch*
- *AXIS Dome Intrusion Switch C*
- *AXIS Door Switch A*

Protezione estesa

Le istruzioni per la protezione estesa approfondiscono gli argomenti relativi alla protezione descritti in e . Benché si possano applicare le istruzioni di protezione predefinita e di base direttamente sul proprio dispositivo Axis, la protezione estesa necessita della partecipazione attiva di tutta la catena di fornitura, dell'organizzazione dell'utente finale e dell'infrastruttura IT e/o di rete sottostante.

Limitare l'esposizione a Internet

CSC #12: Gestione dell'infrastruttura di rete

Sconsigliamo l'esposizione del dispositivo Axis come server Web pubblico o la concessione a client sconosciuti dell'accesso di rete al dispositivo in qualsiasi altro modo. Per le piccole organizzazioni e gli individui che non utilizzano un VMS o necessitano dell'accesso ai video da posizioni remote, consigliamo AXIS Companion.

AXIS Companion impiega il software client Windows/iOS/Android, è gratis e mette a disposizione un modo semplice per eseguire l'accesso ai video in sicurezza senza esporre il dispositivo Axis a Internet. Per ulteriori informazioni su AXIS Companion, vedere *axis.com/companion*.

Nota

Tutte le organizzazioni che usano un VMS devono consultare il fornitore VMS per le migliori prassi sull'accesso video remoto.

Limitare l'esposizione della rete

CSC #12: Gestione dell'infrastruttura di rete

Un modo diffuso per ridurre i rischi di esposizione della rete consiste nell'isolamento fisico e virtuale dei dispositivi di rete e delle relative infrastrutture e applicazioni. Esempi di tali infrastrutture e applicazioni sono video management software (VMS), registratori video di rete (NVR) e altri tipi di apparecchiature di sorveglianza.

Consigliamo l'isolamento dei dispositivi Axis e dell'infrastruttura e delle applicazioni correlate su una rete locale non connessa alla rete aziendale e di produzione.

Per l'applicazione della protezione di base, tutelare la rete locale e la relativa infrastruttura (router, switch) dagli accessi non autorizzati con l'aggiunta di meccanismi di sicurezza di rete multilivello. Esempi di tali meccanismi sono la segmentazione VLAN, le funzionalità di routing limitate, la rete privata virtuale (VPN) per l'accesso da sito a sito o WAN, il firewall a livello di rete 2/3 ed elenchi di controllo degli accessi (ACL).

Per ampliare la protezione di base, consigliamo l'applicazione di tecniche di ispezione di rete più avanzate, come l'ispezione profonda dei pacchetti e il rilevamento delle intrusioni. Ciò aggiungerà una protezione costante e completa dei rischi all'interno della rete. La protezione estesa della rete necessita di software e/o apparecchi hardware dedicati.

Scansione delle vulnerabilità di rete

CSC #1: Inventario e controllo delle risorse aziendali
CSC #12: Gestione dell'infrastruttura di rete

Si possono usare scanner di sicurezza di rete per l'esecuzione di valutazioni delle vulnerabilità dei dispositivi di rete. Il fine di una valutazione di vulnerabilità è mettere a disposizione una revisione sistematica di potenziali vulnerabilità della sicurezza e errori di configurazione.

Consigliamo l'esecuzione di valutazioni di vulnerabilità regolari dei dispositivi Axis e delle relative infrastrutture. Prima dell'avvio della scansione, assicurarsi che i dispositivi Axis siano stati aggiornati all'ultima versione disponibile di AXIS OS, cha sia sulla traccia LTS o attiva.

Consigliamo inoltre di rivedere il report di scansione e filtrare i falsi positivi noti per i dispositivi Axis, che è possibile trovare su *Guida scansione vulnerabilità AXIS OS*. Invia il report e qualsiasi nota supplementare con un ticket per l'helpdesk *all'assistenza Axis* su axis.com.

Protezione estesa

Public key infrastructure (PKI) attendibile

CSC #3: Protezione dati
CSC #12: Gestione dell'infrastruttura di rete

Consigliamo l'implementazione nei dispositivi Axis di certificati del server Web e del client attendibili e firmati da un'autorità di certificazione (CA) pubblica o privata. Un certificato firmato dalla CA con catena di attendibilità convalidata permette la rimozione di avvisi sul certificato nel browser quando ci si connette tramite HTTPS. Un certificato firmato dalla CA assicura inoltre l'autenticità del dispositivo Axis quando si implementa una soluzione di controllo degli accessi di rete (NAC). Ciò riduce il rischio di attacchi da un computer che impersoni un dispositivo Axis.

Si può usare AXIS Device Manager, messo a disposizione con un servizio CA integrato, per il rilascio di certificati firmati ai dispositivi Axis.

Autenticazione di controllo degli accessi di rete IEEE 802.1X

CSC #6: Gestione del controllo degli accessi
CSC #13: Monitoraggio e difesa rete

I dispositivi Axis supportano il controllo degli accessi di rete basato su porta IEEE 802.1x attraverso il metodo EAP-TLS. Per una protezione ottimale, consigliamo di usare i certificati client firmati da un'autorità di certificazione (CA) attendibile al momento di autenticare il proprio dispositivo Axis.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Impostazione > Opzioni di sistema > Sicurezza > IEEE 802.1X
≥ 7.10	Impostazioni > Sistema > Sicurezza > IEEE 802.1X
≥ 10.9	Sistema > Sicurezza > IEEE 802.1X

IEEE 802.1AE MACsec

CSC #3: Protezione dati
CSC #6: Gestione del controllo degli accessi

I dispositivi Axis supportano IEEE 802.1AE MACsec (Media Access Control Security), un protocollo di rete ben definito che protegge crittograficamente i collegamenti Ethernet punto a punto sul livello di rete 2 garantendo la riservatezza e l'integrità delle trasmissioni di dati tra due host. Dal momento che MACsec funziona al basso livello 2 dello stack di rete, aggiunge un ulteriore livello di sicurezza ai protocolli di rete che non offrono funzionalità di crittografia native (ARP, NTP, DHCP, LLDP, CDP...) e a quelli che lo offrono (HTTPS, TLS).

Lo standard IEEE 802.1AE MACsec descrive due modalità di funzionamento, una modalità Pre-Shared Key (PSK)/Static CAK configurabile manualmente e una modalità Master Session/Dynamic CAK automatica che utilizza le sessioni EAP-TLS IEEE 802.1X. Il dispositivo Axis supporta entrambe le modalità.

Per ulteriori informazioni su 802.1AE MACsec e su come configurarlo nei dispositivi OS AXIS, vedere *IEEE 802.1AE* nella knowledge base del sistema operativo AXIS.

Identità dispositivo sicura IEEE 802.1AR

CSC #1: Inventario e controllo delle risorse aziendali
CSC #13: Monitoraggio e difesa rete

I dispositivi Axis dotati di Axis Edge Vault supportano lo standard di rete IEEE 802.1AR. Ciò permette l'onboarding automatico e sicuro dei dispositivi Axis nella rete tramite l'ID dispositivo Axis, un certificato univoco installato nel dispositivo nel corso della produzione. Per un esempio di onboarding sicuro dei dispositivi, leggi di più in *Integrazione sicura dei dispositivi Axis nelle reti Aruba*.

Per ulteriori informazioni, visitare il white paper su *Axis Edge Vault*. Per eseguire il download della catena di certificati Axis Device ID, che si usa per la convalida dell'identità dispositivo dei dispositivi Axis, consultare *Archivio public key infrastructure* su axis.com.

Protezione estesa

Monitoraggio SNMP

CSC #8: Gestione registro di controllo

I dispositivi Axis supportano i seguenti protocolli SNMP:

- **SNMP v1**: supportato unicamente per ragioni legacy, non usare.
- **SNMP v2c**: si può usare su un segmento di rete protetto.
- **SNMP v3**: consigliato ai fini del monitoraggio.

I dispositivi Axis supportano anche il monitoraggio MIB-II e Axis Video MIB. Per eseguire il download di Axis Video MIB, consultare *Axis Video MIB* nella Knowledge Base di AXIS OS.

Per saperne di più su come si configura SNMP in AXIS OS, consultare *SNMP (Simple Network Management Protocol)* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Configurazione > Opzioni di sistema > Rete > SNMP
≥ 7.10	Impostazioni > Sistema > SNMP
≥ 10.9	Sistema > Rete > SNMP

Remote syslog (Syslog remoto)

CSC #8: Gestione registro di controllo

Si può configurare un dispositivo Axis affinché invii tutti i messaggi di registro crittografati a un server syslog centrale. Ciò rende più semplice eseguire i controlli e impedisce che i messaggi nel registro nel dispositivo Axis siano eliminati, che sia in modo intenzionale/dannoso o non intenzionale. In base ai criteri aziendali, è anche in grado di offrire un tempo di archiviazione prolungato dei registri del dispositivo.

Per saperne di più su come si abilita il server syslog remoto in varie versioni AXIS OS, consultare *Syslog* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	Per ottenere istruzioni, consultare *Syslog* nel portale AXIS OS
≥ 7.10	Impostazioni > Sistema > TCP/IP
≥ 10.9	Sistema > Registri

Streaming video sicuro (SRTP/RTSPS)

CSC #3: Protezione dati

A partire da AXIS OS 7.40, i dispositivi Axis supportano lo streaming video sicuro tramite RTP, detto anche SRTP/RTSPS. SRTP/RTSPS usa un metodo di trasporto crittografato end-to-end sicuro per far sì che unicamente i client autorizzati ricevano il flusso video dal dispositivo Axis. Consigliamo l'abilitazione di SRTP/RTSPS se il video management system (VMS) lo supporta. Se disponibile, usare SRTP invece dello streaming video RTP non crittografato.

Nota

SRTP/RTSPS crittografa unicamente i dati del flusso video. Per le attività di configurazione amministrative, consigliamo l'abilitazione di HTTPS unicamente per eseguire la crittografia di questo tipo di comunicazione.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Avanzate > Configurazione normale > Rete > RTSPS
≥ 7.10	Impostazioni > Sistema > Configurazione normale > Rete > RTSPS
≥ 10.9	Sistema > Configurazione normale > Rete > RTSPS

Video firmato

CSC #3: Protezione dati

A partire da AXIS OS 10.11, i dispositivi Axis dotati di Axis Edge Vault supportano il video firmato. Con video firmato, i dispositivi Axis possono aggiungere una firma al flusso video per assicurarsi che il video sia intatto e per verificarne l'origine con il dispositivo che lo ha prodotto. Anche il Video Management System (VMS) o il sistema di gestione delle prove (EMS) possono verificare l'autenticità del video fornito da un dispositivo Axis.

Per ulteriori informazioni, visitare il white paper su *Axis Edge Vault*. Per individuare i certificati root Axis usati per convalidare l'autenticità del video firmato, consultare *Accesso al dispositivo* nella Knowledge Base di AXIS OS.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7,10	N/D
≥ 7.10	N/D
≥ 10.9	Sistema > Configurazione normale > Immagine > Video firmato

Guida introduttiva

La guida introduttiva mette a disposizione una breve panoramica delle impostazioni che vanno configurate per la protezione dei dispositivi Axis dotati di AXIS OS 5.51 e versioni successive. Tratta gli argomenti relativi alla protezione che si possono consultare in , tuttavia non tratta gli argomenti in perché richiedono una configurazione approfondita e specifica per il cliente, caso per caso.

Consigliamo di usare AXIS Device Manager per proteggere molteplici dispositivi Axis rapidamente ed efficientemente. Se serve usare un'altra applicazione per la configurazione del dispositivo o se bisogna solo proteggere alcuni dispositivi Axis, consigliamo l'uso dell'API VAPIX.

Errori di configurazione frequenti

Dispositivi esposti a Internet
CSC #12: Gestione dell'infrastruttura di rete

Sconsigliamo l'esposizione del dispositivo Axis come server Web pubblico o la concessione a client sconosciuti dell'accesso di rete al dispositivo in qualsiasi altro modo. Per ulteriori informazioni, consultare .

Password comune
CSC # 4: Configurazione sicura delle risorse e del software aziendali
CSC #5: Gestione account

Consigliamo fortemente di usare una password univoca per ciascun dispositivo anziché una password generica per tutti i dispositivi. Per le istruzioni, vedere and .

Accesso anonimo
CSC #4: Configurazione sicura delle risorse e del software aziendali
CSC #5: Gestione account.

Sconsigliamo di permettere agli utenti anonimi l'accesso alle impostazioni video e di configurazione nel dispositivo senza dover fornire le credenziali di accesso. Per ulteriori informazioni, consultare .

Comunicazione sicura disabilitata
CSC #3: Protezione dati

Sconsigliamo l'uso del dispositivo impiegando metodi di accesso e comunicazione non sicuri, quali HTTP o l'autenticazione di base, nell'ambito dei quali le password sono trasferite senza crittografia. Per ulteriori informazioni, consultare . Per ottenere raccomandazioni sulla configurazione, consultare .

Versione di AXIS OS obsoleta
CSC #2: Inventario e controllo delle risorse software

Si consiglia fortemente l'uso del dispositivo Axis con l'ultima versione di AXIS OS disponibile, sia sulla traccia LTS che su quella attiva. Entrambe le tracce mettono a disposizione le ultime patch di sicurezza e le correzioni di bug. Per ulteriori informazioni, consultare .

Protezione di base tramite API VAPIX

Si può usare l'API VAPIX per proteggere i dispositivi Axis nell'ambito degli argomenti trattati in . In questa tabella si possono trovare tutte le impostazioni di configurazione di protezione di base a prescindere dalla versione AXIS OS del proprio dispositivo Axis.

Alcune impostazioni di configurazione potrebbero non essere più disponibili nella versione AXIS OS del proprio dispositivo perché certe funzionalità sono state rimosse nel tempo per incrementare la sicurezza. Un errore quando si esegue la chiamata VAPIX potrebbe indicare che la funzionalità non è più disponibile nella versione di AXIS OS.

Guida introduttiva

Scopo	Chiamata API VAPIX
*Disabilitazione di POE nelle porte di rete non usate**	`http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*Disabilitazione del traffico di rete nelle porte di rete non usate***	`http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
Disabilitare protocollo di rilevamento Bonjour	`https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
Disabilitare protocollo di rilevamento UPnP®	`https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no` `https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no`
Disabilitare protocollo di rilevamento WebService	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
Disabilitare la connessione a cloud con un clic (O3C)	`https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
Disabilitare l'accesso di manutenzione SSH del dispositivo	`https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
Disabilitare l'accesso di manutenzione FTP del dispositivo	`https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
Disabilitare la configurazione dell'indirizzo IP ARP-Ping	`https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
Disabilitare la configurazione dell'indirizzo IP Zero-Conf	`http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`

Abilitare solo HTTPS	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`

Abilitare solo TLS 1.2 e TLS 1.3	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no` `https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`

Scopo	Chiamata API VAPIX
Configurazione crittografia sicura TLS 1.2	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.Ciphers=ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384`

*Abilitare protezione contro attacchi a forza bruta****	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.ActivatePasswordThrottling=on`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSBlockingPeriod=10`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSPageInterval=1`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteCount=20`
	`https://ip-address/axis-cgi/param.cgi?action=update&System.PreventDoSAttack.DoSSiteInterval=1`

Disabilitare l'ambiente dell'editor di script	`https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no`
Abilitare una migliore registrazione degli accessi utente	`https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On`
Abilitare protezione da replay-attack ONVIF	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
Disabilitare l'accesso all'interfaccia Web del dispositivo	`https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`
Disabilitare intestazione server HTTP/OpenSSL	`https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`

Disabilitare il visualizzatore anonimo e l'accesso PTZ	`https://ip-address/axis-cgi/param.cgi?action=update&root.Network.RTSP.ProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.System.BoaProtViewer=password`
	`https://ip-address/axis-cgi/param.cgi?action=update&root.PTZ.BoaProtPTZOperator=password`

Scopo	Chiamata API VAPIX
Impedire l'installazione di applicazioni ACAP che richiedono privilegi root	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
Impedire l'installazione di applicazioni ACAP non firmate	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

** Sostituire "X" con il numero di porta effettivo in "port=X". Esempi: "port=1" disabiliterà la porta 1 and "port=2" disabiliterà la porta 2.*
*** Sostituire "1" con il numero di porta effettivo in "eth1.1". Esempi: "eth1.1" disabiliterà la porta 1 e "eth1.2" disabiliterà la porta 2.*
**** Dopo 20 tentativi di accesso non riusciti entro un secondo, l'indirizzo IP del client viene bloccato per 10 secondi. A ogni richiesta non riuscita entro l'intervallo di pagina di 30 secondi, risulterà nell'estensione di altri 10 secondi del periodo di blocco DoS.*

Protezione di base attraverso AXIS Device Manager (Extend)

Si possono usare AXIS Device Manager e AXIS Device Manager Extend per proteggere i dispositivi Axis relativamente agli argomenti trattati in . Usare questo *file di configurazione*, che consiste delle stesse impostazioni di configurazione elencate in .

Alcune impostazioni di configurazione potrebbero non essere più disponibili nella versione AXIS OS del proprio dispositivo perché certe funzionalità sono state rimosse nel tempo per incrementare la sicurezza. AXIS Device Manager e AXIS Device Manager Extend rimuoveranno in automatico tali impostazioni dalla configurazione di protezione.

Nota

Dopo aver caricato il file di configurazione, il dispositivo Axis sarà configurato solo su HTTPS e l'interfaccia Web sarà disabilitata. Si può modificare il file di configurazione sulla base delle proprie esigenze, ad esempio con la rimozione o l'aggiunta di parametri.

AXIS OS Hardening Guide
Ver. M48.2
Data: Settembre 2024
Codice art.
© Axis Communications AB, 2022 - 2024