AXIS D4100-VE Mk II Network Strobe Siren

使用手冊

目錄

安裝

開始使用

⚠ 警告

閃爍或頻閃光線可能會引起光敏性癲癇患者的症狀發作。

在網路上尋找裝置

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™	Firefox®	Edge™	Safari®
Windows®	建議	建議	✓	
macOS®	建議	建議	✓	✓
Linux®	建議	建議	✓	
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 [Settings (設定) > Safari > Advanced (進階) > Experimental Features (實驗功能)]，並停用 [NSURLSession Websocket]。

開啟設備的網頁介面

1. 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)]。

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 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。

設定您的設備

安裝警報器後關閉維護模式

⚠ 小心

為保護安裝人員免受聽力損傷和強光刺眼，建議在安裝設備時開啟維護模式。

首次安裝設備時，維護模式預設為開啟。當設備處於維護模式時，警報器不發出聲音，並且燈發出白色脈衝光圖案。

前往 [概觀] > [維護] 以關閉 [維護模式]。

開啟維護模式

如果要執行設備的服務，請前往 [概觀] > [維護] 並開啟 [維護模式]。然後暫停普通的燈光和警報器活動。

設定一個設定檔

設定檔是設定組態集合。您最多可以擁有 30 個具有不同優先順序和模式的設定檔。

如果要設定新的設定檔：

1. 前往 [設定檔]，然後按一下 [+ 建立]。
2. 輸入 [名稱] 和 [說明]。
3. 選取您的設定檔所需的 [燈光] 和 [警報器] 設定。
4. 設定燈光和警報器 [優先順序]，然後按一下 [儲存]。

如果要編輯設定檔，請按一下 [⋮] 並選取 [編輯]。

匯入或匯出設定檔

如果要使用已預先定義組態的的設定檔，可以將其匯入：

1. 前往 [設定檔]，然後按一下 [+ 匯入]。
2. 瀏覽以找到檔案或拖曳要匯入的檔案。
3. 按一下 Save (儲存)。

如果要複製一個或多個設定檔並儲存到其他設備，可以將其匯出：

1. 選取設定檔。
2. 按一下 [匯出]。
3. 瀏覽以找到 .json 檔案。

設定直接 SIP (P2P)

在相同 IP 網路中的幾個使用者代理之間進行通訊，而且不需要 PBX 伺服器可以提供的額外功能時，請使用點對點設定。若要更能了解 P2P 的運作方式，請參閱。

如需有關設定選項的詳細資訊，請參閱。

1. 前往系統 > SIP > SIP 設定，並選取啟用 SIP。
2. 若要允許裝置接聽來電，請選取 [Allow incoming calls (允許撥入的通話)]。
3. 在來電處理下方，設定來電逾時和持續時間。

4. 在連接埠下方，請輸入連接埠號碼。
   - SIP 連接埠 — 用於 SIP 通訊的網路連接埠。通過此連接埠的訊號流量並不會加密。預設連接埠號碼為 5060。如有需要，請輸入其他連接埠號碼。
   - TLS 連接埠 — 用於加密 SIP 通訊的網路連接埠。通過此連接埠的訊號流量會以傳輸層安全性 (TLS) 加密。預設連接埠號碼為 5061。如有需要，請輸入其他連接埠號碼。
   - RTP start port (RTP 起始連接埠) — 輸入用於 SIP 通話中第一個 RTP 媒體串流的連接埠。媒體傳輸的預設起始連接埠為 4000。某些防火牆可能會封鎖特定連接埠號碼上的 RTP 流量。連接埠號碼必須介於 1024 至 65535 之間。
5. 在 [NAT 周遊] 中，選取您想要為 NAT 周遊啟用的通訊協定。

附註

當裝置從 NAT 路由器或防火牆後面連接到網路時，請使用 NAT 周遊。如需詳細資訊，請參閱 。

6. 在音訊下方，為 SIP 通話至少選取一個具有所需音質的聲音轉碼器。拖放即可變更優先順序。
7. 在其他下方，請選取其他選項。
   - [UDP 轉 TCP 切換] — 選取此選項可讓通話將傳輸通訊協定暫時從 UDP (使用者資料包通訊協定) 切換成 TCP (傳輸控制通訊協定)。切換的原因是為了避免資料分散，如果某個要求是在最大傳輸單元的 200 個位元組以內，或是大於 1300 個位元組，則可以進行切換。
   - 允許透過重新寫入 — 選取啟此選項可傳送本機 IP 位址，而不傳送路由器的公用 IP 位址。
   - 允許聯絡人重新寫入 — 選取啟此選項可傳送本機 IP 位址，而不傳送路由器的公用 IP 位址。
   - 向伺服器進行登錄的間隔 — 設定設備多久一次向現有 SIP 帳戶的 SIP 伺服器進行登錄。
   - DTMF 承載類型 — 變更 DTMF 預設的承載類型。
8. 按一下 Save (儲存)。

透過伺服器 (PBX) 設定 SIP

應該在 IP 網路內外無限數量的使用者代理之間進行通訊時，請使用 PBX 伺服器。可以根據 PBX 提供者將其他功能新增到設定中。若要更能了解 P2P 的運作方式，請參閱。

如需有關設定選項的詳細資訊，請參閱。

1. 向您的 PBX 提供者要求以下資訊：
   - 使用者 ID
   - 網域
   - 密碼
   - 驗證 ID
   - 來電顯示
   - 登錄伺服器
   - RTP 起始連接埠
2. 若要新增帳戶，請前往系統 > SIP > SIP 帳戶，然後按一下 + 帳戶。
3. 請輸入從 PBX 供應商收到的詳細資訊。
4. 請選取已註冊。
5. 選取傳輸模式。
6. 按一下 Save (儲存)。
7. SIP 設定的設定方式與點對點設定相同。如需詳細資訊，請參閱 。

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 [System (系統) > Events (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 [Name (名稱)]。
3. 選取必須符合才能觸發動作的 [Condition (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. 選取裝置在條件符合時所應執行的 [Action (動作)]。

附註

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。

觸發警報時啟動設定檔

此範例說明如何在數位輸入訊號變更時觸發警報。

設定連接埠的方向輸入：

1. 前往 [系統] > [配件] > [I/O 埠]。
2. 前往 [連接埠 1] > [正常位置]，然後按一下 [電路閉合]。

建立規則：

1. 前往 [系統] > [事件]，並新增規則。
2. 輸入規則名稱。
3. 在條件清單中，選取 [I/O] > [數位輸入]。
4. 選取 [連接埠 1]。
5. 在動作清單中，選取在規則作用時執行 燈光和警報器設定檔。
6. 選取要啟動的設定檔。
7. 按一下 Save (儲存)。

透過 SIP 啟動設定檔

此範例說明如何透過 SIP 觸發警報。

啟用 SIP：

1. 前往系統 > SIP > SIP 設定。
2. 選取 [啟用 SIP] 和 [允許來電]。
3. 按一下 Save (儲存)。

建立規則：

1. 前往 [系統] > [事件]，並新增規則。
2. 輸入規則名稱。
3. 在條件清單中，選取 [通話] > [狀態]。
4. 在狀態清單中，選取 [作用中]。
5. 在動作清單中，選取在規則作用時執行 燈光和警報器設定檔。
6. 選取要啟動的設定檔。
7. 按一下 Save (儲存)。

透過 SIP 擴充功能控制多個設定檔

啟用 SIP：

1. 前往系統 > SIP > SIP 設定。
2. 選取 [啟用 SIP] 和 [允許來電]。
3. 按一下 Save (儲存)。

建立規則以啟動設定檔：

1. 前往 [系統] > [事件]，並新增規則。
2. 輸入規則名稱。
3. 在條件清單中，選取 [通話] > [狀態變更]。
4. 在原因清單中，選取 [被設備接受]。
5. 在 [呼叫方向]，選取 [撥入]。
6. 在 [本機 SIP URI]，輸入 sip:[Ext]@[IP address]，其中 [Ext] 是用於設定檔的副檔名，[IP 位址] 是設備位址。例如 sip:1001@192.168.0.90。
7. 在動作清單中，選取 [燈光和警報器] > 執行 燈光和警報器設定檔。
8. 選取要啟動的設定檔。
9. 選取動作 [啟動]。
10. 按一下 Save (儲存)。

建立規則以停止設定檔：

1. 前往 [系統] > [事件]，並新增規則。
2. 輸入規則名稱。
3. 在條件清單中，選取 [通話] > [狀態變更]。
4. 在原因清單中，選取 [終止]。
5. 在 [呼叫方向]，選取 [撥入]。
6. 在 [本機 SIP URI]，輸入 sip:[Ext]@[IP address]，其中 [Ext] 是用於設定檔的副檔名，[IP 位址] 是設備位址。例如 sip:1001@192.168.0.90。
7. 在動作清單中，選取 [燈光和警報器] > 執行 燈光和警報器設定檔。
8. 選取您要停止的設定檔。
9. 選取動作 [停止]。
10. 按一下 Save (儲存)。

重複這些步驟，為您要透過 SIP 控制的每個設定檔建立啟動和停止規則。

執行兩個具有不同優先順序的設定檔

如果執行兩個具有不同優先順序的設定檔，編號優先順序較高的設定檔將中斷編號優先順序較低的設定檔。

附註

如果執行兩個優先順序相同的設定檔，最新的設定檔將取消前一個。

此範例說明如何將設備設定為在由數位 I/O 埠觸發時顯示一個優先順序為 4 的設定檔，而非優先順序為 3 的其他設定檔。

建立設定檔：

1. 建立優先順序為 3 的設定檔。
2. 建立另一個優先順序為 4 的設定檔。

建立規則：

1. 前往 [系統] > [事件]，並新增規則。
2. 輸入規則名稱。
3. 在條件清單中，選取 [I/O] > [數位輸入]。
4. 選取連接埠。
5. 在動作清單中，選取在規則作用時執行 燈光和警報器設定檔。
6. 選取編號優先順序最高的設定檔。
7. 按一下 Save (儲存)。
8. 前往 [設定檔] 並啟動編號優先順序最低的設定檔。

當攝影機偵測到位移時，系統會透過虛擬輸入啟動閃光警報器

此範例說明每當安裝在攝影機中的應用程式 AXIS Motion Guard 偵測到位移時，如何將攝影機連接至閃光警報器，並啟用閃光警報器中的設定檔。

開始之前：

- 在閃光警報器中使用操作者或系統管理員權限建立新帳戶。
- 在閃光警報器中建立設定檔。
- 在攝影機中設定 AXIS Motion Guard，然後建立名為「攝影機設定檔」的設定檔。

在攝影機中建立兩位接收者：

1. 在攝影機的設備介面中，前往 [系統 > 事件 > 接收者]，然後新增接收者。
2. 輸入下列資訊：
   - [Name (名稱)]：啟用虛擬連接埠
   - 類型：HTTP
   - URL：http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
請將 <IPaddress> 換成閃光警報器的位址。
   - 新建立閃光警報器帳戶的帳戶和密碼。
3. 按一下 [測試]，以確認所有資料都有效。
4. 按一下 Save (儲存)。
5. 使用下列資訊加入第二位接收者：
   - [Name (名稱)]：停用虛擬連接埠
   - 類型：HTTP
   - URL：http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
請將 <IPaddress> 換成閃光警報器的位址。
   - 新建立閃光警報器帳戶的帳戶和密碼。
6. 按一下 [測試]，以確認所有資料都有效。
7. 按一下 Save (儲存)。

在攝影機中建立兩條規則：

1. 前往 [規則]，並新增規則。
2. 輸入下列資訊：
   - [Name (名稱)]：啟用虛擬 IO1
   - [Condition (條件)]： 應用程式 > Motion Guard：攝影機設定檔
   - [Action (動作)]： [通知 > 透過 HTTP 傳送通知]
   - [接收者]： 啟用虛擬連接埠

- 查詢字串後綴：schemaversion=1&port=1

3. 按一下 Save (儲存)。
4. 使用下列資訊新增另一條規則：
   - [Name (名稱)]：停用虛擬 IO1
   - [Condition (條件)]： 應用程式 > Motion Guard：攝影機設定檔
   - 選取 [Invert this condition (反轉此條件)]。
   - [Action (動作)]： [通知 > 透過 HTTP 傳送通知]
   - [接收者]： 停用虛擬連接埠
   - 查詢字串後綴：schemaversion=1&port=1
5. 按一下 Save (儲存)。

在閃光警報器中建立規則：

1. 在閃光警報器地網頁介面中，前往 [系統 > 事件] 並新增規則。
2. 輸入下列資訊：
   - [Name (名稱)]：在虛擬輸入 1 上觸發
   - 條件：I/O > 虛擬輸入
   - 連接埠：1
   - [Action (動作)]： [燈光和警報器 > 在規則作用中時執行燈光和警報器設定檔]
   - 設定檔：選取新建立的設定檔
3. 按一下 Save (儲存)。

當攝影機偵測到位移時，通過 HTTP post 啟動閃光警報器

此範例說明每當安裝在攝影機中的應用程式 AXIS Motion Guard 偵測到位移時，如何將攝影機連接至閃光警報器，並啟用閃光警報器中的設定檔。

開始之前：

- 在閃光警報器中使用操作者或管理員的角色建立新使用者。
- 在閃光警報器中建立一個名為：「閃光警報器設定檔」的設定檔。
- 在攝影機中設定 AXIS Motion Guard，然後建立名為：「攝影機設定檔」的設定檔。
- 確保使用韌體版本為 10.8.0 或更高版本的 AXIS Device Assistant。

在攝影機中建立接收者：

1. 在攝影機的設備介面中，前往 [系統 > 事件 > 接收者]，然後新增接收者。
2. 輸入下列資訊：
   - [Name (名稱)]：閃光警報器
   - 類型：HTTP
   - URL： http://<IPaddress>/axis-cgi/siren_and_light.cgi
     請將 <IPaddress> 換成閃光警報器的位址。
   - 新建立閃光警報器使用者的使用者名稱和密碼。
3. 按一下 [測試]，以確認所有資料都有效。
4. 按一下 Save (儲存)。

在攝影機中建立兩條規則：

1. 前往 [規則]，並新增規則。
2. 輸入下列資訊：

- [Name (名稱)]：啟動有位移的閃光警報器
- [Condition (條件)]： 應用程式 > Motion Guard：攝影機設定檔
- [Action (動作)]： [通知 > 透過 HTTP 傳送通知]
- [接收者]：[閃光警報器]。
  該資訊必須與您之前在 [事件 > 接收者 > 名稱] 底下輸入的資訊相同。
- 方法： Post
- [機身]：

```
{ 「api 版本」：「1.0」， 「方法」：「啟動」， 「參數」：{ 「設定檔」：「閃光警報器設定檔」 } }
```

確保在 [「設定檔」 ： <>] 下輸入的資訊與在閃光警報器建立設定檔時輸入的資訊相同，在此案例為：「閃光警報器設定檔」。

3. 按一下 Save (儲存)。
4. 使用下列資訊新增另一條規則：
   - [Name (名稱)]：停用有位移的閃光警報器
   - [Condition (條件)]： 應用程式 > Motion Guard：攝影機設定檔
   - 選取 [Invert this condition (反轉此條件)]。
   - [Action (動作)]： [通知 > 透過 HTTP 傳送通知]
   - [接收者]： 閃光警報器
     該資訊必須與您之前在 [事件 > 接收者 > 名稱] 底下輸入的資訊相同。
   - 方法： Post
   - [機身]：

```
{ 「api 版本」：「1.0」， 「方法」：「停止」， 「參數」：{ 「設定檔」：「閃光警報器設定檔」 } }
```

確保在 [「設定檔」 ： <>] 下輸入的資訊與在閃光警報器建立設定檔時輸入的資訊相同，在此案例為：「閃光警報器設定檔」。

5. 按一下 Save (儲存)。

攝影機偵測到位移時啟用 MQTT 上的閃光警報器

此範例說明每當安裝在攝影機中的應用程式 AXIS Motion Guard 偵測到位移時，如何將攝影機連接至 MQTT 上的閃光警報器，並啟用閃光警報器中的設定檔。

開始之前：

- 在閃光警報器中建立設定檔。
- 設定 MQTT 代理人並取得代理人的 IP 位址、使用者名稱和密碼。
- 在攝影機中設定 AXIS Motion Guard。

在攝影機中設定 MQTT 用戶端：

1. 在攝影機的設備介面中，前往 [系統 > MQTT > MQTT 用戶端 > 代理人]，並輸入下列資訊：
   - [Host (主機)]：代理人 IP 位址
   - 用戶端 ID：例如攝像機 1
   - [Protocol (協定)]：代理人設定使用的通訊協定
   - [Port (連接埠)]：代理人使用的連接埠編號
   - 代理人 [使用者名稱] 和 [密碼]
2. 按一下 [儲存] 和 [連接]。

在攝影機中建立兩道適用 MQTT 發佈的規則：

1. 前往 [System (系統) > Events (事件) > Rules (規則)]，並新增規則。

2. 輸入下列資訊：
   - [Name (名稱)]：偵測到位移
   - [Condition (條件)]： 應用程式 > 位移警報
   - 動作：MQTT > 傳送 MQTT 發佈訊息
   - [Topic (主題)]：位移
   - [Payload (承載)]：開啟
   - 服務品質 (QoS)：0、1 或 2
3. 按一下 Save (儲存)。
4. 使用下列資訊新增另一條規則：
   - [Name (名稱)]：無位移
   - [Condition (條件)]： 應用程式 > 位移警報
     - 選取 [Invert this condition (反轉此條件)]。
   - 動作：MQTT > 傳送 MQTT 發佈訊息
   - [Topic (主題)]：位移
   - [Payload (承載)]：關閉
   - 服務品質 (QoS)：0、1 或 2
5. 按一下 Save (儲存)。

在閃光警報器中設定 MQTT 用戶端：

1. 在閃光警報器的設備介面中，前往 [系統 > MQTT > MQTT 用戶端 > 代理人]，並輸入下列資訊：
   - [Host (主機)]：代理人 IP 位址
   - 用戶端 ID：警報器 1
   - [Protocol (協定)]：代理人設定使用的通訊協定
   - [Port (連接埠)]：代理人使用的連接埠編號
   - 使用者名稱和密碼
2. 按一下 [儲存] 和 [連接]。
3. 前往 MQTT 訂閱並新增訂閱。
   輸入下列資訊：
   - [Subscription filter (訂閱篩選條件)]：位移
   - [Subscription type (訂閱類型)]：具狀態
   - 服務品質 (QoS)：0、1 或 2
4. 按一下 Save (儲存)。

在閃光警報器中建立一道適用 MQTT 訂閱的規則：

1. 前往 [System (系統) > Events (事件) > Rules (規則)]，並新增規則。
2. 輸入下列資訊：
   - [Name (名稱)]：偵測到位移
   - 條件：MQTT > 具狀態
   - [Subscription filter (訂閱篩選條件)]： 位移
   - [Payload (承載)]：開啟
   - [Action (動作)]： [燈光和警報器 > 在規則作用中時執行燈光和警報器設定檔]
   - [Profile (設定檔)]：選取您要使用的設定檔。
3. 按一下 Save (儲存)。

深入瞭解

工作階段初始通訊協定 (SIP)

工作階段初始通訊協定 (SIP) 是用來設定、維護及終止 VoIP 通話。您可以在稱為 SIP 使用者代理的兩方或多方之間撥打電話。若要撥打 SIP 電話，您可以使用像是 SIP 電話、軟體式電話或啟用 SIP 的 Axis 裝置等。

實際的音訊或影像會透過傳輸通訊協定 (例如即時傳輸通訊協定 (RTP)) 在 SIP 使用者代理之間進行交換。

您可以使用點對點設定在本地網路上撥打電話，也可以使用 PBX 跨網路撥打電話。

點對點 SIP (P2PSIP)

最基本類型的 SIP 通訊直接發生在兩個或多個 SIP 使用者代理之間。這稱為點對點 SIP (P2PSIP)。如果發生在本地網路上，則只需要使用者代理的 SIP 位址。在這種情況下，典型的 SIP 位址會是 `sip:<local-ip>`。

專用交換機 (PBX)

當您在本地 IP 網路外撥打 SIP 電話時，專用交換機 (PBX) 可以當做中心點。PBX 的主要元件是 SIP 伺服器，它也稱為 SIP Proxy 或登錄伺服器。PBX 的運作方式類似於傳統的總機，可顯示用戶端的目前狀態，並允許進行通話轉接、語音信箱和重新導向等作業。

PBX SIP 伺服器可以設定為本地或異地實體。它可以在內部網路上代管，或由第三方供應商代管。當您在網路之間撥打 SIP 電話時，電話會透過一組 PBX 路由傳遞，這些 PBX 會查詢要聯繫的 SIP 位址的位置。

每個 SIP 使用者代理都會向 PBX 註冊，然後可以藉由撥打正確的分機聯繫其他人。在這種情況下，典型的 SIP 位址會是 `sip:<user>@<domain>` 或 `sip:<user>@<registrar-ip>`。SIP 位址與其 IP 位址不相關，而且只要裝置已向 PBX 註冊，PBX 就可以讓裝置可供存取。

NAT 周遊

當 Axis 設備位於私人網路 (LAN)，而您希望可以從該網路外部存取此設備時，請使用 NAT (網路位址轉譯) 周遊。

附註

路由器必須支援 NAT 周遊和 UPnP®。

視網路環境而定，各 NAT 通訊協定可以分開使用或採用不同組合。

- ICE - ICE (互動式連線建立) 通訊協定可以提高找到最有效率路徑的機會，以在對等裝置之間成功進行通訊。如果您也啟用 STUN 和 TURN，便可提高 ICE 通訊協定的機率。
- STUN - STUN (NAT 工作階段周遊公用程式) 是主從網路通訊協定，可讓 Axis 設備判斷其是否位於 NAT 或防火牆之後，且倘若如此，則取得對應的公用 IP 位址和連接埠號碼 (分配給遠端主機的連線)。輸入 STUN 伺服器位址，例如 IP 位址。
- TURN - TURN (Traversal Using Relays around NAT) 是一種通訊協定，可讓 NAT 路由器或防火牆之後的裝置透過 TCP 或 UDP 接收來自其他主機的傳入資料。輸入 TURN 伺服器和登入資訊。

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。

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)]：查看設備資訊，包括 AXIS 作業系統版本和序號。

狀態

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 操作系統強化指南。

[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。

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。

設備資訊

顯示該設備的 AXIS 作業系統版本和序號等資訊。

[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。

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。

概觀

訊號 LED 狀態

顯示在設備上執行的不同訊號 LED 活動。訊號 LED 狀態清單中最多可以同時有 10 個活動。兩項或更多活動同時執行時，優先順序最高的活動會顯示訊號 LED 狀態。該列將會在狀態清單中醒目提示。

警報器狀態

顯示在設備上執行的不同警報器活動。警報器狀態清單中最多可以同時有 10 個活動。兩項或更多活動同時執行時，則會執行優先順序最高的活動。該列將會在狀態清單中醒目提示。

維護

[維護模式]：在設備維護期間開啟以暫停燈光和警報器活動。開啟維護模式時，設備會顯示三角形的白色脈動燈光圖案，並且警報器會靜音。它可以保護安裝人員免受聽力損傷和刺眼強光的影響。

維護的優先順序為 11。只有具有更高優先順序的系統特定活動才能中斷維護模式。

維護模式在重新開機後仍然存在。例如，如果您將時間設定為 2 小時，關閉設備並在一小時後將其重新啟動，該設備將再進入維護模式一小時。

當您重設預設設定時，該設備將返回維護模式。

持續時間

- 連續：選取讓該設備保持在維護模式，直到您將其關閉。
- [時間]：選取以設定關閉維護模式的時間。

健全狀況檢查

[Check (檢查)]：對設備執行健全狀況檢查，判斷其燈光和警報器是否正常運作。設備將一次開啟一個燈光部分並播放測試音。如果設備未通過健全狀況檢查，請參閱系統日誌中的詳細資訊。

為了獲得準確結果，請務必在室溫下執行健全狀況檢查。

設定檔

設定檔

設定檔是設定組態集合。您最多可以擁有 30 個具有不同優先順序和模式的設定檔。列出的設定檔概述了名稱、優先順序以及燈光和警報器設定。

Create (建立)：按一下可建立設定檔。

- [預覽/停止預覽]：在儲存設定檔之前啟動或停止預覽。

附註

您不可有兩個同名的設定檔。

- [Name (名稱)]：輸入設定檔的名稱。
- [Description (說明)]：輸入設定檔的說明。
- [照明]：從下拉選單選取您想要哪種 [模式]、[速度]、[強度] 和 [顏色]。
- [警笛]：從下拉選單中選取您要哪種警笛 [模式] 和 [強度]。
- 僅開始或停止燈光或警報器的預覽。
- [Duration (持續時間)]：設定活動的持續時間。
  - 連續：一旦啟動之後，就會持續運轉到停止為止。
  - [時間]：設定活動將持續多久的指定時間。
  - [重複次數]：設定活動應重複的次數。
- [Priority (優先順序)]：將活動的優先順序設定為 1 到 10 之間的數字。優先順序數字大於 10 的活動無法自狀態清單中移除。優先順序大於 10 的活動共有三種，分別是維護 (11)、辨識 (12) 和健全狀況檢查 (13)。

Import (匯入)：新增一個或多個已預先定義組態的設定檔。

- [新增]：加入新的設定檔。
- [刪除並新增]：已刪除舊的設定檔，您可以上傳新的設定檔。
- 覆寫：更新的設定檔會覆寫現有的設定檔。

若要複製設定檔並儲存其他設備，請選取一個或多個設定檔，然後按一下 [匯出]。隨即匯出 .json 檔案。

開始建立設定檔。該設定檔及其活動會在狀態清單中出現。

選擇 [Edit (編輯)]、[Copy (複製)]、[Export (匯出)] 或者 [Delete (刪除)] 設定檔。

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 (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。
  - [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。

- [Format (格式化)]：選擇輸入設備的緯度和經度時使用的格式。
- [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)]：選取以允許網路路由器自動為裝置指派 IP 位址。我們建議適用大多數網路的自動 IP (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。

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。

全域代理伺服器

[Http proxy (Http 代理伺服器)]：根據允許的格式指定全域代理伺服器或 IP 位址。

[Https proxy (Https 代理伺服器)]：根據允許的格式指定全域代理伺服器或 IP 位址。

http 和 https 代理伺服器允許的格式：

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

附註

重新啟動設備，以應用全域代理伺服器設定。

[No proxy (沒有代理伺服器)]：使用 [No proxy (沒有代理伺服器)] 繞過全域代理伺服器。輸入清單中的選項之一，或輸入多個選項，以逗號分隔的選項：

- 保留空白
- 指定 IP 位址
- 指定 CIDR 格式的 IP 位址
- 指定網域名稱，例如：www.<domain name>.com
- 指定特定網域中的所有子網域，例如 .<domain name>.com

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，裝置會中斷與 O3C 服務的連接。註冊該設備後，[Always (永遠)] 就會啟用，而且該設備會保持與 O3C 服務連線。
- [Always (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。如果裝置上的控制按鈕是在接觸不到的位置，請使用此選項。
- [No (否)]：停用 O3C 服務。

[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。
    - [Warm start (暖啟動)]：在您變更 SNMP 設定時傳送設陷訊息。
    - [Link up (上行連結)]：在連結從下行變更為上行時，傳送設陷訊息。
    - [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。有關選取哪個私密金鑰的更多資訊，請前往 *help.axis.com/en-us/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+) (安全元件 (CC EAL6+))]：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

[Activate (啟用)]：開啟防火牆。

[Default Policy (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。

- [Address (位址)]：輸入您想要允許或拒絕存取之 IPv4/IPv6 或 CIDR 格式的位址。
- [Protocol (協定)]：選取您想要允許或拒絕存取的通訊協定。
- [Port (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。
- [Policy (政策)]：選取規則的原則。

＋：按一下以建立其他規則。

[Add rules (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。
- [Confirm rules (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。

[Pending rules (待處理規則)]：您尚未確認的最新已測試規則概觀。

附註

有時間限制的規則將顯示在 [Active rules (作用中規則)] 下，直到顯示的計時器結束或您確認為止。如果未進行確認，一旦定時器結束，它們就會顯示在 [Pending rules (待處理規則)] 下，並且防火牆將恢復為先前定義的設定。如果確認規則，它們將取代目前作用中規則。

[Confirm rules (確認規則)]：按一下以啟用待處理規則。

[Active rules (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。

自訂簽署的 AXIS 作業系統憑證

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 作業系統憑證。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 作業系統憑證。

[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。

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。

匿名存取

[Allow anonymous viewing (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。

[Allow anonymous PTZ operating (允許匿名 PTZ 操作)]：開啟可讓匿名使用者水平移動、傾斜和變焦影像。

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 9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。

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。

附註

最多可以建立 256 項動作規則。

[+ Add a rule (新增規則)]：建立規則。

[Name (名稱)]：輸入規則的名稱。

[Wait between actions (在動作之間等待)]：輸入規則相繼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。

[Condition (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*。

[Use this condition as a trigger (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。

[Invert this condition (反轉此條件)]：如果您希望條件與您的選擇相反，請選取此選項。

[+ Add a condition (新增條件)]：按一下可新增其他的條件。

[Action (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

您可以設定讓裝置將事件通知接收者，或使其傳送檔案。

附註

如果您設定讓設備使用 FTP 或 SFTP，請勿變更或移除新增到檔案名稱中的唯一序號。否則每個事件只能傳送一個影像。

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。

附註

您最多可以建立 20 接收者。

[+ Add a recipient (新增接收者)]：按一下可新增接收者。

[Name (名稱)]：輸入接收者的名稱。

[Type (類型)]：從清單中選取：

- FTP
  - [Host (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 [System (系統) > Network (網路) > IPv4 and IPv6 (IPv4 和 IPv6)] 下方指定 DNS 伺服器。
  - [Port (連接埠)]：輸入 FTP 伺服器所使用的連接埠編號。預設為 21。
  - [Folder (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。
  - [Username (使用者名稱)]：輸入登入的使用者名稱。
  - [Password (密碼)]：輸入登入的密碼。
  - [Use temporary file name (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。
  - [Use passive FTP (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要求的指令碼。例如，http://192.168.254.10/cgi-bin/notify.cgi。
  - [Username (使用者名稱)]：輸入登入的使用者名稱。
  - [Password (密碼)]：輸入登入的密碼。
  - [Proxy (代理伺服器)]：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要求的指令碼。例如，https://192.168.254.10/cgi-bin/notify.cgi。
  - [Validate server certificate (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。
  - [Username (使用者名稱)]：輸入登入的使用者名稱。
  - [Password (密碼)]：輸入登入的密碼。
  - [Proxy (代理伺服器)]：如果必須傳遞 Proxy 伺服器才能連線至 HTTPS 伺服器，請開啟並輸入必要的資訊。
- 網路儲存裝置
  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。
  - [Host (主機)]：輸入網路儲存空間的 IP 位址或主機名稱。
  - [Share (共用區)]：輸入主機上共用區的名稱。
  - [Folder (資料夾)]：輸入要儲存檔案所在目錄的路徑。
  - [Username (使用者名稱)]：輸入登入的使用者名稱。
  - [Password (密碼)]：輸入登入的密碼。

- SFTP
  - [Host (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 [System (系統) > Network (網路) > IPv4 and IPv6 (IPv4 和 IPv6)] 下方指定 DNS 伺服器。
  - [Port (連接埠)]：輸入 SFTP 伺服器所使用的連接埠編號。預設值為 22。
  - [Folder (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。
  - [Username (使用者名稱)]：輸入登入的使用者名稱。
  - [Password (密碼)]：輸入登入的密碼。
  - [SSH host public key type (MD5) (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 host public key type (SHA256) (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*。
  - [Use temporary file name (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 or VMS (SIP 或 VMS)]：
  [SIP]：選取以撥打 SIP 電話。
  [VMS]：選取以撥打 VMS 電話。
  - [From SIP account (來自 SIP 帳戶)]：從清單中選取。
  - 至 SIP 位址：輸入 SIP 位址。
  - [Test (測試)]：按一下可測試通話設定是否有效。
- 電子郵件
  - [Send email to (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。
  - [Send email from (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。
  - [Username (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。
  - [Password (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。
  - [Email server (SMTP) (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。
  - [Port (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。
  - [Encryption (加密)]：若要使用加密，請選取 SSL 或 TLS。
  - [Validate server certificate (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 authentication (POP 驗證)]：開啟此選項以輸入 POP 伺服器的名稱，例如：pop.gmail.com。

附註

對於定時或內容相似的電子郵件，部分電子郵件供應商有設定安全篩選條件，無法接收或檢視大量附件。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
  - — [Host (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 [System (系統) > Network (網路) > IPv4 and IPv6 (IPv4 和 IPv6)] 下方指定 DNS 伺服器。
  - — [Port (連接埠)]：輸入用於存取伺服器的連接埠編號。

[Test (測試)]：按一下可測試設定。

內容功能表包含：

[View recipient (檢視接收者)]：按一下可檢視所有接收者詳細資訊。

[Copy recipient (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。

[Delete recipient (刪除接收者)]：按一下可永久刪除接收者。

預約排程

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。

[+ Add schedule (新增預約排程)]：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 topic name (包括主題名稱)]：選取包括在 MQTT 主題中描述條件的主題。

[Include topic namespaces (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。

[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。

MQTT 浮水印

附註

在新增 MQTT 覆蓋修飾詞之前連接到 MQTT 代理。

[+ Add overlay modifier (新增浮水印修飾詞)]：按一下可新增新的浮水印修飾詞。

[Topic filter (主題篩選)]：新增包含要在浮水印中顯示的資料的 MQTT 主題。

[Data field (資料欄位)]：指定要在浮水印中顯示的訊息有效負載的按鍵，假設訊息採用 JSON 格式。

[Modifier (修飾詞)]：建立浮水印時使用產生的修飾詞。

- #XMP 開頭的修飾詞會顯示從主題接收到的所有資料。
- #XMD 開頭的修飾詞會顯示資料欄位中指定的資料。

SIP

設定

工作階段初始通訊協定 (SIP) 用於使用者之間的互動式通訊工作階段。工作階段可以包含聲音和影像。

[SIP setup assistant (SIP 設定輔助)]：按一下可逐步設定 SIP。

啟用 SIP：勾選此選項就可以開始撥打和接聽 SIP 通話。

[Allow incoming calls (允許撥入的通話)]：勾選此選項可允許其他 SIP 裝置的來電。

來電處理
- [Calling timeout (通話逾時)]：設定無人接聽時嘗試通話的最長持續時間。
- [Incoming call duration (來電持續時間)]：設定撥入通話可以持續的最長時間 (最長 10 分鐘)。
- [End calls after (在以下時間後結束通話)]：設定通話可以持續的最長時間 (最長 60 分鐘)。如果您不希望限制通話時間長度，請選取 [Infinite call duration (無限通話時間)]。

連接埠
連接埠號碼必須介於 1024 至 65535 之間。
- [SIP port (SIP 連接埠)]：用於 SIP 通訊的網路連接埠。通過此連接埠的訊號流量並不會加密。預設連接埠號碼為 5060。如有需要，請輸入其他連接埠號碼。
- [TLS port (TLS 連接埠)]：用於加密 SIP 通訊的網路連接埠。通過此連接埠的訊號流量會以傳輸層安全性 (TLS) 加密。預設連接埠號碼為 5061。如有需要，請輸入其他連接埠號碼。
- [RTP start port (RTP 起始連接埠)]：針對 SIP 通話中第一個 RTP 媒體串流使用的網路連接埠。預設起始連接埠號碼為 4000。某些防火牆會封鎖特定連接埠號碼上的 RTP 流量。

NAT 周遊
當裝置位於私人網路 (LAN)，而您希望可以從該網路外部使用此裝置時，請使用 NAT (網路位址轉譯) 周遊。

附註

若要讓 NAT 周遊功能運作，路由器必須支援此功能。路由器也必須支援 UPnP®。

視網路環境而定，各 NAT 通訊協定可以分開使用或採用不同組合。
- [ICE]：ICE (互動式連線建立) 通訊協定可以提高找到最有效率路徑的機會，以在對等設備之間成功進行通訊。如果您也啟用 STUN 和 TURN，便可提高 ICE 通訊協定的機率。
- [STUN]：STUN (NAT 工作階段周遊公用程式) 是主從網路通訊協定，可讓設備判斷其是否位於 NAT 或防火牆之後，且倘若如史，則取得對應的公用 IP 位址和連接埠號碼 (分配給遠端主機的連線)。輸入 STUN 伺服器位址，例如 IP 位址。
- [TURN]：TURN (Traversal Using Relays around NAT) 是一種通訊協定，可讓 NAT 路由器或防火牆之後的設備透過 TCP 或 UDP 接收來自其他主機的傳入資料。輸入 TURN 伺服器位址和登入資訊。

聲音
- [Audio codec priority (音訊轉碼器優先順序)]：為 SIP 通話至少選取一個具有所需音質的聲音轉碼器。拖放即可變更優先順序。

附註

由於接收者轉碼器在通話時有決定性影響，因此選取的轉碼器必須符合通話接收者的轉碼器。
- [Audio direction (音訊方向)]：選取允許的音訊方向。

[其他]
- [UDP-to-TCP switching (UDP 轉 TCP 切換)]：選取此選項可讓通話將傳輸通訊協定暫時從 UDP (使用者資料包通訊協定) 切換成 TCP (傳輸控制通訊協定)。切換的原因是為了避免資料分散，如果某個要求是在最大傳輸單元的 200 個位元組以內，或是大於 1300 個位元組，則可以進行切換。
- [Allow via rewrite (允許透過重寫)]：選取啟此選項可傳送本機 IP 位址，而不傳送路由器的公用 IP 位址。
- [Allow contact rewrite (允許聯絡人重寫)]：選取啟此選項可傳送本機 IP 位址，而不傳送路由器的公用 IP 位址。
- [Register with server every (向伺服器進行登錄的間隔)]：設定設備多久一次向現有 SIP 帳戶的 SIP 伺服器進行登錄。

- [DTMF payload type (DTMF 承載類型)]：變更 DTMF 預設的承載類型。
- [Max retransmissions (最大重新傳輸次數)]：設定設備在停止嘗試之前，嘗試連接到 SIP 伺服器的最大次數。
- [Seconds until failback (故障恢復前的秒數)]：設定設備在故障轉移到次要 SIP 伺服器後，嘗試重新連接到主 SIP 伺服器的秒數。

帳戶

目前所有的 SIP 帳戶都會在 [SIP accounts (SIP 帳戶)] 下方列出。如果是已註冊帳戶，其彩色圓圈可讓您了解狀態。

- 帳戶以 SIP 伺服器成功登錄。
- 帳戶發生問題。可能原因包括授權失敗、帳戶認證錯誤，或 SIP 伺服器找不到帳戶。

[peer to peer (default) (點對點 (預設))] 帳戶是自動建立的帳戶。如果您至少建立一個其他帳戶，並將該帳戶設為預設，則可刪除此帳戶。當您未指定要從哪個 SIP 帳戶進行通話，即進行 VAPIX® Application Programming Interface (API) 通話時，一律使用預設帳戶。

[+ Add account (新增帳戶)]：按一下可建立新的 SIP 帳戶。

- [Active (作用中)]：選取此選項即可使用帳戶。
- [Make default (設為預設)]：選取此選項可讓此帳戶做為預設帳戶。必須有一個預設帳戶，而且只能有一個預設帳戶。
- [Answer automatically (自動接聽)]：選取以自動接聽來電。
- [Prioritize IPv6 over IPv4 (優先處理 IPv6，再處理 IPv4)]：選取優先處理 IPv6 位址，再處理 IPv4 位址。當您連線到同時解析 IPv4 和 IPv6 位址的點對點帳戶或網域名稱時，這非常有用。只有對應到 IPv6 位址的網域名稱才能優先處理 IPv6。
- [Name (名稱)]：輸入描述性名稱。例如，此名稱可以是姓氏和名字、角色或地點。此名稱不是唯一的。
- [User ID (使用者 ID)]：輸入指派給裝置的唯一分機號碼或電話號碼。
- [Peer-to-peer (點對點)]：用於對本機網路上的其他 SIP 設備進行直接通話。
- [Registered (已註冊)]：用於透過 SIP 伺服器，與本機網路外的 SIP 裝置進行通話。
- [Domain (網域)]：如果可用，請輸入公用網域名稱。與其他帳戶通話時，此帳戶將顯示為 SIP 位址。
- [Password (密碼)]：輸入與 SIP 帳戶相關的密碼，以用於驗證進入 SIP 伺服器。
- [Authentication ID (驗證 ID)]：輸入用於對 SIP 伺服器進行驗證的驗證 ID。如果與使用者 ID 相同，則無需輸入驗證 ID。
- [Caller ID (來電顯示)]：從裝置向通話接收者展示的名稱。
- [Registrar (登錄伺服器)]：輸入登錄伺服器的 IP 位址。
- [Transport mode (傳輸模式)]：選取帳戶的 SIP 傳輸模式：UPD、TCP 或 TLS。
- [TLS version (TLS 版本)] (僅使用傳輸模式 TLS)：選取要使用的 TLS 版本。版本 [v1.2] 和 [v1.3] 是最安全的。[Automatic (自動)] 選取系統可以處理的最安全的版本。
- [Media encryption (媒體加密)] (僅使用傳輸模式 TLS)：選取用於 SIP 通話的媒體 (音訊和視訊) 加密類型。
- [Certificate (憑證)] (僅使用傳輸模式 TLS)：選取憑證。
- [Verify server certificate (驗證伺服器憑證)] (僅使用傳輸模式 TLS)：勾選此選項可驗證伺服器憑證。
- [Secondary SIP server (次要 SIP 伺服器)]：當裝置向主要 SIP 伺服器註冊失敗時，如果您想要讓該裝置嘗試在次要 SIP 伺服器上註冊，請選取此選項。
- [SIP secure (SIP 安全)]：選取此選項可使用安全工作階段初始通訊協定 (SIPS)。SIPS 以 TLS 傳輸模式來加密流量。
- Proxy
  - [+ Proxy (代理伺服器)]：按一下可新增 Proxy。
  - [Prioritize (設定優先權)]：如果您已新增兩個或多個 Proxy，按一下此選項可設定它們的優先權。

- [Server address (伺服器位址)]：輸入 SIP Proxy 伺服器的 IP 位址。
- [Username (使用者名稱)]：必要時，請輸入 SIP proxy 伺服器的使用者名稱。
- [Password (密碼)]：必要時，輸入 SIP Proxy 伺服器的密碼。

• 影像
- [View area (觀看區域)]：選取要用於視訊通話的觀看區域。如果您選取 [無]，就會使用原生畫面。
- [Resolution (解析度)]：選取要用於視訊通話的解析度。解析度會影響所需的頻寬。
- [Frame rate (影格速率)]：選取用於視訊通話的每秒影格數。影格張數會影響所需的頻寬。
- [H.264 profile (H.264 設定檔)]：選取要用於視訊通話的設定檔。

DTMF

[+ Add sequence (新增序列)]：按一下以建立新增雙音多頻 (DTMF) 序列。若要建立透過按鍵音啟用的規則，請前往 [Events (事件) > Rules (規則)]。

[Sequence (序列)]：輸入啟用規則的字元。允許的字元：0—9、A-D、# 和 *。

[Description (說明)]：輸入要按序列觸發之動作的說明。

[Accounts (帳戶)]：選取將使用 DTMF 序列的帳戶。如果選擇 [peer-to-peer (點對點)]，所有點對點帳戶將共用相同的 DTMF 序列。

傳輸協定

選取每個帳戶要使用的通訊協定。所有點對點帳戶共用相同的通訊協定設定。

[Use RTP (RFC2833) (使用 RTP (RFC2833))]：開啟此選項可允許在 RTP 封包中使用雙音多頻 (DTMF) 訊號、其他單音訊號和電話事件。

[Use SIP INFO (RFC2976) (使用 SIP INFO (RFC2976))]：開啟此選項可將 INFO 方法納入 SIP 通訊協定。INFO 方法會新增通常與工作階段相關的選用應用程式層資訊。

測試通話

[SIP account (SIP 帳戶)]：選擇要從哪個帳戶撥打測試通話。

[SIP address (SIP 位址)]：輸入 SIP 位址，然後按一下 ，以撥打測試通話並驗證帳戶有效。

存取清單

[Use access list (使用存取清單)]：開啟以限制誰可以向設備通話。

[Policy (政策)]：
- [Allow (允許)]：選取僅允許來自存取清單中的來源的來電。
- [Block (封鎖)]：選取僅封鎖來自存取清單中的來源的來電。

[+ Add source (新增來源)]：按一下可在存取清單中建立新增項目。

[SIP source (SIP 來源)]：輸入來源的來電 ID 或 SIP 伺服器位址。

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。

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。

[CA certificate set (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

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 作業系統版本。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 作業系統版本。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 作業系統版本。
- [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 作業系統版本。
- [Autorollback (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 作業系統版本。

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

疑難排解

[Reset PTR (重設 PTR)] ：如果 [Pan (水平移動)]、[Tilt (傾斜)] 或 [Roll (滾動)] 設定因某種原因未如預期般運作，請重設 PTR。PTR 馬達一律會在新的攝影機中進行校準。但校準有時可能會遺失，例如在攝影機斷電，或在手動移動馬達的情況下。重設 PTR 時，攝影機會重新校準並返回其出廠預設設定位置。

[Calibration (校正)] ：按一下 [Calibrate (校正)] 將水平移動、傾斜和滾動馬達重新校準為其預設位置。

[Ping]：若要檢查裝置是否可以到達特定位址，請輸入要 ping 的主機名稱或 IP 位址，然後按一下 [Start (開始)]。

[Port check (連接埠檢查)]：若要驗證從裝置到特定 IP 位址和 TCP/UDP 連接埠的連接，請輸入要檢查的主機名稱或 IP 位址和連接埠編號，然後按一下 [Start (開始)]。

網路追蹤

重要

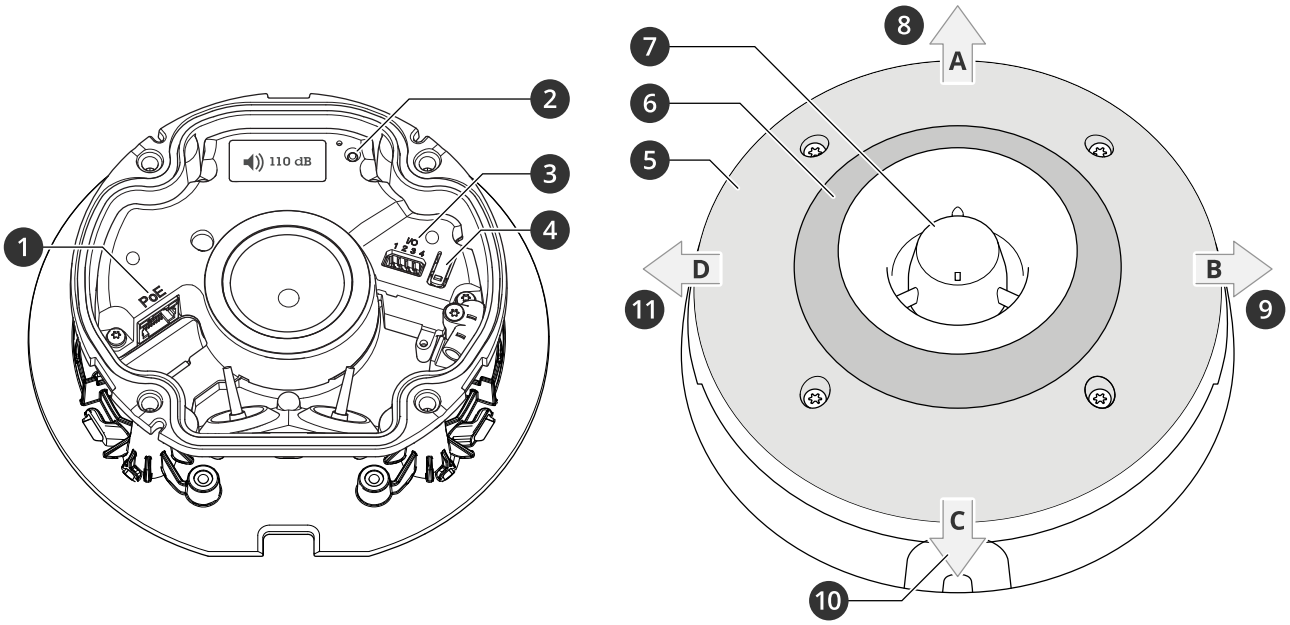
網路追蹤檔案可能包含機密資訊，例如憑證或密碼。

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 [Download (下載)]。

規格

產品總覽



1 *PoE網路接頭*
2 *狀態 LED 指示燈*
3 *I/O 連接端子*
4 *控制按鈕*
5 *白光 LED*
6 *RGBA (紅色、藍色、綠色、黃色) LED*
7 *警報器*
8 *光線方向 A*
9 *光線方向 B*
10 *光線方向 C*
11 *光線方向 D*

LED 指示燈

狀態LED燈號	指示
綠色	啟動完成後，綠色常亮 10 秒表示正常操作。
黃色	在啟動過程中、重設為出廠預設設定或還原設定時，保持常亮。

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 。
- 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

網路接頭

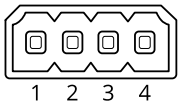
支援乙太網路供電 (PoE) 的 RJ45 乙太網路接頭。

I/O 連接端子

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。

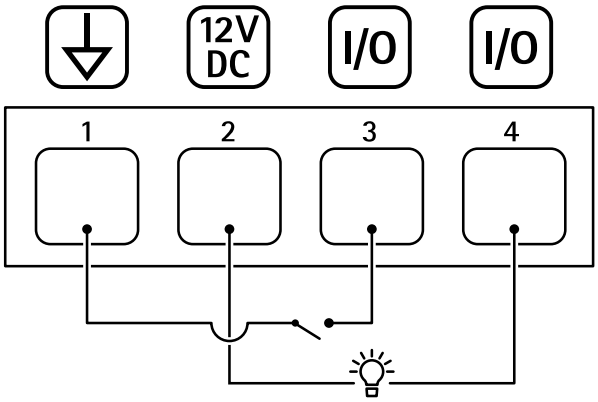
數位輸出 - 用於連接繼電器和 LED 等外接式設備。連接的設備可透過 VAPIX® 應用程式開發介面、事件或設備網頁介面加以啟動。

4 針接線端子



功能	針腳	附註	規格
DC 接地	1		0 VDC
DC 輸出	2	可用於電源輔助設備。 注意：此接腳只能當做電源輸出使用。	12 VDC 最大負載 = 50 mA
可設定 (輸入或輸出)	3—4	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 VDC
		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。	0 到最大30 VDC，漏極開路，100 mA

範例:



1 *DC 接地*
2 *DC 輸出 12 V，最大 50mA*
3 *I/O 設定為輸入*
4 *I/O 設定為輸出*

燈光模式名稱

關閉
穩定
穩定白光+閃爍的色彩
輪流
脈衝
上升 3 步驟

連續快速的閃光 3 次
連續快速的閃光 4 次
連續快速的閃光 3 次並漸暗
連續快速的閃光 4 次並漸暗
短暫明亮的閃光 1 次
短暫明亮的閃光 3 次
短暫明亮的閃光 1 次 (白光 + 穩定顏色)
短暫明亮的閃光 3 次 (白光 + 穩定顏色)
方向 A + 穩定顏色
方向 B + 穩定顏色
方向 C + 穩定顏色
方向 D + 穩定顏色
旋轉白光 + 穩定顏色
旋尾白光 + 穩定色色
隨機白光 + 穩定顏色
快速旋轉白光 + 穩定顏色
穩定的白光 + 穩定的顏色

聲音模式名稱

警報：高音警報
警報：低音警報
警報：鳥類
警報：船用喇叭
警報：汽車警報
警報：汽車警報聲快
警報：經典時鐘
警報：第一位參加者
警報：恐怖
警報：工業
警報：單一嗶聲
警報：柔和的四連嗶聲
警報：柔和的三聲嗶聲
警報：三連高音
通知：已接受
通知：通話

通知：已拒絕
通知：完成
通知：進入
通知：失敗
通知：匆忙
通知：訊息
通知：下一步
通知：開啟
警報器：輪流
警報器：Bouncy
警報器：Evac
警報器：Falling pitch
警報器：Home soft

清潔設備

設備可以使用溫水和溫和的非研磨性肥皂清潔。

注意

- 刺激性化學物質可能會損壞設備。請勿使用窗戶清潔劑或丙酮等化學物質來清潔設備。
- 請勿將清潔劑直接噴灑在設備上。而是將清潔劑噴在非研磨性布上，然後用它來清潔設備。
- 避免在陽光直射或高溫下清潔，因為這樣會造成污漬。

1. 使用一罐壓縮空氣移除設備上的灰塵和鬆散污垢。
2. 如有必要，請用超細纖維軟布沾上溫水和溫和的非研磨性肥皂來清潔設備。
3. 為避免出現污漬，請使用乾淨的非研磨性布擦乾設備。

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15—30秒，直到狀態LED指示燈開始閃爍黃色。
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. 請使用安裝與管理軟體工具來指派 IP 位址、設定密碼，並存取裝置。
   axis.com/support 上的支援頁面中有提供安裝與管理軟體工具。

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 作業系統選項

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，建議主動式常規提供的 AXIS 作業系統。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 作業系統版本

我們設備的功能取決於 AXIS 作業系統。對問題進行故障排除時，建議您先從檢查目前 AXIS 作業系統版本開始著手。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 作業系統版本：

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 作業系統版本。

升級 AXIS 作業系統

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 作業系統中提供這些功能)，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 作業系統升級設備時，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 作業系統版本和版本資訊，請前往 *axis.com/support/device-software*。

1. 將 AXIS 作業系統檔案下載至電腦，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。

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 AXIS 作業系統時發生問題

AXIS 作業系統升級失敗	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 作業系統檔案。請檢查 AXIS 作業系統檔案名稱是否與您的設備相對應，然後重試。
升級 AXIS 作業系統後發生問題	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

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 裝置與網路的連接。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：`Reply from <IP address>: bytes=32; time=10...` (來自 `<IP` 位址> 的回覆：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，然後重新安裝裝置。 • 如果您收到：`Request timed out` (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，然後重新安裝裝置。
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 裝置中的固定 IP 位址。這表示，如果另一個裝置也使用同一個預設的固定 IP 位址，則存取該裝置可能會發生問題。

無法從瀏覽器存取設備

無法登入	啟用 HTTPS 時，請確定嘗試登入時使用的是正確的通訊協定 (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。請參考 。
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，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)]。

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 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*。

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。

聲音發生問題	
該設備沒有預期的那麼響亮	檢查設備是否正確關閉，喇叭或揚聲器元件上是否有障礙物。
該設備沒有聲音	檢查設備是否在 [維護模式]。如果是處於維護模式，請將其關閉。

燈光發生問題	
該設備沒有預期的那麼明亮	檢查是否使用了 PoE Class 4 電源。 檢查該設備的環境溫度。如果該設備安裝在高溫環境中，燈光會自動變暗。

效能考量

以下是最重要的考量因素：

- 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*。

T10223803_zh_tw

2025-04 (M1.6)