AXIS A9210 Network I/O Relay Module

使用手冊

開始使用

開始使用

在網路上尋找設備

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該設備：

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

**若要在 iOS 15 或 iPadOS 15 中使用 AXIS OS 網頁介面，請前往 [設定 > Safari > 進階 > 實驗功能]，並停用 [NSURLSession Websocket]。*

如需更多關於建議使用的瀏覽器資訊，請前往 *AXIS OS 入口網站*。

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. 輸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。請參閱*建立管理員帳戶 2*。

有關您可能在設備網頁介面中遇到的所有控制項和選項的說明，請參閱 *網頁介面 6*。

建立管理員帳戶

首次登入設備必須建立管理員帳戶。

1. 輸入使用者名稱。
2. 輸入密碼。請參閱 *安全密碼 2*。
3. 重新輸入密碼。
4. 接受授權合約。
5. 按一下新增帳戶。

重要

設備沒有預設帳戶。如果遺失管理員帳戶的密碼，必須重設該設備。請參閱*重設為出廠預設設定 32*。

開始使用

安全密碼

重要

Axis 設備會以純文字格式透過網路傳送最初設定的密碼。若要在初次登入後保護您的設備，請設定安全且加密的 HTTPS 連線，然後變更密碼。

設備密碼是您的資料和服務的主要保護機制。Axis 設備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。

確認沒有人竄改韌體

若要確保設備有其原始 Axis 韌體，或要在安全攻擊後完全控制設備：

1. 重設為出廠預設值。請參閱*重設為出廠預設設定 32*。

   重設後，安全開機可保證回復設備的狀態。

2. 對設備進行設定和安裝。

網頁介面概觀

這段影片為您提供設備網頁介面的概觀。

如需觀看此影片，請前往此文件的網頁版本。

help.axis.com/?&piaId=92430&section=web-interface-overview

Axis 設備網頁介面

設定您的設備

設定 I/O 埠

1. 前往 [設備 > I/O 和繼電器 > AXIS A9210 > I/O]。
2. 按一下 ⌄ 以展開 I/O 埠設定。
3. 重新命名連接埠。
4. 設定正常狀態。開路請按一下 ，若為閉路則按一下 。
5. 若要將 I/O 埠設定為輸入：
   5.1 在方向下方，按一下 。
   5.2 若要監控輸入狀態，請開啟受監控。請參閱 *受監控的輸入 31*。

   備註

   在 API 中，受監控的 I/O 埠的運作方式與受監控的輸入埠不同。如需詳細資訊，請前往 *VAPIX® Library*。
6. 若要將 I/O 埠設定為輸出：
   6.1 在方向下方，按一下 。
   6.2 若要檢視啟動和停用已連接設備的 URL，請前往切換連接埠 URL。

設定繼電器

1. 前往 [設備 > I/O 和繼電器 > AXIS A9210 > 繼電器]。
2. 按一下 ⌄ 以展開繼電器設定。
3. 開啟繼電器。
4. 重新命名繼電器。
5. 若要檢視啟動和停用繼電器的 URL，請前往切換連接埠 URL。

設定事件規則

如需深入了解，請查看我們的指南 *開始使用事件規則*。

觸發動作

1. 前往 [系統 > 事件]，並新增規則。規則定義設備將執行特定動作的時間點。您可以將規則設定為排程、循環或手動觸發。
2. 輸入名稱。
3. 選取必須符合才能觸發動作的條件。如果您為規則指定多項條件，則必須符合所有條件才能觸發動作。

4. 選取設備在條件符合時所應執行的動作。

備註

如果對使用中規則進行變更，則必須重新開啟規則，才能讓變更生效。

網頁介面

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。

備註

對本節中所述功能及設定的支援會因設備不同而有所不同。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。
-  [變更帳戶]：登出目前帳戶並登入新帳戶。
-  [登出]：從目前帳戶登出。

 內容功能表包含：

- [分析資料]：接受可共用非個人瀏覽器資料。
- 意見反應：分享任何意見反應，以協助我們改善使用者體驗。
- 法律資訊：檢視有關 Cookie 和授權的資訊。
- 關於：查看設備資訊，包括韌體版本和序號。

狀態

設備資訊

顯示該設備的韌體版本和序號等資訊。

[升級韌體]：升級您的設備韌體。前往可用來進行韌體升級的 [維護] 頁面。

時間同步狀態

顯示 NTP 同步資訊，包括該設備是否與 NTP 伺服器同步以及下次同步前的剩餘時間。

[NTP 設定]：檢視和更新 NTP 設定。前往可變更 NTP 設定的 [日期和時間] 頁面。

安全性

網頁介面

顯示已啟用設備的存取類型，以及正在使用的加密協議。設定建議是依據 AXIS OS 強化指南。

[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]

顯示連接數和已連接的用戶端數。

[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。

I/O 埠和繼電器

設定

輸入

- 名稱：編輯文字以重新命名該連接埠。
- 方向：指明這是一個輸入埠。
- 正常狀態：開路請按一下 ，閉路則按一下 。
- 受監控：如果有人竄改與數位 I/O 設備的連線，請開啟此選項，讓設備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)。
  - 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。

輸出：開啟以啟動已連接的設備。

- 名稱：編輯文字以重新命名該連接埠。
- 方向：指明它是一個輸出埠。
- 正常狀態：開路請按一下 ，閉路則按一下 。
- 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。

I/O：當連接埠設定為輸出時，開啟以啟動已連接的設備。

- 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。
- 正常狀態：開路請按一下 ，閉路則按一下 。
- 受監控：如果有人竄改與數位 I/O 設備的連線，請開啟此選項，讓設備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。

網頁介面

繼電器

- 繼電器：開啟或關閉繼電器。
- 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。關閉空機門控制器的此設定。

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。

- 受監控的輸入：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。

應用程式

[新增應用程式]：安裝新增應用程式。

[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。

[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。

[允許 root 權限應用程式]：開啟以允許具有 root 權限的應用程式，完整存取該設備。

查看 AXIS OS 和 ACAP 應用程式中的安全性更新。

備註

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。

[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：

- [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。
- 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。
- [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。

- [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。
- [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，也會將該授權從設備中移除。
- [設定]：設定參數。
- [刪除]：從設備永久刪除應用程式。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。

備註

我們建議您將該設備的日期和時間與 NTP 伺服器同步。

[同步]：選取同步該設備的日期和時間的選項。

- [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。
  - 手動 NTS KE 伺服器：輸入一台或兩台 NTP 伺服器的 IP 位址。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。
- 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。
  - 備援 NTP 伺服器：輸入一台或兩台備援伺服器的 IP 位址。
- 自動日期和時間 (手動 NTP 伺服器)：與您選擇的 NTP 伺服器同步。
  - 手動 NTP 伺服器：輸入一台或兩台 NTP 伺服器的 IP 位址。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。
- 自訂日期和時間：手動設定日期和時間。按一下 [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。

[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。
- [手動]：從下拉式清單選取時區。

備註

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使用此資訊將設備放置在地圖上。

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

網路

IPv4

網頁介面

自動指派 IPv4：選取以允許網路路由器自動為設備指派 IP 位址。我們建議適用大多數網路的自動 IP (DHCP)。

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。

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。

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。

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。

備註

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

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

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。

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 -。

[DNS 伺服器]

[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)。

搜尋網域：使用不完整的主機名稱時，請按一下 [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 伺服器]：按一下 [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。

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。

若要在設備上使用 HTTPS，您必須安裝 HTTPS 憑證。前往 [系統 > 安全性] 以建立和安裝憑證。

網頁介面

允許存取方式：選取是否允許使用者透過 [HTTP]、[HTTPS]，或是 [HTTP 與 HTTPS] 通訊協定連線至該設備。

備註

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 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 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。

憑證：選取憑證來為設備啟用 HTTPS。

網路發現通訊協定

[Bonjour®]：啟用此選項可允許在網路上自動搜尋。

Bonjour 名稱：輸入可在網路上看到的易記名稱。預設名稱為設備名稱和網卡號碼。

[UPnP®]：開啟以允許在網路上自動搜尋。

UPnP 名稱：輸入可在網路上看到的易記名稱。預設名稱為設備名稱和網卡號碼。

[WS-發現]：開啟以允許在網路上自動搜尋。

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*。

[允許 O3C]：

- [單鍵]：此為預設設定。按住該設備上的控制按鈕，以透過網際網路連線至 O3C 服務。您必須在按下控制按鈕後 24 小時內，向 O3C 服務註冊設備。否則，該設備會中斷與 O3C 服務的連線。註冊該設備後，[永遠] 就會啟用，而且該設備會保持與 O3C 服務連線。
- 永遠：該設備會不斷嘗試透過網際網路連線至 O3C 服務。註冊該設備後，它就會與 O3C 服務保持連線。如果無法觸及該設備上的控制按鈕，請使用此選項。
- 否：停用 O3C 服務。

Proxy 設定：如有需要，輸入 Proxy 設定以連線至 proxy 伺服器。

主機：輸入 Proxy 伺服器的位址。

連接埠：輸入用於存取的連接埠號碼。

登入和密碼：如有需要，輸入 proxy 伺服器的使用者名稱和密碼。

[驗證方法]：

- [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，其安全性較摘要方法低。
- 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。
- 自動：此選項可讓設備根據支援的方法自動選取驗證方法。相較於 [基本] 方法，這會優先採用 [摘要] 方法。

擁有者驗證金鑰 (OAK)：按一下 [取得金鑰] 以擷取擁有者驗證金鑰。這只有在設備不使用防火牆或 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) 允許遠端管理網路設備。

SNMP：選取要使用的 SNMP 版本。

- v1 和 v2c：
  - 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 [公開]。
  - [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。
  - 啟用設陷：開啟以啟動設陷報告。設備使用設陷將重要的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。
  - 設陷位址：輸入管理伺服器的 IP 位址或主機名稱。
  - 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。
  - 設陷：
  - 冷啟動：在設備啟動時傳送設陷訊息。
  - 暖啟動：在您變更 SNMP 設定時傳送設陷訊息。
  - 上行連結：在連結從下行變更為上行時，傳送設陷訊息。
  - 驗證失敗：在驗證嘗試失敗時傳送設陷訊息。

備註

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。
  - 「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，您必須將設備重設回出廠預設設定。

安全性

[憑證]

憑證會用來驗證網路上的設備。設備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。自我簽署的憑證提供的保護有限，可以暫時在取得 CA 核發的憑證之前使用。
- [CA 憑證]
  您可以使用 CA 憑證來驗證對等憑證，例如當設備連線至受 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。設備有數個預先安裝的 CA 憑證。

支援以下格式：

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

重要

如果將設備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。

+ [新增憑證]：按一下可新增憑證。

- [更多] ⌄ ：顯示更多要填寫或選取的欄位。
- [安全金鑰儲存區]：選取使用 [安全元件] 或者 [信任的平台模組 2.0] 以安全地儲存私密金鑰。有關選取哪個私密金鑰的更多資訊，請前往 *help.axis.com/en-us/axis-os#cryptographic-support*。
- [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：

- [憑證資訊]：檢視已安裝之憑證的屬性。
- [刪除憑證]：刪除憑證。
- [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。

[安全金鑰儲存區] ⓘ ：

- [安全元件 (CC EAL6+)]：選取使用安全元件作為安全金鑰儲存區。
- [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。

[IEEE 802.1x and IEEE 802.1AE MACsec]

IEEE 802.1x 是一種連接埠型網路存取控制 (Network Admission Control) 的 IEEE 標準，為有線及無線網路設備提供安全驗證。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。

憑證

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

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。

[驗證方法]：選取用於驗證的 EAP 類型。預設選項是 [EAP-TLS]。[EAP-PEAP/MSCHAPv2] 是更安全的選項。

[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 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，該設備都會嘗試自行驗證。

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 版本：選取網路交換器所使用的 EAPOL 版本。

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

[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。

只有當您使用 EAP-TLS 作為驗證方法時，才可使用這些設定：

[模式]

- 動態 CAK/EAP-TLS：預設選項。安全連線後，設備會檢查網路上的 MACsec。
- 靜態 CAK/預先共用金鑰 (PSK)：選取以設定連接到網路的金鑰名稱和值。

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

- [密碼]：輸入您的使用者身分識別的密碼。
- [Peap 版本]：選取網路交換器所使用的 Peap 版本。
- [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。

防止暴力破解攻擊

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。

封鎖期間：輸入阻擋暴力破解攻擊的秒數。

封鎖條件：輸入開始封鎖前每秒允許的驗證失敗次數。您在頁面層級和設備層級上都可以設定允許的失敗次數。

[防火牆]

[啟用]：開啟防火牆。

[預設政策]：選取防火牆的預設狀態。

- [允許：] 允許與設備的所有連接。該選項是預設的。
- [拒絕：] 拒絕與設備的所有連接。

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

- 位址：輸入您想要允許或拒絕存取之 IPv4/IPv6 或 CIDR 格式的位址。
- [通訊協定]：選取您想要允許或拒絕存取的通訊協定。
- 連接埠：輸入您想要允許或拒絕存取的連接埠號碼。您可以新增 1 到 65535 之間的連接埠號碼。
- [政策]：選取規則的原則。

+ ：按一下以建立其他規則。

[新增規則：] 按一下以新增您定義的規則。

- [以秒為單位的時間：] 設定測試規則的時間限制。預設時間限制設定為 300 秒。若要立即啟用規則，請將時間設定為 0 秒。
- [確認規則：] 確認規則及其時間限制。如果您設定的時間限制超過 1 秒，則該規則將在這段時間內啟用。如果您已將時間設定為 0，這些規則將立即啟用。

[待處理規則]：您尚未確認的最新已測試規則概觀。

備註

有時間限制的規則會顯示在 [待定規則] 和 [作用中規則] 下，直到超過設定的時間，或直到您確認為止。如果不確認規則，它們只會出現在 [待定規則] 下，並且防火牆會退回至先前定義的設定。如果確認規則，它們將取代目前作用中規則。

[確認規則]：按一下以啟用待處理規則。

[作用中規則]：您目前在設備上執行之規則的概觀。

：按一下以刪除作用中規則。

：按一下以刪除所有規則，包括待定規則和作用中規則。

自訂的已簽署韌體憑證

若要在設備上安裝 Axis 的韌體或其他自訂韌體，您需要自訂簽署的韌體憑證。該憑證會確認此韌體是否由設備擁有者和 Axis 核准。韌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 建立自訂簽署的韌體憑證。

[安裝]：按一下以安裝憑證。安裝韌體之前需要先安裝憑證。

⋮ 內容功能表包含：

- [刪除憑證]：刪除憑證。

帳戶

[帳戶]

+ [新增帳戶]：按一下可新增帳戶。您最多可以新增 100 個帳戶。

[帳戶]：輸入唯一的帳戶名稱。

[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。

[再次輸入密碼]：再次輸入相同的密碼。

[權限]：

- [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。
- [操作者]：可存取所有設定，但以下除外：
  - 所有 [系統] 設定。
  - 新增應用程式。
- 觀看者：無法存取變更任何設定。

⋮ 內容功能表包含：

[更新帳戶]：編輯帳戶特性。

[刪除帳戶]：刪除帳戶。您無法刪除 root 帳戶。

[匿名存取]

[允許匿名觀看]：開啟可允許任何人以觀看者的身分存取設備，而無須登入帳戶。

[允許匿名 PTZ 操作] ⓘ ：開啟可讓匿名使用者水平轉動、上下轉動和變焦影像。

[SSH 帳戶]

+ [新增 SSH 帳戶]：按一下可新增新的 SSH 帳戶。

- [限制 root 存取]：開啟以限制需要 root 存取權限的功能。
- [啟用 SSH]：開啟以使用 SSH 服務。

[帳戶]：輸入唯一的帳戶名稱。

[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。

[再次輸入密碼]：再次輸入相同的密碼。

[註解]：輸入註解 (可選)。

⋮ 內容功能表包含：

[更新 SSH 帳戶]：編輯帳戶特性。

[刪除 SSH 帳戶]：刪除帳戶。您無法刪除 root 帳戶。

[OpenID 設定]

重要

輸入正確的值以確保您可以再次登入設備。

[用戶端 ID]：輸入 OpenID 使用者名稱。

[撥出 Proxy]：輸入 OpenID 連接的 proxy 位址以使用 proxy 伺服器。

[管理者申請]：輸入管理者角色的值。

[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

[操作者申請]：輸入操作者角色的值。

[需要申請]：輸入權杖中應包含的資料。

[觀看者申請]：輸入觀看者角色的值。

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

[範圍]：可以作為權杖一部分的可選範圍。

[用戶端秘密]：輸入 OpenID 密碼

[儲存]：按一下以儲存 OpenID 值。

[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。

事件

規則

規則定義了觸發產品執行動作的條件。此清單顯示目前在產品中設定的所有規則。

備註

最多可以建立 256 項動作規則。

+ [新增規則]：建立規則。

[名稱]：輸入規則的名稱。

[在動作之間等待]：輸入規則啟動之間必須經過的最短時間 (hh:mm:ss)。例如，這在規則是由日夜模式條件所啟動的情況下很有幫助，可避免日出與日落期間的微小光線變化重複啟動規則。

條件：從清單中選取條件。條件必須符合，才能讓設備執行動作。如果定義了多個條件，所有的條件都必須符合才會觸發動作。有關特定條件的資訊，請參閱*事件規則新手入門*。

[使用此條件作為觸發]：選取此選項，使這第一個條件僅用作起始觸發器。這表示，規則一經啟動後，只要所有其他條件都符合，無論第一個條件的狀態如何，該規則仍會繼續啟用。如果沒有選取此選項，只要所有條件都符合，規則就會處於作用中。

反轉此條件：如果您希望條件與您的選取相反，請選取此選項。

+ 新增條件：按一下可新增其他的條件。

動作：從清單中選取動作，並輸入其所需的資訊。有關特定動作的資訊，請參閱*事件規則新手入門*。

接收者

您可以設定讓設備將事件通知接收者，或使其傳送檔案。此清單會顯示產品中目前設定的所有接收者，以及這些接收者組態的相關資訊。

備註

您最多可以建立 20 接收者。

+ 新增接收者：按一下可新增接收者。

名稱：輸入接收者的名稱。

類型：從清單中選取：

- [FTP]
  - 主機：輸入伺服器的 IP 位址或主機名稱。如果輸入主機名稱，請確定已在 [系統 > 網路 > IPv4 和 IPv6] 下方指定 DNS 伺服器。
  - 連接埠：輸入 FTP 伺服器所使用的連接埠編號。預設為 21。
  - 資料夾：輸入要儲存檔案所在目錄的路徑。如果 FTP 伺服器中尚不存在此目錄，您將會在上傳檔案時收到錯誤訊息。
  - 使用者名稱：輸入登入的使用者名稱。
  - 密碼：輸入登入的密碼。
  - 使用暫存檔案名稱：選取使用自動產生的暫存檔案名稱來上傳檔案。上傳完成時，檔案會重新命名為所需的名稱。如果上傳中止/中斷，您不會收到任何損毀的檔案。不過，仍然可能收到暫存檔。如此一來，您就知道所有具有所需名稱的檔案都是正確的。
  - [使用被動 FTP]：在正常情況下，產品只需要求目標 FTP 伺服器開啟資料連線。設備會主動對目標伺服器起始 FTP 控制和資料連線。如果設備與目標 FTP 伺服器之間有防火牆，一般都需要進行此操作。
- HTTP
  - URL：輸入 HTTP 伺服器的網路位址以及將處理該要求的指令碼。例如，http://192.168.254.10/cgi-bin/notify.cgi。
  - [使用者名稱]：輸入登入的使用者名稱。
  - 密碼：輸入登入的密碼。

- Proxy：如果必須傳遞 Proxy 伺服器才能連線至 HTTP 伺服器，請開啟並輸入必要的資訊。
- HTTPS
  - URL：輸入 HTTPS 伺服器的網路位址以及將處理該要求的指令碼。例如，https://192.168.254.10/cgi-bin/notify.cgi。
  - [驗證伺服器憑證]：選取此選項以驗證 HTTPS 伺服器所建立的憑證。
  - 使用者名稱：輸入登入的使用者名稱。
  - 密碼：輸入登入的密碼。
  - Proxy：如果必須透過 Proxy 伺服器才能連接至 HTTPS 伺服器，請開啟並輸入必要的資訊。
- [網路儲存空間]
  您可以新增 NAS (網路附加儲存) 等網路儲存空間，並將其用作儲存檔案的接收者。檔案會以 Matroska (MKV) 檔案格式儲存。
  - 主機：輸入網路儲存空間的 IP 位址或主機名稱。
  - 共用區：輸入主機上共用區的名稱。
  - 資料夾：輸入要儲存檔案所在目錄的路徑。
  - 使用者名稱：輸入登入的使用者名稱。
  - 密碼：輸入登入的密碼。
- [SFTP]
  - 主機：輸入伺服器的 IP 位址或主機名稱。如果輸入主機名稱，請確定已在 [系統 > 網路 > IPv4 和 IPv6] 下方指定 DNS 伺服器。
  - 連接埠：輸入 SFTP 伺服器所使用的連接埠編號。預設為 22。
  - 資料夾：輸入要儲存檔案所在目錄的路徑。如果 SFTP 伺服器中尚不存在此目錄，您將會在上傳檔案時收到錯誤訊息。
  - 使用者名稱：輸入登入的使用者名稱。
  - 密碼：輸入登入的密碼。
  - SSH 主機公開金鑰類型 (MD5)：輸入遠端主機公開金鑰的指紋 (32 位數十六進位字串)。SFTP 用戶端使用主機金鑰類型為 RSA、DSA、ECDSA 和 ED25519 的 SSH-2 來支援 SFTP 伺服器。RSA 是進行交涉時的首選方法，其次是 ECDSA、ED25519 和 DSA。務必輸入您的 SFTP 伺服器所使用的正確 MD5 主機金鑰。雖然 Axis 設備同時支援 MD5 和 SHA-256 雜湊金鑰，但我們建議使用 SHA-256，因為它的安全性比 MD5 更強。有關如何使用 Axis 設備設定 SFTP 伺服器的更多資訊，請前往 *AXIS OS 入口網站*。
  - SSH 主機公開金鑰類型 (SHA256)：輸入遠端主機公開金鑰的指紋 (43 位數 Base64 編碼字串)。SFTP 用戶端使用主機金鑰類型為 RSA、DSA、ECDSA 和 ED25519 的 SSH-2 來支援 SFTP 伺服器。RSA 是進行交涉時的首選方法，其次是 ECDSA、ED25519 和 DSA。務必輸入您的 SFTP 伺服器所使用的正確 MD5 主機金鑰。雖然 Axis 設備同時支援 MD5 和 SHA-256 雜湊金鑰，但我們建議使用 SHA-256，因為它的安全性比 MD5 更強。有關如何使用 Axis 設備設定 SFTP 伺服器的更多資訊，請前往 *AXIS OS 入口網站*。
  - 使用暫存檔案名稱：選取使用自動產生的暫存檔案名稱來上傳檔案。上傳完成時，檔案會重新命名為所需的名稱。如果上傳中止或中斷，您不會收到任何損毀的檔案。不過，仍然可能收到暫存檔。如此一來，您就知道所有具有所需名稱的檔案都是正確的。
- [SIP 或 VMS] ：
  [SIP]：選取以撥打 SIP 電話。
  [VMS]：選取以撥打 VMS 電話。
  - 來自 SIP 帳戶：從清單中選取。
  - 至 SIP 位址：輸入 SIP 位址。
  - 測試：按一下可測試通話設定是否有效。
- 電子郵件
  - [將電子郵件傳送至]：輸入電子郵件要傳送到的電子郵件地址。若要輸入多個地址，請使用逗號將地址隔開。
  - 從此寄件者傳送電子郵件：輸入傳送伺服器的電子郵件地址。
  - 使用者名稱：輸入郵件伺服器的使用者名稱。如果郵件伺服器不需要驗證，請讓此欄位保持空白。
  - 密碼：輸入郵件伺服器的密碼。如果郵件伺服器不需要驗證，請讓此欄位保持空白。
  - [電子郵件伺服器 (SMTP)]：輸入 SMTP 伺服器的名稱，例如：smtp.gmail.com、smtp.mail.yahoo.com。
  - [連接埠]：使用 0-65535 這個範圍的值，輸入 SMTP 伺服器的連接埠編號。預設值為 587。

- 加密：若要使用加密，請選取 SSL 或 TLS。
- 驗證伺服器憑證：如果您使用加密，請選取此選項來驗證設備的身分識別。憑證可以自行簽署，或由憑證機構 (CA) 發出。
- [POP 驗證]：開啟此選項以輸入 POP 伺服器的名稱，例如：pop.gmail.com。

備註

部分電子郵件供應商設有安全過濾器，可防止使用者接收或檢視大量附件，或接收排程的電子郵件和類似訊息。檢查電子郵件供應商的安全性政策，以避免您的電子郵件帳戶遭鎖定，或是收不到預期的電子郵件。

• TCP
- 主機：輸入伺服器的 IP 位址或主機名稱。如果輸入主機名稱，請確定已在 [系統 > 網路 > IPv4 和 IPv6] 下方指定 DNS 伺服器。
- 連接埠：輸入用於存取伺服器的連接埠編號。

測試：按一下可測試設定。

內容功能表包含：

檢視接收者：按一下可檢視所有接收者詳細資訊。

複製接收者：按一下可複製接收者。複製時，您可以對新的接收者進行變更。

刪除接收者：按一下可永久刪除接收者。

排程

排程和脈衝可以當做規則中的條件使用。此清單會顯示產品中目前設定的所有排程和脈衝，以及其組態的相關資訊。

新增排程：按一下可建立排程或脈衝。

手動觸發器

手動觸發是用來手動觸發動作規則。例如，手動觸發可在產品安裝和設定期間用來驗證動作。

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設備。Axis 設備韌體中的 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。

將設備設定為 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。用戶端可以傳送和接收訊息。中介者則負責在用戶端之間配發訊息。

您可以在 *AXIS OS 入口網站*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 用戶端

連線：開啟或關閉 MQTT 用戶端。

狀態：顯示 MQTT 用戶端目前的狀態。

中介者

主機：輸入 MQTT 伺服器的主機名稱或 IP 位址。

通訊協定：選取要使用的通訊協定。

連接埠：輸入連接埠號碼。

- 1883 是 TCP 上的 MQTT 的預設值
- 8883 是透過 SSL 的 MQTT 的預設值
- 80 是 WebSocket 上的 MQTT 的預設值
- 443 是 WebSocket Secure 上的 MQTT 的預設值

[ALPN 通訊協定]：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。

使用者名稱：輸入用戶端將用來存取伺服器的使用者名稱。

密碼：輸入使用者名稱的密碼。

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。

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]：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]：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。

[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。

逾時：允許連線完成的間隔時間 (以秒為單位)。預設值：60

設備主題首碼：在 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 公開發行索引標籤上公開條件。

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。

傳送訊息：開啟以傳送訊息。

使用預設：關閉以輸入您自己的預設訊息。

主題：輸入預設訊息的主題。

承載：輸入預設訊息的內容。

保留：選取以保持用戶端在此主題上的狀態

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。

傳送訊息：開啟以傳送訊息。

使用預設：關閉以輸入您自己的預設訊息。

主題：輸入預設訊息的主題。

承載：輸入預設訊息的內容。

保留：選取以保持用戶端在此主題上的狀態

QoS：變更封包流的 QoS 層。

MQTT 發佈

使用預設主題字首：選取使用預設主題字首，此字首是在 MQTT 用戶端索引標籤的設備主題字首中定義。

包括主題名稱：選取包括在 MQTT 主題中描述條件的主題。

包括主題命名空間：選取以便包括在 MQTT 主題中的 ONVIF 主題命名空間。

包括序號：選取在 MQTT 承載中包括設備的序號。

+ 新增條件：按一下可新增條件。

保留：定義要傳送為保留的 MQTT 訊息。

- 無：傳送所有訊息為不保留。
- 屬性：僅傳送狀態訊息為保留。
- 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

+ 新增訂閱：按一下可加入新的 MQTT 訂閱。

訂閱過濾：輸入您要訂閱的 MQTT 主題。

使用設備主題首碼：將訂閱過濾當做首碼新增至 MQTT 主題。

訂閱類型：

- 無狀態：選取將 MQTT 訊息轉換為無狀態訊息。
- 具狀態：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。

記錄

報告和記錄

報告

- [檢視設備伺服器報告]：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。
- [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。
- [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

- 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。
- [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。

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，協助您對問題進行疑難排解。

追蹤時間：選取追蹤持續期間 (秒或分鐘)，然後按一下 [下載]。

遠端系統記錄

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。

+ 伺服器：按一下可新增伺服器。

主機：輸入伺服器的主機名稱或 IP 位址。

[格式化]：選取要使用的 syslog 訊息格式。

- Axis
- RFC 3164
- RFC 5424

[通訊協定]：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)

[連接埠]：編輯連接埠號碼以使用不同的連接埠。

[嚴重性]：選取觸發時要傳送的訊息。

[CA 憑證組]：查看目前設定或新增憑證。

一般設定

一般設定適用於具有 Axis 設備組態設定經驗的進階使用者。大部分的參數都可以透過本頁面進行設定和編輯。

維護

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。

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)
- 靜態 IP 位址
- Default router
- [子網路遮罩]
- 802.1X 設定
- O3C 設定
- DNS 伺服器 IP 位址

[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。

備註

所有 Axis 設備韌體皆經過數位簽署，以確保您僅將經過驗證的韌體安裝於設備上。這會進一步提高 Axis 設備的整體最低網路安全等級。如需詳細資訊，請參閱位於 *axis.com* 的「已簽署的韌體、安全開機，以及私密金鑰的安全性」白皮書。

韌體升級：升級到新的韌體版本。新韌體版本可以包含改良的功能、錯誤修正和全新功能。我們建議您永遠都使用最新版本。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：

- 標準升級：升級到新的韌體版本。
- 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韌體版本。
- 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韌體版本。

韌體回復：回復到之前安裝的韌體版本。

深入了解

網路安全

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。其所提供的功能可以確保設備的身分識別和完整性，並保護您的敏感性資訊免遭未經授權的存取。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，並結合邊際設備安全性的專業技術。

已簽署的韌體

已簽署的韌體由使用私密金鑰簽署韌體映像的軟體廠商實作。韌體附加簽章時，設備將會在接受韌體安裝前驗證韌體。如果設備偵測到韌體完整性遭入侵，將會拒絕韌體升級。

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。安全開機以簽署的韌體為基礎，確保設備僅能使用授權的韌體開機。

安全金鑰儲存區

用於保護私有金鑰和密碼作業安全執行的防竄改環境。如果發生安全漏洞，這可以防止未經授權的存取和惡意擷取。根據安全要求，Axis 設備可能會有一個或多個硬體式加密計算模組，這些模組會提供硬體保護的安全金鑰儲存區。根據安全要求，Axis 設備可能會有一個或多個硬體式加密計算模組，例如 TPM 2.0 (信賴平台模組) 或安全元件，和/或 TEE (可信賴執行環境)，這些都會提供硬體保護的安全金鑰儲存區。此外，選取的 Axis 產品具有 FIPS 140-2 等級 2 認證的安全金鑰儲存區。

Axis 設備 ID

對於建立對設備身分識別的信任來說，能夠驗證設備的來源至關重要。在製造過程中，會為包含 Axis Edge Vault 的設備指派一個唯一、原廠佈建且符合 IEEE 802.1AR 標準的 Axis 設備 ID 憑證。它的作用就像護照一樣，可以證明設備的來源。設備 ID 做為由 Axis 根憑證簽署的憑證，會安全且永久地存放在安全金鑰儲存區中。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

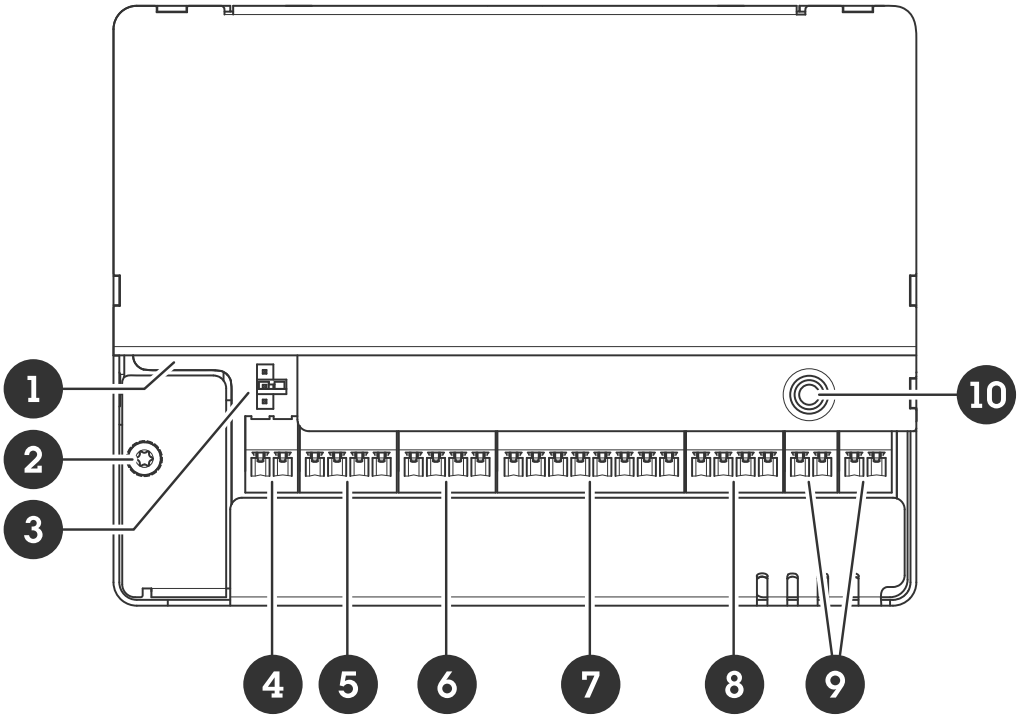
加密檔案系統

安全金鑰庫可防止資訊被惡意洩露，並透過對檔案系統執行強加密來防止設定竄改。這可確保在設備未使用、未經授權存取設備和/或 Axis 設備失竊時，無法擷取或竄改儲存在檔案系統中的資料。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

產品概觀



1 網路連接器
2 接地位置
3 繼電器跳線
4 電源接頭
5 繼電器接頭
6 輸入 1 連接器
7 RS485 和 I/O 連接端子
8 I/O 連接端子
9 輸入 2 連接器
10 控制按鈕

規格

LED 指示燈

LED	顏色	指示
狀態	綠色	綠燈常亮表示正常操作。
	琥珀色	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。
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。
	琥珀色	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。
電源	綠色	正常操作。
	琥珀色	升級韌體時綠色/琥珀色交替閃爍。
繼電器	綠色	繼電器已啟用。[1]
	熄滅	繼電器未啟用。

1. COM 連接至 NO 時，繼電器處於作用中狀態。

按鈕

控制按鈕

控制按鈕用於：

- 將產品重設為出廠預設值。請參閱*重設為出廠預設設定 32*。
- 透過網際網路連接至單鍵雲端連線 (O3C) 服務。若要連線，請按住按鈕約 3 秒鐘，直到狀態 LED 開始閃爍綠色。

接頭

網路連接器

支援增強型乙太網路供電 (PoE+) 的 RJ45 乙太網路連接器。

UL：乙太網路供電 (PoE) 應透過乙太網路 IEEE 802.3af/802.3，Type 1 Class 3 或 PoE+ IEEE 802.3，Type 2 Class 4 功率受限注入器提供 44—57 V DC，15.4 W/30 W。PoE 已通過 UL 對 AXIS T8133 Midspan 30 W 1-port 的評估。

電源優先順序

此設備可由 PoE 或 DC 輸入供電。請參閱*網路連接器 26*和*電源接頭 27*。

- 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。

電源接頭

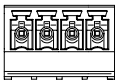
2 針腳接線端子，用於 DC 電源輸入。使用符合安全額外低電壓 (SELV) 的限功率電源 (LPS)，可以是額定輸出功率限制在 ≤100 W 或額定輸出電流限制在 ≤5 A 的電源。

功能	針腳	備註	規格
DC 接地 (GND)	1		0 V DC
DC 輸入	2	不使用乙太網路供電的情況下為設備供電。 注意：此針腳只能做為電源輸入使用。	12 V DC，最大 36 W

UL：DC 電源根據應用場合，由 UL 603 列名電源供應器在適當額定值下提供。

繼電器接頭

一個 C 型繼電器的一組 4 針腳接線端子，可用於 (例如) 控制門鎖或介面。如果用於電感性負載 (如門鎖)，請將一個二極體與負載並聯以防止瞬態電壓。



功能	針腳	備註	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 與 DC 接地之間連接失效安全鎖。 如果不使用跳線，則兩個繼電器針腳會與電路的其餘部分電氣隔離。	最大電流 = 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 與 DC 接地之間連接失效安全鎖。 如果不使用跳線，則兩個繼電器針腳會與電路的其餘部分電氣隔離。	

繼電器電源跳線

規格

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。

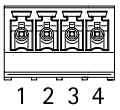
可用於連接 GND 與 NO 之間或 GND 與 NC 針腳之間的鎖。

電源	最大功率，於 12 V DC	最大功率，於 24 V DC
DC IN	2000 mA	1000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

輸入 1 連接器

一組 4 針腳接線端子，用於輸入。

可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 *受監控的輸入 31*。



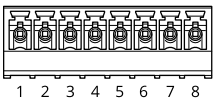
功能	針腳	備註	規格
DC 接地	1, 3		0 V DC
輸入	2, 4	數位輸入或受監控的輸入 - 分別連接到針腳 1 或 3 以啟動，或浮接 (不連接) 以停用。	0 到最大 30 V DC

重要

如果符合下列纜線需求，最多可支援的纜線長度達 200 公尺 (656 英呎)： AWG 24。

RS485 和 I/O 連接端子

一組 8 針腳接線端子，包括 4 針 RS485 和 4 針 I/O。



RS485

功能	針腳	備註	規格
DC 接地 (GND)	1		0 V DC
DC 輸出 (+12 V)	2	為輔助設備 (如 Modbus 感應器) 供電。	12 V DC，最大 200 mA
A	3		
B	4		

規格

I/O

功能	針腳	備註	規格
數位輸出	5	如果用於電感性負載 (如繼電器)，請將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
數位輸出	6	如果用於電感性負載 (如繼電器)，請將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
輸入	7	數位輸入或受監控的輸入 - 連接到針腳 1 以啟動，或浮接 (不連接) 以停用。	0 到最大 30 V DC
數位輸出	8	如果用於電感性負載 (如繼電器)，請將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

- 如果符合下列纜線需求，對 RS485 最多可支援的纜線長度達 1000 公尺 (3281 英呎)： 1 條有屏蔽的雙絞線，AWG 24，120 歐姆阻抗。
- 對 I/O 最多可支援的纜線長度達 200 公尺 (656 英呎)。

I/O 連接端子

將輔助連接器搭配外部設備結合位移偵測、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。

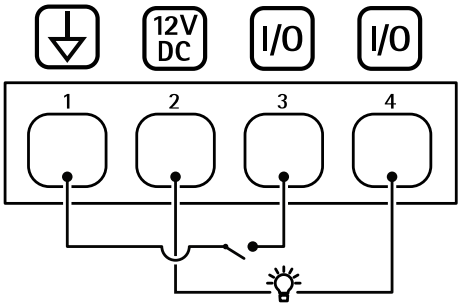
數位輸出 - 用於連接繼電器和 LED 等外接式設備。連接的設備可以由 VAPIX® 應用程式開發介面或從產品的網頁加以啟動。

4 針腳接線端子

功能	針腳	備註	規格
DC 接地	1		0 V DC
DC 輸出	2	可用來為輔助設備供電。 注意： 此針腳只能當做電源輸出使用。	12 V DC 最大負載 = 總計 50 mA

規格

可設定 (輸入或輸出)	3—4	數位輸入或受監控的輸入 - 連接到針腳 1 以啟動，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)，請將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 I/O 可以驅動 12 V DC、50 mA (合計最大) 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，則每個 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

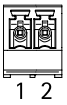


1 DC 接地
2 DC 輸出 12 V
3 I/O 設定為輸入
4 I/O 設定為輸出

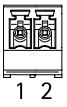
輸入 2 連接器

用於外部設備的兩個 2 針腳接線端子，例如：玻璃破碎偵測器或火災偵測器。

UL：連接器未經 UL 評估用於防盜或火警用途。



功能	針腳	備註	規格
DC 接地	1		0 V DC
輸入	2	數位輸入或受監控的輸入 - 連接到針腳 1 以啟動，或浮接 (不連接) 以停用。	0 到最大 30 V DC



規格

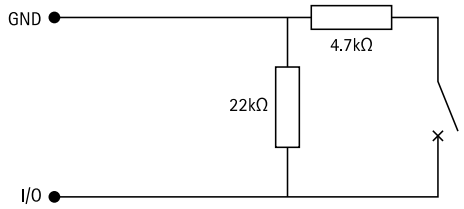
功能	針腳	備註	規格
DC 接地	1		0 V DC
輸入	2	數位輸入或受監控的輸入 - 連接到針腳 1 以啟動，或浮接 (不連接) 以停用。	0 到最大 30 V DC

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。

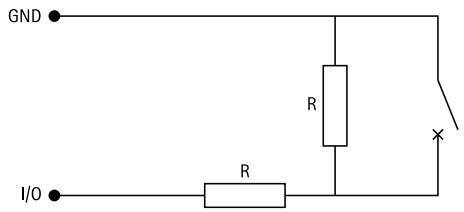
第一並聯連接

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。



備註

建議使用雙絞線和遮蔽型纜線。將屏蔽設備連接至 0 V DC。

狀態	說明
開啟	受監控的開關為開啟模式。
關閉	受監控的開關為已關閉模式。
短路	I/O 或輸入 1-5 纜線對 GND 短路。
切斷	I/O 或輸入 1-5 纜線已切斷並保持開路，沒有通往 GND 的電流路徑。

疑難排解

重設為出廠預設設定

重要

重設為出廠預設值應小心使用。重設為出廠預設值會將 IP 位址在內的所有設定，都重設為出廠預設值。

若要將產品重設為出廠預設值：

1. 將產品斷電。
2. 按住控制按鈕，同時重新接通電源。請參閱*產品概觀 25*。
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。產品已重設為出廠預設值。如果網路中沒有可用的 DHCP 伺服器，預設的 IP 位址會是 `192.168.0.90`。
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 [維護] > [出廠預設值]，並按一下 [預設]。

韌體選項

Axis 根據主動式常規或長期支援 (LTS) 常規提供產品韌體管理。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，建議主動式常規提供的韌體。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 產品韌體策略的詳細資訊，請前往 *axis.com/support/device-software*。

檢查目前的韌體版本

韌體是決定網路設備功能的軟體。對問題進行故障排除時，建議您先從檢查目前韌體版本開始著手。最新韌體版本可能包含修復特定問題的修正。

若要檢查目前的韌體：

1. 前往設備的網頁介面 > [狀態]。
2. 請參閱 [設備資訊] 下的韌體版本。

升級韌體

重要

- 升級韌體時，系統會儲存預先設定和自訂的設定 (假如新韌體中提供這些功能)，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。

備註

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

1. 將韌體檔案下載至電腦，請前往 *axis.com/support/device-software* 免費下載。
2. 以管理員身分登入設備。
3. 前往 [維護 > 韌體升級]，並按一下 [升級]。

升級完成後，產品會自動重新啟動。

技術問題、線索和解決方式

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。

升級韌體時發生問題	
韌體升級失敗	如果韌體升級失敗，則設備會重新載入之前的韌體。最常見的原因是上傳了錯誤的韌體檔案。請檢查韌體檔案名稱是否與您的設備相對應，然後重試。
升級韌體後發生問題	如果您在升級韌體後遇到問題，請從 [維護] 頁面回復之前安裝的版本。

設定 IP 位址時發生問題	
設備位在不同的子網路上	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。
另一個設備正在使用此 IP 位址	中斷 Axis 設備與網路的連接。執行 ping 命令 (在命令/DOS 視窗中，輸入 `ping` 和設備的 IP 位址)： • 如果您收到：`回覆自 <IP 位址>: 位元組=32; 時間=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，然後重新安裝設備。 • 如果您收到：`要求逾時`，這表示此 IP 位址可供 Axis 設備使用。請檢查所有接線，然後重新安裝設備。
IP 位址可能與相同子網路上的另一個設備發生衝突	在 DHCP 伺服器設定動態位址之前會使用 Axis 設備中的固定 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。

無法從瀏覽器存取設備	
無法登入	當啟用 HTTPS 時，請確定嘗試登入時有使用正確的通訊協定 (HTTP 或 HTTPS)。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。請參閱 *重設為出廠預設設定 32*。
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。使用設備的型號或序號來識別設備，如果已設定 DNS 名稱，則使用該名稱來識別。 如有需要，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 設備中的日期和時間設定必須與 NTP 伺服器同步。前往 [系統 > 日期和時間]。

疑難排解

設備可在本機加以存取，但無法從外部存取

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 Companion： 免費，非常適合具有基本監控需求的小型系統使用。
- AXIS Camera Station： 有 30 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*。

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，則可以透過開放連接埠 (例如 443) 交涉 MQTT 的使用。請洽詢伺服器/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。

聯絡支援人員

如需更多協助，請前往 *axis.com/support*。

使用手冊
AXIS A9210 Network I/O Relay Module
版本 M2.2
日期： 4 月 2024
零件編號 T10202445