

AXIS OS Hardening Guide

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

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 sicuro dipende dai suoi utenti, dai processi e dalle tecnologie. 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 (percorso Active o LTS) nonché ai dispositivi precedenti che eseguono 4.xx e 5.xx.

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.

Il diagramma dell'architettura di sicurezza di AXIS OS illustra le funzionalità di cybersecurity di AXIS OS ai vari livelli. Fornisce una panoramica completa delle fondamenta di sicurezza, dell'hardware dedicato, del sistema operativo AXIS OS e del livello di applicazione e controllo accessi.

Access control	Access control management Local user device management with password complexity indicator Federated user device management through OpenID Connect (RFC6749, 1.3.1 Authorization Code) providing ADFS-integration that unlocks features such as password complexity enforcement, rotation, automatic account lock-out Multi-factor authentication (MFA), Microsoft AD entitlement functionality		Privacy Use of diagnostics data Minimalistic approach to how much customer-specific data should be stored
Application	Application security TLS-based application security (MQTT, SFTP, NTS, HTTPS, WebRTC) Encrypted video streaming (RTSPS/SRTP, HTTPS), Secure remote syslog		
Operating system	Encryption and data protection OpenSSL 1.1.1 and 3.0 X.509 certificate PKI and cryptography Transport layer security (TLS 1.2/TLS 1.3) SD card encryption (AES-XTS-Plain64 256bit) Encrypted file system (AES-XTS-Plain64 256bit), Signed video	Default security HTTPS enabled by default Brute-Force Delay Protection Host-based Firewall Network time security (NTS) Insecure TLS versions disabled UART/Debug port disabled	Enterprise network security IEEE 802.1X (network access control) IEEE 802.1AR (secure device identity) IEEE 802.1AE (MAC security, MACsec)
	AXIS OS Operating System Common Linux-based operating system with more than 95% industry-standard open-source software components such as OpenSSL, Apache, Curl and others. Active track for feature growth and 5-year long-term support tracks (LTS) for 3rd party integration and backwards-compatibility use cases.		
Silicon assisted security (chip)	Hardware root-of-trust ARM-based system-on-chip (SoC) security Trusted Execution Environment (TEE/OP-TEE) Trusted platform module (TPM 2.0), Secure element		Secure key storage Tamper-protected storage and operation of cryptographic keys such as customer uploaded private keys, video signing keys and the Axis Device ID.
	Security foundation	Axis Security Development Model Axis security development model (ASDM) 3rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)	Compliance Common Criterial EAL FIPS 140 ETSI EN 303 645

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

Autenticazione

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.

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.

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

Autenticazione digest

CSC #3: Protezione dei dati

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 dei 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, detta protezione con ritardo dagli attacchi di forza bruta, è disponibile in AXIS OS 7.30 e versioni successive.

La protezione con ritardo dagli attacchi di forza bruta è abilitata per impostazione predefinita a partire da AXIS OS 11.5. Per esempi di configurazione e raccomandazioni dettagliate, vedere *Protezione con ritardo dagli attacchi di 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

Edge storage

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

CSC #3: Protezione dei dati

A partire da Axis OS 12.0, l'opzione di montaggio noexec è stata aggiunta come opzione predefinita per le condivisioni di rete montate. In questo modo si disabilita l'esecuzione diretta dei file binari dal disco di rete montato. Le schede SD erano già state aggiunte a questa opzione nelle versioni precedenti di AXIS OS.

Inoltre, i dispositivi Axis con AXIS OS 10.10 e versioni successive supportano l'esportazione crittografata delle 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

Protezione della rete

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	Trasporti	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.
UPnP	49152	TCP	Usato da applicazioni di terzi per trovare il dispositivo Axis tramite il protocollo di rilevamento UPnP®. NOTA: Disabilitato per

Protocollo	Porta	Trasporti	Commenti
			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 ulteriori informazioni riguardanti la tecnologia edge-to-edge, consultare il documento tecnico *Tecnologia edge-to-edge*.

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

*** In AXIS OS 12.1 e versioni successive il protocollo Webservice Discovery (WS-Discovery) è disattivato per impostazione predefinita.

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.

HTTPS abilitato

CSC #3: Protezione dei 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. In AXIS OS 10.10 e nelle versioni successive, il certificato autofirmato è stato sostituito dal certificato ID dispositivo sicuro IEEE 802.1AR.

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. In AXIS OS 9.80 e nelle versioni successive, è possibile utilizzare l'API VAPIX con header HTTP personalizzati per configurare header HTTP(S) aggiuntivi.

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.

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

Autenticazione 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 dei 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 di AXIS OS.

Identità dispositivo sicura IEEE 802.1AR

CSC #1: Inventario e controllo delle risorse aziendali

CSC #13: Monitoraggio e difesa rete

I dispositivi Axis con Axis Edge Vault supportano lo standard di rete IEEE 802.1AR, che consente di integrare in modo automatico e sicuro i dispositivi Axis nella rete grazie all'ID dispositivo Axis, un certificato univoco installato sul dispositivo durante la 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.

Interfaccia UART/debug

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

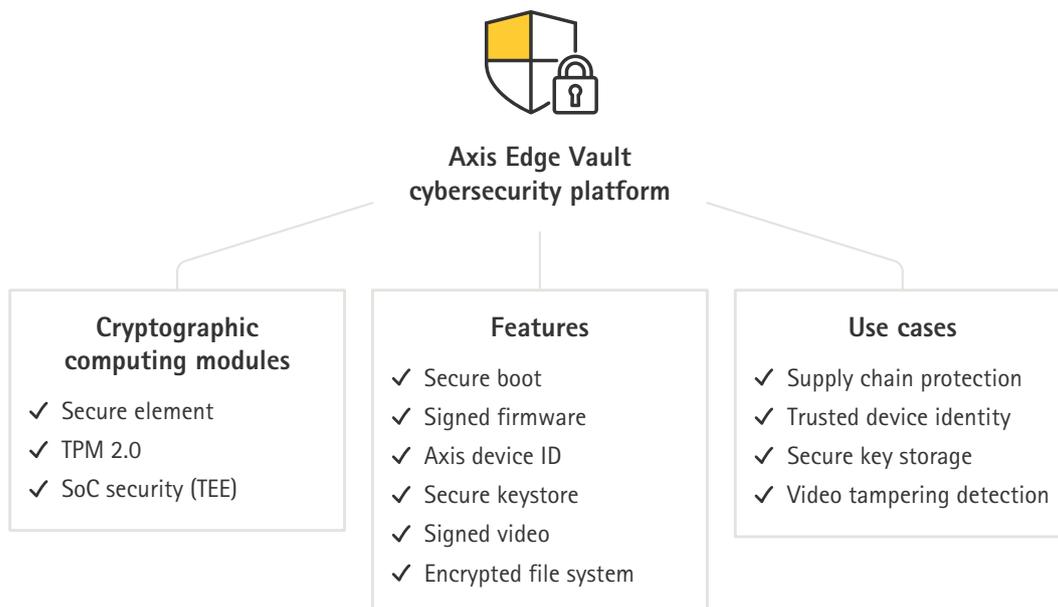
Ogni dispositivo Axis è dotato di una cosiddetta interfaccia fisica UART (Universal Asynchronous Receiver Transmitter), a volte detta "porta di debug" o "console seriale". L'interfaccia stessa è fisicamente accessibile solo attraverso uno smontaggio completo del dispositivo Axis. L'interfaccia UART/debug 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. È basata su solidi moduli di calcolo crittografico (Secure Element e TPM) e sicurezza del SoC (TEE e Secure Boot), combinati con le competenze di Axis nella sicurezza dei dispositivi edge. Axis Edge Vault gode di solide radici di attendibilità stabilite dall'avvio sicuro e dal firmware firmato. Queste funzionalità permettono di avere una catena ininterrotta di software convalidato crittograficamente per la catena di fiducia da cui dipendono tutte le operazioni sicure.

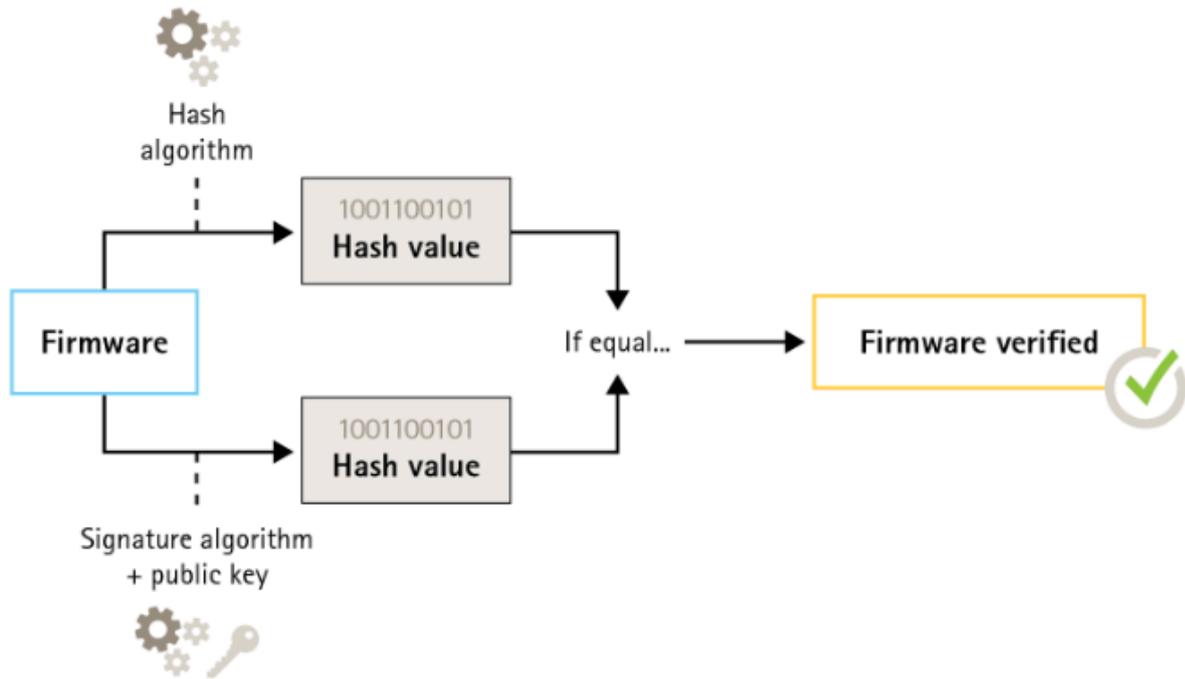
I dispositivi Axis con Axis Edge Vault riducono al minimo l'esposizione dei clienti ai rischi per la cybersecurity, prevenendo l'intercettazione e l'estrazione dannosa di informazioni sensibili. Axis Edge Vault assicura in più che il dispositivo Axis sia un'unità affidabile nella rete del cliente.



Firmware con firma digitale

CSC #2: Inventario e controllo delle risorse software

AXIS OS è firmato digitalmente 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.

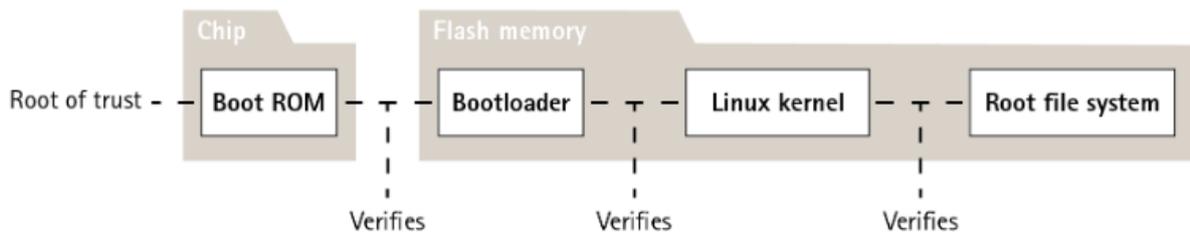


Per ulteriori informazioni, visitare il white paper su *Axis Edge Vault*.

Secure Boot

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 (keystore)

CSC #6: Gestione del controllo degli accessi

il keystore fornisce un'archiviazione delle informazioni crittografiche basata su hardware e protetta dalle manomissioni. 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).



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

File system criptato

CSC #3: Protezione dei 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-Plain64 256bit. 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*.

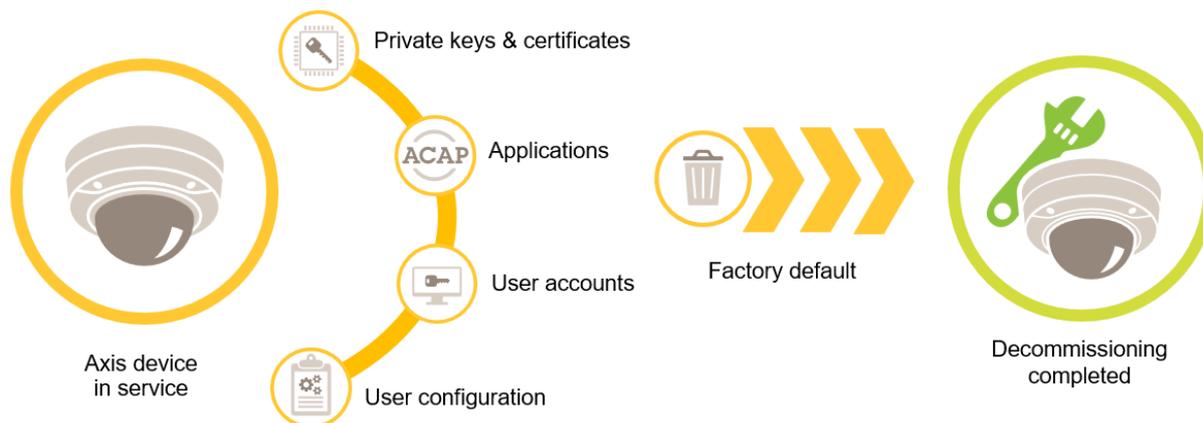
Smaltimento

CSC #3: Protezione dei 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.

Si noti che l'emissione di un comando di ripristino dei valori predefiniti di fabbrica non cancella immediatamente i dati, ma il dispositivo si riavvia e la cancellazione dei dati avviene durante l'avvio del sistema. Non è quindi sufficiente emettere il comando di ripristino dei valori predefiniti di fabbrica, ma è necessario che il dispositivo si riavvii e completi il boot prima di essere spento per garantire che la cancellazione dei dati sia stata 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
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

* La procedura di firmware con firma digitale utilizza certificati personalizzati che consentono agli utenti di caricare AXIS OS e altri componenti.

** Le registrazioni e le immagini memorizzate sull'archivio locale (scheda SD, disco di rete) devono essere eliminate dall'utente separatamente. Per ulteriori informazioni, vedere *Formattazione delle schede SD Axis* nella Knowledge Base di AXIS OS.

*** Tutte le configurazioni create dall'utente, dalla creazione di utenti alle configurazioni di rete, O3C, eventi, immagini, PTZ e sistema.

**** Il dispositivo mantiene le applicazioni preinstallate ma elimina tutte le configurazioni effettuate dall'utente.

***** I dati di produzione (calibrazione, certificati di produzione 802.1AR) e le statistiche di durata includono informazioni non sensibili e non relative all'utente.

Protezione di base

La protezione di base è il livello di protezione minimo raccomandato per i dispositivi Axis. I parametri di protezione di base sono "configurabili in modalità edge". Questo significa che possono essere configurati direttamente sul dispositivo Axis senza ulteriori dipendenze da infrastrutture di rete, sistemi di gestione video o gestione prove (VMS, EMS), dispositivi o applicazioni di terze parti.

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, vedere .

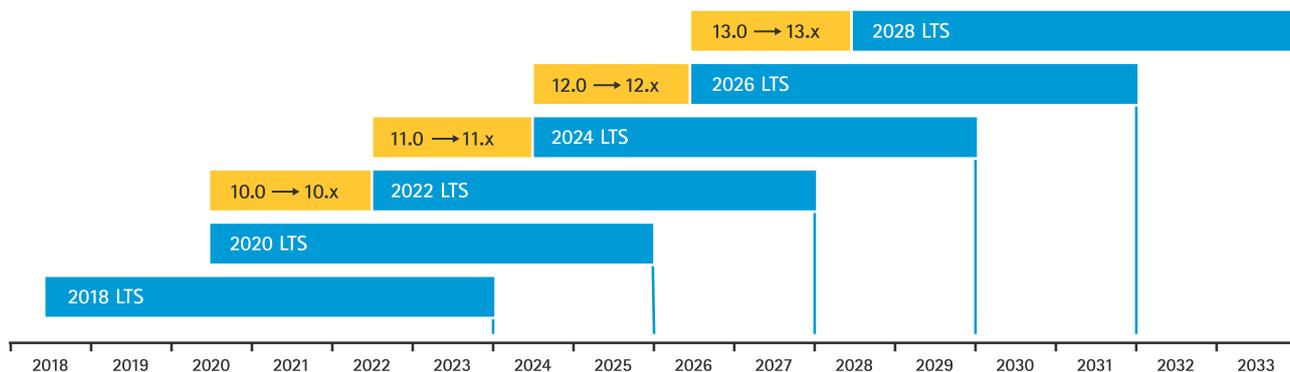
Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Manutenzione > Impostazione predefinita
7.10	Impostazioni > Sistema > Manutenzione > Impostazione predefinita
≥ 10.9	Manutenzione > Impostazione predefinita

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 percorsi per AXIS OS: il percorso Active e il percorso LTS (Long-Term Support). Benché entrambi comprendano le ultime patch per le vulnerabilità critiche, nei percorsi 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. Visita *Firmware* presso axis.com per eseguire il download di AXIS OS per il tuo dispositivo.

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

AXIS OS 2018 LTS - Security Updates Timeline

2018 → 2019 → 2020 → 2021 → 2022

Version	Month	Components
8.40.2	May	OpenSSL
8.40.2.2	July	OpenSSH, OpenSSL, TLSv1.3
8.40.3.1	December	Apache, OpenSSL
8.40.3.2	February	Linux kernel, CURL
8.40.4	July	Apache, CURL, OpenSSL
8.40.4.1	November	Apache
8.40.4.2	April	CURL, OpenSSL
8.40.4.3	October	Apache, CURL, OpenSSH, OpenSSL
8.40.4.4	January	Apache, CURL, OpenSSL
8.40.4.5	May	Apache, OpenSSL
8.40.4.6	July	Apache, CURL, OpenSSL
8.40.4.7	October	CURL, OpenSSL
8.40.4.8	December	CURL, OpenSSL

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

Creare account dedicati

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

CSC #5: Gestione degli account

I dispositivi Axis possono avere due tipi di account: un account amministratore e un account utente client. L'account amministratore è l'account principale per la gestione del dispositivo. È fondamentale riservarlo solo alle attività di amministrazione. Durante la configurazione del dispositivo, è necessario creare un nome utente e una password per l'account amministratore.

Oltre all'account amministratore, creare un utente client con privilegi limitati per le operazioni quotidiane. Ciò consente di gestire il dispositivo in modo sicuro, riducendo il rischio di compromettere la password dell'amministratore. Si consiglia di utilizzare l'account utente client per le attività che non richiedono privilegi di amministrazione completi.

Quando si creano le password per uno dei due account, si consiglia di applicare linee guida come le raccomandazioni NIST o BSI sulle password, che richiedono che le nuove password siano sufficientemente lunghe e complesse. I dispositivi Axis supportano password fino a 64 caratteri. Le password al di sotto di 8 caratteri sono considerate deboli.

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

Disabilitare l'accesso all'interfaccia Web

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

CSC #5: Gestione degli 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.

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

Configurare impostazioni di rete, data e ora

CSC #4: CSC #8: Gestione dei registri di audit

CSC #12: Gestione dell'infrastruttura di rete

È importante configurare correttamente le impostazioni di rete, data e ora per mantenere il dispositivo Axis funzionale e sicuro. Queste impostazioni influiscono su vari comportamenti del dispositivo, come la comunicazione di rete, l'accesso e la convalida dei certificati.

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. Rivedere la topologia di rete ogni volta che si aggiungono nuovi componenti. Si consiglia di utilizzare la configurazione di indirizzi IP statici per garantire la raggiungibilità della rete e ridurre al minimo la dipendenza da server di rete che potrebbero essere vulnerabili agli attacchi, come i server DHCP.

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

Un'accurata sincronizzazione dell'ora è essenziale per mantenere gli accessi al sistema, convalidare i certificati digitali e abilitare servizi come HTTPS, IEEE e 802.1x. Si consiglia di sincronizzare l'orologio del dispositivo con i server NTP (Network Time Protocol) o NTS (Network Time Security). In AXIS OS 11.1 è stata aggiunta NTS (Network Time Security), una variante crittografata e sicura di Network Time Protocol (NTP). Si consiglia di configurare più server orari per ottenere una maggiore precisione e tenere conto di potenziali guasti. Se non è possibile ospitare server orari locali, considerare l'utilizzo di server NTP o NTS pubblici. 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 dei dati

Scheda SD

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

Disco di rete (NAS)

Se si usa un NAS (Network Attached Storage) come dispositivo di registrazione, consigliamo di tenerlo in un'area protetta con accesso limitato e di abilitare la crittografia del 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

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 individuazione in 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
≥ 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.

Le versioni TLS obsolete sono state rimosse da AXIS OS 12.0 e non sono disponibili nelle versioni successive.

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 interfonni 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 utilizzato solo per la risoluzione di problemi e il debug. L'accesso FTP è stato rimosso da AXIS OS 11.1 e non è disponibile 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. Si consiglia di disabilitare l'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. È supportato dai dispositivi Axis con versioni precedenti ad AXIS OS 5.50. Si consiglia di disabilitare l'accesso a Telnet.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 5.50	Per trovare istruzioni, consultare <i>Accesso ai dispositivi</i> 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

USB

A partire da AXIS OS 12.1, AXIS D1110 è dotato dell'opzione per disabilitare la porta USB. Lasciare incustodite le porte USB 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
≥ 12.1	Sistema > > Accessori > Configurazione USB

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

Introdotta in AXIS OS 11.9, il firewall host-based è una funzione di sicurezza che consente di creare regole che regolano il traffico in ingresso in base all'indirizzo IP e/o ai numeri di porta TCP/UDP. Questo aiuta a prevenire accessi non autorizzati al dispositivo o ai suoi servizi.

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

Filtro indirizzi IP

I dispositivi con AXIS OS 11.8 e versioni precedenti utilizzano il filtro indirizzi IP per impedire l'accesso da client non autorizzati. Si consiglia di configurare il dispositivo in modo da consentire gli indirizzi IP degli host di rete autorizzati o rifiutare i non autorizzati.

Se si sceglie di consentire gli indirizzi IP, aggiungere sempre al proprio elenco tutti i client autorizzati, compresi i server VMS e i client amministrativi.

Versione di AXIS OS	Percorso configurazione Interfaccia Web
< 7.10	Configurazione > Opzioni di sistema > Sicurezza > Filtro indirizzi IP
7.10	Impostazioni > Sistema > TCP/IP > Filtro indirizzi IP
10.9 – 11.8	Impostazioni > Sicurezza > Filtro indirizzi IP

Nota

È possibile abilitare registri più dettagliati dei tentativi di accesso alla rete per aiutare l'utente a identificare i tentativi di accesso indesiderati da parte di altri host della rete. A tale scopo, andare a **System > Plain config > Network** e Network Filter Log.

HTTPS

CSC #3: Protezione dei dati

HTTP e HTTPS sono abilitati per impostazione predefinita sui dispositivi Axis a partire da AXIS OS 7.20. Mentre l'accesso HTTP non è protetto e non prevede crittografia, HTTPS cripta 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 di accesso

CSC #1: Inventario e controllo delle risorse aziendali

CSC #8: Gestione dei registri di audit

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*
- *Interruttore sportello A AXIS*

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 e alla rete

CSC #12: Gestione dell'infrastruttura di rete

Si consiglia di evitare di esporre qualsiasi dispositivo Axis come server web pubblico o di consentire in qualsiasi altro modo l'accesso alla rete a client sconosciuti. Per le piccole aziende e i privati che non utilizzano software di gestione video (VMS) o che hanno bisogno di accedere ai video da remoto, AXIS Camera Station Edge è una buona opzione.

AXIS Camera Station Edge è disponibile gratuitamente su Windows, iOS e Android e offre un modo semplice per accedere ai video in modo sicuro senza esporre il dispositivo a Internet. Per maggiori informazioni, vedere axis.com/products/axis-camera-station-edge.

Nota

Se la vostra azienda utilizza un VMS, consultate il fornitore del VMS per conoscere le prassi ottimali di accesso remoto ai video.

L'isolamento dei dispositivi di rete e delle relative infrastrutture e applicazioni riduce il rischio di esposizione della rete.

Consigliamo di isolare i dispositivi Axis, l'infrastruttura e le applicazioni correlate su una rete locale separata dalla 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 utilizzando più meccanismi di sicurezza di rete. Questi possono includere la segmentazione VLAN, capacità di routing limitate, VPN per il controllo degli accessi da sito a sito o WAN, firewall di livello 2/3 della rete e liste di controllo degli accessi (ACL).

Per ampliare la protezione di base, applicare tecniche avanzate di ispezione della rete, come l'ispezione approfondita dei pacchetti e il rilevamento intrusioni. Questo migliora la protezione dalle minacce all'interno della rete. Si noti che la protezione estesa della rete richiede in genere dispositivi software e/o hardware specializzati.

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 di avviare la scansione, assicurarsi che i dispositivi Axis siano stati aggiornati all'ultima versione disponibile di AXIS OS, sul percorso LTS o Active.

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.

Public key infrastructure (PKI) attendibile

CSC #3: Protezione dei 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 una catena di fiducia convalidata aiuta a rimuovere gli avvisi di certificato del browser quando ci si connette tramite HTTPS. Un certificato firmato dalla CA garantisce inoltre l'autenticazione del dispositivo Axis quando si implementa una soluzione di controllo degli accessi alla 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.

Remote syslog (Syslog remoto)

CSC #8: Gestione dei registri di audit

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 <i>Syslog</i> nel portale AXIS OS
7.10	Impostazioni > Sistema > TCP/IP
≥ 10.9	Sistema > Registri

Streaming video sicuro (SRTP/RTSPS)

CSC #3: Protezione dei dati

A partire da AXIS OS 7.40, i dispositivi Axis supportano lo streaming video sicuro su RTP, noto anche come SRTP/RTSPS. SRTP/RTSPS utilizza un metodo di trasporto sicuro e crittografato end-to-end per garantire che solo 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 con firma

CSC #3: Protezione dei 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

Nota

Gli errori di configurazione comuni elencati di seguito aumentano potenzialmente la superficie di attacco del dispositivo Axis e ne riducono i livelli di difesa in termini di cybersecurity, con conseguente aumento del rischio di sfruttamento, uso improprio o funzionamento non sicuro del dispositivo.

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, vedere .

Password comune

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

CSC #5: Gestione degli 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 degli 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, vedere .

Comunicazione sicura disabilitata

CSC #3: Protezione dei 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, vedere . Per ottenere raccomandazioni sulla configurazione, consultare .

Versione di AXIS OS obsoleta

CSC #2: Inventario e controllo delle risorse software

Si consiglia fortemente di utilizzare il dispositivo Axis con l'ultima versione di AXIS OS disponibile, sul percorso LTS o Active. Entrambi i percorsi mettono a disposizione le ultime patch di sicurezza e le correzioni di bug. Per ulteriori informazioni, vedere .

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.

Scopo	Chiamata API VAPIX
<i>Disabilitazione di POE nelle porte di rete non usate*</i>	<code>http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enablId=no</code>
<i>Disabilitazione del traffico di rete nelle porte di rete non usate**</i>	<code>http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }</code>
<i>Disabilitare protocollo di rilevamento Bonjour</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no</code>
<i>Disabilitare protocollo di rilevamento UPnP®</i>	<code>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</code>
<i>Disabilitare protocollo di rilevamento WebService</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no</code>
<i>Disabilitare la connessione a cloud con un clic (O3C)</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no</code>
<i>Disabilitare l'accesso di manutenzione SSH del dispositivo</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no</code>
<i>Disabilitare l'accesso di manutenzione FTP del dispositivo</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no</code>
<i>Disabilitare la configurazione dell'indirizzo IP ARP-Ping</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no</code>
<i>Disabilitare la configurazione dell'indirizzo IP Zero-Conf</i>	<code>http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no</code>
<i>Abilitare solo HTTPS</i>	<code>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</code>
<i>Abilitare solo TLS 1.2 e TLS 1.3</i>	<code>https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no</code>

Scopo	Chiamata API VAPIX
<i>Configurazione crittografia sicura TLS 1.2</i>	<pre>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</pre>
<i>Abilitare protezione contro attacchi a forza bruta***</i>	<pre>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</pre>
<i>Disabilitare l'ambiente dell'editor di script</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no</pre>
<i>Abilitare una migliore registrazione degli accessi utente</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog= On</pre>
<i>Abilitare protezione da replay-attack ONVIF</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update&WebService. UsernameToken. ReplayAttackProtection=yes</pre>
<i>Disabilitare l'accesso all'interfaccia Web del dispositivo</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update&System. WebInterfaceDisabled=yes</pre>
<i>Disabilitare intestazione server HTTP/OpenSSL</i>	<pre>https://ip-address/axis-cgi/param.cgi?action=update&System. HTTPServerTokens=no</pre>
<i>Disabilitare il visualizzatore anonimo e l'accesso PTZ</i>	<pre>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</pre>

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

* Sostituire "X" con il numero di porta effettivo in "port=X". Esempi: "port=1" disabilita la porta 1 e "port=2" disabilita la porta 2.

** Sostituire "1" con il numero di porta effettivo in "eth1.1". Esempi: "eth1.1" disabilita la porta 1 e "eth1.2" disabilita la porta 2.

*** Dopo 20 tentativi di accesso falliti nell'arco di 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.

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.

