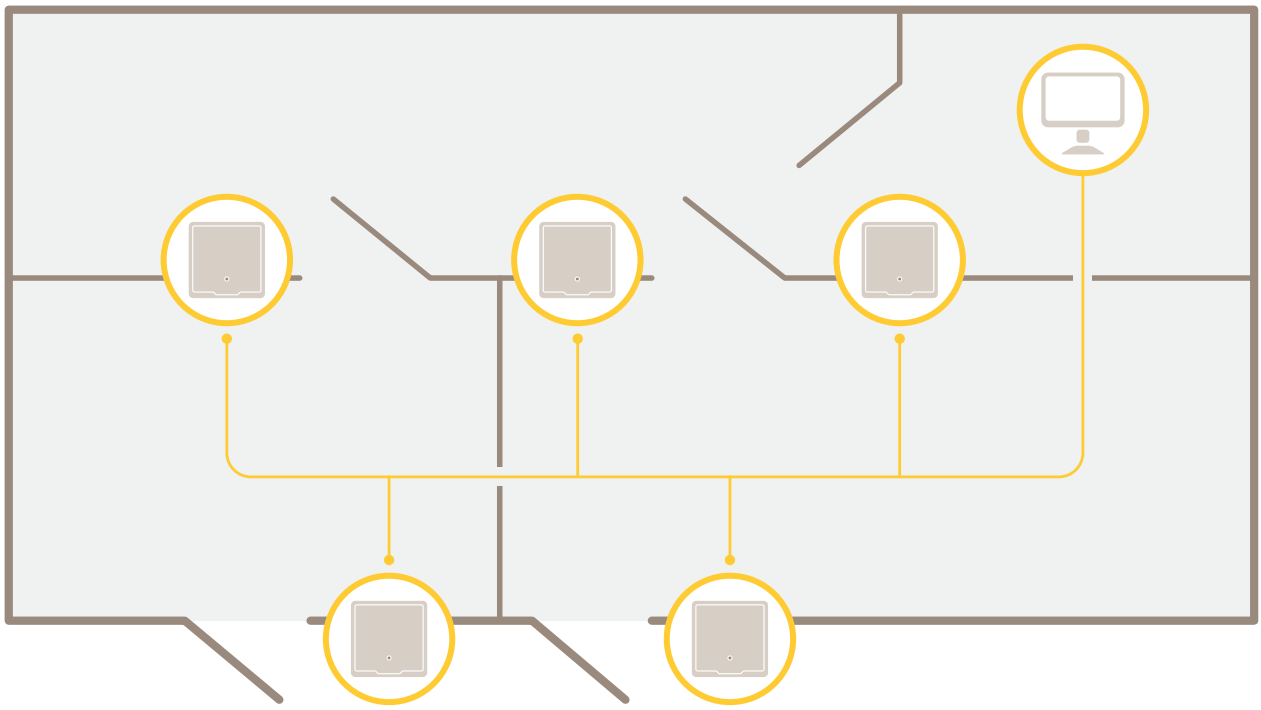
AXIS A1610-B Network Door Controller

使用手冊

目錄

解決方案總覽



網路門禁控制器可以輕鬆地和現有 IP 網路連接並由 IP 網路供電，無需進行特殊佈線。

每個網路門禁控制器都是可輕鬆安裝在門附近的智慧型裝置。它最多可以為四個讀卡機供電並加以控制。

開始使用

在網路上尋找裝置

若要在網路上尋找 Axis 設備，並在 Windows® 中為其指派 IP 位址，請使用 AXIS IP Utility 或 AXIS Device Manager。這兩個應用程式都可從 *axis.com/support* 免費下載。

如需有關如何尋找和指派 IP 位址的詳細資訊，請前往*如何指派 IP 位址以及存取您的設備*。

瀏覽器支援

您可以透過下列瀏覽器使用設備：

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
其他作業系統	*	*	*	*

✓：建議

*：支援，但有限制

開啟設備的網頁介面

1. 開啟瀏覽器，然後輸入 Axis 設備的 IP位址或主機名稱。
   如果您不知道 IP 位址，請使用 AXIS IP Utility 或 AXIS Device Manager，在網路上尋找設備。
2. 請鍵入使用者名稱和密碼。如果是第一次存取設備，必須建立管理員帳戶。請參考 。

有關設備網頁介面中的所有控制項和選項的說明，請參閱 。

建立管理員帳戶

首次登入設備必須建立管理員帳戶。

1. 請輸入使用者名稱。
2. 請輸入密碼。請參考 。
3. 重新輸入密碼。
4. 接受授權合約。
5. 按一下 [Add account (新增帳戶)]。

重要

設備沒有預設帳戶。如果您遺失了管理員帳戶的密碼，則必須重設設備。請參考 。

安全密碼

重要

使用 HTTPS (預設啟用) 透過網路設定密碼或其他敏感設定。HTTPS 支援安全和加密的網路連線，藉此保護敏感資料，例如密碼。

設備密碼是您的資料和服務的主要保護機制。Axis 裝置不會強制實施密碼原則，因為它們可能在各種類型的安裝中使用。

為了保護您的資料，我們強烈建議您採取以下措施：

- 使用至少包含 8 個字元的密碼，最好是由密碼產生器所建立。
- 不要洩露密碼。
- 定期變更密碼，至少一年變更一次。

請確定沒有人竄改設備軟體

若要確保設備有其原始 AXIS OS，或要在安全攻擊後完全控制設備：

1. 重設為出廠預設設定。請參考 。
   重設後，安全開機可保證回復設備的狀態。
2. 對裝置進行設定和安裝。

網頁介面概觀

這段影片為您提供設備網頁介面的概觀。

Axis 裝置網頁介面

設定您的設備

有關設備的設定方式，請參閱 *AXIS Camera Station 使用手冊*或第三方解決方案。

新增 AXIS A9910

- 在門控制器的網頁介面中，前往 [Device (設備) > I/Os and relays (I/O 和繼電器)]。
- 按一下 [Add encryption key (新增加密金鑰)]。
- 若您之前已經產生加密金鑰，請輸入該金鑰並按一下 [OK (確認)]。
- 若要產生加密金鑰：
  - 按一下 [Generate key (產生金鑰)]。
  - 按一下 [Export key (匯出金鑰)] 可儲存該金鑰。如果加密金鑰遺失，您將無法存取該設備。
  - 按一下OK (確認)。
- 按一下 [Add AXIS A9910 (新增 AXIS A9910)]。
- 輸入名稱並選取 RS485 連接埠以及要使用的位址。
- 按一下OK (確認)。

電梯控制

在電梯艙內安裝讀卡機後，您可以使用門控制器和 AXIS A9910 控制進入樓層的權限。請參閱。

透過連結到單一門控制器和 AXIS A9910 擴充模組，最多可以連接 16 個樓層：

- 擴充模組使用控制器上的一個讀卡機連接埠。
- 另一個讀卡機連接埠由放置在電梯艙內的讀卡機使用。

網頁介面

在網頁瀏覽器中輸入該設備的 IP 位址，就可連上該設備的網頁介面。

附註

對本節中所述功能及設定的支援會因裝置不同而有所不同。此圖示 表示該功能或設定僅適用於部分設備。

顯示或隱藏主功能表。

存取版本須知。

存取產品說明。

變更語言。

設定淺色或深色主題。

使用者功能表包含：

- 登入的使用者相關資訊。
- [Change account (變更帳戶)]：登出目前帳戶並登入新帳戶。
- [Log out (登出)]：從目前帳戶登出。

內容功能表包含：

- [Analytics data (分析資料)]：接受可共用非個人瀏覽器資料。
- [Feedback (意見反應)]：分享任何意見反應，以協助我們改善使用者體驗。
- [Legal (法律資訊)]：檢視有關 Cookie 和授權的資訊。
- [About (關於)]：檢視設備資訊，包括 AXIS OS 版本和序號。

狀態

設備資訊

顯示該設備的 AXIS OS 版本和序號等資訊。

[Upgrade AXIS OS (升級 AXIS 作業系統)]：升級您的設備軟體。前往可用來進行升級的 [維護] 頁面。

時間同步狀態

顯示 NTP 同步資訊，包括裝置是否與 NTP 伺服器同步以及下次同步前的剩餘時間。

[NTP settings (NTP 設定)]：檢視和更新 NTP 設定。前往可變更 NTP 設定的 [Time and location (時間和地點)] 頁面。

安全

顯示已啟用設備的存取類型、正在使用的加密協議以及是否允許未簽署的應用程式。設定建議依據 AXIS OS 強化指南。

[Hardening guide (強化指南)]：連結至 *AXIS OS 強化指南*，以深入了解 Axis 設備上的網路安全和最佳實踐。

已連接的用戶端

顯示連線數和已連線的用戶端數。

[View details (檢視詳細資訊)]：檢視並更新已連接用戶端的清單。此清單顯示每個連接的 IP 位址、通訊協定、連接埠、狀態和 PID/流程。

裝置

I/O 和繼電器

AXIS A9910

[+ Add encryption key (新增加密金鑰)]：按一下即可設定加密金鑰，確保通訊加密。

[+ Add AXIS A9910 (新增 AXIS A9910)]：按一下可新增擴充模組。

- [Name (名稱)]：編輯文字以重新命名該擴充模組。
- [Address (位址)]：顯示擴充模組所連接的位址。
- [Device software version (設備軟體版本)]：顯示擴充模組的目前軟體版本。
- [Upgrade device software (升級設備軟體)]：按一下可升級擴充模組軟體。您可以選擇升級到門控制器附帶的版本，或上傳您選擇的版本。

I/O

I/O：當連接埠設定為輸出時，開啟以啟動已連接的設備。

- [Name (名稱)]：編輯文字以重新命名該連接埠。
- [方向]：按一下 或 以設定為輸入或輸出。
- [Normal state (正常狀態)]：開路請按一下 ，閉路請按一下 。
- 受監控：如果有人竄改與數位 I/O 裝置的連線，請開啟此選項，讓裝置可以偵測和觸發動作。除了偵測輸入是開路還是閉路之外，您還可以偵測是否有人對其進行竄改 (即切斷或短路)。若要監控連線，必須在外部 I/O 迴路中附加其他硬體 (線路終端電阻器)。只有當連接埠設定為輸入時才會出現。
  - 如要使用第一並聯連接，請選取使用 22 KΩ 並聯電阻和 4.7 KΩ 串聯電阻的第一並聯連接。
  - 如要使用第一串聯連接，請選取第一串聯連接並從電阻值下拉式清單中選取一個電阻值。
- 切換連接埠 URL：顯示透過 VAPIX® 應用程式開發介面啟動和停用已連接設備的 URL。只有當連接埠設定為輸出時才會出現。

繼電器

- 繼電器：開啟或關閉繼電器。
- [Name (名稱)]：編輯文字以重新命名該繼電器。
- [方向]：指明它是一個輸出繼電器。
- 切換連接埠 URL：顯示透過 VAPIX® 應用程式開發介面啟動和停用繼電器的 URL。

警報

設備位移：開啟以在偵測到設備移動時觸發系統警報。

外殼開啟：開啟以在偵測到打開的門控制器外殼時觸發系統警報。關閉準系統門控制器的此設定。

外部篡改：開啟以在偵測到外部篡改時觸發系統中的警報。例如，有人開啟或關閉外部機箱時。

- 監督式輸入：開啟以監控輸入狀態並設定線路終端電阻器。
  - 如要使用第一並聯連接，請選取使用 22 KΩ 並聯電阻和 4.7 KΩ 串聯電阻的第一並聯連接。
  - 如要使用第一串聯連接，請選取第一串聯連接並從電阻值下拉式清單中選取一個電阻值。

周邊設備

讀卡機

新增讀卡機：按一下可新增讀卡機。

AXIS A4612：您最多可以為控制器新增 16 台藍牙讀卡機，而不需要授權。

- [Name (名稱)]：輸入讀卡機名稱。
- 讀卡機：從下拉式選單選擇讀卡機。
- [IP address (IP 位址)]：輸入讀卡機主機的 IP 位址。
- [Username (使用者名稱)]：輸入讀卡機的使用者名稱。
- [Password (密碼)]：輸入讀卡機的密碼。
- 忽略伺服器憑證驗證：開啟即可略過驗證。
- [I/O ports and relays (I/O 埠和繼電器)]：展開以設定 I/O 埠和繼電器。
  - [Port (連接埠)]：顯示連接埠的名稱。
  - [方向]：指明這是一個輸入埠或輸出埠。
  - [Normal state (正常狀態)]：開路請按一下  ，閉路請按一下  。

AXIS License Plate Verifier (需要在 AXIS Camera Station 中重新設定)

- [Name (名稱)]：輸入讀卡機名稱。
- [API-key (API 金鑰)]：輸入 API 金鑰。
- [Generate (產生)]：按一下可產生 API 金鑰。
- [Copy API-key (複製 API 金鑰)]：按一下可複製 API 金鑰並儲存到安全位置。

AXIS Barcode Reader (需要在 AXIS Camera Station 中重新設定)

- [Name (名稱)]：輸入讀卡機名稱。
- [API-key (API 金鑰)]：輸入 API 金鑰。
- [Generate (產生)]：按一下可產生 API 金鑰。
- [Copy API-key (複製 API 金鑰)]：按一下可複製 API 金鑰並儲存到安全位置。

Axis 對講讀卡機 (需要在 AXIS Camera Station 中重新設定)

- [Name (名稱)]：輸入讀卡機名稱。
- 讀卡機：從下拉式選單選擇讀卡機。
- [IP address (IP 位址)]：輸入讀卡機主機的 IP 位址。
- [Username (使用者名稱)]：輸入讀卡機的使用者名稱。
- [Password (密碼)]：輸入讀卡機的密碼。
- 忽略伺服器憑證驗證：開啟即可略過驗證。

[Edit (編輯)]：選取一個讀卡機並按一下 [Edit (編輯)] 可對所選讀卡機進行變更。

[Delete (刪除)]：選取讀卡機並按一下 [Delete (刪除)] 可刪除所選讀卡機。

無線鎖

使用 AH30 通訊集線器可以連接最多 16 個 ASSA ABLOY Aperio 無線鎖。無線鎖需要授權。

附註

您必須將 AH30 通訊集線器安裝在安全側。

連接通訊集線器：按一下可連接無線鎖。

升級

升級讀卡機：按一下可升級讀卡機軟體。只有在支援的讀卡機上線時才能升級。

[Upgrade converters (升級轉換器)]：按一下可升級轉換器軟體。只有在支援的轉換器上線時才能升級。

應用程式

[Add app (新增應用程式)]：安裝新增應用程式。

[Find more apps (搜尋更多應用程式)]：尋找更多要安裝的應用程式。您將進入 Axis 應用程式的概觀頁面。

[Allow unsigned apps (允許未簽署的應用程式)]：開啟以允許安裝未簽署的應用程式。

查看 AXIS OS 和 ACAP 應用程式中的安全性更新。

附註
如果同時執行數個應用程式，設備的效能可能會受到影響。

使用應用程式名稱旁邊的開關啟動或停止應用程式。

[Open (開啟)]：存取該應用程式的設定。可用的設定會根據應用程式而定。部分應用程式無任何設定。

內容功能表可以包含以下一個或多個選項：

- [Open-source license (開放原始碼授權)]：檢視有關應用程式中使用的開放原始碼授權的資訊。
- [App log (應用程式記錄)]：檢視應用程式事件記錄。當您聯絡支援人員時，此記錄會很有幫助。
- [Activate license with a key (用金鑰啟用授權)]：如果應用程式需要授權，您需要啟用授權。如果您的設備無法網際網路存取，請使用此選項。
  如果您沒有授權金鑰，請前往 *axis.com/products/analytics*。您需要授權代碼和 Axis 產品序號才可產生授權金鑰。
- [Activate license automatically (自動啟用授權)]：如果應用程式需要授權，您需要啟用授權。如果您的設備可以存取網際網路，請使用此選項。您需要授權代碼，才可以啟用授權。
- [Deactivate the license (停用授權)]：停用授權以將其替換為其他授權，例如，當您從試用授權變更為完整授權時。如果您停用授權，也會將該授權從裝置中移除。
- [Settings (設定)]：設定參數。
- [Delete (刪除)]：從裝置永久刪除應用程式。如果您不先停用授權，授權仍會繼續啟用。

系統

時間和地點

日期和時間

時間格式取決於網路瀏覽器的語言設定。

附註

我們建議您將該設備的日期和時間與 NTP 伺服器同步。

[Synchronization (同步)]：選取同步該設備的日期和時間的選項。

- [Automatic date and time (PTP) (自動日期和時間 (PTP))]：使用精確時間通訊協定同步。
- [Automatic date and time (manual NTS KE servers) (自動日期和時間 (手動 NTS KE 伺服器))]：與連線到 DHCP 伺服器的安全 NTP 金鑰建置伺服器同步。
  - [Manual NTS KE servers (手動 NTS KE 伺服器)]：輸入一台或兩台 NTP 伺服器的 IP 地址。使用兩台 NTP 伺服器時，設備會根據兩者的輸入同步和調整其時間。
  - [Trusted NTS KE CA certificates 受信任的 NTS KE CA 憑證]：選取用於安全 NTS KE 時間同步的受信任 CA 憑證，或維持為「無」。
  - [Max NTP poll time (NTP 輪詢時間上限)]：選取設備在輪詢 NTP 伺服器，以取得更新時間前，其應等候的時間上限。
  - [Min NTP poll time (NTP 輪詢時間下限)]：選取設備在輪詢 NTP 伺服器，以取得更新時間前，其應等候的時間下限。
- [Automatic date and time (NTP servers using DHCP) (自動日期和時間 (使用 DHCP 的 NTP 伺服器))]：與連線到 DHCP 伺服器的 NTP 伺服器同步。
  - [Fallback NTP servers (備援 NTP 伺服器)]：輸入一台或兩台備援伺服器的 IP 位址。
  - [Max NTP poll time (NTP 輪詢時間上限)]：選取設備在輪詢 NTP 伺服器，以取得更新時間前，其應等候的時間上限。
  - [Min NTP poll time (NTP 輪詢時間下限)]：選取設備在輪詢 NTP 伺服器，以取得更新時間前，其應等候的時間下限。
- Automatic date and time (manual NTP servers) (自動日期和時間 (手動 NTP 伺服器))：與您選擇的 NTP 伺服器同步。
  - [Manual NTP servers (手動 NTP 伺服器)]：輸入一台或兩台 NTP 伺服器的 IP 地址。使用兩台 NTP 伺服器時，設備會根據兩者的輸入同步和調整其時間。
  - [Max NTP poll time (NTP 輪詢時間上限)]：選取設備在輪詢 NTP 伺服器，以取得更新時間前，其應等候的時間上限。
  - [Min NTP poll time (NTP 輪詢時間下限)]：選取設備在輪詢 NTP 伺服器，以取得更新時間前，其應等候的時間下限。
- [Custom date and time (自訂日期和時間)]：手動設定日期和時間。按一下 [Get from system (從系統取得)]，以從您的電腦或行動設備擷取日期和時間設定。

[Time zone (時區)]：選取要使用的時區。時間將自動調整至日光節約時間和標準時間。

- [DHCP]：採用 DHCP 伺服器的時區。設備必須連接到 DHCP 伺服器，才能選取此選項。
- [Manual (手動)]：從下拉式清單選取時區。

附註

系統在所有錄影、記錄和系統設定中使用該日期和時間設定。

裝置位置

輸入裝置的所在位置。您的影像管理系統可以根據這項資訊，將裝置放於地圖上。

- [Latitude (緯度)]：赤道以北的正值。
- [Longitude (經度)]：本初子午線以東的正值。
- [Heading (指向)]：輸入裝置朝向的羅盤方向。0 代表正北方。
- [Label (標籤)]：輸入設備的描述性名稱。
- [Save (儲存)]：按一下以儲存您的裝置位置。

網路

IPv4

[Assign IPv4 automatically (自動指派 IPv4)]：選取 IPv4 自動 IP (DHCP) 以允許網路自動指派您的 IP 位址、子網路遮罩和路由器，無需手動設定。我們建議大多數網路使用自動 IP 指派 (DHCP)。

[IP address (IP 位址)]：輸入設備的唯一 IP 位址。您可以在隔離的網路內任意指派固定 IP 位址，但每個位址都必須是唯一的。為了避免發生衝突，建議您在指派固定 IP 位址之前先聯絡網路管理員。

[Subnet mask (子網路遮罩)]：請輸入子網路遮罩定義局部區域網路內的位址。局部區域網路以外的任何位址都會經過路由器。

[Router (路由器)]：輸入預設路由器 (閘道) 的 IP 位址，此路由器用於連接與不同網路及網路區段連接的設備。

[Fallback to static IP address if DHCP isn't available (如果 DHCP 無法使用，則以固定 IP 位址為備援)]：如果 DHCP 無法使用且無法自動指派 IP 位址，請選取是否要新增固定 IP 位址以用作備援。

附註

如果 DHCP 無法使用且設備使用固定位址備援，則固定位址將設定為有限範圍。

IPv6

[Assign IPv6 automatically (自動指派 IPv6)]：選取以開啟 IPv6，以及允許網路路由器自動為設備指派 IP 位址。

主機名稱

[Assign hostname automatically (自動分配主機名稱)]：選取才能讓網路路由器自動為設備指派主機名稱。

[Hostname (主機名稱)]：手動輸入主機名稱，當成是存取設備的替代方式。伺服器報告和系統記錄使用主機名稱。允許的字元有 A-Z、a-z、0-9 和 -。

[Enable dynamic DNS updates (啟用動態 DNS 更新)]： 允許您的裝置在 IP 位址變更時自動更新其網域名稱伺服器記錄。

[Register DNS name (註冊 DNS 名稱)]：輸入指向您裝置的 IP 位址的唯一網域名稱。允許的字元有 A-Z、a-z、0-9 和 -。

[TTL]：存活時間 (TTL) 設定 DNS 記錄在需要更新之前保持有效的時間。

DNS 伺服器

[Assign DNS automatically (自動指派 DNS)]：選取以允許 DHCP 伺服器自動將搜尋網域和 DNS 伺服器位址指派給設備。我們建議適用大多數網路的自動 DNS (DHCP)。

[Search domains (搜尋網域)]：使用不完整的主機名稱時，請按一下 [Add search domain (新增搜尋網域)]，並輸入要在其中搜尋該設備所用主機名稱的網域。

[DNS servers (DNS 伺服器)]：點選 [Add DNS server (新增 DNS 伺服器)]，並輸入 DNS 伺服器的 IP 位址。此選項可在您的網路上將主機名稱轉譯成 IP 位址。

附註

如果 DHCP 已停用，依賴自動網路設定的功能 (例如主機名稱、DNS 伺服器、NTP 等) 可能會停止運作。

HTTP 和 HTTPS

HTTPS 是一種通訊協定，可為使用者的頁面要求例外網頁伺服器傳回的頁面提供加密。加密的資訊交換使用保證伺服器真確性的 HTTPS 憑證進行管制。

若要在裝置上使用 HTTPS，您必須安裝 HTTPS 憑證。前往 [System (系統) > Security (安全性)] 以建立並安裝憑證。

[Allow access through (允許存取方式)]：選取允許使用者連線至設備所透過的方法是 [HTTP]、[HTTPS] 還是 [HTTP and HTTPS (HTTP 與 HTTPS)] 通訊協定。

附註

如果透過 HTTPS 檢視加密的網頁，則可能會發生效能下降的情況，尤其是在您第一次要求頁面時，更明顯。

[HTTP port (HTTP 連接埠)]：輸入要使用的 HTTP 連接埠。該設備允許連接埠 80 或 1024-65535 範圍內的任何連接埠。如果以管理員身分登入，您還可以輸入任何在 1-1023 範圍內的連接埠。如果您使用此範圍內的連接埠，就會收到警告。

[HTTPS port (HTTPS 連接埠)]：輸入要使用的 HTTPS 連接埠。該設備允許連接埠 443 或 1024-65535 範圍內的任何連接埠。如果以管理員身分登入，您還可以輸入任何在 1-1023 範圍內的連接埠。如果您使用此範圍內的連接埠，就會收到警告。

[Certificate (憑證)]：選取憑證來為設備啟用 HTTPS。

網路發現協定

[Bonjour®]：啟用此選項可允許在網路上自動搜尋。

[Bonjour name (Bonjour 名稱)]：輸入可在網路上看到的易記名稱。預設名稱為裝置名稱和 MAC 位址。

[UPnP®]：啟用此選項可允許在網路上自動搜尋。

[UPnP name (UPnP 名稱)]：輸入可在網路上看到的易記名稱。預設名稱為裝置名稱和 MAC 位址。

[WS-Discovery (WS 發現)]：啟用此選項可允許在網路上自動搜尋。

[LLDP and CDP (LLDP 和 CDP)]：啟用此選項可允許在網路上自動搜尋。關閉 LLDP 和 CDP 可能會影響 PoE 功率交涉。若要解決 PoE 功率交涉的任何問題，請將 PoE 交換器配置為僅用於硬體 PoE 功率交涉。

單鍵雲端連線

單鍵雲端連線 (O3C) 與 O3C 服務一起提供輕鬆且安全的網際網路連線，讓您可以從任何位置存取即時和錄影的影像。如需詳細資訊，請參閱 *axis.com/end-to-end-solutions/hosted-services*。

[Allow O3C (允許 O3C)]：

- [One-click (單鍵)]：此為預設選項。若要連接 O3C，請按下設備上的控制按鈕。根據設備型號，按下並放開或按住，直到狀態 LED 燈號閃爍。在 24 小時內向 O3C 服務註冊設備以啟用 [Always (永遠)] 並保持連線。若未註冊，設備會中斷與 O3C 的連線。
- [Always (永遠)]：該設備會持續嘗試透過網際網路連線至 O3C 服務。註冊該設備後，它就會保持連線。如果控制按鈕位於接觸不到的位置，請使用這個選項。
- [No (否)]：中斷與 O3C 服務的連線。

[Proxy settings (代理伺服器設定)]：如有需要，輸入 Proxy 設定以連線至 proxy 伺服器。

[Host (主機)]：輸入 Proxy 伺服器的位址。

[Port (連接埠)]：輸入用於存取的連接埠號碼。

[Login (登入)] 和 [Password (密碼)]：如有需要，輸入 proxy 伺服器的使用者名稱和密碼。

[Authentication method (驗證方法)]：

- [Basic (基本)]：此方法對 HTTP 而言是相容性最高的驗證配置。因為會將未加密的使用者名稱和密碼傳送至伺服器，其安全性較 Digest (摘要) 方法低。
- [Digest (摘要)]：該方法永遠都會在網路上傳輸已加密的密碼，因此更加安全。
- [Auto (自動)]：此選項可讓裝置根據支援的方法自動選取驗證方法。它會在考慮採用 [Basic (基本)] 方法之前優先選擇 [Digest (摘要)] 方法。

[Owner authentication key (OAK) (擁有者驗證金鑰 (OAK))]：按一下 [Get key (取得金鑰)] 以擷取擁有者驗證金鑰。這只有在裝置不使用防火牆或 Proxy 的情況下連線至網際網路時，才有可能。

SNMP

簡易網路管理通訊協定 (SNMP) 允許遠端管理網路裝置。

[SNMP]：選取要使用的 SNMP 版本。

- [v1 and v2c (v1 和 v2c)]：
  - [Read community (讀取群體)]：輸入唯讀存取所有支援之 SNMP 物件的群體名稱。預設值為 [public (公開)]。
  - [Write community (寫入群體)]：輸入對所有支援的 SNMP 物件 (唯讀物件除外) 有讀取或寫入存取權限的群體名稱。預設值為 [write (寫入)]。
  - [Activate traps (啟用設陷)]：開啟以啟動設陷報告。裝置使用設陷將重要事件或狀態變更的訊息傳送至管理系統。在網頁介面中，您可以設定 SNMP v1 和 v2c 的設陷。如果您變更至 SNMP v3 或關閉 SNMP，就會自動關閉設陷。如果使用 SNMP v3，您可以透過 SNMP v3 管理應用程式設定設陷。
  - [Trap address (設陷位址)]：輸入管理伺服器的 IP 位址或主機名稱。
  - [Trap community (設陷群體)]：輸入設備傳送設陷訊息至管理系統時要使用的群體。
  - [Traps (設陷)]：
    - [Cold start (冷啟動)]：在裝置啟動時傳送設陷訊息。
    - [Link up (上行連結)]：在連結從下行變更為上行時，傳送設陷訊息。
    - [Link down (下行連結)]：在連結從上行變更為下行時，傳送設陷訊息。
    - [Authentication failed (驗證失敗)]：在驗證嘗試失敗時傳送設陷訊息。

附註

開啟 SNMP v1 和 v2c 設陷時，您會啟用所有的 Axis Video MIB 設陷。如需詳細資訊，請參閱 *AXIS OS 入口網站 > SNMP*。

- [v3]：SNMP v3 是更安全的版本，提供加密和安全密碼。若要使用 SNMP v3，建議您啟用 HTTPS，因為密碼到時會透過 HTTPS 傳送。這也可以避免未經授權的一方存取未加密的 SNMP v1 及 v2c 設陷。如果使用 SNMP v3，您可以透過 SNMP v3 管理應用程式設定設陷。
  - [Password for the account "initial" (「initial」帳戶的密碼)]：輸入名為「initial」之帳戶的 SNMP 密碼。雖然不啟動 HTTPS 也傳送密碼，但不建議這樣做。SNMP v3 密碼僅可設定一次，且最好只在 HTTPS 啟用時設定。設定密碼之後，密碼欄位就不再顯示。若要再次設定密碼，您必須將裝置重設回出廠預設設定。

安全

憑證

憑證會用來驗證網路上的裝置。裝置支援兩種類型的憑證：

- [用戶端/伺服器憑證]
  用戶端/伺服器憑證驗證設備的身分識別，可以自行簽署，或由憑證機構 (CA) 發出。自行簽署的憑證提供的保護有限，可以暫時在取得憑證機構發行的憑證之前使用。
- CA 憑證
  您可以使用 CA 憑證來驗證對等憑證，例如當裝置連線至受 IEEE 802.1X 保護的網路時，確認驗證伺服器的身分識別是否有效。裝置有數個預先安裝的 CA 憑證。

支援以下格式：

- 憑證格式：.PEM、.CER 和 .PFX
- 私人金鑰格式：PKCS#1 與 PKCS#12

重要

如果將裝置重設為出廠預設設定，則會刪除所有憑證。任何預先安裝的 CA 憑證都將會重新安裝。

[+ Add certificate (新增憑證)]：按一下可新增憑證。逐步指南將開啟。

- [More (更多) ⌄]：顯示更多要填寫或選取的欄位。
- [Secure keystore (安全金鑰儲存區)]：選取使用 [Trusted Execution Environment (SoC TEE) (信任的執行環境)]、[Secure element (安全元件)] 或 [Trusted Platform Module 2.0 (信任的平台模組 2.0)] 以安全地儲存私密金鑰。有關選取哪個安全金鑰儲存區的更多資訊，請前往 *help.axis.com/axis-os#cryptographic-support*。
- [Key type (金鑰類型)]：從下拉式清單中選取預設或不同的加密演算法以保護憑證。

⋮ 內容功能表包含：

- [Certificate information (憑證資訊)]：檢視已安裝之憑證的屬性。
- [Delete certificate (刪除憑證)]：刪除憑證。
- [Create certificate signing request (建立憑證簽署要求)]：建立憑證簽署要求，以傳送至註冊機構申請數位身分識別憑證。

[Secure keystore (安全金鑰儲存區)ⓘ]：

- [Trusted Execution Environment (SoC TEE) (信任的執行環境)]：選取使用 SoC TEE 作為安全金鑰儲存區。
- [Secure element (CC EAL6+, FIPS 140-3 Level 3) (安全元件 (CC EAL6+，FIPS 140-3 等級 3))ⓘ]：選取使用安全元件作為安全金鑰儲存區。
- [Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2) (信任的平台模組 2.0 (CC EAL4+，FIPS 140-2 等級 2))ⓘ]：選取使用 TPM 2.0 作為安全金鑰儲存區。

[網路存取控制和加密]

IEEE 802.1x

IEEE 802.1x 是一種連接埠型網路存取控制 (Network Admission Control) 的 IEEE 標準，為有線及無線網路裝置提供安全驗證。IEEE 802.1x 以 EAP (可延伸的驗證通訊協定) 為架構基礎。

若要存取受 IEEE 802.1x 保護的網路，網路設備必須對本身進行驗證。驗證是由驗證伺服器 (通常為 RADIUS 伺服器，例如，FreeRADIUS 和 Microsoft Internet Authentication Server) 執行。

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec 是一項針對媒體存取控制 (MAC) 安全性的 IEEE 標準，它定義了媒體存取獨立通訊協定的非連線型資料機密性和完整性。

憑證

不使用 CA 憑證進行設定時，伺服器憑證驗證會遭停用，無論裝置連接到哪個網路，裝置都會嘗試自行驗證。

使用憑證時，在 Axis 的實作中，設備和驗證伺服器使用 EAP-TLS (可延伸的驗證通訊協定 - 傳輸層安全性)，透過數位憑證自行驗證。

若要允許該設備透過憑證存取受保護的網路，您必須在該設備上安裝已簽署的用戶端憑證。

[Authentication method (驗證方法)]：選取用於驗證的 EAP 類型。

[Client certificate (用戶端憑證)]：選取用戶端憑證以使用 IEEE 802.1x。驗證伺服器使用憑證驗證用戶端的身分識別。

[CA certificates (CA 憑證)]：選取 CA 憑證以驗證伺服器的身分識別。未選取任何憑證時，無論連接到哪個網路，裝置都會嘗試自行驗證。

EAP identity (EAP 身分識別)：輸入與用戶端憑證相關聯的使用者身分識別。

[EAPOL version (EAPOL 版本)]：選取網路交換器所使用的 EAPOL 版本。

[Use IEEE 802.1x (使用 IEEE 802.1x)]：選取以使用 IEEE 802.1x 通訊協定。

只有當您使用 IEEE 802.1x PEAP-MSCHAPv2 作為驗證方法時，才可使用這些設定：

- [Password (密碼)]：輸入您的使用者身分識別的密碼。
- [Peap version (Peap 版本)]：選取網路交換器所使用的 Peap 版本。
- [Label (標籤)]：選取 1 使用客戶端 EAP 加密；選取 2 使用客戶端 PEAP 加密。選取使用 Peap 版本 1 時網路交換器使用的標籤。

只有當您使用 IEEE 802.1ae MACsec (靜態 CAK/預先共用金鑰) 作為驗證方法時，才可使用這些設定：

- [Key agreement connectivity association key name (金鑰協定連接關聯金鑰名稱)]：輸入連接關聯名稱 (CKN)。它必須是 2 到 64 (能被 2 整除) 的十六進位字元。CKN 必須在連接關聯中手動設定，並且必須在連結兩端相符才能初始啟用 MACsec。
- [Key agreement connectivity association key (金鑰協定連接關聯金鑰)]：輸入連接關聯金鑰 (CAK)。它的長度應是 32 或 64 個十六進位字元。CAK 必須在連接關聯中手動設定，並且必須在連結兩端相符才能初始啟用 MACsec。

防止暴力破解

[Blocking (封鎖)]：開啟以阻擋暴力破解攻擊。暴力破解攻擊使用試誤法來猜測登入資訊或加密金鑰。

[Blocking period (封鎖期間)]：輸入阻擋暴力破解攻擊的秒數。

[Blocking conditions (封鎖條件)]：輸入開始封鎖前每秒允許的驗證失敗次數。您在頁面層級和裝置層級上都可以設定允許的失敗次數。

防火牆

防火牆：開啟以啟動防火牆。

[Default Policy (預設政策)]：選取您希望防火牆如何處理規則未涵蓋的連線請求。
- 接受：允許與設備的所有連線。該選項是預設的。
- 拒絕： 封鎖與該設備的所有連線。

若要對預設原則設定例外，您可以建立允許或封鎖從特定位址、通訊協定和連接埠連接到設備的規則。

+ 新規則：按一下可建立規則。

規則類型：
- 濾波器：選取允許或封鎖符合規則中定義條件的設備連線。
  - [Policy (政策)]：為防火牆規則選取 接受 或 拒絕。
  - IP 範圍：選取要指定允許或封鎖的位址範圍。在 開始 和 結束 中使用 IPv4/IPv6。
  - [IP address (IP 位址)]：輸入您想要允許或封鎖的位址。使用 IPv4/IPv6 或 CIDR 格式。
  - [Protocol (協定)]：選取要允許或封鎖的網路傳輸協定 (TCP、UDP 或兩者)。如果選取傳輸協定，也必須指定連接埠。
  - MAC：輸入您想要允許或封鎖的設備 MAC 位址。
  - 連接埠範圍：選取要指定允許或封鎖的連接埠範圍。將其加入 開始 和 結束 中。
  - [Port (連接埠)]：輸入您想要允許或封鎖的連接埠號碼。連接埠號碼必須介於 1 至 65535 之間。
  - 流量類型：選取您想要允許或封鎖的流量類型。
    - 單點傳送：從單一發送者到單一接收者的流量。
    - 廣播：從單一發送者到網路上所有設備的流量。
    - 多點傳送：從一個或多個發送者到一個或多個接收者的流量。
- 限制：選擇接受符合規則中定義條件的設備連線，但套用限制，以減少過多的流量。
  - IP 範圍：選取要指定允許或封鎖的位址範圍。在 開始 和 結束 中使用 IPv4/IPv6。
  - [IP address (IP 位址)]：輸入您想要允許或封鎖的位址。使用 IPv4/IPv6 或 CIDR 格式。
  - [Protocol (協定)]：選取要允許或封鎖的網路傳輸協定 (TCP、UDP 或兩者)。如果選取傳輸協定，也必須指定連接埠。
  - MAC：輸入您想要允許或封鎖的設備 MAC 位址。
  - 連接埠範圍：選取要指定允許或封鎖的連接埠範圍。將其加入 開始 和 結束 中。
  - [Port (連接埠)]：輸入您想要允許或封鎖的連接埠號碼。連接埠號碼必須介於 1 至 65535 之間。
  - 單位：選取要允許或封鎖的連線類型。
  - 期間：選取與 數量 相關的時間段。
  - 數量：設定在設定 週期 內允許設備連線的最大次數。最大數量為 65535。
  - 突增：輸入在設定 期間 內允許超過設定 數量 一次的連線數量。一旦達到該數量，就只允許在設定時間內使用設定數量。
  - 流量類型：選取您想要允許或封鎖的流量類型。
    - 單點傳送：從單一發送者到單一接收者的流量。
    - 廣播：從單一發送者到網路上所有設備的流量。
    - 多點傳送：從一個或多個發送者到一個或多個接收者的流量。

測試規則：按一下以測試您定義的規則。
- 以秒為單位的測試時間：設定測試規則的時間限制。

- 回復：按一下可將防火牆回復到測試規則之前的狀態。
- 套用規則：按一下即可啟動規則，無需測試。我們不建議您這樣做。

自訂簽署的 AXIS OS 憑證

若要在設備上安裝 Axis 的測試軟體或其他自訂軟體，您需要自訂簽署的 AXIS OS 憑證。該憑證會確認此軟體是否由設備擁有者和 Axis 核准。軟體僅可在以其唯一序號和晶片 ID 識別的特定設備上執行。由於 Axis 持有簽署憑證的金鑰，因此僅可由 Axis 建立自訂簽署的 AXIS OS 憑證。

[安裝]：按一下以安裝憑證。安裝軟體之前需要先安裝憑證。

⋮ 內容功能表包含：

- [Delete certificate (刪除憑證)]：刪除憑證。

帳戶

帳戶

[+ Add account (新增帳戶)]：按一下可新增帳戶。您最多可以新增 100 個帳戶。

[Account (帳戶)]：輸入唯一的帳戶名稱。

[New password (新的密碼)]：輸入帳戶的密碼。密碼長度必須介於 1 到 64 個字元之間。密碼中僅允許使用可列印的 ASCII 字元 (代碼 32 到 126)，例如：字母、數字、標點符號及某些符號。

[Repeat password (再次輸入密碼)]：再次輸入相同的密碼。

[Privileges (權限)]：

- [Administrator (管理員)]：可存取所有設定。管理員也可以新增、更新和移除其他帳戶。
- [Operator (操作者)]：可存取所有設定，但以下除外：
  — 所有 [System (系統)] 設定。
- [Viewer (觀看者)]：無法存取變更任何設定。

⋮ 內容功能表包含：

[Update account (更新帳戶)]：編輯帳戶特性。

[Delete account (刪除帳戶)]：刪除帳戶。您無法刪除 root 帳戶。

SSH 帳戶

[+ Add SSH account (新增 SSH 帳戶)]：按一下可新增新的 SSH 帳戶。

- [Enable SSH (啟用 SSH)]：開啟以使用 SSH 服務。

[Account (帳戶)]：輸入唯一的帳戶名稱。

[New password (新的密碼)]：輸入帳戶的密碼。密碼長度必須介於 1 到 64 個字元之間。密碼中僅允許使用可列印的 ASCII 字元 (代碼 32 到 126)，例如：字母、數字、標點符號及某些符號。

[Repeat password (再次輸入密碼)]：再次輸入相同的密碼。

[Comment (註解)]：輸入註解 (可選)。

⋮ 內容功能表包含：

[Update SSH account (更新 SSH 帳戶)]：編輯帳戶特性。

[Delete SSH account (刪除 SSH 帳戶)]：刪除帳戶。您無法刪除 root 帳戶。

虛擬主機

[+ Add virtual host (新增虛擬主機)]：按一下以新增新的虛擬主機。

[Enabled (已啟用)]：選取使用該虛擬主機。

[Server name (伺服器名稱)]：輸入伺服器的名稱。僅使用數字 0-9、字母 A-Z 和連字號 (-)。

[Port (連接埠)]：輸入伺服器所連接的連接埠。

[Type (類型)]：選取要使用的驗證類型。在 [Basic (基本)]、[Digest (摘要)] 和 [Open ID (開放 ID)] 之間選取。

⋮ 內容功能表包含：

- [Update (更新)]：更新虛擬主機。
- [Delete (刪除)]：刪除虛擬主機。

[Disabled (已停用)]：該伺服器已停用。

OpenID 設定

重要

如果您無法使用 OpenID 登入，請使用您在設定 OpenID 以登入時所使用的 Digest 或 Basic 認證。

[Client ID (用戶端 ID)]：輸入 OpenID 使用者名稱。

[Outgoing Proxy (撥出代理伺服器)]：輸入 OpenID 連接的 proxy 位址以使用 proxy 伺服器。

[Admin claim (管理者申請)]：輸入管理者角色的值。

[Provider URL (提供者 URL)]：輸入 API 端點驗證的網頁連結。格式應為 https://[insert URL]/.well-known/openid-configuration

[Operator claim (操作者申請)]：輸入操作者角色的值。

[Require claim (需要申請)]：輸入權杖中應包含的資料。

[Viewer claim (觀看者申請)]：輸入觀看者角色的值。

[Remote user (遠端使用者)]：輸入值以識別遠端使用者。這有助於在設備的網頁介面中顯示目前使用者。

[Scopes (範圍)]：可以作為權杖一部分的可選範圍。

[Client secret (用戶端秘密)]：輸入 OpenID 密碼

[Save (儲存)]：按一下以儲存 OpenID 值。

[Enable OpenID (啟用 OpenID)]：開啟以關閉目前連接並允許從提供者 URL 進行設備驗證。

MQTT

MQTT (訊息佇列遙測傳輸) 是物聯網 (IoT) 的標準傳訊通訊協定。這旨在簡化 IoT 整合，並廣泛用於各種行業，以較少程式碼量和最低網路頻寬來連接遠端裝置。Axis 設備軟體中的 MQTT 用戶端可以簡化設備中所產生資料及事件與本身並非影像管理軟體 (VMS) 之系統的整合。

將裝置設定為 MQTT 用戶端。MQTT 通訊是以用戶端與中介者這兩個實體為基礎所建構。用戶端可以發送和接收訊息。中介者則負責在用戶端之間配發訊息。

您可以在 *AXIS OS 知識庫*中深入了解 MQTT。

ALPN

ALPN 是 TLS/SSL 擴充功能，允許在用戶端與伺服器之間連接的交握階段中選取應用程式通訊協定。這用於透過其他通訊協定 (例如 HTTP) 所用的同一個連接埠來啟用 MQTT 流量。在某些情況下，可能沒有開放供 MQTT 通訊使用的專用通訊埠。在這種情況下，解決方案是使用 ALPN 交涉，將 MQTT 用作防火牆所允許之標準連接埠上的應用程式通訊協定。

MQTT 客戶

[Connect (連線)]：開啟或關閉 MQTT 用戶端。

[Status (狀態)]：顯示 MQTT 用戶端目前的狀態。

中介者

[Host (主機)]：輸入 MQTT 伺服器的主機名稱或 IP 位址。

[Protocol (協定)]：選取要使用的通訊協定。

[Port (連接埠)]：輸入連接埠號碼。

- 1883 是 [MQTT over TCP (TCP 上的 MQTT)] 的預設值
- 8883 是 [MQTT over SSL (SSL 上的 MQTT)] 的預設值
- 80 是 [MQTT over WebSocket (WebSocket 上的 MQTT)] 的預設值
- 443 是 [MQTT over WebSocket Secure (WebSocket Secure 上的 MQTT)] 的預設值

[ALPN protocol (ALPN 協定)]：輸入 MQTT 代理人提供者提供的 ALPN 通訊協定名稱。這僅適用於透過 SSL 的 MQTT 和透過 WebSocket Secure 的 MQTT。

[Username (使用者名稱)]：輸入用戶端將用來存取伺服器的使用者名稱。

[Password (密碼)]：輸入使用者名稱的密碼。

[Client ID (用戶端 ID)]：輸入用戶端 ID。用戶端連接至伺服器時，傳送至伺服器的用戶端識別碼。

[Clean session (清除工作階段)]：控制連線和中斷連線時的行為。選取後，系統會在連線和中斷連線時捨棄狀態資訊。

[HTTP proxy (HTTP 代理伺服器)]：最大長度為 255 位元組的 URL。如果不使用 HTTP proxy，則可以將該欄位留空。

[HTTPS proxy (HTTPS 代理伺服器)]：最大長度為 255 位元組的 URL。如果不使用 HTTPS proxy，則可以將該欄位留空。

[Keep alive interval (保持連線間隔)]：讓用戶端偵測伺服器何時不再可用，而不必等候冗長的 TCP/IP 逾時。

[Timeout (逾時)]：允許連線完成的間隔時間 (以秒為單位)。預設值：60

[Device topic prefix (設備主題首碼)]：在 [MQTT client (MQTT 用戶端)] 索引標籤上的連線訊息和 LWT 訊息主題預設值使用，並在 [MQTT publication (MQTT 公開發行)] 索引標籤上公開條件。

[Reconnect automatically (自動重新連線)]：指定用戶端是否應在中斷連接後自動重新連線。

連線訊息

指定是否要在建立連線時送出訊息。

[Send message (傳送訊息)]：開啟以傳送訊息。

[Use default (使用預設)]：關閉以輸入您自己的預設訊息。

[Topic (主題)]：輸入預設訊息的主題。

[Payload (承載)]：輸入預設訊息的內容。

[Retain (保留)]：選取以保持用戶端在此 [Topic (主題)] 上的狀態

[QoS]：變更封包流的 QoS 層。

最終聲明訊息

最後遺言機制 (LWT) 允許用戶端在連線至中介者時提供遺言以及其認證。如果用戶端於稍後某個時間點突然斷線 (可能是因為電源中斷)，則中介者可藉其傳送訊息至其他用戶端。LWT 訊息的格式與一般訊息無異，路由機制也相同。

[Send message (傳送訊息)]：開啟以傳送訊息。

[Use default (使用預設)]：關閉以輸入您自己的預設訊息。

[Topic (主題)]：輸入預設訊息的主題。

[Payload (承載)]：輸入預設訊息的內容。

[Retain (保留)]：選取以保持用戶端在此 [Topic (主題)] 上的狀態

[QoS]：變更封包流的 QoS 層。

MQTT 發佈

[Use default topic prefix (使用預設主題字首)]：選取使用預設主題字首，此字首是在 [MQTT client (MQTT 用戶端)] 索引標籤的設備主題字首中定義。

[Include condition (包括條件)]：選取包括在 MQTT 主題中描述條件的主題。

[Include namespaces (包括命名空間)]：選取以便包括在 MQTT 主題中的 ONVIF 主題命名空間。

[Include serial number (包括序號)]：選取在 MQTT 承載中包括設備的序號。

[+ Add condition (新增條件)]：按一下可新增條件。

[Retain (保留)]：定義要傳送為保留的 MQTT 訊息。

- [None (無)]：傳送所有訊息為不保留。
- [Property (屬性)]：僅傳送狀態訊息為保留。
- [All (全部)]：傳送具狀態和無狀態訊息，並且皆予以保留。

[QoS]：選取 MQTT 發佈所需的服務品質等級。

MQTT 訂閱

[+ Add subscription (新增訂閱)]：按一下可加入新的 MQTT 訂閱。

[Subscription filter (訂閱篩選條件)]：輸入您要訂閱的 MQTT 主題。

[Use device topic prefix (使用設備主題首碼)]：將訂閱過濾當做首碼新增至 MQTT 主題。

[Subscription type (訂閱類型)]：

- [Stateless (無狀態)]：選取將 MQTT 訊息轉換為無狀態訊息。
- [Stateful (有狀態)]：選取將 MQTT 訊息轉換為條件。承載會用作狀態。

[QoS]：選取 MQTT 訂閱所需的服務品質等級。

配件

I/O埠

使用數位輸入連接可在開路和閉路之間切換的外部裝置，例如：PIR 感應器、門或窗磁簧感應器和玻璃破裂偵測器。

使用數位輸出連接外接裝置，例如繼電器和 LED。您可以透過 VAPIX® 應用程式開發介面或網頁介面來啟動連接的設備。

連接埠

[Name (名稱)]：編輯文字以重新命名該連接埠。

[Direction (方向)]： 表示此連接埠是輸入埠。 表示這是輸出埠。如果該連接埠可設定，則可以按一下圖示以在輸入和輸出之間變更。

[Normal state (正常狀態)]：開路請按一下 ，閉路請按一下 。

[Current state (目前狀態)]：顯示連接埠目前的狀態。當目前的狀態不同於正常狀態時，便會啟動輸入或輸出。設備中斷連接時，或電壓超過 1 VDC 時，設備的輸入會有開路。

附註

在重新啟動期間，輸出電路為開路。當重新啟動完成時，電路會回到正常位置。如果您變更此頁面上的任何設定，不論是否有任何作用中的觸發器，輸出電路都會回到其正常位置。

[Supervised (受監控)]：如果有人竄改與數位 I/O 裝置的連線，請開啟此選項，讓裝置可以偵測和觸發動作。除了偵測輸入是開路還是閉路之外，您還可以偵測是否有人對其進行竄改 (即切斷或短路)。若要監控連線，必須在外部 I/O 迴路中附加其他硬體 (線路終端電阻器)。

記錄檔

報表和紀錄

報告

- [View the device server report (檢視裝置伺服器報告)]：在快顯視窗中檢視有關產品狀態的資訊。存取記錄會自動包含在伺服器報告中。
- [Download the device server report (下載設備伺服器報告)]：它會建立一個 .zip 檔案，其中包含 UTF—8 格式的完整伺服器報告文字檔，以及目前即時影像畫面的快照。當聯絡支援人員時，一定要附上伺服器報告 .zip 檔。
- [Download the crash report (下載當機報告)]：下載封存檔，其中包含有關伺服器狀態的詳細資訊。當機報告包含了伺服器報告中的資訊以及詳細的偵錯資訊。此報告可能會包含敏感性資訊，例如網路追蹤。產生報告可能需要幾分鐘的時間。

記錄檔

- [View the system log (檢視系統記錄)]：按一下可顯示有關系統事件的資訊，例如設備啟動、警告和重大訊息。
- [View the access log (檢視存取記錄)]：按一下可顯示所有嘗試存取設備但卻失敗的狀況，例如：當使用錯誤的登入密碼時。
- [View the audit log 檢視稽核記錄]：按一下可顯示有關使用者和系統活動的資訊，例如成功或失敗的身分驗證和組態設定。

網路追蹤

重要

網路追蹤檔案可能包含機密資訊，例如憑證或密碼。

網路追蹤檔案可以記錄網路上的活動，協助您針對問題進行疑難排解。

[Trace time (追蹤時間)]：選取追蹤持續期間 (秒或分鐘)，然後按一下 [下載]。

遠端系統日誌

Syslog 是訊息記錄的標準。它允許分離產生訊息的軟體、儲存軟體的系統，以及報告及分析訊息的軟體。每則訊息皆標記有設施代碼，以指示產生訊息的軟體類型，並為訊息指派嚴重性級別。

[+ Server (伺服器)]：按一下可新增伺服器。

[Host (主機)]：輸入伺服器的主機名稱或 IP 位址。

[Format (格式化)]：選取要使用的 Syslog 訊息格式。

- 安迅士
- RFC 3164
- RFC 5424

[Protocol (協定)]：選取要使用的通訊協定：

- UDP (預設連接埠為 514)
- TCP (預設連接埠為 601)
- TLS (預設連接埠為 6514)

[Port (連接埠)]：編輯連接埠號碼以使用不同的連接埠。

[Severity (嚴重性)]：選取要在觸發時要傳送的訊息。

[Type (類型)]：選擇您想要傳送的日誌類型。

測試伺服器設定：在儲存設定之前，向所有伺服器發送測試訊息。

[CA certificate set (CA 憑證組)]：查看目前設定或新增憑證。

維護

[Restart (重新啟動)]：重新啟動設備。這不會影響目前的任何設定。執行中的應用程式會自動重新啟動。

[Restore (還原)]：將大多數設定回復成出廠預設值。之後您必須重新設定設備和應用程式、重新安裝未預先安裝的任何應用程式，以及重新建立任何事件和預設點。

重要

還原後僅會儲存的設定是：

- 開機通訊協定 (DHCP 或靜態)
- 固定 IP 位址
- 預設路由器
- 子網路遮罩
- 802.1X 設定
- O3C 設定
- DNS 伺服器 IP 位址

[Factory default (出廠預設值)]：將所有設定回復成出廠預設值。之後您必須重設 IP 位址，以便存取設備。

附註

所有 Axis 設備軟體皆經過數位簽署，以確保您僅將經過驗證的軟體安裝於設備上。這會進一步提高 Axis 裝置的整體最低網路安全等級。如需詳細資訊，請參閱 *axis.com* 上的「Axis Edge Vault」白皮書。

[AXIS OS upgrade (AXIS 作業系統升級)]：升級到新的 AXIS OS 版本。新發行版本可能會包含改良功能、錯誤修正和全新功能。我們建議您永遠都使用最新的 AXIS OS 版本。若要下載最新版本，請前往 *axis.com/support*。

升級時，您可以在三個選項之間進行選擇：

- [Standard upgrade (標準升級)]：升級到新的 AXIS OS 版本。
- [Factory default (出廠預設值)]：升級並將所有設定回復成出廠預設值。選擇此選項後，升級後將無法恢復到之前的 AXIS OS 版本。
- 自動回復：升級並在設定的時間內確認升級。如果您不確認，設備將回復到之前的 AXIS OS 版本。

[AXIS OS rollback (AXIS 作業系統回復)]：回復到之前安裝的 AXIS OS 版本。

深入瞭解

網路安全

如需有關網路安全的產品特定資訊，請參閱產品的型錄，網址為 axis.com。

如需有關 AXIS OS 中網路安全的詳細資訊，請閱讀 *AXIS OS 強化指南*。

已簽署的作業系統

已簽署的作業系統由使用私密金鑰簽署 AXIS OS 影像的軟體廠商實作。簽章附加至作業系統時，設備將會在安裝簽章前驗證軟體。如果設備偵測到軟體完整性遭入侵，將會拒絕 AXIS OS 升級。

安全開機

安全開機是一種開機程序，由未間斷的軟體 (以密碼編譯驗證) 鏈結組成，從不可變動的記憶體 (開機 ROM) 開始。安全開機以簽署的作業系統為基礎，確保設備僅能使用授權的軟體開機。

Axis Edge Vault (憑證伺服器)

Axis Edge Vault (憑證伺服器)提供一個防護安迅士設備的硬體網路安全平台。它所具備的功能可以確保設備的身分識別和完整性，並保護您的機密資訊免受未經授權的存取。其建立在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)基礎上，並結合邊際設備安全的專業知識。

Axis 裝置 ID

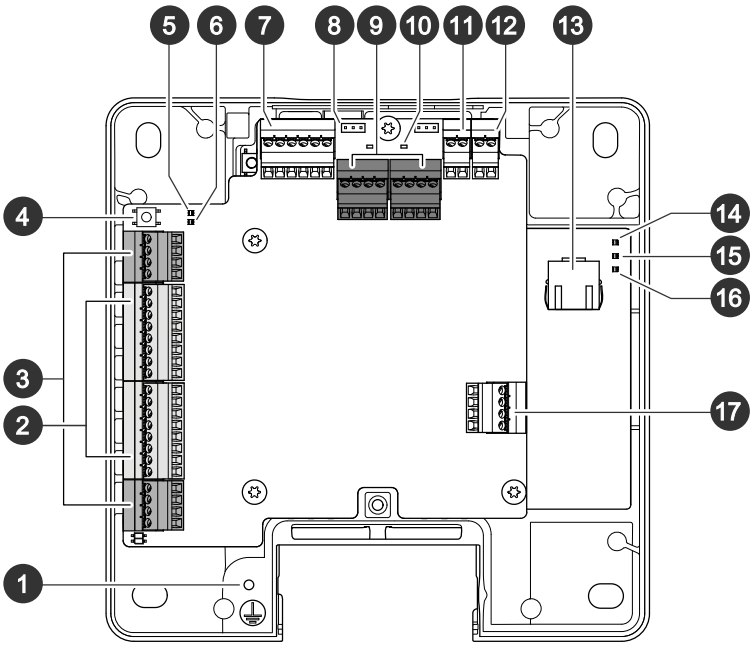
能夠驗證設備的來源，是在設備識別中建立信任的關鍵。生產期間，搭配Axis Edge Vault (憑證伺服器)的設備會被指派一個獨特、原廠佈建且符合IEEE 802.1AR的安迅士設備ID憑證。這可作為通行護照證明設備的來源。設備ID安全且永久儲存在安全金鑰儲存區內，作為以安迅士根憑證簽署的憑證。客戶的 IT 基礎架構可以利用設備 ID 達到自動化安全設備上線和安全設備識別

如果要深入了解 Axis 設備的網絡安全功能，請前往 *axis.com/learning/white-papers*，並搜尋網路安全。

規格

有 UL 標示的文字僅適用於 UL 294 安裝。

產品總覽



1 *接地位置*
2 *讀卡機接頭，2 個*
3 *門組接頭，2 個*
4 *控制按鈕*
5 *繼電器過電流 LED*
6 *讀卡機過電流 LED*
7 *輔助連接器*
8 *繼電器跳線，2 個*
9 *繼電器接頭，2 個*
10 *繼電器 LED，2 個*
11 *12 V 備用電源輸入*
12 *電源接頭*
13 *網路接頭*
14 *電源指示燈*
15 *狀態LED燈號*
16 *網路 LED*
17 *外部連接器*

LED 指示燈

LED	彩色	指示
網路	綠色	常亮表示已連線到 100 MBit/s 網路。閃爍表示有網路活動。
	黃色	常亮表示已連線到 10 MBit/s 網路。閃爍表示有網路活動。
	熄滅	無網路連線。
狀態	綠色	綠燈常亮表示正常操作。
	黃色	在啟動和還原設定時保持常亮。
	紅色	緩慢閃爍表示升級失敗。

電源	綠色	正常運作。
	黃色	升級韌體時綠色/琥珀色交替閃爍。
繼電器過電流	紅色	短路或偵測到過電流時常亮。
	熄滅	正常運作。
讀卡機過電流	紅色	短路或偵測到過電流時常亮。
	熄滅	正常運作。
繼電器	綠色	繼電器啟動。[1]
	熄滅	繼電器未啟用。

附註

- 狀態 LED 可以設定為有活躍的事件時閃爍。
- 狀態 LED 可以設定為閃爍以供設備識別之用。移至 [設定 > 其他控制器組態 > 系統選項 > 維護]。

按鈕

控制按鈕

控制按鈕用於：
- 將產品重設為出廠預設設定。請參考 。

接頭

網路接頭

支援增強型乙太網路供電 (PoE+) 的 RJ45 乙太網路接頭。

UL：乙太網路供電（PoE）應符合 UL 294 所列之 IEEE 802.3af/802.3at Type 1 Class 3 或高功率乙太網路供電（PoE+）IEEE 802.3at Type 2 Class 4 的功率限制標準，提供 44—57 V DC，15.4 W / 30 W 。乙太網路供電（PoE）已通過 UL 配備 AXIS T8133 30 W 1 埠中跨電源供應器核准。

電源優先順序

此設備可由 PoE 或 DC 輸入供電。請參閱 和 。

- 當設備供電前同時連接 PoE 和 DC 時，採用 PoE 供電。
- PoE 和 DC 均已連接，並且 PoE 目前正在供電。當 PoE 中斷時，該設備使用 DC 供電，無需重新啟動。
- PoE 和 DC 均已連接，並且 DC 目前正在供電。當 DC 中斷時，該設備重新啟動並使用 PoE 供電。
- 當在啟動時使用 DC 並且在該設備啟動後連接 PoE 時，使用 DC 供電。
- 當在啟動時使用 PoE 並且在該設備啟動後連接 DC 時，使用 PoE 供電。

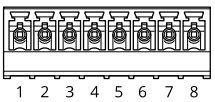
讀卡機接頭

兩組支援 RS485 和 Wiegand 通訊協定的 8 針腳接線端子，用於與讀卡機進行通訊。

兩個讀卡機連接埠之間共用指定的功率輸出值。這表示會為所有連接至門控制器的讀卡機保留 500 mA (12 V DC)。

在產品網頁中選取要使用的通訊協定。

1. *COM* 連到 *NO* 時繼電器啟動。



對 RS485 進行設定

功能	針腳	附註	規格
DC 接地 (GND)	1		0 V DC
DC 輸出（+12 V）	2	為讀卡機供電。	12 V DC，最大 500 mA (所有讀卡機合計)
RX/TX	3—4	全雙工：RX。半雙工：RX/TX。	
TX	5—6	全雙工：TX。	
可設定 (輸入或輸出)	7—8	數位輸入 — 連接到接腳 1 以啟用，或浮接 (不連接) 以停用。	0 到最大 30 V DC
		數位輸出 — 如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。	0 到最大 30 V DC，漏極開路，100 mA

重要

- 讀卡機由控制器供電時，最多可支援的纜線長度達 200 公尺 (656 英呎)。
- 讀卡機不由控制器供電時，若電纜符合1條AWG 20-16 電屏雙絞線的要求，讀卡機允許數據線最長可達 1000 公尺（3280.8 英尺）。

對 Wiegand 進行設定

功能	針腳	附註	規格
DC 接地 (GND)	1		0 V DC
DC 輸出（+12 V）	2	為讀卡機供電。	12 V DC，最大 500 mA (所有讀卡機合計)
D0	3		
D1	4		
O	5—6	數位輸出，漏極開路	
可設定 (輸入或輸出)	7—8	數位輸入 — 連接到接腳 1 以啟用，或浮接 (不連接) 以停用。	0 到最大 30 V DC
		數位輸出 — 如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。	0 到最大 30 V DC，漏極開路，100 mA

重要

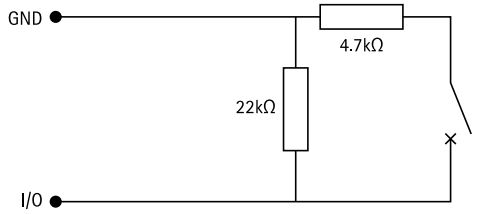
- 讀卡機由控制器供電時，最多可支援的纜線長度達 150 公尺 (500 英呎)。
- 讀卡機不由控制器供電時，若電纜符合AWG 20-16 的要求，讀卡機允許數據線最長可達 150 公尺（500 英尺）。

受監控的輸入

若要使用受監控的輸入，請根據下圖安裝線路終端電阻器。

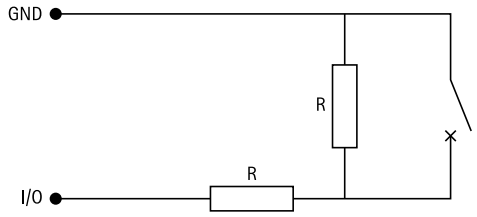
第一並聯連接

電阻值必須為 4.7 kΩ 和 22 kΩ。



第一串聯連接

電阻值必須相同，可能的值為 1 kΩ、2.2 kΩ、4.7 kΩ 和 10 kΩ。



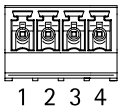
附註

建議使用雙絞線和屏蔽線。將屏蔽裝置連接至 0 V DC。

門組接頭

兩組用於門禁監控裝置的 4 針接線端子 (數位輸入)。

門禁監控器支援使用線路終端電阻器進行監控。如果連接中斷，則觸發警報。若要使用受監督的輸入，請安裝線路終端電阻器。使用受監控輸入的連接圖。請參閱 。



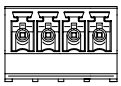
功能	針腳	附註	規格
DC 接地	1, 3		0 V DC
輸入	2, 4	用於與門禁監視器通訊。 數位輸入監督式輸入：分別連到 PIN 1 或 3 啟動，浮接（不連線）停用。	0 到最大 30 V DC

重要

若符合AWG 24纜線要求，合格電纜最長可達 200 公尺（656 英尺）。

繼電器接頭

C 型繼電器的兩組 4 針接線端子，可用於 (例如) 控制門鎖透或大門介面。



功能	針腳	附註	規格
DC 接地 (GND)	1		0 V DC
NO	2	常開。 用於連接繼電器設備。在 NO 和 DC 接地之間連接故障安全鎖。 若不使用跳線，則兩繼電器接點需與電路其他部分電氣分離。	最大電流 = 每台繼電器 2 A 最大電壓 = 30 V DC
COM	3	通用	
NC	4	常閉。 用於連接繼電器設備。在 NC 和 DC 接地之間連上故障安全鎖。 若不使用跳線，則兩繼電器接點需與電路其他部分電氣分離。	

繼電器電源跳線

裝上繼電器電源跳線時，跳線會將 12 V DC 或 24 V DC 連接至繼電器 COM 針腳。

這可用於連接 GND 與 NO 之間或 GND 與 NC 針腳之間的鎖。

電源	最大功率，於 12 V DC[2]	最大功率，於 24 V DC[2]
DC IN	1 800 mA	750 mA
PoE	900 mA	410 mA

注意

如果門鎖無極性，建議您加裝一個外接續流二極體。

輔助連接器

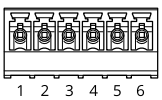
將輔助連接器搭配外部裝置結合位移偵測、事件觸發和警報通知等功能使用。除了 0 V DC 參考點和電源 (DC 輸出) 以外，輔助連接器也會提供介面來連接：

數位輸入 - 用於連接可在開路和閉路之間切換的設備，例如 PIR 感應器、門/窗磁簧感應器和玻璃破裂偵測器。

受監控的輸入 - 能夠偵測數位輸入上的防竄改功能。

數位輸出 - 用於連接繼電器和 LED 等外接裝置，所連裝置可經 VAPIX® 應用程式開發介面或產品網頁啟動。

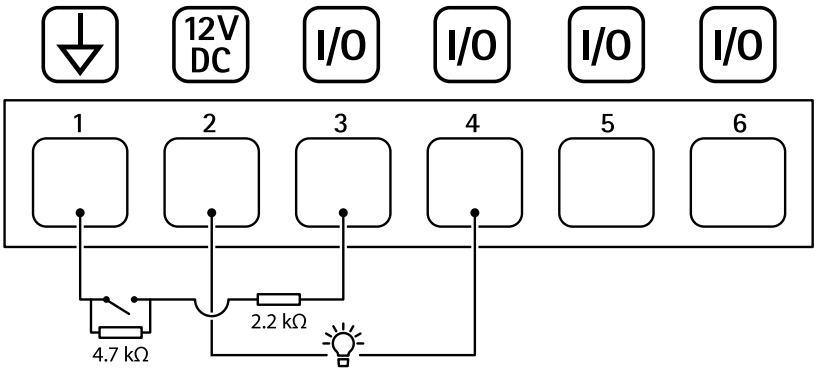
6 針接線端子



功能	針腳	附註	規格
DC 接地	1		0 V DC

2. 電力由兩個繼電器及*AUX I/O 12 V DC*共享。

DC 輸出	2	可用於電源輔助設備。 注意：此針腳只能用作電源輸出和安全端，因為它與繼電器共享電源。	12 V DC 最大負載 = 每個 I/O 各 50 mA
可設定 (輸入或輸出)	3—6	數位輸入或受監控的輸入 — 連接至針腳 1 以啟用，或浮接 (不連接) 以停用。若要使用受監督的輸入，請安裝線路終端電阻器。有關如何連接電阻器的資訊，請參閱連接圖。	0 到最大 30 V DC
		數位輸出 — 作用中時，內部會連接到針腳 1 (DC 接地)，非作用中時為浮接 (不連接)。如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。如果使用內部 12 V DC 輸出 (針腳 2)，則每個 I/O 都可以驅動 12 V DC、50 mA (最大) 外部負載。如果將漏極開路連接與外部電源供應器搭配使用，則 I/O 可以管理 0—30 V DC、100 mA 的 DC 電源。	0 到最大 30 V DC，漏極開路，100 mA

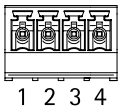


1 *DC 接地*
2 *DC 輸出 12 V，最大 50 mA*
3 *I/O 設定為受監控的輸入*
4 *I/O 設定為輸出*
5 *可設定的 I/O*
6 *可設定的 I/O*

外部連接器

用於外部裝置的 4 針接線端子，例如玻璃破碎偵測器或火災探測器。

UL：接頭未經 UL 防盜火警用評估。



功能	針腳	附註	規格
DC 接地	1, 3		0 V DC
可設定 (輸入或輸出)	2, 4	數位輸入 — 連接到針腳 1 或 3 以啟用，或浮接 (不連接) 以停用。	0 到最大 30 V DC
		數位輸出 — 連接到針腳 1 或 3 以啟用，或浮接 (不連接) 以停用。如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。	0 到最大 30 V DC，漏極開路，100 mA

電源接頭

2 針接線端子，用於 DC 電源輸入。使用符合安全額外低電壓 (SELV) 的限功率電源 (LPS)，可以是額定輸出功率限制在 ≤100 W 或額定輸出電流限制在 ≤5 A 的電源。

功能	針腳	附註	規格
0 V DC (-)	1		0 V DC
DC 輸入	2	不使用乙太網路供電的情況下為控制器供電。 注意：此針腳只能當做電源輸入使用。	10.5—28 V DC，最大 36 W

UL：DC 電源根據使用場合，由 UL 294、UL 293 或 UL 603 所列電源供應器以適當額定值供應。

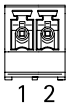
12 V 備用電源輸入

適用於內建充電器的備用方案。12 V DC 輸入。

UL：接頭未經 UL 評估。

重要

使用電池輸入時，必須串聯外接 3A 慢熔保險絲。



功能	針腳	附註	規格
0 V DC (-)	1		0 V DC
電池輸入	2	無其他電源時用來為門禁控制器供電。 注意：此針腳只能當做電池電源輸入使用。僅用於連接至 UPS。	11 — 13.7 V DC，最大 36 W

故障排除

重設為出廠預設設定

重要

當重設為出廠預設設定時應特別謹慎。這種處理方式會將包括 IP 位址在內的所有設定都還原為出廠預設值。

若要將產品重設為出廠預設設定：

1. 將產品斷電。
2. 按住控制按鈕，同時重新接通電源。請參考 。
3. 繼續按住控制按鈕 25 秒，直到狀態 LED 指示燈第二次變成琥珀色。
4. 放開控制按鈕。當狀態LED指示燈轉變成綠色時，即完成重設程序。如果網路中沒有可用的 DHCP 伺服器，設備 IP 位址將預設為下列其中一個位址：
   - AXIS OS 12.0 及更高版本的設備： 從連結本機位址子網路 (169.254.0.0/16) 取得
   - AXIS OS 11.11 及更早版本的設備： 192.168.0.90/24
5. 使用安裝與管理軟體工具來指派 IP 位址、設定密碼，並存取產品。

您還可以透過設備的網頁介面將參數重設為出廠預設值。前往 [Maintenance (維護)] > [Factory default (出廠預設值)]，並按一下 [Default (預設)]。

AXIS OS 選項

Axis 根據主動式常規或長期支援 (LTS) 常規提供設備軟體管理。屬於主動式常規者意味著可以持續存取所有最新的產品功能，而 LTS 常規會提供固定平台，定期發佈主要著重於錯誤修正和安全性更新的韌體。

如果想要存取最新功能，或是您使用 Axis 端對端系統產品系列時，建議使用主動式常規提供的 AXIS OS。如果您使用不會持續依據最新主動式常規進行驗證的第三方整合，則建議使用 LTS 常規。使用 LTS 時，這些產品可以在不引入任何重大功能變更或影響任何現有整合的情況下維護網路安全。如需 Axis 設備軟體策略的詳細資訊，請前往 *axis.com/support/device-software*。

檢查目前的 AXIS OS 版本

我們設備的功能取決於 AXIS OS。對問題進行故障排除時，建議您先從檢查目前 AXIS OS 版本開始著手。最新版本可能包含解決特定問題的修正檔案。

若要檢查目前的 AXIS OS 版本：

1. 前往設備的網頁介面 > [Status (狀態)]。
2. 請參閱 [Device info (設備資訊)] 下的 AXIS OS 版本。

升級 AXIS OS

重要

- 升級設備軟體時，系統會儲存預先設定和自訂的設定 (假如新的 AXIS OS 中提供這些功能)，但 Axis Communications AB 不做此保證。
- 請確保該設備在升級過程中持續連接電源。

附註

使用主動式常規的最新 AXIS OS 版本升級設備時，該產品會獲得最新的可用功能。在升級之前，請務必閱讀每個新版本所提供的升級指示和版本資訊。若要尋找最新的 AXIS OS 版本和版本資訊，請前往 *axis.com/support/device-software*。

附註

由於使用者、群組、認證及其他資料的資料庫會在 AXIS OS 升級後更新，因此初次啟動可能需要幾分鐘才能完成。所需時間取決於資料量。

1. 將 AXIS OS 檔案下載至電腦，請前往 *axis.com/support/device-software* 免費下載。
2. 以管理員身分登入裝置。
3. 前往 [Maintenance (維護) > AXIS OS upgrade (AXIS 作業系統升級)]，並按一下 [Upgrade (升級)]。

升級完成後，產品會自動重新啟動。

4. 重新啟動產品後，清除網頁瀏覽器的快取。

技術問題及可能的解決方案

升級 AXIS OS 時發生問題

AXIS OS 升級失敗

如果升級失敗，則設備會重新載入之前的版本。最常見的原因是上傳了錯誤的 AXIS OS 檔案。請檢查 AXIS OS 檔案名稱是否與您的設備相對應，然後重試。

升級 AXIS OS 後發生問題

如果您在升級後遇到問題，請從 [Maintenance (維護)] 頁面回復之前安裝的版本。

設定 IP 位址時發生問題

無法設定 IP 位址

- 如果設備所使用的 IP 位址及用來存取設備的電腦的 IP 位址位在不同的子網路上，您將無法設定 IP 位址。請與您的網路管理員聯繫，以取得 IP 位址。
- 可能有另一個設備正在使用此 IP 位址。檢查：
  1. 中斷 Axis 裝置與網路的連接。
  2. 在命令/DOS 視窗中，輸入 `ping` 和設備的 IP 位址。
  3. 如果您收到：`Reply from <IP address>: bytes=32; time=10...` 這表示網路上可能有另一個設備正在使用此 IP 位址。請向網路管理員索取新的 IP 位址，然後重新安裝裝置。
  4. 如果您收到：`Request timed out`，這表示此 IP 位址可供 Axis 設備使用。請檢查所有接線，然後重新安裝裝置。
- 可能與相同子網路上的另一個設備發生 IP 位址衝突。在 DHCP 伺服器設定動態位址之前會使用 Axis 裝置中的固定 IP 位址。這表示，如果另一個設備也使用同一個預設的固定 IP 位址，則存取該設備可能會發生問題。

存取設備時發生問題

從瀏覽器存取設備時無法登入

HTTPS 已啟用時，務必使用正確的傳輸協定 (HTTP 或 HTTPS) 登入。您可能需要在瀏覽器的網址欄位中手動輸入 `http` 或 `https`。

如果遺失 root 帳戶的密碼，則必須將設備重設為出廠預設設定。如需說明，請參閱 。

DHCP 已變更 IP 位址

從 DHCP 伺服器取得的 IP 位址是動態的，而且可能會變更。如果 IP 位址已變更，請使用 AXIS IP Utility 或 AXIS Device Manager，在網路上尋找設備。使用裝置的型號或序號來識別裝置，如果已設定 DNS 名稱，則使用該名稱來識別。

如有需要，您可以手動指派固定 IP 位址。如需相關指示，請前往 *axis.com/support*。

使用 IEEE 802.1X 時的憑證錯誤

若要讓驗證正常運作，Axis 裝置中的日期和時間設定必須與 NTP 伺服器同步。前往 [System (系統) > Date and time (日期和時間)]。

不支援此瀏覽器

如需查看推薦瀏覽器清單，請參閱。

無法從外部存取設備

若要從外部存取設備，建議您使用下列其中一個適用於 Windows® 的應用程式：

- AXIS Camera Station Edge：免費，非常適合有基本監控需求的小型系統。
- AXIS Camera Station 5：有 30 天免費試用版，非常適合中小型系統使用。
- AXIS Camera Station Pro：有 90 天免費試用版，非常適合中小型系統使用。

如需相關指示和下載，請前往 *axis.com/vms*。

MQTT 問題

無法透過連接埠 8883 與基於 SSL 的 MQTT 連接

防火牆會封鎖使用連接埠 8883 的流量，因其認為這種流量不安全。

在某些情況下，伺服器/中介者可能無法為 MQTT 通訊提供特定連接埠。仍然可以透過 HTTP/HTTPS 流量通常使用的連接埠來使用 MQTT。

- 如果伺服器/中介者支援 WebSocket/WebSocket Secure (WS/WSS) (通常在連接埠 443 上)，請改用此通訊協定。請洽詢伺服器/中介者提供者，以了解是否支援 WS/WSS，以及所需使用的連接埠和基本路徑。
- 如果伺服器/中介者支援 ALPN，可以透過開放的連接埠 (例如 443) 交涉使用 MQTT。請諮詢伺服器/中介者提供者，以了解是否支援 ALPN，以及所需使用的 ALPN 通訊協定和連接埠。

如果在這裡找不到您要的內容，請嘗試 *axis.com/support* 中的疑難排解區段。

效能考量

需要考慮的最重要因素：

- 由於基礎設施不佳而導致的網路密集使用會影響頻寬。

聯絡支援人員

如需更多協助，請前往 *axis.com/support*。

T10181936_zh_tw

2025-11 (M9.5)