

AXIS OS Hardening Guide

AXIS OS Hardening Guide

[AXIS OS 入口網站](#) | [AXIS OS 版本資訊](#) | [AXIS OS 知識庫](#) | [AXIS OS 安全性公告](#)

AXIS OS Hardening Guide

簡介

簡介



AXIS OS Hardening Guide for Axis edge devices

Axis Communications 致力於在設備的設計、開發和測試中應用網路安全最佳實務，以盡可能地降低可能被駭客攻擊利用的缺陷之風險。不過，整個供應商供應鏈和使用者組織必須保護網路、其設備及其支援的服務。安全的環境取決於其使用者、流程和技術。本指南的目的是協助您確保網路、設備和服務安全。

Axis 設備面臨的最明顯的威脅是實體破壞、人為破壞和竄改。為了保護產品免受這些威脅，務必選取防人為破壞型號或外殼、依照建議的方式安裝並保護纜線。

Axis 設備屬於網路端點，就像是電腦和行動電話。許多都設有網頁介面，但此介面卻會暴露出所連線系統的漏洞。在本指南中，我們將說明如何降低這些風險。

本指南為所有參與 Axis 影像解決方案建置安裝的人員提供技術建議。其中包括建議的基準設定和強化指南 (已將不斷演進的威脅態勢納入考量)。您可能需要查閱產品的使用手冊以了解如何進行特定設定。請注意，Axis 設備已進行 AXIS OS 7.10 和 10.9 的網頁介面更新，變更組態路徑。

網頁介面組態

本指南說明如何進行 Axis 設備網頁介面內的設備設定。組態路徑根據設備上安裝的 AXIS 作業系統版本而有所不同：

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 安全性 > IEEE 802.1X。
≥ 7.10	設定 > 系統 > 安全性
≥ 10.9	系統 > 安全性

範圍

本指南適用於執行 AXIS OS (LTS 或主動式軌道) 的所有 AXIS OS 產品，以及執行 4.xx 和 5.xx 的舊版產品。


















The operating system for Axis edge devices.

AXIS 作業系統安全性架構

AXIS OS 安全性架構圖概述跨各層的 AXIS OS 網路安全功能，為安全性基礎、矽輔助安全性、AXIS OS 作業系統以及應用程式和門禁管制層提供一個全方位的檢視。

AXIS OS Hardening Guide

簡介

 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 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	1 0 1 0 0 1 0 1 1 0 1 0	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 3 rd 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	Secure software development Axis security development model (ASDM) 3 rd party penetration tests Bug bounty program with Bugcrowd Software Bill of Material (SBOM)		Certification Common criteria CC EAL4+ / EAL6+ FIPS 140-2 ETSI EN 303 645		Trusted device identity Axis Edge Vault cybersecurity platform Secure boot with Signed Firmware (code-signing) Axis Device ID (IEEE 802.1AR)	

按一下滑鼠右鍵並在新分頁中開啟影像以獲得更好的視覺體驗。

安全通知

我們建議您訂閱 [Axis 安全通知服務](#) 接收有關 Axis 產品、解決方案和服務中新發現的漏洞的資訊，以及如何確保 Axis 設備安全的資訊。

CIS 保護層級

我們遵循在網際網路安全中心 (CIS) 控制第 8 版所概述的方法來構建我們的網路安全框架建議。CIS 控制以前稱為 SANS Top 20 關鍵安全控制，提供 18 類關鍵安全控制 (CSC)，聚焦於解決組織中最常見的網路安全風險類別。

本指南透過為每個強化主題新增 CSC 編號 (CSC#) 來引用關鍵安全控制。如需 CSC 類別的詳細資訊，請參閱 [cisecurity.org](https://www.cisecurity.org) 中的 18 類 [CIS 關鍵安全控制](#)。

AXIS OS Hardening Guide

預設保護

預設保護

Axis 設備已預設保護設定。有一些安全控制不需要您設定。這些控制提供設備基本的防護，為更廣泛的強化奠定基礎。

預設為停用

CSC #4：企業資產和軟體的安全設定

在設定管理員密碼之前，Axis 設備不會運作。

若要了解如何設定設備存取，請參閱 AXIS OS 知識庫中的 [設備存取](#)。

憑證存取

設定管理員密碼後，只能透過使用有效的使用者名稱/密碼憑證進行身分驗證，以存取管理員功能和/或影像串流。我們不建議您使用啟用未經授權存取的功能，例如匿名觀看與維持多點傳送模式。

網路通訊協定

CSC #4：企業資產和軟體的安全設定

預設情況下，Axis 設備中僅啟用最少數量的網路通訊協定和服務。在此表中您可以看到其內容。

通訊協定	連接埠	傳輸	註解
HTTP	80	TCP	一般 HTTP 流量，例如網頁介面存取、VAPIX 和 ONVIF API 介面或 edge-to-edge 通訊*
HTTPS	443	TCP	一般 HTTPS 流量，例如網頁介面存取、VAPIX 和 ONVIF API 介面或 edge-to-edge 通訊*
RTSP	554	UDP	由 Axis 設備用於影像/音訊串流
RTP	臨時連接埠範圍*	UDP	由 Axis 設備用於影像/音訊串流
UPnP	49152	TCP	由第三方應用程式用於透過 UPnP 探索通訊協定探索 Axis 設備
Bonjour	5353	UDP	由第三方應用程式用於透過 mDNS 探索通訊協定 (Bonjour) 探索 Axis 設備
SSDP	1900	UDP	由第 3 方應用程式用於透過 SSDP (UPnP) 探索 Axis 設備
WS-Discovery	3702	UDP	由第三方應用程式用於透過 WS-Discovery 通訊協定 (ONVIF) 探索 Axis 設備

* 如需 edge-to-edge 端對端的詳細資訊，請參閱 [Edge-to-edge 端對端技術](#)。

AXIS OS Hardening Guide

預設保護

****根據 RFC 6056 自動在連接埠號碼內配置。如需詳細資訊，請參閱 Wikipedia 文章臨時埠。**

我們建議您盡可能停用未使用的網路通訊協定和服務。有關預設使用或可以根據設定啟用的服務的完整清單，請參閱 AXIS OS 知識庫中的 *常用網路連接埠*。

例如，您需要手動啟用 Axis 影像監控裝置 (如網路攝影機) 中的音訊輸入/輸出和麥克風功能，同時在 Axis 對講機和網路喇叭中，音訊輸入/輸出和麥克風功能为主要功能，因此預設為啟用。

UART/偵錯介面

CSC #4：企業資產和軟體的安全設定

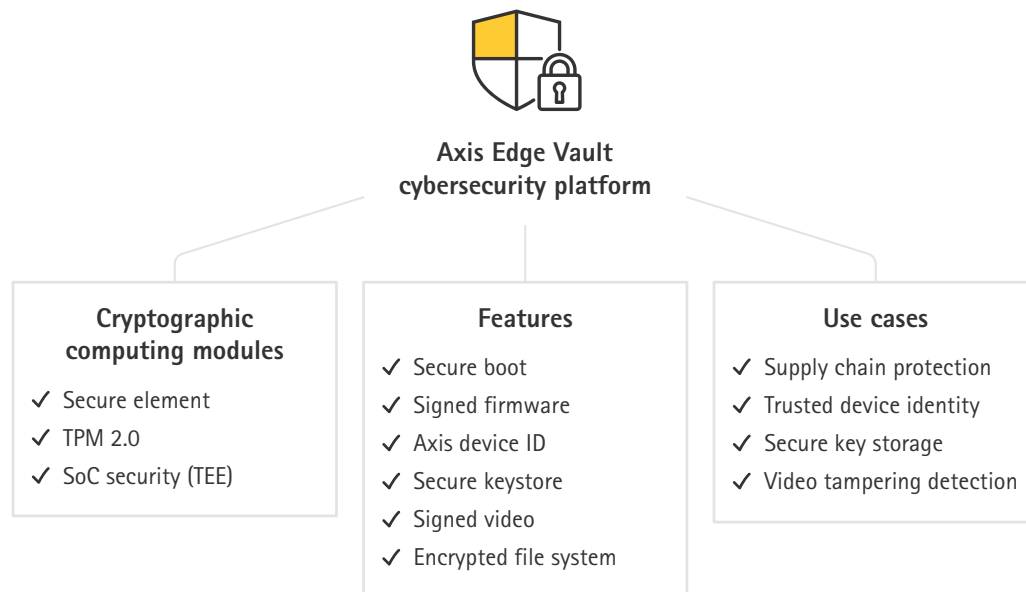
每個 Axis 設備都包含一個所謂的實體 UART (通用異步接收器發送器) 介面，有時稱為「偵錯連接埠」或「序列主控台」。介面本身僅可透過對 Axis 設備進行大量拆卸的方式，進行實體存取。UART/偵錯介面僅用於 Axis 內部研發工程專案期間的產品開發和偵錯目的。

在搭載 AXIS OS 10.10 及更早版本的 Axis 設備中，預設啟用 UART/偵錯介面，但它需要經過身分驗證的存取，並且在未經身分驗證時不會暴露任何敏感資訊。自 AXIS OS 10.11 起，UART/偵錯介面預設為停用。啟用該介面的唯一方法是透過 Axis 提供的設備唯一自訂憑證進行解鎖。

Axis Edge Vault

Axis Edge Vault 提供保護 Axis 設備安全的硬體式網路安全平台。建立在加密計算模組 (安全元件和 TPM) 和 SoC 安全性 (TEE 和安全開機) 的堅實基礎上，並結合邊緣設備安全性的專業技術。Axis Edge Vault 以透過安全啟動和已簽署韌體建立的強大信任 root 為基礎。這些功能為所有安全操作所依賴的信任鏈提供了不間斷的加密驗證軟體鏈。

配備 Axis Edge Vault 的 Axis 設備可防止竊聽和惡意擷取敏感資訊，進而盡可能地減少客戶面臨的網路安全風險。Axis Edge Vault 也確保 Axis 設備成為客戶網路中值得信賴的可靠單元。



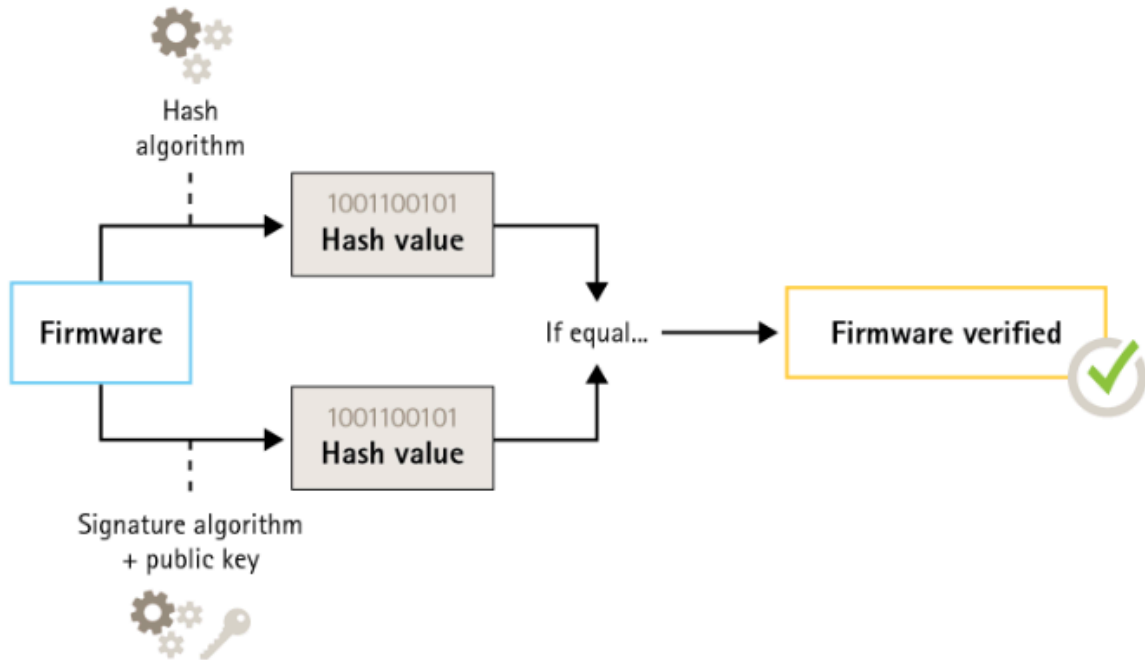
已簽署的韌體

CSC #2：軟體資產的盤點和控制

AXIS OS 自版本 9.20.1 起簽署。每次升級設備上的 AXIS 作業系統版本時，設備將會透過加密簽名驗證來檢查更新檔案的完整性，並拒絕任何遭到篡改的檔案。這會防止攻擊者引誘使用者安裝受感染的檔案。

AXIS OS Hardening Guide

預設保護

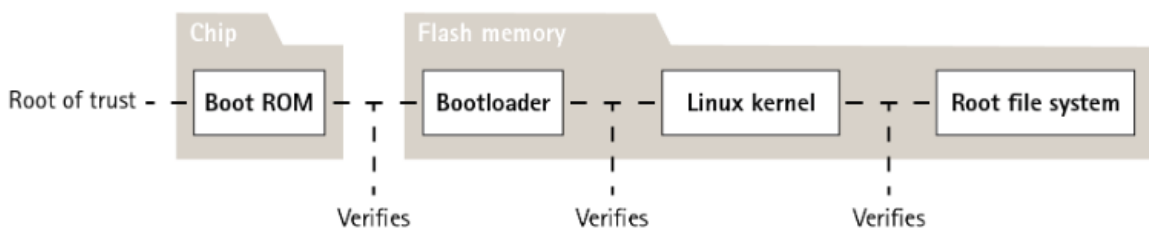


如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。

安全開機

CSC #2：軟體資產的盤點和控制

大多數 Axis 設備都具有安全開機順序，以保護設備的完整性。安全開機可防止您部署遭篡改的 Axis 設備。



如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。

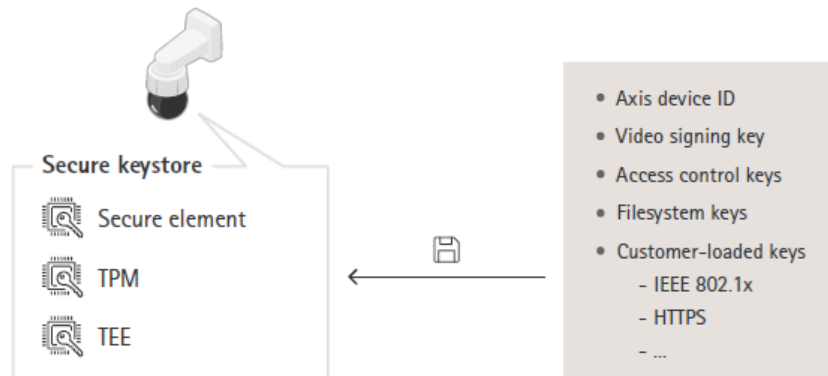
安全金鑰儲存區

CSC #6：門禁管制管理

安全金鑰庫提供基於硬體、防竄改的加密資訊儲存區。它可保護 Axis 設備 ID 以及客戶上傳的加密資訊，同時在發生安全漏洞時防止未經授權的存取和惡意擷取。視安全性的需求而定，Axis 設備可能使用一或多個此類模組，例如 TPM 2.0 (信賴平台模組)、安全元件，和/或使用 TEE (可信賴執行環境)。

AXIS OS Hardening Guide

預設保護



如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。

加密的檔案系統

CSC #3：資料保護

惡意對手可能會嘗試透過拆卸快閃記憶體並透過快閃讀卡機設備存取，從檔案系統中擷取資訊。但是，如果有人獲得 Axis 設備的實體存取權限和/或竊取該 Axis 設備，Axis 設備能夠保護檔案系統免受惡意資訊洩露和設定竄改。當 Axis 設備關閉時，檔案系統上的資訊採用 AES-XTS-Plain64 256 位元加密。在安全啟動過程中，讀寫檔案系統被解密，並且可以被 Axis 設備安裝和使用。

如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。

已啟用 HTTPS

CSC #3：資料保護

自 AXIS OS 7.20 起，預設情況下使用自我簽署的憑證啟用 HTTPS，並附上自我簽署的憑證，以安全的方式設定設備密碼。自 AXIS OS 10.10 起，自我簽署的憑證已被 IEEE 802.1AR 安全設備 ID 憑證取代。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 安全性 > HTTPS
≥ 7.10	設定 > 系統 > 安全性 > HTTP 和 HTTPS
≥ 10.9	系統 > 網路 > HTTP 和 HTTPS

預設 HTTP 標頭

預設情況下，AXIS 作業系統具有最常見的安全相關 HTTP 標頭，可提升出廠預設設定狀態下的基本網路安全性。自 AXIS OS 9.80 起，您可以使用自訂 HTTP 標頭 VAPIX API 來設定其他 HTTP 標頭。

如需 HTTP 標頭 VAPIX API 的詳細資訊，請參閱 *VAPIX Library*。

若要閱讀更多關於預設 HTTP 標頭的資訊，請參閱 AXIS OS 知識庫中的 *預設 HTTP 標頭*。

摘要式驗證

CSC #3：資料保護

存取設備的用戶端將使用密碼進行身分驗證，該密碼在透過網路傳送時應加密。因此，我們建議僅使用摘要式身分驗證，而不是基本或基本和摘要式身分驗證。這能降低網路偵測器獲取密碼的風險。

AXIS OS Hardening Guide

預設保護

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > 網路 > 網路 HTTP 身分驗證策略
≥ 7.10	設定 > 系統 > 一般設定 > 網路 > 網路 HTTP 身分驗證策略
≥ 10.9	系統 > 一般設定 > 網路 > 網路 HTTP 身分驗證策略

ONVIF 重播攻擊防護

CSC #3 : 資料保護

重播攻擊防護是 Axis 設備中預設啟用的一項標準安全功能。其目的為透過新增額外的安全標頭 (其中包括 UsernameToken、有效時間戳記、隨機數和密碼摘要) 來確保基於 ONVIF 的使用者身分驗證得到足夠的安全性。密碼摘要是根據系統中已儲存的密碼、隨機數和時間戳計算得出的。密碼摘要的目的是驗證使用者並避免重播攻擊，因此摘要會被緩存。我們建議您確保啟用此設定。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > 系統 > 啟用重播攻擊保護
≥ 7.10	設定 > 系統 > 一般設定 > WebService > 啟用重播攻擊保護
≥ 10.9	系統 > 一般設定 > WebService > 啟用重播攻擊保護

防止暴力破解攻擊

CSC #4 : 企業資產和軟體的安全設定

CSC #13 : 網路監控與防禦

Axis 設備具有預防機制，可識別和阻止來自網路的暴力攻擊，例如猜測密碼。此功能稱為**暴力破解延遲保護**，從 AXIS OS 7.30 及更新版本起可用。

自 AXIS OS 11.5 起，已預設啟用暴力破解延遲保護。詳細的設定範例和建議，請參閱 AXIS OS 知識庫中的**暴力破解延遲保護**。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	設定 > 系統 > 一般設定 > 系統 > PreventDosAttack
≥ 10.9	系統 > 安全性 > 防止暴力破解攻擊

退役

CSC #3 : 資料保護

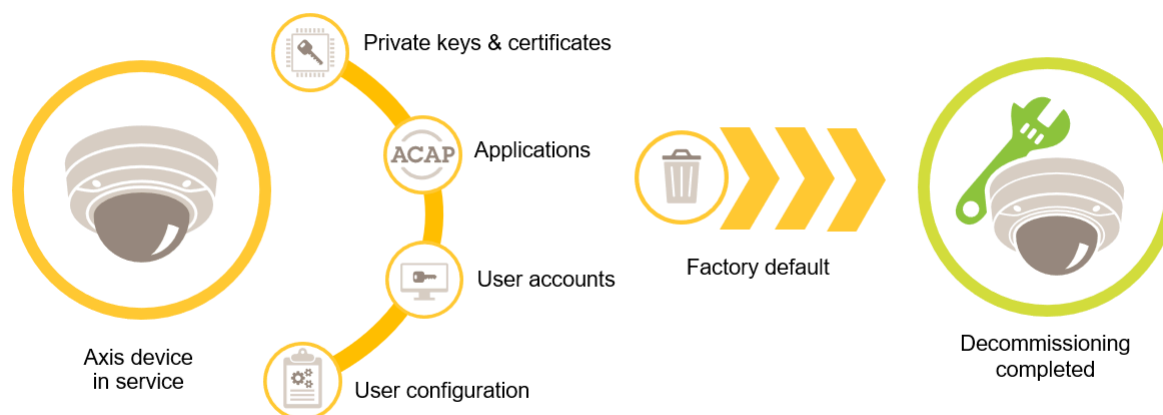
Axis 設備使用揮發性和非揮發性記憶體，雖然切斷設備的電源時都會清除揮發性記憶體，但儲存在非揮發性記憶體中的資訊仍然存在，並在啟動時再次可用。我們避免簡單移除資料指標以使儲存資料對檔案系統不可見的常見做法，而這正是需要重設為出廠預設值的原因。NAND 快閃記憶體使用 UBI 功能「移除磁碟區」，而 eMMC 快閃記憶體也使用等效功能，表示不再使用儲存區塊。然後儲存控制器將相應地擦除這些儲存區塊。

將 Axis 設備除役時，建議您將設備重設回出廠預設設定，這樣會清除儲存在設備非揮發性記憶體中的任何資料。

請注意，發布出廠預設值命令不會立即清除資料，而是設備會重新啟動，並在系統啟動時進行資料清除。因此，僅發布出廠預設值命令是不夠的，還必須允許設備在關閉前重新啟動並完成開機，以確保資料清除已完成。

AXIS OS Hardening Guide

預設保護



AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 維護 > 預設設定
≥ 7.10	設定 > 系統 > 維護 > 預設設定
≥ 10.9	維護 > 預設設定

此表包含有關非揮發性記憶體中儲存的資料的更多資訊。

資訊和資料	出廠預設設定後已刪除
VAPIX 和 ONVIF 使用者名稱和密碼	是
憑證和私鑰	是
自我簽署的憑證	是
TPM 和 Axis Edge Vault 儲存的資訊	是
WLAN 設定和使用者/密碼	是
自訂憑證*	否
SD 卡加密金鑰	是
SD 卡資料**	否
網路共享設定和使用者/密碼	是
網路共享資料*	否
使用者設定***	是
已上傳的應用程式 (ACAP)****	是
生產資料和壽命統計*****	否
已上傳的圖形和浮水印	是
RTC 時鐘資料	是

AXIS OS Hardening Guide

預設保護

* 已簽署韌體流程使用可讓使用者上傳 Axis OS 等等的自訂憑證。

** 儲存在邊緣存儲 (SD 卡、網路共享) 上的錄像和影像必須由使用者另行刪除。如需詳細資訊，請參閱 AXIS OS 知識庫中的格式化 Axis SD 卡。

*** 所有使用者進行的設定，從建立帳戶到網路、O3C、事件、影像、PTZ 和系統設定。

**** 設備雖然會保留任何預先安裝的應用程式，但會刪除所有使用者對其所進行的任何設定。

***** 生產資料 (校準、802.1AR 生產憑證) 以及生命週期統計包括非敏感和非使用者相關資訊。

AXIS OS Hardening Guide

基本強化

基本強化

基本強化是建議 Axis 設備的最低保護層級。基本強化主題是「可在邊緣設定」。這表示它們可以在 Axis 設備中設定，而無須進一步仰賴第三方網路基礎架構、影像或證據管理系統 (VMS、EMS)、設備或應用程式。

出廠預設設定

CSC #4：企業資產和軟體的安全設定

設定您的設備前，請確保其處於出廠預設設定狀態。您需要從使用者資料清除或除役時，也應將設備重設回出廠預設設定。如需詳細資訊，請參閱。

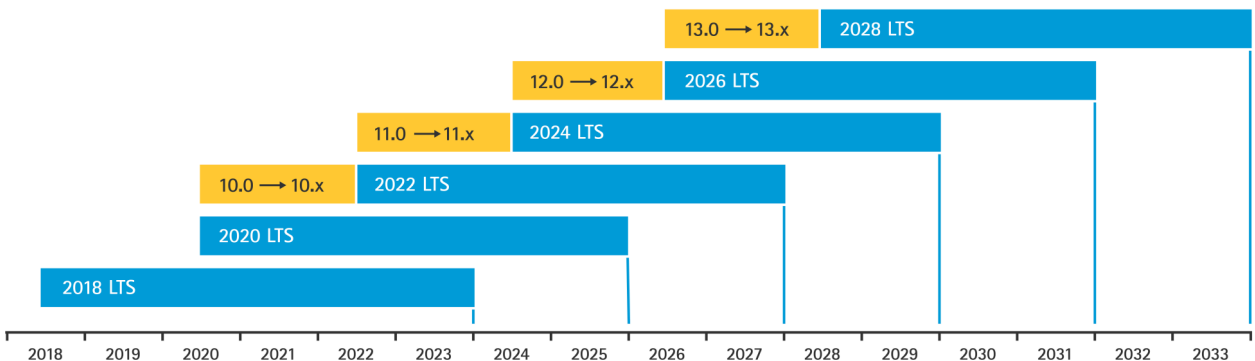
AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 維護 > 預設設定
≥ 7.10	設定 > 系統 > 維護 > 預設設定
≥ 10.9	維護 > 預設設定

升級到最新的 AXIS OS

CSC #2：軟體資產的盤點和控制

修補軟體是網路安全的一個重要層面。攻擊者通常會嘗試利用眾所周知的漏洞，如果他們獲得對未修補服務的網路存取權限，他們可能會成功攻擊。確保您務必使用最新的 AXIS OS，因為它可能包含針對已知漏洞的安全修補程式。特定的版本須知可能會明確提及關鍵的安全修復，但並非所有一般修復。

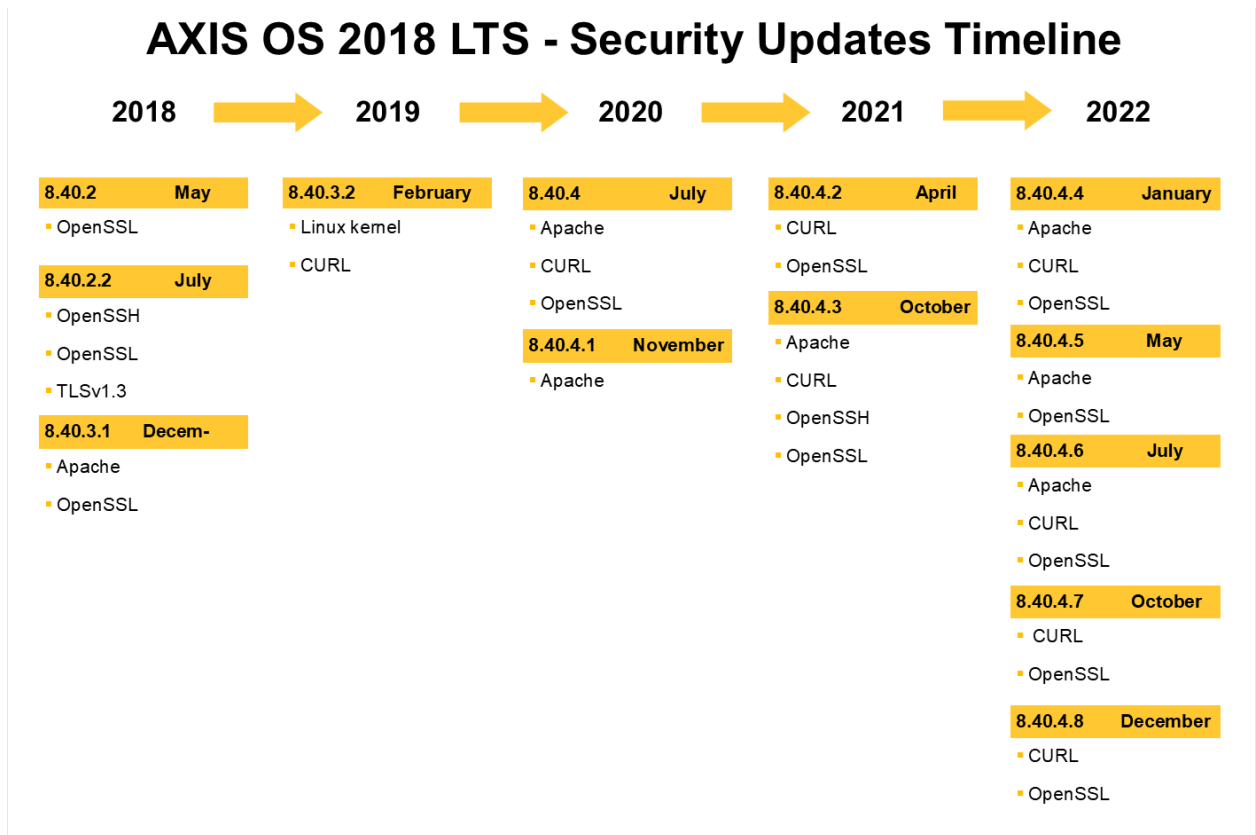
Axis 維護兩種類型的 AXIS OS 軌道：主動式軌道和長期支援 (LTS) 軌道。雖然這兩種類型都包含最新的關鍵漏洞修補程式，但 LTS 軌道不包含新功能，以盡可能地降低相容性問題的風險。如需詳細資訊，請參閱 AXIS OS 資訊中的 *AXIS OS 生命週期*。



Axis 提供了對即將發表的版本的預測，其中包括了重要的新功能、錯誤修復和安全修補程式資訊。若閱讀更多資訊，請參閱 AXIS OS 資訊中 *即將發表的版本*。請造訪 axis.com 網站中的 *韌體*，以下載您設備的 AXIS OS。

此圖表說明了確保 Axis 設備保持在最新狀態的重要性。

基本強化



AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 維護 > 升級伺服器
≥ 7.10	設定 > 系統 > 維護 > 韌體升級
≥ 10.9	維護 > 韌體升級

設定設備 root 密碼

CSC #4 : 企業資產和軟體的安全設定

CSC #5 : 帳戶管理

設備 root 帳戶是主要的設備管理帳戶。使用 root 帳戶前，您需要設定設備密碼。確保使用高強度密碼並將 root 帳戶的使用僅限於管理任務。我們不建議在日常生產中使用 root 帳戶。

操作 Axis 設備時，使用相同的密碼可以簡化管理，但卻會擴大遭到入侵和資料外洩的漏洞。對每個 Axis 設備使用唯一的密碼可提供較高的安全性，但會增加設備管理的複雜性。我們建議您定期變更設備上的密碼。

我們建議您執行新密碼必須夠長、夠複雜的準則，例如 *NIST 密碼建議*。Axis 設備支援最多 64 個字元的密碼。密碼少於 8 個字元一般視為弱強度。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 基本設定 > 使用者
≥ 7.10	設定 > 系統 > 使用者

AXIS OS Hardening Guide

基本強化

AXIS 作業系統版本	網頁介面設定路徑
≥ 10.9	系統 > 使用者
≥ 11.6	系統 > 帳戶

建立專用帳戶

CSC #4 : 企業資產和軟體的安全設定

CSC #5 : 帳戶管理

預設 root 帳戶具有完全權限，應保留用於管理任務。我們建議您建立一個具有有限權限的用戶端使用者帳戶用於日常操作。這降低了設備管理員密碼洩露的風險。

如需詳細資訊，請參閱 *影像監控系統中的身分和存取管理白皮書*。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 基本設定 > 使用者
≥ 7.10	設定 > 系統 > 使用者
≥ 10.9	系統 > 使用者
≥ 11.6	系統 > 帳戶

限制網頁介面存取

CSC #5 : 帳戶管理

Axis 設備有一個網頁伺服器，允許使用者透過標準網頁瀏覽器存取設備。網頁介面用於設定、維護和故障排除。它不適合用於日常操作，例如，作為用戶端觀看影片。

在日常操作期間，唯一允許與 Axis 設備互動的用戶端是影像管理系統 (VMS) 或設備管理和工具，例如 AXIS Device Manager。絕不允許系統使用者直接存取 Axis 設備。如需詳細資訊，請參閱。

停用網頁介面存取

CSC #4 : 企業資產和軟體的安全設定

自 AXIS OS 9.50 起，您可以停用 Axis 設備的網頁介面。將 Axis 設備部署到系統中 (或新增到 AXIS Device Manager) 後，我們建議您刪除組織內人員透過網頁瀏覽器存取設備的選項。如果設備帳戶密碼在組織內共用，此做法可帶來另一層安全性。更安全的選項是透過專屬的應用程式設定 Axis 設備的存取權，以提供進階的身分存取管理 (IAM) 架構、更高的追溯性和保護，以免帳戶洩漏。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	設定 > 系統 > 一般設定 > 系統 > 網頁介面已停用
≥ 10.9	系統 > 一般設定 > 系統 > 網頁介面已停用

設定網路設定

CSC #12 : 網路基礎架構管理

AXIS OS Hardening Guide

基本強化

設備 IP 設定取決於網路配定，例如 IPv4/IPv6、靜態或動態 (DHCP) 網路位址、子網路遮罩和預設路由器。我們建議您在新增新類型的組件時檢查您的網路拓撲。

我們也建議您在 Axis 設備上使用固定 IP 位址設定，以確保網路可達性並消除對網路中可能成為攻擊目標的伺服器 (如 DHCP 伺服器) 的依賴性。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 基本設定 > TCP/IP
≥ 7.10	設定 > 系統 > TCP/IP
≥ 10.9	系統 > 網路

設定日期和時間設定

CSC #8 : 稽核日誌管理

從安全角度來看，設定正確的日期和時間非常重要。例如，這可確保系統日誌會有正確資訊的時間戳，並且可以在執行時驗證和使用數位憑證。如果沒有正確的時間同步，依賴於數位憑證 (例如 HTTPS、IEEE 和 802.1x) 的服務可能無法正常運作。

我們建議您將 Axis 設備時鐘與網路時間通訊協定 (NTP，未加密) 伺服器或最好與網路時間安全性 (NTS，加密) 伺服器同步。網路時間安全性 (NTS) 是網路時間通訊協定 (NTP) 的加密和安全變體，已新增至 AXIS OS 11.1 中。我們建議您設定多個時間伺服器以獲得更高的時間同步準確度，但也要考慮到故障轉移情境，其中設定的時間伺服器之一可能不可用。

對於無法自行提供本地時間伺服器實例的個人和小型組織來說，使用公共 NTP 或 NTS 伺服器可以作為替代方案。有關 Axis 設備中 NTP/NTS 的更多資訊，請參閱 AXIS OS 知識庫中的 *NTP* 和 *NTS*。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 基本設定 > 日期和時間
≥ 7.10	設定 > 系統 > 日期和時間
≥ 10.9	系統 > 日期和時間
≥ 11.6	系統 > 時間和位置

邊際儲存加密

CSC #3 : 資料保護

SD 卡

如果 Axis 設備支援並使用安全數位 (SD) 卡儲存影片錄影資料，我們建議您套用加密。這將防止未經授權的個人播放已移除的 SD 卡中儲存的影像。

若要了解有關 Axis 設備中 SD 卡加密的更多資訊，請參閱 AXIS OS 知識庫中的 *SD 卡支援*。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 儲存
≥ 7.10	設定 > 系統 > 儲存
≥ 10.9	系統 > 儲存

網路共享 (NAS)

如果您使用網路附加儲存 (NAS) 作為錄影設備，我們建議您將其保護在存取受限的鎖定區域中，並啟用硬碟加密。Axis 設備利用 SMB 作為網路通訊協定來連接到 NAS 以儲存影像錄影。雖然 SMB 的早期版本 (1.0 和 2.0) 不

AXIS OS Hardening Guide

基本強化

提供任何安全性或加密，但更高版本 (2.1 及更新版本) 提供任何安全性或加密，這就是為什麼我們建議您在生產過程中使用更高版本的原因。

若要了解有關您將 Axis 設備連線至網路共享時正確 SMB 設定的更多資訊，請參閱 AXIS OS 知識庫中的 [網路共享](#)。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 儲存
≥ 7.10	設定 > 系統 > 儲存
≥ 10.9	系統 > 儲存

匯出錄影加密

CSC #3 : 資料保護

自 AXIS OS 10.10 起，Axis 設備支援邊緣錄影的加密匯出。我們建議使用此功能，因為它可以防止未經授權的個人播放匯出的影像資料。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	錄影內容

應用程式 (ACAP)

CSC #4 : 企業資產和軟體的安全設定

您可以將應用程式上傳到 Axis 設備以擴充其功能。其中許多應用程式都有自己的使用者介面 (用於與某項功能進行互動)。應用程式可使用 AXIS OS 所提供的安全性功能。

Axis 設備預先安裝了多個 Axis 根據 Axis 安全開發模型 (ASDM) 開發的應用程式。如需 Axis 應用程式的詳細資訊，請參閱 [axis.com](#) 上的 [分析](#)。

對於第 3 方應用程式，我們建議您聯絡供應商，了解有關應用程式運作和測試的安全性，以及是否根據常見最佳實務安全性開發模型進行開發的證據。在第 3 方應用程式中發現的漏洞必須直接報告給第 3 方供應商。

我們建議您僅操作受信任的應用程式，並從 Axis 設備中移除未使用的應用程式。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 應用程式
≥ 7.10	設定 > 應用程式
≥ 10.9	應用程式

停用未使用的服務/功能

CSC #4 : 企業資產和軟體的安全設定

儘管未使用的服務和功能不會立即構成安全威脅，但停用未使用的服務和功能以減少不必要的風險是一種很好的實務。請繼續閱讀以深入了解您可以在不使用時停用的服務和功能。

AXIS OS Hardening Guide

基本強化

未使用的實體網路連接埠

自 AXIS OS 11.2 起，具有多個網路連接埠的設備 (例如 AXIS S3008) 提供可以停用網路連接埠的 PoE 和網路流量的選項。讓未使用的網路連接埠處於無人看管和使用中狀態會帶來嚴重的安全風險。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	N/A
≥ 11.2	系統 > 乙太網路供電

網路發現通訊協定

Bonjour、UPnP、ZeroConf 和 WS-Discovery 等探索通訊協定是支援服務，可讓您更輕鬆地在網路上找尋 Axis 設備及其服務。部署設備並將設備新增到 VMS 後，我們建議您停用探索通訊協定，以阻止 Axis 設備宣布其在網路上的存在。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > 網路 > 網路 Bonjour 已啟用、網路 UPnP 已啟用、網路 ZeroConf 已啟用、網路 UPnP NATTraversal 已啟用*
	N/A
≥ 7.10	設定 > 系統 > 一般設定 > 網路 > 網路 Bonjour 已啟用、網路 UPnP 已啟用、網路 ZeroConf 已啟用、網路 UPnP NATTraversal 已啟用*
	設定 > 系統 > 一般設定 > WebService > 探索模式
≥ 10.9	設定 > 一般設定 > 網路 > 網路 Bonjour 已啟用、UPnP 已啟用、ZeroConf 已啟用
	系統 > 一般設定 > WebService > DiscoveryMode > 啟用 WS-Discovery 可探索模式

* 該功能已在 AXIS 10.12 中移除，且無法在更新的版本中使用

過時的 TLS 版本

我們建議您在將 Axis 設備投入生產之前停用舊版、過時的和不安全的 TLS 版本。過時的 TLS 版本通常預設處於停用狀態，但可在 Axis 設備中啟用它們，以向下相容尚未執行 TLS 1.2 和 TLS 1.3 的第三方應用程式。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > HTTPS > 允許 TLSv1.0 和/或允許 TLSv1.1
≥ 7.10	設定 > 系統 > 一般設定 > HTTPS > 允許 TLSv1.0 和/或允許 TLSv1.1
≥ 10.9	系統 > 一般設定 > HTTPS > 允許 TLSv1.0 和/或允許 TLSv1.1

指令碼編輯器環境

我們建議您停用對於指令碼編輯器環境的存取。指令碼編輯器僅用於故障排除和偵錯目的。

指令碼編輯器已在 AXIS OS 10.11 中移除，且無法在更新的版本中使用。

AXIS OS Hardening Guide

基本強化

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	設定 > 系統 > 一般設定 > 系統 > 啟用腳本編輯器 (editcgi)
≥ 10.9	系統 > 一般設定 > 系統 > 啟用腳本編輯器 (editcgi)

HTTP 伺服器標頭

預設情況下，Axis 設備在與網路上的用戶端進行 HTTP 連線期間，宣布其目前的 Apache 和 OpenSSL 版本。當您定期使用網路安全掃描器時，此資訊非常實用，這是因為此項資訊更詳細地報告特定 AXIS 作業系統版本中的明顯漏洞。

您可以停用 HTTP 伺服器標頭，以減少在 HTTP(S) 連線期間的資訊暴露。但是，我們僅建議您在根據我們的建議操作設備並隨時保持最新狀態時才停用標頭。

自 AXIS OS 10.6 起，已開始提供停用 HTTP(S) 伺服器標頭的選項。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	設定 > 系統 > 一般設定 > 系統 > HTTP 伺服器標頭註釋
≥ 10.9	系統 > 一般設定 > 系統 > HTTP 伺服器標頭註釋

音訊

在 Axis 影像監控產品 (例如網路攝影機) 中，音訊輸入/輸出和麥克風功能預設處於停用狀態。如果您需要音訊功能，則須在使用前啟用功能。在以音訊輸入/輸出和麥克風功能為主要功能的 Axis 產品中，例如 Axis 對講機和網路喇叭，預設情況下會啟用音訊功能。

如果您用不到音訊功能，我們建議您停用音訊功能。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > 音訊 > 音訊 A* > 已啟用
≥ 7.10	設定 > 音訊 > 允許音訊
≥ 10.9	音訊 > 設備設定

SD 卡插槽

Axis 設備通常支援至少一張 SD 卡，以提供影片錄影資料的本機邊際儲存。如果您用不到 SD 卡，我們建議您完全停用 SD 卡插槽。AXIS OS 9.80 提供停用 SD 卡插槽的選項。

如需詳細資訊，請參閱 AXIS OS 知識庫中的 [停用 SD 卡](#)。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	設定 > 系統 > 一般設定 > 儲存 > SD 硬碟已啟用
≥ 10.9	系統 > 一般設定 > 儲存 > SD 硬碟已啟用

AXIS OS Hardening Guide

基本強化

FTP 存取

FTP 是一種不安全的通訊協定，僅用於故障排除和偵錯目的。FTP 存取已從 AXIS OS 11.1 刪除，且無法在更新的版本中使用。我們建議您停用 FTP 存取並使用安全 SSH 存取進行疑難排解。

如需 SSH 詳細資訊，請參閱 AXIS OS 入口網站中的 *SSH 存取*。如需使用 FTP 偵錯選項的資訊，請參閱 AXIS OS 入口網站中的 *FTP 存取*。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 一般設定 > 網路 > FTP 已啟用
≥ 7.10	設定 > 系統 > 一般設定 > 網路 > FTP 已啟用
≥ 10.9	系統 > 一般設定 > 網路 > FTP 已啟用

SSH 存取

SSH 是一種安全通訊協定，僅用於故障排除和偵錯目的。自 AXIS OS 5.50 起，Axis 設備均支持此功能。我們建議您停用 SSH 存取。

如需使用 SSH 偵錯選項的詳細資訊，請參閱 AXIS OS 知識庫中的 *SSH 存取*。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 一般設定 > 網路 > SSH 已啟用
≥ 7.10	設定 > 系統 > 一般設定 > 網路 > SSH 已啟用
≥ 10.9	系統 > 一般設定 > 網路 > SSH 已啟用

Telnet 存取

Telnet 是一種不安全的通訊協定，僅用於故障排除和偵錯目的。AXIS OS 5.50 之前版本的 Axis 設備支援此功能。我們建議您停用 Telnet 存取。

AXIS 作業系統版本	網頁介面設定路徑
< 5.50	如需說明，請參閱 AXIS OS 知識庫中的 <i>設備存取</i> 。
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	N/A

ARP/Ping

ARP/Ping 是一種使用如 AXIS IP Utility 等工具設定 Axis 設備 IP 位址的方法。該功能已在 AXIS OS 7.10 中移除，且無法在更新的版本中使用。我們建議您在安裝 AXIS OS 7.10 及更舊版本的 Axis 設備中停用此功能。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > 網路 > ARP/Ping
≥ 7.10	N/A
≥ 10.9	N/A

AXIS OS Hardening Guide

基本強化

IP 位址過濾

CSC #1 : 企業資產的盤點和控制
CSC#4 : 企業資產和軟體的安全設定
CSC #13 : 網路監控與防禦

IP 位置過濾可防止未經授權的用戶端存取 Axis 設備。我們建議您將設備設定為允許授權網路主機 IP 位址，或拒絕未經授權的網路主機的 IP 位址。

如果您選擇允許 IP 位址，請務必使用將所有授權用戶端 (VMS 伺服器和管理用戶端) 新增到您的清單中。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 安全性 > IP 位址過濾
≥ 7.10	設定 > 系統 > TCP/IP > IP 位址過濾
≥ 10.9*	設定 > 安全性 > IP 位址過濾

在 AXIS OS 11.9 及更新版本中，IP 位址過濾器已由新的主機防火牆取代。

主機防火牆

CSC #1 : 企業資產的盤點和控制
CSC#4 : 企業資產和軟體的安全設定
CSC #13 : 網路監控與防禦

使用者可以使用防火牆建立規則，透過 IP 位址和/或 TCP/UDP 連接埠號碼來管制流向設備的輸入流量。因此，可以防止未經授權的用戶端存取 Axis 設備或設備上的特定服務。

如果將預設政策設定為「拒絕」，請務必將所有授權用戶端 (VMS 和管理用戶端) 和/或連接埠新增至您的清單。

AXIS 作業系統版本	網頁介面設定路徑
≥ 11.9	設定 > 安全性 > 防火牆

HTTPS

CSC #3 : 資料保護

自 AXIS OS 7.20 起，Axis 設備預設為啟用 HTTP 和 HTTPS。HTTP 存取不加密，不安全，而 HTTPS 會對用戶端和 Axis 設備之間的流量進行加密。我們建議您對 Axis 設備上的所有管理任務使用 HTTPS。

如需設定說明，請參閱和。

僅 HTTPS

我們建議您將 Axis 設備設定為僅使用 HTTPS (無 HTTP 存取可用)。這將自動啟用 HSTS (HTTP 嚴格傳輸安全)，進一步提升設備的安全性。

自 AXIS OS 7.20 起，Axis 設備具有自我簽署的憑證。雖然自我簽署的憑證在設計上不受信任，但它足以在初始設定期間以及手邊沒有可用的公開金鑰基礎架構 (PKI) 時安全地存取 Axis 設備。如果可用，應移除自我簽署的憑證並替換為所選 PKI 機構發行的正確簽署的用戶端憑證。自 AXIS OS 10.10 起，自我簽署的憑證已被 IEEE 802.1AR 安全設備 ID 憑證取代。

AXIS OS Hardening Guide

基本強化

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 安全性 > HTTPS
≥ 7.10	設定 > 系統 > 安全性 > HTTP 和 HTTPS
≥ 10.9	系統 > 網路 > HTTP 和 HTTPS

HTTPS 密碼

Axis 設備支援並使用 TLS 1.2 和 TLS 1.3 加密套件，以安全地加密 HTTPS 連線。所使用的特定 TLS 版本和加密套件取決於連接到 Axis 設備的用戶端，並據此進行交涉。將 Axis 設備重設為出廠預設設定後，加密清單可根據 Axis 所提供最新可用的最佳實務組態自動更新。

如需參照和透明度，請使用在和中列出的安全強式加密套件。

TLS 1.2 及更低版本

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

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > HTTPS > 密碼
≥ 7.10	設定 > 系統 > 一般設定 > HTTPS > 密碼
≥ 10.9	系統 > 一般設定 > HTTPS > 密碼

TLS 1.3

根據預設，僅符合 TLS 1.3 規格的強式加密套件可用：

TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384

使用者無法設定這些套件。

存取日誌

CSC #1：企業資產的盤點和控制

CSC #8：稽核日誌管理

存取日誌將詳細地記錄使用者對 Axis 設備的存取，進而讓稽核和門禁管制管理變得更輕鬆。我們建議將此功能與遠端 syslog 伺服器結合使用，以便 Axis 設備可以將其日誌傳送到中央日誌記錄環境。這將簡化日誌訊息的儲存及其保留時間。

如需詳細資訊，請參閱 AXIS OS 知識庫中的 [設備存取記錄](#)。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > 系統 > 存取日誌
≥ 7.10	設定 > 系統 > 一般設定 > 系統 > 存取日誌
≥ 10.9	系統 > 一般設定 > 系統 > 存取日誌

基本強化

實體防竄改配件

CSC #1 : 企業資產的盤點和控制

CSC#12 : 網路基礎架構管理

Axis 提供實體入侵和/或防竄改開關作為選購附件，以強化 Axis 設備的實體保護。這些開關可以觸發警報，讓 Axis 設備可以向所選的用戶端傳送通知或警報。

有關 Axis 設備可用防竄改附件的更多資訊，請參閱：

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

擴展強化

擴展強化

擴展強化的說明是由中所述的強化主題所打造。但雖然您可以直接在 Axis 設備中套用預設和基本強化說明，但擴展強化需要整個供應商供應鏈以及最終使用者組織和底層 IT 和/或網路基礎架構的積極參與。

限制網際網路暴露

CSC #12：網路基礎架構管理

我們不建議您將 Axis 設備公開為公共網頁伺服器，或您以任何其他方式允許未知用戶端獲得對設備的網路存取權限。我們建議對於不操作 VMS 也不需要從遠端位置存取影像的小型組織和人員使用 AXIS Companion。

AXIS Companion 採用 Windows/iOS/Android 用戶端軟體，這是免費且提供一種安全地存取影像的簡單方法，而無需將 Axis 設備暴露在網際網路上。如需 AXIS Companion 的詳細資訊，請參閱 axis.com/companion。

備註

所有使用 VMS 的組織都應諮詢 VMS 供應商，了解有關遠端影像存取的最佳實務。

限制網路曝光

CSC #12：網路基礎架構管理

降低網路暴露風險的常見方法為以實體與虛擬的方式隔離網路裝置和相關基礎架構及應用程式。此類基礎設施和應用程式的範例包括影像管理軟體 (VMS)、網路影像錄影機 (NVR) 和其他類型的監控設備。

我們建議您隔離未連接到生產和業務網路的本機網路上的 Axis 設備和相關基礎設施和應用程式。

若要應用基本強化，請新增多層的網路安全機制，以保護本機網路及其基礎設施 (路由器、交換器) 不會受到未經授權的存取。此類機制的範例包括 VLAN 分段、受限的路由功能、用於站點到站點或 WAN 存取的虛擬專用網路 (VPN)、網路層 2/3 防火牆，以及門禁管制清單 (ACL)。

為了擴大基本強化，我們建議您套用更先進的網路檢測技術，例如深度資料包檢測和入侵偵測。這將在網路內套用一致且全面的威脅防護。擴展網路強化需要專用的軟體和/或硬體設備。

網路漏洞掃描

CSC #1：企業資產的盤點和控制

CSC #12：網路基礎架構管理

您可以使用網路安全掃描器對網路設備執行漏洞評估。漏洞評估的目的是對潛在的安全漏洞和錯誤設定進行系統檢閱。

我們建議您定期對 Axis 設備及其相關基礎架構進行漏洞評估。開始掃描前，請確定您的 Axis 設備已更新至最新可用的 AXIS 作業系統版本 (LTS 或主動式軌道)。

我們也建議您檢閱掃描報告並篩選掉 Axis 設備的已知誤報，您可以在 *AXIS OS 漏洞掃描程式指南* 中找到這些資訊。請將報告和任何其他備註應透過服務台報修單提交至 axis.com 上的 Axis 支援部門。

可信公開金鑰基礎架構 (PKI)

CSC #3：資料保護

CSC #12：網路基礎架構管理

我們建議您在由公共或私有憑證授權單位 (CA) 信任和簽署的 Axis 設備中部署網頁伺服器 and 用戶端憑證。具有經驗證信任鏈的 CA 簽署憑證有助於在透過 HTTPS 連線時移除瀏覽器憑證警告。部署網路存取控制 (NAC) 解決方案時，CA 簽署憑證也可確保 Axis 設備的真確性。這可以降低攻擊電腦冒充 Axis 設備的風險。

AXIS OS Hardening Guide

擴展強化

您可以使用具有內建 CA 服務的 AXIS Device Manager 向 Axis 設備發行已簽署的憑證。

IEEE 802.1X 網路存取控制

CSC #6 : 門禁管制管理

CSC #13 : 網路監控與防禦

Axis 設備支援透過 802.1X-EAP-TLS 方法的基於 IEEE 802.1X 連接埠的網路門禁管制。為了獲得最佳保護，我們建議您在驗證 Axis 設備時使用可信任的憑證授權單位 (CA) 簽署的用戶端憑證。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 安全性 > IEEE 802.1X。
≥ 7.10	設定 > 系統 > 安全性 > IEEE 802.1X
≥ 10.9	系統 > 安全性 > IEEE 802.1X

IEEE 802.1AE MACsec

CSC #3 : 資料保護

CSC #6 : 門禁管制管理

Axis 設備支援 802.1AE MACsec，這是一種定義明確的網路通訊協定，可透過加密方式保護網路第 2 層上的點對點乙太網路連結，確保兩台主機之間資料傳輸的機密性和完整性。由於 MACsec 在網路堆疊的第 2 層運行，因此它為不提供本機加密功能 (ARP、NTP、DHCP、LLDP、CDP...) 以及提供類似功能的網路通訊協定 (HTTPS、TLS)，新增了額外的安全層。

IEEE 802.1AE MACsec 標準描述了兩種操作模式：手動設定的預先共用金鑰 (PSK)/靜態 CAK 模式，和使用 IEEE 802.1X EAP-TLS 工作階段的自動主工作階段/動態 CAK 模式。Axis 設備支援兩種模式。

有關 802.1AE MACsec 以及如何在 AXIS OS 設備中設定它的更多資訊，請參閱 AXIS OS 知識庫中的 *IEEE 802.1AE*。

IEEE 802.1AR 安全設備身分

CSC #1 : 企業資產的盤點和控制

CSC#13 : 網路監控與防禦

配備 Axis Edge Vault 的 Axis 設備支援網路標準 IEEE 802.1AR。該標準允許透過 Axis 設備 ID (生產過程中安裝在設備中的唯一憑證) 自動安全地將 Axis 設備接入網路。如需安全設備上線的範例，請在 *將 Axis 設備安全整合到 Aruba 網路* 中閱讀更多資訊。

如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。若要下載 Axis 設備 ID 憑證鏈 (用於驗證 Axis 設備身分)，請參閱 axis.com 上的 *公開金鑰基礎架構儲存庫*。

SNMP 監控

CSC #8 : 稽核日誌管理

Axis 設備支援以下 SNMP 通訊協定：

- SNMP v1 : 僅出於保留原因而受支援，請勿使用。
- SNMP v2c : 可以在受保護的網段上使用。
- SNMP v3 : 建議用於監控目的。

Axis 設備也支援監控 MIB-II 和 AXIS Video MIB。若要下載 AXIS Video MIB，請參閱 AXIS OS 知識庫中的 *AXIS Video MIB*。

若要深入了解如何在 AXIS OS 中設定 SNMP，請參閱 AXIS OS 知識庫中的 *SNMP (簡易網路管理通訊協定)*。

AXIS OS Hardening Guide

擴展強化

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 網路 > SNMP
≥ 7.10	設定 > 系統 > SNMP
≥ 10.9	系統 > 網路 > SNMP

遠端系統記錄檔

CSC #8 : 稽核日誌管理

您可以將 Axis 設備設定為將所有加密的日誌訊息傳送到中央 syslog 伺服器。這讓稽核變得更容易，並防止日誌訊息在 Axis 設備中被有意/惡意或無意地刪除。這也允許根據公司政策延長設備日誌的保留時間。

如需您如何啟用 AXIS 作業系統版本中遠端系統記錄檔伺服器的詳細資訊，請參閱 AXIS OS 知識庫中的 [系統記錄檔](#)。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	如需說明，請參閱 AXIS OS 入口網站中的 系統記錄檔
≥ 7.10	設定 > 系統 > TCP/IP
≥ 10.9	系統 > 日誌

安全影像串流 (SRTP/RTSPS)

CSC #3 : 資料保護

自 AXIS OS 7.40 起，Axis 設備能支援透過 RTP (也稱為 SRTP/RTSPS) 的安全影像串流。SRTP/RTSPS 使用安全的端對端加密傳輸方法，確保僅授權用戶端才能接收來自 Axis 設備的影像串流。如果影像管理系統 (VMS) 支援，我們建議您啟用 SRTP/RTSPS。如果可用，請使用 SRTP 而非未加密的 RTP 影像串流。

備註

SRTP/RTSPS 僅會將影像串流資料加密。對於管理組態任務，我們建議您僅啟用 HTTPS，以將此類型通訊加密。

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 進階 > 一般設定 > 網路 > RTSPS
≥ 7.10	設定 > 系統 > 一般設定 > 網路 > RTSPS
≥ 10.9	系統 > 一般設定 > 網路 > RTSPS

已簽署的影像

CSC #3 : 資料保護

自 AXIS OS 10.11 起，具有 Axis Edge Vault 的 Axis 設備支援已簽署的影像。藉由已簽署的影像，Axis 設備可以向其影像串流新增簽名，以確保影像完好無損，並透過將其追溯至製作它的 Axis 設備來驗證其來源。影像管理系統 (VMS) 或證據管理系統 (EMS) 也可以驗證 Axis 設備提供的影像的真實性。

如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。若要找出用於驗證已簽署影像真實性的 Axis root 憑證，請參閱 AXIS OS 知識庫中的 [設備存取](#)。

AXIS OS Hardening Guide

擴展強化

AXIS 作業系統版本	網頁介面設定路徑
< 7.10	N/A
≥ 7.10	N/A
≥ 10.9	系統 > 一般設定 > 影像 > 已簽署影像

AXIS OS Hardening Guide

快速入門指南

快速入門指南

快速入門指南提供您在強化 AXIS OS 5.51 及更新版本的 Axis 裝置時應進行的設定概觀。其中涵蓋了您可以在中讀到的強化主題，然而，並未涵蓋中的主題，因為這些需要根據具體情況進行廣泛的和客戶特定的設定。

我們建議您使用 AXIS Device Manager 以快速且經濟高效的方式強化多個 Axis 設備。如果您需要使用其他應用程式進行設備設定，或只需要強化一些 Axis 設備，我們建議您使用 VAPIX API。

常見設定錯誤

暴露於網際網路的設備

CSC#12：網路基礎架構管理

我們不建議您將 Axis 設備公開為公共網頁伺服器，或您以任何其他方式允許未知用戶端獲得對設備的網路存取權限。如需詳細資訊，請參閱。

常用密碼

CSC#4：企業資產和軟體的安全設定

CSC #5：帳戶管理

我們強烈建議每個設備使用唯一的密碼，而不是在所有設備上使用通用密碼。有關相關指示，請參閱和。

匿名存取

CSC#4：企業資產和軟體的安全設定

CSC #5：帳戶管理。

我們不建議您允許匿名使用者在不提供登入認證的情況下存取設備中的影像和組態設定。如需詳細資訊，請參閱。

安全通訊已停用

CSC#3：資料保護

我們不建議您使用不安全的通訊和存取方法 (例如 HTTP 或基本身分驗證) 來操作設備，其中密碼會在未經加密的情況下傳輸。如需詳細資訊，請參閱。如需組態建議事項，請參閱。

過時的 AXIS 作業系統版本

CSC#2：軟體資產的盤點和控制

我們強烈建議您在 (LTS) 或主動式軌道上使用最新可用的 AXIS 作業系統版本來操作設備。這兩個軌道都提供最新的安全修補程式和錯誤修復。如需詳細資訊，請參閱。

透過 VAPIX API 進行基本強化

您可以使用 VAPIX API，根據中涵蓋的主題強化您的 Axis 設備。在此表中，您可以找到所有基本強化設定，無論 Axis 設備的 AXIS 作業系統版本為何。

在您的設備的 AXIS 作業系統版本中已不再能夠使用某些設定，因為已經隨著時間移除了某些功能以提升安全性。如果您在發出 VAPIX 呼叫時收到錯誤，則可能是該功能在 AXIS 作業系統版本中已不再能夠使用。

用途	VAPIX API 呼叫
停用未使用網路連接埠中的 POE*	<code>http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no</code>
停用未使用網路連接埠中的網路流量**	<code>http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }</code>

AXIS OS Hardening Guide

快速入門指南

用途	VAPIX API 呼叫
停用 Bonjour 探索通訊協定	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no</code>
停用 UPnP 探索通訊協定	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.Enabled=no</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&Network.UPnP.NATTraversal.Enabled=no</code>
停用 WebService 探索通訊協定	<code>https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no</code>
停用單鍵雲端連線 (O3C)	<code>https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no</code>
停用設備 SSH 維護存取	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no</code>
停用設備 FTP 維護存取	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no</code>
停用 ARP-Ping IP 位址設定	<code>https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no</code>
停用 Zero-Conf IP 位址設定	<code>http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no</code>
僅啟用 HTTPS	<code>https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https</code>
僅啟用 TLS 1.2 和 TLS 1.3	<code>https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no</code> <code>https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no</code>
TLS 1.2 安全密碼設定	<code>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</code>

AXIS OS Hardening Guide

快速入門指南

用途	VAPIX API 呼叫
啟用暴力破解攻擊保護**	<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>
停用腳本編輯器環境	<pre> https://ip-address/axis-cgi/param.cgi?action=update &System.EditCgi=no </pre>
啟用改善的使用者存取日誌記錄	<pre> https://ip-address/axis-cgi/param.cgi?action=update &System.AccessLog=On </pre>
啟用 ONVIF 重播攻擊保護	<pre> https://ip-address/axis-cgi/param.cgi?action=update &WebService.UsernameToken.ReplayAttackProtection=yes </pre>
停用設備網頁介面存取	<pre> https://ip-address/axis-cgi/param.cgi?action=update &System.WebInterfaceDisabled=yes </pre>
停用 HTTP/OpenSSL 伺服器標頭	<pre> https://ip-address/axis-cgi/param.cgi?action=update &System.HTTPServerTokens=no </pre>
停用匿名觀看者和 PTZ 存取	<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>
防止安裝需要 root 權限的 ACAP 應用程式	<pre> http://ip-address/axis-cgi/applications/config.cgi?action=set &name=AllowRoot&value=false </pre>
防止安裝未簽署的 ACAP 應用程式	<pre> http://ip-address/axis-cgi/applications/config.cgi?action=set &name=AllowUnsigned&value=false </pre>

* 將「X」取代為「port=X」中的實際連接埠號碼。範例：「port=1」將停用連接埠 1，「port=2」將停用連接埠 2。

** 將「1」換成「eth1.1」中的連接埠號碼。範例：「eth1.1」將停用連接埠 1，「eth1.2」將停用連接埠 2。

*** 一秒內嘗試登入 20 次失敗後，用戶端 IP 位址將被封鎖 10 秒。30 秒呼叫間隔內的每個後續失敗請求都將導致 DoS 阻止期再延長 10 秒。

AXIS OS Hardening Guide

快速入門指南

透過 AXIS Device Manager (擴展) 進行基本強化

您可以使用 AXIS Device Manager 和 AXIS Device Manager Extend，根據中涵蓋的主題強化 Axis 設備。使用此 **設定檔案** (由在中列出的相同組態設定組成)。

在您的設備的 AXIS 作業系統版本中已不再能夠使用某些設定，因為已經隨著時間移除了某些功能以提升安全性。AXIS Device Manager 和 AXIS Device Manager Extend 將自動從強化設定中移除這些設定。

備註

上傳設定檔案後，Axis 設備將設定為僅 HTTPS，並且網頁介面將被停用。您可以透過例如移除或新增參數來根據需求修改設定檔案。

