AXIS OS強化指南

AXIS OS 入口網站 | AXIS OS 鑑證指南 | AXIS OS 安全漏洞掃描程式指南 | 安全公告 | AXIS OS 版本須知 | AXIS OS 知識庫 | AXIS OS YouTube 播放清單

引言

AXIS OS 強化指南為執行 AXIS OS 的 Axis 設備提供加強安全性的實用指引。本指南說明建議的組態設定、功能和操作規範，以協助縮小攻擊面、保護資料及確保設備在整個生命週期內的可靠操作。本指南的目的為協助系統管理員、整合商及安防專業人員按照業界實務經驗，以安全可靠的方式建置和維護 Axis 產品。

網頁介面組態設定
本篇將講解在Axis裝置網頁介面中如何設定裝置。組態路徑根據設備上安裝的 AXIS OS 版本而有所不同：

AXIS OS 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
≥ 10.9	系統 > 安全

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，以及執行設備軟體 4.xx 和 5.xx 的舊版產品。

AXIS OS 產品設計用於專業安防或營運分析系統，以及與影像管理系統 (VMS) 和設備管理應用程式等其他產品整合。

本產品可供技術熟練的人員在非專業環境使用，但並非設計供個人消費者在居家環境使用。

本產品採用預設安全原則，但務必遵循本強化指南，才能達到更高的安全等級。部分整合系統提供典型安全系統設計指南，相關內容可參閱 *help.axis.com*。

CIS 保護層級

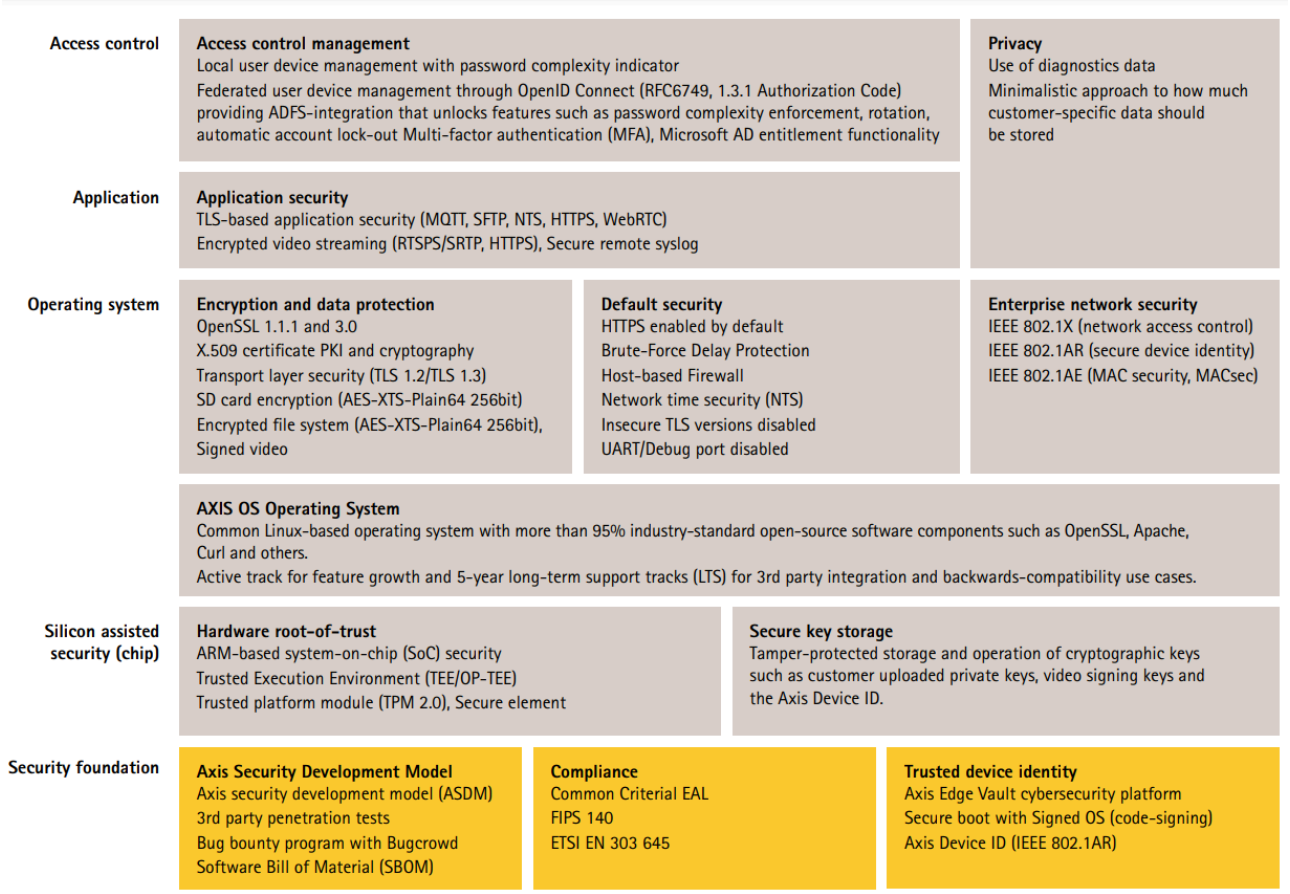
我們遵循在網際網路安全中心 (CIS) 控制第 8 版所概述的方法來構建我們的網路安全框架建議。CIS 控制以前稱為 SANS Top 20 關鍵安全控制，提供 18 類關鍵安全控制 (CSC)，聚焦於解決組織中最常見的網路安全風險類別。

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 中的 *18 類 CIS 關鍵安全控制*。

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。

AXIS OS安全架構圖有各級AXIS OS網路安全功能。完整介紹安全基礎設備、矽基安全技術、AXIS OS作業系統以及應用程式和存取控制層。



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。

驗證

預設為停用

CSC #4：企業資產和軟體的安全組態設定

在設定管理員密碼之前，Axis 設備不會運作。

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。

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*。

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。建議您依照此處所述啟用 HTTPS。如果不可行，建議您僅使用摘要式驗證，請勿使用基本驗證，也不要同時使用基本和摘要式驗證。這能降低網路偵測器獲取密碼的風險。

AXIS OS 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 OS 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

CSC #4：企業資產和軟體的安全組態設定
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。

從AXIS OS 11.5開始，預設啟用暴力延遲保護。詳細相關組態設定範例和建議，請參閱AXIS OS知識庫中的*暴力攻擊延遲保護*。

AXIS OS 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 > 防止暴力破解攻擊

稽核日誌

CSC #1：企業資產的庫存和控制
CSC #8：審計日誌管理

稽核日誌用於網路安全相關目的，例如事件處理，並且有助於建立對相關事件和動作的長期監控。我們建議使用遠端 syslog 伺服器或其他網路監控應用程式，讓 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*稽核日誌*。

AXIS OS 版本	網頁介面設定路徑
< 7.10	N/A
7.10	N/A
≥ 12.5	系統 > 日誌

邊際儲存

CSC #4：企業資產和軟體的安全組態設定

CSC #3：資料保護

從AXIS OS 12.0開始，noexec掛載選項已新增為已掛載網路共用的預設選項。這將停用從掛載的網絡共享直接執行二進位文件。SD卡已在舊版AXIS OS中新增了這個選項。

此外，搭載 AXIS OS 10.10 及更高版本的 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 OS 版本	網頁介面設定路徑
< 7.10	N/A
7.10	N/A
≥ 10.9	錄影檔案

網路安全

網路通訊協定

CSC #4：企業資產和軟體的安全組態設定

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，如下所示。

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	TCP	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 設備注意：在AXIS OS 12中預設為停用。0.

協定	連接埠	傳輸	註解
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 設備注意：在 AXIS OS 12中預設為停用。0.
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

* 如需邊際對邊際的詳細資訊，請參閱白皮書 *邊際對邊際技術*。

** 根據 RFC 6056 自動在預先定義的連接埠號碼範圍內配置。如需詳細資訊，請參閱維基百科文章 *臨時連接埠*。

*** 在 AXIS OS 12.1 及更高版本中，預設為停用 WebService 探索 (WS-Discovery) 通訊協定。

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/輸出和麥克風功能是主要功能，且預設為啟用。

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。在AXIS OS 10.10以上版本中，自簽憑證已由IEEE 802.1AR安全裝置ID憑證取代。

預設情況下，AXIS OS 具有最常見的安全相關 HTTP(S) 標頭，可提升出廠預設狀態下的基本網路安全性。在AXIS OS 9.80以上版本中，可使用自訂HTTP標題VAPIX API來設定其他HTTP(S)標題。

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*。

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

IEEE 802.1X網路存取控制

CSC #6：存取控制管理
CSC #13：網路監控與防禦

Axis 設備支援透過 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 OS 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

在 AXIS OS 12.6 中，我們為 S3008 和 S3008 MK II 錄影主機新增了 802.1x 驗證。如果您要連線的設備具有 Axis 設備 ID，但不支援 MACsec，請前往 [System (系統) > Network ports (網路連接埠)]，然後在連接埠的 [Security (安全性)] 下，選取「Authentication required (需驗證)」。這樣可確保只有具備 Axis 設備 ID 的設備才能連線。

IEEE 802.1AE MACsec

CSC #3：資料保護
CSC #6：存取控制管理

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。

在 AXIS OS 12.6 中，我們為 S3008 和 S3008 MK II 錄影主機新增了 802.1AE MACsec 支援。如果您要連線的設備具有 Axis 設備 ID 且支援 MACsec，請前往 [System (系統) > Network ports (網路連接埠)]，然後在連接埠的 [Security (安全性)] 下，選取「MACsec secured required (需 MACsec 加密)」。這樣可以同時強制執行 802.1x 驗證與 MACsec 加密。

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：企業資產的庫存和控制
CSC #13：網路監控與防禦

配備Axis Edge Vault的Axis裝置支援網路標準IEEE 802.1AR。使Axis裝置以Axis裝置ID（生產期間裝在裝置中的唯一憑證）自動安全地進入網絡。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*。

UART/偵錯介面

CSC #4：企業資產和軟體的安全組態設定

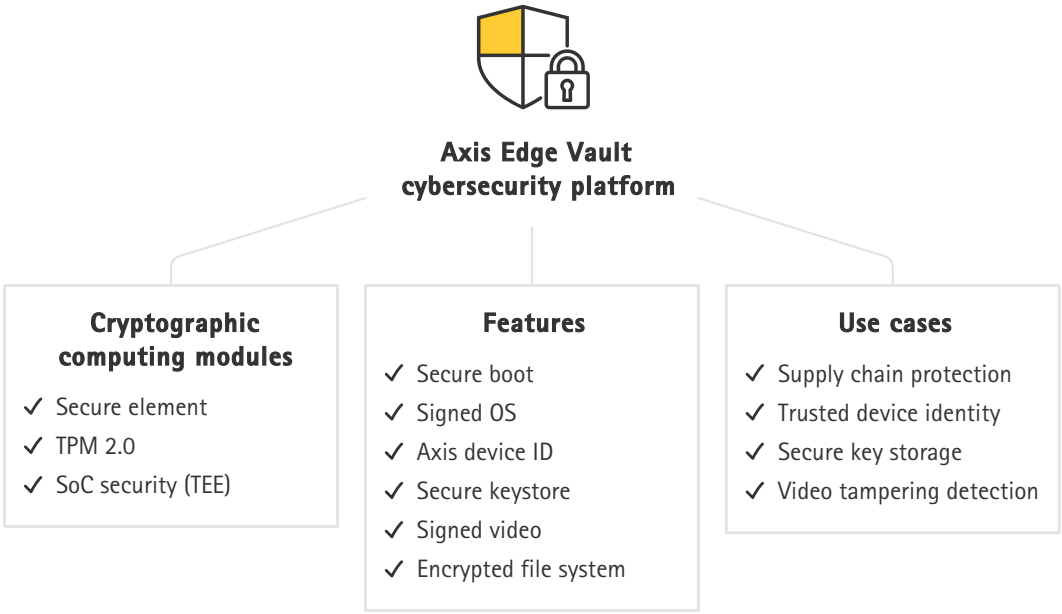
每台Axis裝置都有所謂的實體UART（通用異步接收器發射器）接口，亦稱為「偵錯端口」或「序列控制臺」。要拆接只能大量拆卸Axis裝置。UART/偵錯介面僅用於 Axis 內部研發工程專案期間的產品開發和偵錯目的。

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 (憑證伺服器)

Axis Edge Vault 提供保護 Axis 設備安全的硬體式網路安全平台。其仰賴強大的密碼學運算模組(安全元件和TPM)與SoC安全(TEE和安全開機)基礎，並結合邊際設備安全的專業知識。Axis Edge Vault 以透過安全開機和已簽署 OS 建立的強大信任 root 為基礎。這些功能可建立堅固的密碼學驗證軟體鏈建構之信任鏈，這是所有安全操作的基礎。

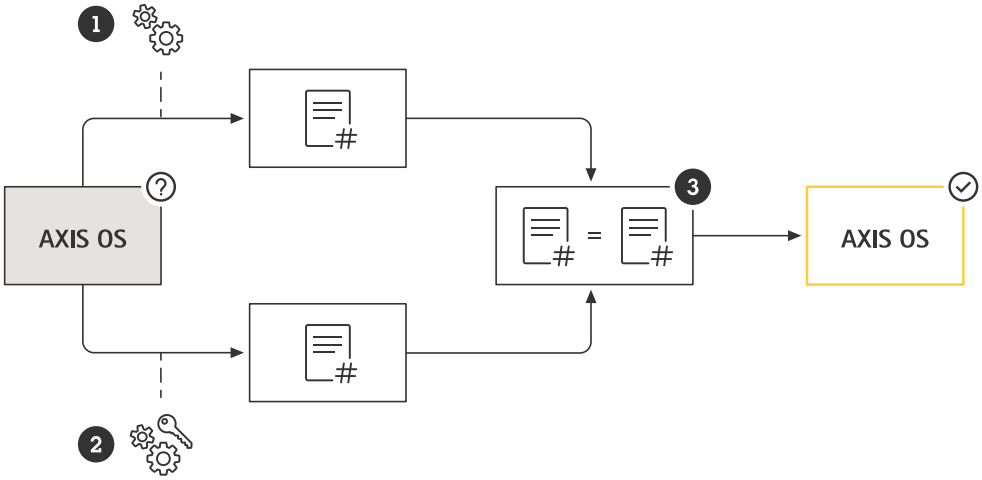
配備 Axis Edge Vault 的設備可防止竊聽和惡意擷取敏感資訊，進而盡可能地減少面臨的網路安全風險。Axis Edge Vault 也確保 Axis 設備成為網路中值得信賴的可靠單元。



已簽署的作業系統

CSC #2：庫存和控制軟體資產

AXIS OS 已於 9.20.1 版本簽署。升級版本時，設備將透過加密簽署驗證來檢查更新檔案的完整性，並拒絕已竄改的檔案。這會防止攻擊者誘騙使用者安裝受感染的檔案。



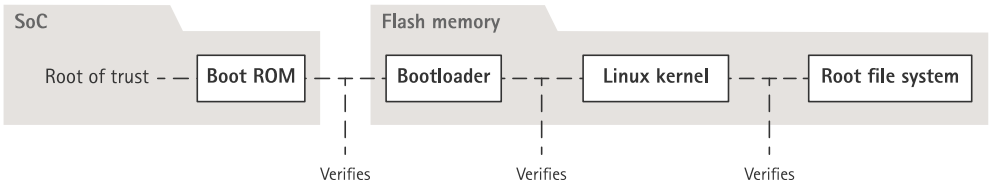
1) 設備計算 AXIS OS 的雜湊值。2) 設備使用公開金鑰解密簽署，取得雜湊值。3) 如果結果相符，則 OS 簽署通過驗證。

如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。

安全開機

CSC #2：庫存和控制軟體資產

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。

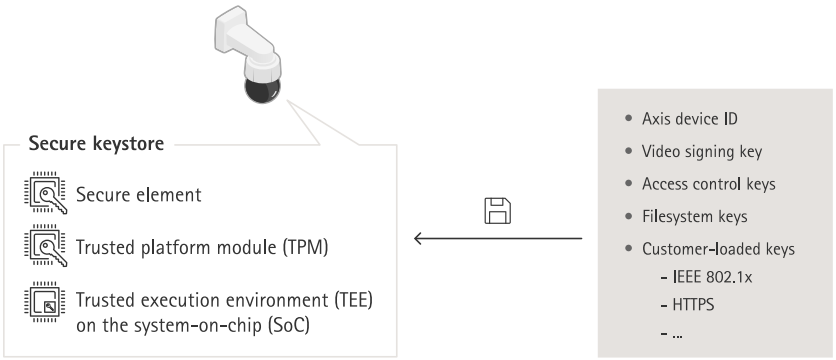


如需詳細資訊，請參閱 *Axis Edge Vault* 上的白皮書。

安全金鑰儲存區

CSC #6：存取控制管理

安全金鑰儲存區可用硬體防竄改方式儲存密碼學資訊。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)。



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。

軟體購買清單 (SBOM)

CSC #1：企業資產的庫存和控制

軟體購買清單 (SBOM) 用於管理安全漏洞及提升供應鏈透明度，是強化 Axis 產品信任度的重要工具。axis.com 上發佈的每個設備軟體版本都附帶 SBOM。

退役

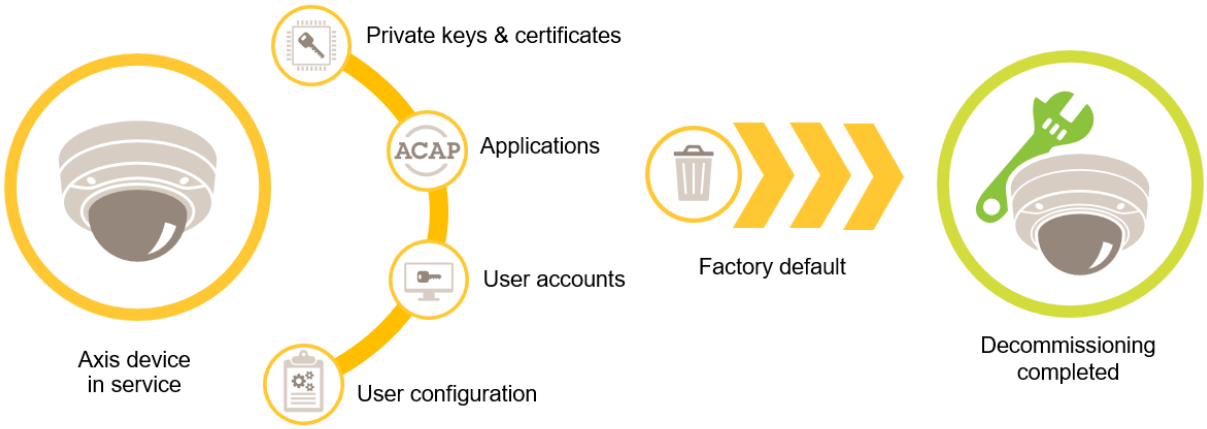
CSC #3：資料保護

Axis 設備使用揮發性和非揮發性記憶體。雖然揮發性記憶體在切斷設備的電源時會被清除，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」。eMMC 快閃記憶體使用等效功能，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，發起還原出廠預設值不會立即清除數據，會在裝置重新啟動，於系統啟動期間清除。 因此若要刪除資料，不僅要發起還原出廠預設值，還要讓設備在關閉電源前重新啟動完成。

此客戶資料清除程序採用 NIST SP-800-88 Revision 1 所述的「清除」消毒技術。



AXIS OS 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 記憶卡加密金鑰	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

*已簽署的 OS 使用自訂憑證，讓使用者可上傳 (還有其他功能) AXIS OS。
** 儲存在邊際儲存區 (SD 卡、網路共用區) 的錄影檔案及影像需要使用者手動操作才能刪除。清除 SD 卡上的客戶資料是根據 NIST SP-800-88 Revision 1 Cryptographic Erase (CE) 進行，清除 HDD (S30 錄影主機系列) 上的資料則是遵循 NIST SP-800-88 Revision 1 Clear。如需詳細資訊，請參閱 AXIS OS 知識庫中的。
***所有用於使用者的組態設定，從建立帳號到網路、O3C、事件、影像、PTZ和系統組態設定。
****裝置會保留所有預先安裝的應用程式，但會刪除所有使用者自訂的組態設定
*****生產資料（校正、802.1AR生產憑證）和使用週期統計資料，包括非機密和非使用者相關資訊。

基本強化

基本強化是建議 Axis 設備的最低保護層級。基礎強化之目的在於「可於終端設定」。也就是說，可直接在Axis裝置上設定，無須靠其他網絡設備、影片或證據管理系統（VMS、EMS）、裝置或應用程式。

出廠預設設定

CSC #4：企業資產和軟體的安全組態設定

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 *退役, on page 10*。

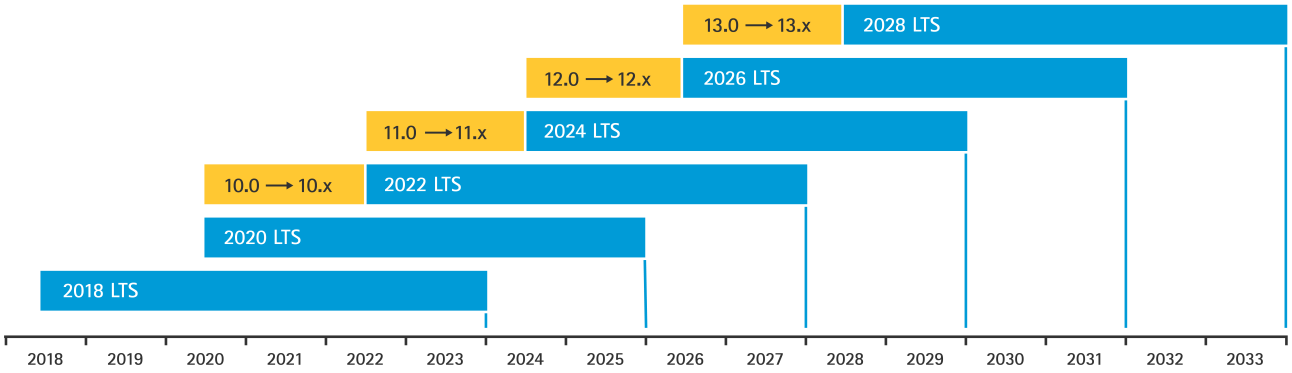
AXIS OS 版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 維護 > 預設設定
7.10	設定 > 系統 > 維護 > 預設設定
≥ 10.9	維護 > 出廠預設值

升級到最新的 AXIS OS

CSC #2：庫存和控制軟體資產

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 版本，因為它可能包含針對已知安全漏洞的安全性更新。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。雖然這兩種都包含最新的關鍵安全漏洞修補程式，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*設備軟體*，以下載您設備的 AXIS OS。

AXIS OS 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 > AXIS OS 升級

建立專用帳戶

CSC #4：企業資產和軟體的安全組態設定

CSC #5：帳號管理

Axis裝置可有兩類帳號：系統管理員和用戶端使用者。系統管理員為管理裝置的主要帳號，請務必僅指派給系統管理職務。設定裝置時，需為管理員建立使用者名稱和密碼。

除了系統管理員外，還可建立有限日常作業權限的用戶端使用者帳號。如此可讓裝置管理更安全，降低洩露裝置管理員密碼的風險。用戶端使用者帳號建議用於無須完整系統管理權限的職務。

給帳號設密碼時，建議實施NIST或BSI密碼建議標準，新密碼須夠長夠複雜。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。如需詳細資訊，請參閱 AXIS OS 知識庫中的*身分和存取管理*。

執行 AXIS OS 11.6 或更高版本的 Axis 設備支援 OAuth 2.0，可讓集中式身分和存取管理 (IAM) 及聯合身分對設備進行驗證。不需本機設備使用者管理。如需詳細資訊，請參閱 *OAuth 2.0, on page 24*。

AXIS OS 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

設定網路、日期和時間

CSC #4：CSC #8：審計日誌管理
CSC #12：網路基礎設備管理

請務必設對裝置的網路、日期和時間，維護Axis裝置功能和安全。這些設定會影響裝置紀錄的各個方面，包括網路通訊、記錄和憑證驗證。

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。每次新增元件時，請務必檢查網路拓撲。建議使用靜態IP位址，保障網路連線，並避免依賴會被攻擊的網路伺服器，例如DHCP伺服器。

AXIS OS 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

計時精確對維護系統日誌、驗證數位憑證以及啟用HTTPS、IEEE和802.1x及其他服務非常重要。建議將裝置時鐘與網路時間通訊協議(NTP)或網路時間安全(NTS)伺服器同步。網路時間安全(NTS)是網路時間通訊協議(NTP)的加密和安全變數，已新增到AXIS OS 11.1中。建議設定多個時間伺服器，提高準確度，以防萬一故障。如若無法託管當地時間伺服器，請考慮公用NTP或NTS伺服器。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 OS 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記憶卡
如果Axis裝置支援使用安全數位(SD)卡來儲存錄影，建議套用加密。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 OS 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

網路共用(NAS)
如使用網路附加儲存裝置(NAS)作為錄影裝置，建議儲存在有限存取的鎖定區域，並啟用硬碟加密。Axis 設備利用 SMB 作為網路通訊協定協定來連接到 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 OS 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

應用程式 (ACAP)

CSC #4：企業資產和軟體的安全組態設定

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 OS 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

自 AXIS OS 12.0 (2024 年 9 月) 起，ACAP 簽署是必需且預設為啟用，但可以選擇停用。自 AXIS OS 13.0 (2026 年 9 月) 起，ACAP 簽署將成為強制要求，且無法停用。ACAP 在 ACAP 入口網站中使用 SHA-512 和 4096 位元 RSA 私鑰進行簽署，該私鑰安全地儲存在瑞典隆德 Axis 資料中心的 Thales

Luna Network HSM 7 中。Axis 網路設備預先載入 4096 位元 RSA 公開金鑰，以便在安裝 ACAP 之前驗證 ACAP 簽章。公開金鑰儲存在 Axis 網路設備的 Linux 檔案系統中。

停用未使用的服務/功能

CSC #4：企業資產和軟體的安全組態設定

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。

網頁介面存取

CSC #4：企業資產和軟體的安全組態設定

CSC #5：帳號管理

Axis 設備有一個網頁伺服器，允許使用者透過標準瀏覽器存取設備。網頁介面用於組態設定、維護和故障排除，而非日常操作 (例如作為觀看影像的用戶端)。

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) 或設備管理和管理工具，例如 AXIS Device Manager。絕不允許系統使用者直接存取 Axis 設備。

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 OS 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

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 OS 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

網路發現協定

發現協定如Bonjour、UPnP、ZeroConf、WS-Discovery和LLDP/CDP 都可支援服務，更方便在網路上找到Axis裝置及服務。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 OS 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*

AXIS OS 版本	網頁介面設定路徑
	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
≥ 11.11	系統>網路>網路發現協定> LLDP和CDP**

* 該功能已在 AXIS 10.12 中移除，且無法在更新的版本中使用

**停用LLDP和CDP可能會影響PoE電源協商。

資訊揭露

預設情況下，Axis 設備會在與網路上的用戶端 HTTP(S) 連線期間，或透過基本設備資訊 VAPIX API (*https://developer.axis.com/vapix/network-video/basic-device-information/*)，公佈其目前 Apache、OpenSSL 和 AXIS OS 軟體的基本版本。

對於 Rapid7、Tenable Nessus 等網路安全掃描程式或網路監控系統而言，此資訊至關重要，可用於掃描 Axis 設備是否有未解決的安全漏洞。如果沒有該資訊，這些應用程式可能無法在 Axis 設備上正常運作。一般來說，Axis 建議將資訊揭露功能啟用並保持正常運作，協助維護 Axis 設備的軟體更新、情境感知、監控和安全操作。

然而，某些網路安全措施要求將資訊揭露控制在最低限度或完全停用。為了符合這項要求，已設定組態設定參數來停用資訊揭露。 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此項。

Apache/OpenSSL 版本

自 AXIS OS 10.6 起，提供停用 HTTP(S) 伺服器標頭的選項，以減少 HTTP(S) 連線期間的資訊暴露。

AXIS OS 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

AXIS OS 版本	網頁介面設定路徑

≥ 11.11	*https://IP_OR_HOSTNAME/config/web-ui/swagger-ui/?url=/config/discover/apis/basic-device-info/v2/openapi.json#/basic-device-info.v2beta/patch_basic_device_info_v2beta_allowAnonymous*
	
	{
	“data“: false
	}

聲音

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 OS 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 OS 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

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。從AXIS OS 5.50開始，Axis裝置支援。建議停用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 OS 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

USB

從AXIS OS 12.1開始，AXIS D1110新增停用USB連接埠的選項。讓USB插槽沒人顧還可以隨便插非常危險。

AXIS OS 版本	網頁介面設定路徑
< 7.10	N/A
7.10	N/A
≥ 12.1	系統> >配件> USB組態設定

Wi-Fi 功能

部分 Axis 設備可透過內建存取點和 USB Wi-Fi 轉接器提供 Wi-Fi 功能。只有在沒有實體 RJ45 網路連接時按下實體 [WLAN] 設定按鈕，Wi-Fi 才會啟動。無論設備處於出廠預設狀態或運作狀態，此條件均適用。在 AXIS M1075 中，使用者可以使用產品標籤上標示的 SSID 和設備唯一的 SSID 密碼連線到存取點。在部分新推出的 Axis 產品中，只需要 SSID (無需密碼)，這在不影響網路安全的前提下提升安裝體驗。

請參閱使用手冊，了解您的 Axis 設備設定及其 Wi-Fi 功能。以下說明部分支援 Wi-Fi 的 Axis 產品內建存取點功能的運作方式：

- 只有在未設定 Wi-Fi SSID/密碼且沒有實體 RJ45 網路連接的情況下，才能透過按下實體 [WLAN] 設定按鈕來啟用內建存取點。無論設備處於出廠預設狀態或運作狀態，此條件均適用。
- 攝影機連接到使用者設定的存取點後，內建存取點將停用。或者，若使用者在安裝期間按下實體 [WLAN] 設定按鈕，經過 15 分鐘後，此功能將自動停用。

如果設備使用連接的 Wi-Fi 轉接器，建議在設備初始設定期間使用 SSID + 密碼正確設定 Wi-Fi 功能，以獲得最強的安全性。

藍牙

部分 Axis 設備提供內建藍牙功能，在恢復至出廠預設值後，於設備初始狀態進行設定時，使用此功能可以讓您獲得流暢的使用體驗，例如可用於調整影像和鏡頭。

請參閱您的設備的使用手冊，了解其設定和藍牙功能。以下描述說明 Axis 產品的一般藍牙功能：

- 在出廠預設狀態，除非使用者另有設定，否則藍牙會自動啟用，並且在初始開機後保持啟用最長 2 小時。當使用者完成設定或初始開機 2 小時後，不論有無實體 RJ45 網路連接，藍牙都會自動停用。
- 藍牙停用後，使用者無法手動啟用。必須將設備重設為出廠預設狀態，才能恢復藍牙功能。
- 您的設備與 Axis 攝影機之間的藍牙連線使用 HTTPS 隧道，該隧道採用最新的 TLS 1.2/1.3 加密技術。不需要或使用其他內建藍牙安全功能。

限制網路存取

CSC #1：企業資產的庫存和控制
CSC #4：企業資產和軟體的安全組態設定

CSC #13：網路監控與防禦

AXIS OS 11.9 引入主機式防火牆，這項安全功能可建立規則，由 IP 位址和 TCP/UDP 連接埠號來規範傳入流量。可防裝置服務被偷窺盜用。

如果將預設政策設定為「置放」，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 OS 版本	網頁介面設定路徑
≥ 11.9	系統 > 安全 > 防火牆

IP 位址過濾

使用AXIS OS 11.8以前舊的裝置以IP位址篩選，以防偷窺盜用。建議將設備設為允許授權的網路主機 IP 位址，您也可以拒絕未經授權的 IP 位址。

如允許IP位址，請務必將所有授權用戶端（包括VMS伺服器和管理用戶端）新增到清單中。

AXIS OS 版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 安全 > IP 位址過濾
7.10	設定 > 系統 > TCP/IP > IP 位址過濾
10.9 ¡X 11.8	設定 > 安全 > IP 位址過濾

附註

可啟用網路存取嘗試的詳細紀錄，辨識其他網路主機的竊取行為。啟用請前往 系統 > 一般設定 > 網路和網路過濾日誌。

HTTPS

CSC #3：資料保護

從AXIS OS 7.20開始，Axis裝置預設會啟用HTTP和HTTPS。雖然HTTP存取不安全且完全沒有加密，但HTTPS會加密用戶端與Axis裝置之間的流量。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 *僅 HTTPS, on page 20*和 *HTTPS 密碼, on page 21*。

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，有效期至 2038 年 1 月 19 日。雖然自我簽署的憑證在設計上不受被信任，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 版本	網頁介面設定路徑
< 7.10	設定 > 系統選項 > 安全 > HTTPS
7.10	設定 > 系統 > 安全 > 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。所有定期AXIS OS更新期間，可能會更新Axis裝置的可用密碼清單，但不會變更實際的密碼組態設定。變更密碼須由使用者啟動，無論執行Axis還原出廠預設還是手動變更使用者組態設定。從AXIS OS 10.8版開始，執行AXIS OS更新時會自動更新密碼清單。

TLS 1.2 及更低版本

TLS 1.2以下版本可指定Axis裝置重新啟動後要使用的HTTPS密碼。密碼沒有任何限制，但推薦用以下加強密碼：

```
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
```

AXIS OS 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。

擴展強化

擴展強化的說明是依據 *預設保護, on page 4*和 *基本強化, on page 13*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。

限制網際網路和網絡曝光

CSC #12：網路基礎設備管理

請勿將Axis裝置設為公共網路伺服器公開，或讓未知用戶端以其他方式網路存取這台裝置。不使用影片管理軟體(VMS)或需遠端存取影片的小組和個人，AXIS Camera Station Edge是不錯的選擇。

AXIS Camera Station Edge可在Windows、iOS和Android上免費使用，提供簡便的影片安全存取，無需將裝置發佈到網路上。如需更多資訊，請參閱 *axis.com/products/axis-camera-station-edge*。

附註

如貴單位使用虛擬機，請諮詢該方廠商遠端視訊存取相關建議。

隔離網路裝置及相關基礎設備和應用程式，預防網路曝光。

建議將Axis裝置和相關基礎設備和應用程式裝在與生產服務網隔離的本機網絡上。

若要套用基礎強化，請使用各種網路安全機制，保護區域網路及基礎設備（路由器、交換器），避免偷窺。其中包括VLAN分段、限制路由功能、站至站或WAN存取的VPN、網路第2、3層防火牆，以及存取控制清單(ACL)。

若要擴展基礎強化，請採用先進的網路檢查技術，例如深度封包檢查和入侵偵測。加強網路內的威脅防護。提醒您，強化網路防護通常需專門的軟硬體。

網路漏洞掃描

CSC #1：企業資產的庫存和控制
CSC #12：網路基礎設備管理

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 OS 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透過報修單提交至 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：網路基礎設備管理

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和用戶端憑證。配備已驗證信任鏈的CA簽署憑證可在使用者以HTTPS連線時移除瀏覽器憑證警告。部署網路存取控制(NAC)方案時，CA簽署的憑證也能確認Axis裝置真假。這可以降低攻擊電腦冒充 Axis 設備的風險。

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。

遠端 syslog

CSC #8：審計日誌管理

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 OS 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

SNMP

CSC #3：資料保護
CSC #8：審計日誌管理

您可以將 Axis 設備設定為透過 SNMPv3 將加密的 SNMP 健康狀況監控資料傳送到中央 SNMP 伺服器。基於 SNMP 的網路監控讓您能建立警示，以及長時間監控設備。請注意，只有 SNMPv3 提供加密和隱私保護，因此我們非常建議優先採用此版本，而不是 SNMPv1 和 SNMPv2c。

請在 AXIS OS 知識庫中閱讀更多關於 *SNMP* 的資訊。

AXIS OS 版本	網頁介面設定路徑
< 7.10	如需說明，請參閱 AXIS OS 知識庫中的 *SNMP*。
7.10	設定 > 系統 > 網路 > SNMP
≥ 10.9	系統 > 網路 > SNMP

安全影像串流 (SRTP/RTSPS)

CSC #3：資料保護

從AXIS OS 7.40開始，Axis裝置支援以RTP串流安全影片，也稱為SRTP/RTSPS。SRTP/RTSPS使用安全的端到端加密傳輸方法，讓只有授權用戶端才能從Axis裝置接收影片串流。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。

附註

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 OS 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，Axis 設備可以藉此向其影像串流新增簽章，以確保影像完好無損，並透過將其追溯至原始產生設備來驗證其來源。

Axis 提供 *Axis Signed media verifier* 工具，可讓使用者驗證 Axis 設備的錄影內容真實性。我們提供以下三個範例檔案，協助您探索此工具。

- *原始但未簽署的影像*
- *原始且已簽署的影像*
- *經篡改的影像*

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 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

OAuth 2.0

CSC #4：企業資產和軟體的安全組態設定
CSC #5：帳號管理

使用 OAuth 2.0，您可以將執行 AXIS OS 11.6 或更高版本的 AXIS OS 設備整合到集中式身分和存取管理 (IAM) 服務的 IT 基礎架構。讓您能以聯合身分對 Axis 設備進行驗證，而不需本機設備使用者管理。

OAuth 透過使用唯一標記確保每個請求皆有效，降低遭 CSRF 攻擊的風險。

視服務供應商的特色而定，您可以對 Axis 設備使用下列強化身分驗證的安全機制：

- 多重身分驗證 (MFA)
- 強制執行密碼複雜性
- 密碼旋轉
- 限時驗證
- 集中式身分 (使用者/服務帳戶) 管理

如需如何在 AXIS OS 設備中啟用及設定 OAuth 2.0 的詳細資訊，請參閱 AXIS OS 知識庫中的 *OAuth 2.0 OpenID Connect*。

AXIS OS 版本	網頁介面設定路徑
< 7.10	N/A
7.10	N/A
≥ 11.6	系統 > 帳戶 > OpenID 組態設定

實體防竄改配件

CSC #1：企業資產的庫存和控制
CSC #12：網路基礎設備管理

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*

舊版強化

本節涵蓋舊版 AXIS OS 版本或產品中的安全參數設定強化說明。在較新或最新的 LTS 軌道或主動式軌道中找不到這些參數。

腳本編輯器環境

我們建議您停用對於指令碼編輯器環境的存取。腳本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 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)

FTP 存取

FTP通訊協議不安全，僅用於故障排除和除錯目的。FTP存取已從AXIS OS 11.1中刪除，並且在更高版本中不可使用。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 OS 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

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。版本比AXIS OS 5.50舊的Axis裝置支援這個功能。建議停用Telnet存取。

AXIS OS 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*設備存取*。
< 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 OS 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

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，但仍可在 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。

自 AXIS OS 12.0 起，已移除過時的 TLS 版本，且無法在更高版本中使用。

AXIS OS 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 — 11.11.X	系統 > 一般設定 > HTTPS > 允許 TLSv1.0 和/或允許 TLSv1.1

存取日誌

CSC #1：企業資產的庫存和控制
CSC #8：審計日誌管理

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 OS 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

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 *基本強化, on page 13*中讀到的強化主題，然而，並未涵蓋 *擴展強化, on page 22*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

附註

下列常見設定錯誤可能會增加 Axis 設備的攻擊面並減少其網路安全防禦層，導致設備被利用、誤用或不安全操作的風險提高。

裝置網路曝光
CSC #12：網路基礎設備管理

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組態設定
CSC #5：帳號管理

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。如需說明，請參閱 AXIS OS 知識庫中的*身分和存取管理*，以及 *建立專用帳戶, on page 13*。

匿名存取
CSC #4：企業資產和軟體的安全組態設定
CSC #5：帳號管理。

我們不建議您允許匿名使用者在不必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 *預設為停用, on page 4*。

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 *已啟用 HTTPS, on page 7*。如需組態建議事項，請參閱 *摘要式驗證, on page 4*。

AXIS OS 版本過時
CSC #2：庫存和控制軟體資產

我們強烈建議您在 LTS 或主動式軌道上使用最新可用的 AXIS OS 版本來操作 Axis 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 *升級到最新的 AXIS OS, on page 13*。

透過 VAPIX API 進行基本強化

您可以使用 VAPIX API，根據 *基本強化, on page 13* 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組態設定，無論 Axis 設備的 AXIS OS 版本為何。

在您的設備的 AXIS OS 版本中已不再能夠使用某些組態設定，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 OS 版本中已不再能夠使用。

目的	VAPIX API 調用
*停用未使用網路連接埠中的 POE**	`http://ip-address/axis-cgi/nvr/poe/setportmode.cgi?port=X&enabld=no`
*停用未使用網路連接埠中的網路流量***	`http://ip-address/axis-cgi/network_settings.cgi { "apiVersion": "1.17", "method": "setDeviceConfiguration", "params": { "deviceName": "eth1.1", "staticState": "down" } }`
停用 Bonjour 探索通訊協定	`https://ip-address/axis-cgi/param.cgi?action=update&Network.Bonjour.Enabled=no`
停用 UPnP 探索通訊協定	`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`
停用 WebService 探索通訊協定	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.DiscoveryMode.Discoverable=no`
停用單鍵雲端連線 (O3C)	`https://ip-address/axis-cgi/param.cgi?action=update&RemoteService.Enabled=no`
停用設備 SSH 維護存取	`https://ip-address/axis-cgi/param.cgi?action=update&Network.SSH.Enabled=no`
停用設備 FTP 維護存取	`https://ip-address/axis-cgi/param.cgi?action=update&Network.FTP.Enabled=no`
停用 ARP-Ping IP 位址設定	`https://ip-address/axis-cgi/param.cgi?action=update&Network.ARPPingIPAddress.Enabled=no`
停用 Zero-Conf IP 位址設定	`http://ip-address/axis-cgi/param.cgi?action=update&Network.ZeroConf.Enabled=no`
僅啟用 HTTPS	`https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.admin=https` `https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.operator=https` `https://ip-address/axis-cgi/param.cgi?action=update&System.BoaGroupPolicy.viewer=https`
僅啟用 TLS 1.2 和 TLS 1.3	`https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS1=no` `https://ip-address/axis-cgi/param.cgi?action=update&HTTPS.AllowTLS11=no`

目的	VAPIX API 調用
TLS 1.2 安全密碼設定	`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`

*啟用暴力破解攻擊保護***	`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`

停用腳本編輯器環境	`https://ip-address/axis-cgi/param.cgi?action=update&System.EditCgi=no`
啟用改善的使用者存取日誌記錄	`https://ip-address/axis-cgi/param.cgi?action=update&System.AccessLog=On`
啟用 ONVIF 重播攻擊保護	`https://ip-address/axis-cgi/param.cgi?action=update&WebService.UsernameToken.ReplayAttackProtection=yes`
停用設備網頁介面存取	`https://ip-address/axis-cgi/param.cgi?action=update&System.WebInterfaceDisabled=yes`
停用 HTTP/OpenSSL 伺服器標頭	`https://ip-address/axis-cgi/param.cgi?action=update&System.HTTPServerTokens=no`

停用匿名觀看者和 PTZ 存取	`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`

目的	VAPIX API 調用
防止安裝需要 root 權限的 ACAP 應用程式	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowRoot&value=false`
防止安裝未簽署的 ACAP 應用程式	`http://ip-address/axis-cgi/applications/config.cgi?action=set&name=AllowUnsigned&value=false`

*將「X」替換為「port=X」中的實際連接埠號碼。例如：「port=1」將停用1號連接埠 ，「port=2」停用2號連接埠。
**將「1」替換為「eth1.1」中的實際連接埠號碼。例如：「eth1.1」將停用1號連接埠，「eth1.2」將停用2號連接埠。
***在1秒內試誤登入失敗20次後，用戶端IP位址會封鎖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。

透過 AXIS Device Manager (Extend) 進行基本強化

您可以使用 AXIS Device Manager 和 AXIS Device Manager Extend，根據 *基本強化, on page 13*中涵蓋的主題強化 Axis 設備。使用此*設定檔案* (由在 *透過 VAPIX API 進行基本強化, on page 27*中列出的相同組態設定組成)。

在您的設備的 AXIS OS 版本中已不再能夠使用某些組態設定，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。

附註

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。

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。

T10177717_zh_tw

2026-03 (M62.2)