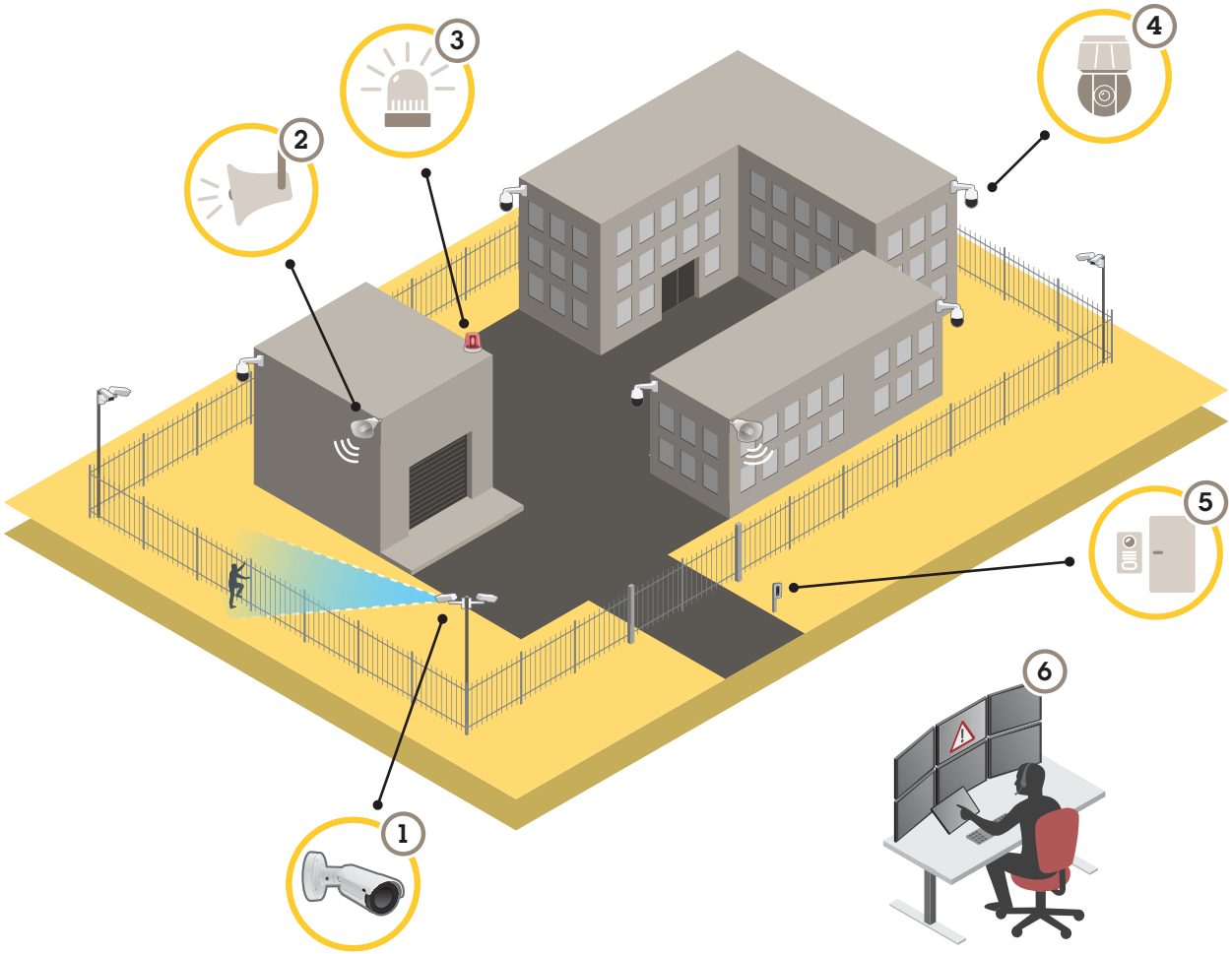
AXIS Q19-E Thermal Camera Series

AXIS Q1951-E Thermal Camera
AXIS Q1952-E Thermal Camera

使用手冊

解決方案總覽



1 *具有 AXIS Perimeter Defender 的熱顯像攝影機*
2 *號角喇叭*
3 *閃爍的信號燈*
4 *PTZ網路攝影機*
5 *門控制器*
6 *監控中心*

周界防護

對於需要入侵偵測的區域，您可以使用具有分析功能的熱顯像攝影機設定周界防護。周界防護的主要目標是盡可能在最早的階段偵測到威脅或實際入侵事件。

若要設定周界防護，您需要在熱顯像攝影機上安裝用於周界監控和防護的分析應用程式。Axis 為此目的提供 AXIS Perimeter Defender 應用程式。您可以閱讀更多關於 AXIS Perimeter Defender 的資訊，請造訪 *axis.com/products/axis-perimeter-defender*

- 若讓可能的入侵者知道您的周界受到防護，請使用閃爍的信號燈 (3)。請參考 。
- 若要發出警告和阻止，請連接一個號角喇叭 (2)，它會播放預先錄製的警告訊息。請參考 。

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 。

請確定沒有人竄改設備軟體

若要確保設備有其原始 AXIS 作業系統，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。

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。

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

安裝

預覽模式

預覽模式非常適合安裝人員在安裝過程中微調攝影機畫面。無需登入即可在預覽模式下存取攝影機畫面。它僅在設備啟動後的有限時間內以出廠預設設定狀態可用。



該影片示範如何使用預覽模式。

設定您的設備

調整影像

本節包含關於設定設備的說明。如需深入了解特定功能的運作方式，請參閱。

使用隱私遮蔽隱藏影像的某些部分

您可以建立一個或多個隱私遮蔽來隱藏影像的某些部分。

1. 請前往 [Video (影片) > Privacy masks (隱私遮蔽)]。
2. 按一下 + 。
3. 按一下新遮蔽並鍵入名稱。
4. 根據您的需求調整隱私遮蔽的大小和位置。
5. 若要變更所有隱私遮蔽的顏色，請按一下 [Privacy masks (隱私遮蔽)] 並選取顏色。

另請參閱

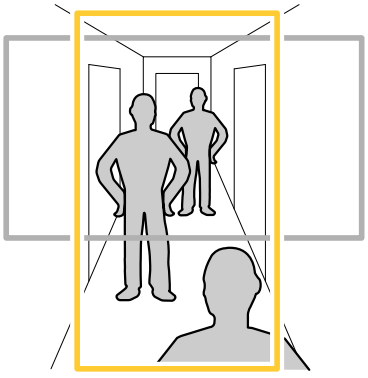
顯示影像浮水印

您可以在影像串流中新增影像做為浮水印。

1. 前往 [Video (影片) > Overlays (浮水印)]。
2. 按一下 [Manage images (管理影像)]。
3. 上傳或拖放影像。
4. 按一下 [Upload (上傳)]。
5. 從下拉式清單中選取 [Image (影像)]，然後按一下 + 。
6. 選取影像和位置。您也可以拖曳即時影像中的浮水印影像來變更位置。

監控狹長區域

使用長廊格式可以更妥善利用狹長區域 (例如樓梯、走廊、道路或隧道) 的完整視野。



1. 視您的設備而定，將攝影機或攝影機中的 3 軸鏡頭旋轉 90° 或 270° 。
2. 如果設備尚未自動旋轉畫面，請前往 [Video (影片) > Installation (安裝)]。
3. 將畫面旋轉 90° 或 270° 。

使用影像穩定功能穩定抖動的影像

影像穩定適用於產品已安裝於無掩蔽位置且會產生震動的位置，例如受風吹或往來車流等因素所致振動影響的環境中使用。

此功能可讓影像變得更平滑、更穩定且不那麼模糊。此外，還會減少壓縮影像的檔案大小，並降低影像串流的傳輸率。

附註

開啟影像穩定時，影像會稍微被裁切，因而降低最大解析度。

1. 前往 [Video (影片) > Installation (安裝) > Image correction (影像修正)]。
2. 開啟 [Image stabilization (影像穩定系統)]。

觀看和錄製影像

本節包含關於設定設備的說明。如需深入了解串流和儲存的運作方式，請參閱。

減少頻寬和儲存空間

重要

減少頻寬可能會導致影像細節遺失。

1. 前往 [Video (影片) > Stream (串流)]。
2. 按一下即時影像中的 。
3. 如裝置可支援，請將 [Video format (影片格式)] 選為 [AV1]。否則請選擇 [H.264]。
4. 前往 [Video (影片) > Stream (串流) > General (一般)]，並增加 [Compression (壓縮)] 值。
5. 前往 [Video (影像) > Stream (串流) > Zipstream]，並執行下列其中一項或多項操作：

   附註

   Zipstream智慧影像壓縮（英文）設定用於MJPEG 以外的所有影片編碼。

   - 選取您要使用的 [Zipstream Strength (強度)]。
   - 開啟 [Optimize for storage (最佳化儲存)]。僅當影像管理軟體支援 B 圖框時才能使用此功能。
   - 開啟 [Dynamic FPS (動態 FPS)]。
   - 開啟 [Dynamic GOP (動態圖片群組 (GOP))]，並設定較高 GOP 長度值的 [Upper limit (上限)]。

附註

大多數網頁瀏覽器都不支援 H.265 解碼，因此設備在其網頁介面中不支援此選項。您可以改用支援 H.265 解碼的影像管理系統或應用程式。

設定網路儲存空間

若要在網路上儲存錄影內容，您需要設定網路儲存空間。

1. 請前往 [System (系統) > Storage (儲存空間)]。
2. 按一下 [Network storage (網路儲存空間)] 下方的 [+ Add network storage (新增網路儲存空間)]。
3. 鍵入主機伺服器的 IP 位址。
4. 請在 [Network share (網路共用硬碟)] 下方鍵入主機伺服器上的共用位置名稱。
5. 請鍵入使用者名稱和密碼。
6. 選取 SMB 版本或保留為 [Auto (自動)]。
7. 如果遭遇暫時性連線問題，或是尚未設定共享，請選取 [Add share without testing (無需測試即可新增共享)]。
8. 按一下 [Add (新增)]。

錄製並觀看影片

直接從攝影機錄製影像

1. 前往 [Video (影片) > Stream (串流)]。
2. 若要開始錄影，請按一下 。

   如果您尚未設定任何儲存空間，請按一下 和 。如需如何設定網路儲存空間的說明，請參閱
3. 若要停止錄影，請再按一下 。

觀看影片

1. 前往 [Recordings (錄影)]。
2. 按一下清單中代表您的錄影內容的 。

設定事件規則

您可以建立規則，好讓您的裝置在發生某些事件時執行動作。規則是由條件和動作所組成，這些條件可用於觸發動作。例如，裝置可以在偵測到位移時開始錄影或傳送電子郵件，或者在錄影中顯示疊加文字浮水印。

如需深入了解，請查看我們的指南*開始使用事件規則*。

用閃爍的信號燈阻止入侵者

使用閃爍的信號燈讓可能的入侵者知道您的周界受到防護。

此範例說明如何連接信號燈，並將其設定為在熱顯像攝影機偵測到入侵時閃爍。在此範例中，信號燈只能在辦公時間以外的時間 (週一至週五 18:00 至 08:00) 啟動閃爍，並且每次啟動時都會閃爍 30 秒。

需要的硬體

- 連接線 (一藍一紅，最小面積：0.25 mm^2，最大面積：0.5 mm^2)
- 閃爍信號燈 (12 V DC，最大 25 mA)

附註

連接電線的最大長度取決於電線面積和閃爍信號燈的功耗。

實體連接設備

1. 將紅色電線連接至攝影機 I/O 連接端子的針腳 2 (DC 輸出，12 V DC)。
2. 將紅色電線的另一端連接至標有 + 在閃爍信號燈上的連接器。
3. 將藍色電線連接至攝影機 I/O 連接端子的針腳 4 (數位輸出)。
4. 將藍色電線的另一端連接至標有 - 在閃爍信號燈上的連接器。

設定 I/O 埠

在攝影機的網頁介面中將閃爍的信號燈連接至攝影機：

1. 前往 [System (系統) > Accessories (配件) > I/O ports (I/O 埠)]。
2. 針對連接埠 2，將其命名為閃爍的信號燈。
3. 在 [正常狀態] 下方，按一下 [ ]，以將連接埠的正常狀態設定為 [開路 (NO)]。這會讓信號燈在事件發生時開始閃爍。

建立規則

為了讓攝影機在偵測到某物時向信號燈傳送通知以開始閃爍，您需要在攝影機中建立規則。

1. 前往 [System (系統) > Events (事件) > Rules (規則)]，並新增規則。
2. 在 [名稱] 中，輸入閃爍的信號燈。

3. 將 [等待動作] (格式為 hh:mm:ss) 設定為 30 秒。
4. 在條件清單中的 [應用程式] 下方，選取 Perimeter Defender 應用程式。
5. 選取 [使用此條件作為觸發]。
6. 按一下 ，以新增另一個條件。
7. 在條件清單中的 [Scheduled and recurring (排程和循環)] 下方，選取 [Schedule (排程)]。
8. 在排程清單中，選取 [After hours (下班後)]。
9. 在動作清單中的 [I/O] 下方，選取 [當規則作用時切換 I/O]。
10. 從連接埠清單中選取 [閃爍的信號燈] 連接埠。
11. 將 [狀態] 設定為 [作用中]。
12. 按一下 Save (儲存)。

用音訊威懾入侵者

使用網路號角喇叭來警告和阻止可能的入侵者。

此範例說明如何連接 Axis 網路號角喇叭，並將其設定為在熱顯像攝影機偵測到入侵時播放音訊檔。在此範例中，只能在辦公時間以外的時間 (週一至週五 18:00 到 08:00) 啟用號角喇叭。

連接設備

1. 前往 [System (系統) > Edge-to-edge (邊際對邊際) > Pairing (配對)]。
2. 輸入喇叭的 IP 位址、使用者名稱和密碼。您需要使用管理員或操作者帳戶。
3. 按一下 [Connect (連線)]。

將音訊檔上傳至攝影機

1. 前往 [音訊 > 音訊檔]，並按一下 。
2. 按一下 [+ 新增音訊檔]。
3. 找到並上傳音訊檔。
4. 按一下 [關閉]。

建立規則

為了讓攝影機在偵測到某物時讓喇叭播放音訊檔，您需要在攝影機中建立規則。

1. 前往 [System (系統) > Events (事件) > Rules (規則)]，並新增規則。
2. 在 [名稱] 中，輸入用音訊威懾。
3. 在條件清單中的 [應用程式] 下方，選取 Perimeter Defender 應用程式。
4. 選取 [使用此條件作為觸發]。
5. 按一下 ，以新增另一個條件。
6. 在條件清單中的 [Scheduled and recurring (排程和循環)] 下方，選取 [Schedule (排程)]。
7. 在排程清單中，選取 [After hours (下班後)]。
8. 在動作清單中，在 [音訊檔] 下，選取 [播放音訊檔]。
9. 在 [音訊檔] 下，選取您已上傳的音訊檔。
10. 在 [音訊輸出] 下，選取 [1] 用於配對的網路喇叭。
11. 按一下 Save (儲存)。

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

請使用 Axis 閃光警報器，以讓可能的入侵者知道您的周界正受到防護。

此範例說明每當 AXIS Motion Guard 偵測到位移時如何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)。

使用輸入訊號偵測竄改

此範例說明如何在輸入訊號遭切斷或短路時傳送電子郵件。如需 I/O 連接端子的詳細資訊，請參閱。

1. 前往 [System (系統) > Accessories (配件) > I/O ports (I/O 埠)]，並開啟 [Supervised (受監控)]。

新增電子郵件接收者：

1. 前往 [System (系統) > Events (事件) > Recipients (接收者)]，並新增一位接收者。
2. 輸入接收者的名稱。
3. 選取 [Email (電子郵件)] 作為通知類型。
4. 輸入接收者的電子郵件地址。
5. 輸入您要攝影機從哪個電子郵件地址傳送通知。
6. 提供傳送電子郵件帳戶的登入詳細資訊，以及 SMTP 主機名稱和連接埠編號。
7. 若要測試您的電子郵件設定，請按一下 [Test (測試)]。
8. 按一下 Save (儲存)。

建立規則：

1. 前往 [System (系統) > Events (事件) > Rules (規則)]，並新增規則。
2. 輸入規則名稱。
3. 請在條件清單中，[I/O] 下方，選取 [Supervised input tampering is active (受監控輸入防竄改功能有效)]。
4. 選取相關連接埠。
5. 在動作清單中，在 [Notifications (通知)] 下方選取 [Send notification to email (傳送通知至電子郵件)]，然後從清單選取接收者。
6. 輸入電子郵件的主旨和訊息。
7. 按一下 Save (儲存)。

如果有人在鏡頭上噴漆，則自動發送電子郵件

啟動防竄改偵測：

1. 前往 [System (系統) > Detectors (偵測器) > Camera tampering (攝影機防破壞)]。
2. 為 [Trigger delay (觸發延遲)] 設定一個值。該值表示發送電子郵件前必須先經過的時間。

新增電子郵件接收者：

3. 前往 [System (系統) > Events (事件) > Recipients (接收者)]，並新增一位接收者。
4. 輸入接收者的名稱。
5. 選取 [Email (電子郵件)]。
6. 輸入電子郵件要傳送到的電子郵件地址。
7. 攝影機沒有本身的電子郵件伺服器，因此必須登入其他電子郵件伺服器才能發送郵件。根據您的電子郵件供應商填寫其餘資訊。

8. 若要傳送測試電子郵件，請按一下 [Test (測試)]。
9. 按一下 Save (儲存)。

建立規則：

10. 前往 [System (系統) > Events (事件) > Rules (規則)]，並新增規則。
11. 輸入規則名稱。
12. 在條件清單的 [Video (影片)] 下，選取 [Tampering (防竄改)]。
13. 在動作清單中，在 [Notifications (通知)] 下方選取 [Send notification to email (傳送通知至電子郵件)]，然後從清單選取接收者。
14. 輸入電子郵件的主旨和訊息。
15. 按一下 Save (儲存)。

聲音

將音訊新增至錄影內容

開啟音訊：

1. 前往 [Video (影像) > Stream (串流) > Audio (音訊)] 並包含音訊。
2. 如果該設備有多輸入來源，請在 [Source (來源)] 中選取正確的來源。
3. 前往 [Audio (音訊) > Device settings (設備設定)]，並開啟正確的輸入來源。
4. 如果您對輸入來源進行任何變更，請按一下 [Apply changes (套用變更)]。

編輯錄影使用串流格式：

5. 前往 [System (系統) > Stream profiles (串流格式)]，並選取串流格式。
6. 選取 [Include audio (包含音訊)]，然後開啟。
7. 按一下 Save (儲存)。

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)]：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。

持續錄影中

顯示正在進行的錄影及其指定的儲存空間。

錄影檔： 檢視正在進行的和篩選的錄影及其來源。如需詳細資料，請參閱：

顯示儲存錄影的儲存空間。

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。

影像

按一下可播放即時影像串流。

按一下可凍結即時影像串流。

按一下可拍取即時影像串流的快照。檔案會儲存在您電腦上的 [下載] 資料夾中。影像檔案名稱為 [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]。快照的大小取決於從接收快照的特定網路瀏覽器引擎套用的壓縮，因此快照的大小可能會與該設備中設定的實際壓縮設定有所不同。

按一下顯示 I/O 輸出埠。例如，使用開關開啟或關閉連接埠的電路以測試外部裝置。

點選手動開啟或關閉紅外線照明。

按一下手動開啟或關閉白光。

按一下以存取螢幕上控制項。若啟用螢幕控制項群組，當使用者在影像管理軟體中以滑鼠右鍵按一下即時串流時，可使用各個群組中的設定。

- [Predefined controls (預先定義的控制項)]：列出預設螢幕控制項。
- [Custom controls (自訂控制項)]：按一下 [Add custom control (新增自訂控制項)] 以建立自訂螢幕控制項。

啟動清洗器。程序開始時，攝影機會移至設定的位置，以接受清洗噴灑。整氣清洗程序完成時，攝影機會返回原本的位置。唯有連接並設定清洗器時，才能看見此圖示。

啟動雨刷。

按一下並選取一個預設點，以前往即時影像中的該預設點。或者，按一下 [Setup (設定)]，以前往預設點頁面。

新增或移除記憶對焦區域。當您新增記憶對焦區域時，攝影機會在該特定的水平轉動/上下轉動範圍儲存對焦設定。當您已經設定記憶對焦區域且攝影機在即時檢視中進入該區域時，攝影機會記得先前儲存的對焦。覆蓋攝影機區域的一半就足以記住對焦。

按一下可選取自動巡弋，然後按一下 [Start (啟動)]，即可播放自動巡弋。或者，按一下 [Setup (設定)]，以前往自動巡弋頁面。

點選可手動開啟加熱器一段選取的時段。

按一下可開始連續錄影即時影像串流。再按一下可停止錄影。如果錄影正在進行中，則會自動在重新開機後繼續錄影。

按一下可顯示所設定供設備使用的儲存空間。如果要設定儲存，您必須以管理員身分登入。

按一下可存取自動追蹤設定。如果按一下 [Analytics (分析) > Autotracking (自動追蹤)] 中的圖示，可以進行更多設定。

按一下可存取更多設定：

- [Video format (影像格式)]：選取即時影像中使用的編碼格式。
- [Autoplay (自動播放)]：開啟後，每次在新的工作階段開啟設備時，都會自動播放靜音的影像串流。
- [Client stream information (用戶端串流資訊)]：開啟此選項可顯示有關顯示即時影像串流之瀏覽器所用影像串流的動態資訊。傳輸率資訊因為資訊來源不同，而與文字浮水印中顯示的資訊有所不同。用戶端軟體資訊中的傳輸率是上一秒的傳輸率，源自裝置的編碼驅動程式。浮水印中的傳輸率是最後 5 秒的平均傳輸率，這來自瀏覽器。這兩個值僅涉及原始影像串流，不包含透過 UDP/TCP/HTTP 在網路上傳輸時所產生的額外頻寬。
- [Adaptive stream (可調式串流)]：開啟此選項可相應於觀看用戶端的實際顯示解析度對影像解析度進行調整，以改善使用者體驗，並協助防止可能發生的用戶端硬體過載。只有在使用瀏覽器的網頁介面觀看影像串流時，才會套用可調式串流。開啟可調式串流時，最大影格張數為 30 fps。如果在啟用可調式串流時拍取快照，則會使用可調式串流所選取的影像解析度。
- [Level grid (水平格線)]：按一下 以顯示水平格線。此格線可協助您判斷影像是否水平對齊。按一下 可隱藏。
- [Pixel counter (畫素計算)]：按一下 以顯示畫素計算。拖曳方塊並調整大小可將您的關注區域包含在其中。您也可以在 [Width (寬度)] 和 [Height (高度)] 欄位中定義方塊的像素大小。
- [Refresh (重新整理)]：按一下 以重新整理即時影像中的靜態畫面。
- [PTZ controls (PTZ 控制)]：開啟以在即時影像中顯示 PTZ 控制。

1:1 按一下可顯示完整解析度的即時影像。如果完整解析度的影像大於螢幕尺寸，請使用較小的影像在畫面中進行瀏覽。

按一下可顯示全螢幕即時影像串流。按 ESC 鍵即可結束全螢幕模式。

安裝

[Capture mode (擷取模式)]：擷取模式是定義攝影機擷取影像方式的預設組態。變更擷取模式時，可能會影響許多其他設定，例如觀看區域和隱私遮蔽。

[Mounting position (安裝位置)]：影像的方向會依攝影機的安裝方式變更。

[Power line frequency (電力頻率)]：為盡量減少影像閃爍的情形，選取您所在地區使用的頻率。美國地區通常使用 60 Hz。世界其他地區大多使用 50 Hz。如果不確定您所在地區的電力頻率，請洽詢當地主管機關。

[Rotate (旋轉)]：選取偏好的影像方向。

影像修正

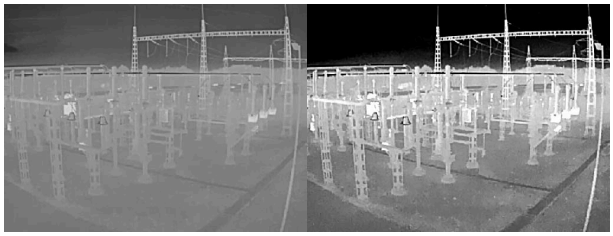
[Image stabilization (影像穩定)]：開啟此選項可獲得更平滑、更穩定且減少模糊的影像。建議您在設備已安裝於無掩蔽位置且受風吹或往來車流等因素所致振動影響的環境中使用影像穩定系統。

[Stabilizer margin (穩定器邊限)]：使用滑桿調整穩定器邊限大小，藉以決定要抑制的震動等級。如果產品是安裝在振動很大的環境中，請將滑桿移向 [Max (最大)]。結果會擷取較小的場景。如果環境振動較少，請將滑桿移向 [Min (最小)]。

影像

外觀

[Contrast (對比)]：使用滑桿調整淺色與深色之間的差異。



[Brightness (亮度)]：使用滑桿調整光線敏感度。這可以讓物件更容易看到。亮度是在擷取影像之後套用，並不會影響影像中的資訊。若要取得暗區中的更多細節，提高增益或加長曝光時間，效果通常更好。



[Sharpness (銳利度)]：使用滑桿調整邊緣對比，可讓影像中的物件顯得更清晰銳利。如果您增加銳利度，可能也會增加所需的傳輸率和儲存空間量。



寬動態範圍(WDR)

[Local contrast (局部對比)]：使用滑桿調整影像的對比。值越高，暗區與亮區之間的對比度越高。

曝光

[Exposure zone (曝光區域)]：使用曝光區域最佳化場景選取部分的曝光，例如入口門前的區域。

附註

曝光區域與原始影像 (未旋轉) 相關聯，而區域名稱會套用至原始影像。例如，這就意味著影像串流旋轉 90° 時，串流中的上方區域會變成右側區域，而左側則變成下方。

- [Automatic (自動)]：適用於大多數情況。
- [Center (中央)]：使用位於影像中央的固定區域來計算曝光。此區域在即時檢視中具有固定的大小和位置。
- [Full (全區)]：使用整個即時影像來計算曝光。
- [Upper (上方)]：使用位於影像上方具有固定大小和位置的區域來計算曝光。
- [Lower (下方)]：使用位於影像下方具有固定大小和位置的區域來計算曝光。
- [Left (左側)]：使用位於影像左側具有固定大小和位置的區域來計算曝光。
- [Right (右側)]：使用位於影像右側具有固定大小和位置的區域來計算曝光。
- [Spot (定點)]：使用即時影像中的某個具有固定大小和位置的區域來計算曝光。
- [Custom (自訂)]：使用即時影像中的某個區域來計算曝光。您可以調整區域的大小和位置。

[Max gain (最大增益)]：選取合適的最大增益。如果增加最大增益，雖能改善低對比影像中細節的可見程度，但也會提高雜訊等級。雜訊較多可能還會導致頻寬與儲存空間的使用量增加。

串流

一般

[Resolution (解析度)]：選取適合監控場景的影像解析度。較高的解析度會增加頻寬與儲存空間。

[Palette (調色盤)]：選取調色板以根據溫度使用不同顏色為影像著色。調色板可以改善小細節的可見度。

[Frame rate (影格速率)]：為了避免網路發生頻寬問題或縮減儲存空間大小，您可以將影格張數限制為固定的數量。如果讓影格張數保持為零，則影格張數會根據目前的情況，保持在盡可能最高的速率。影格張數越高，需要的頻寬及儲存容量就越大。

[P-frames (P 圖框)]：P-frame 是一種預測影像，它僅顯示影像相對於前一圖框的變化。輸入所需的 P 圖框數。數目越大，所需的頻寬就越少。不過，如果發生網路壅塞，影像畫質可能會顯著降低。

[Compression (壓縮)]：使用滑桿調整影像壓縮。高壓縮率會產生較低傳輸率和較低影像畫質。低壓縮率可改善影像畫質，但會在錄影時使用較多頻寬和儲存空間。

[Signed video (已簽署的影像)]：開啟以將已簽署的影像功能新增至影像。已簽署的影像透過新增加密簽名至影像使其免受竄改。

Zipstream

Zipstream 智能影像壓縮技術是為了使影像監控效能最佳化而降低傳輸率的技術，可在 H.264 或 H.265 串流中即時降低平均傳輸率。Axis Zipstream 技術會在有多個關注地區的場景中套用高傳輸率

(例如，有移動物件的場景)。場景較屬靜態時，Zipstream 智能影像壓縮技術會套用較低的傳輸率，藉此降低所需的儲存空間。如需深入了解，請參閱*使用 Axis Zipstream 降低傳輸率*

選取降低傳輸率 [Strength (強度)]：
- [Off (關閉)]：沒有降低傳輸率。
- [Low (低)]：大部分場景不會看到品質退化。這是預設選項，可在所有類型的場景中用來降低傳輸率。
- [Medium (中)]：雖然雜訊減少，但在部分場景中看得出影響，且在較不受關注的地區 (例如沒有動靜的地方)中，細節層次稍有降低。
- [High (高)]：雖然雜訊減少，但在部分場景中看得出影響，而在較不受關注的地區 (例如沒有動靜的地方)中，細節層次會降低。建議將此等級用於雲端連線設備以及用於使用本機儲存空間的設備。
- [Higher (較高)]：雖然雜訊減少，但在部分場景中看得出影響，而在較不受關注的地區 (例如沒有動靜的地方)中，細節層次會降低。
- [Extreme (極高)]：大部分場景中都看得出影響。對傳輸率進行最佳化，讓所需的儲存空間變得盡可能小。

[Optimize for storage (最佳化以儲存)]：開啟以最小化傳輸率，同時保持品質。最佳化不適用於網頁用戶端中顯示的串流。僅當您的 VMS 支援 B 圖框時才能使用此功能。開啟 [Optimize for storage (最佳化以儲存)]，也開啟 [Dynamic GOP (動態圖片群組 (GOP))]。

[Dynamic FPS (動態 FPS)] (每秒影格數)：開啟此選項可讓頻寬根據場景中的活動量改變。活動越多，需要的頻寬就越大。

[Lower limit (下限)]：輸入值即可根據場景位移在最小 fps 與串流預設 fps 之間調整影格張數。建議您在位移非常少的場景中使用下限，此時 fps 可能會降至 1 或更低。

[Dynamic GOP (動態圖片群組 (GOP))]：開啟此選項可根據場景中的活動量動態調整 I 圖框之間的間隔。

[Upper limit (上限)]：輸入最大 GOP 長度，即兩個 I-frame 之間的最大 P-frame 框數。I-frame 是包含完整自我內容的圖框，獨立於其他圖框。

位元速率控制

- [Average (平均)]：選取以自動調整較長時段的傳輸率，並根據可用的儲存提供最佳的影像畫質。
  - 按一下可根據可用儲存空間、保留時間和傳輸率限制計算目標傳輸率。
  - [Target bitrate (目標傳輸率)]：輸入所需的目標傳輸率。
  - [Retention time (保留時間)]：輸入要保留錄影內容的天數。
  - [Storage (儲存)]：顯示可用於串流的預估儲存空間。
  - [Maximum bitrate (最大位元速率)]：開啟此選項可設定傳輸率限制。
  - [Bitrate limit (傳輸率限制)]：輸入高於目標傳輸率的傳輸率限制。
- [Maximum (最大)]：選擇根據網路頻寬設定串流的最大即時傳輸率。
  - [Maximum (最大)]：輸入最大位元速率。
- [Variable (可變)]：選取此選項可讓傳輸率根據場景中的活動量改變。活動越多，需要的頻寬就越大。建議在大多數情況下使用此選項。

方向

[Mirror (鏡像)]：開啟此選項可顯示影像的鏡像。

聲音

[Include (包含)]：開啟要在影像串流中使用的音訊。

[Source (來源)] ：選取要使用的音訊來源。

[Stereo (立體聲)] ：開啟此選項可包含內建音訊以及來自外部麥克風的音訊。

浮水印

＋：按一下可新增浮水印。從下拉清單選取浮水印類型：

- [Text (文字)]：選取顯示文字，此文字整合在即時影像畫面中，並可顯示在所有畫面、錄影內容和快照中。您可以輸入自己的文字，也可以包含預先設定的修改來自動顯示時間、日期和影格張數等資訊。
  - — ：按一下可新增日期修飾詞 `%F` 以顯示 yyyy-mm-dd。
  - — ：按一下可新增時間修飾詞 `%X` 以顯示 hh:mm:ss (24 小時制時鐘)。
  - — [Modifiers (修飾詞)]：按一下可選取清單中任一顯示的修飾詞，將其新增至文字方塊。例如，`%a` 會顯示星期幾。
  - — [Size (大小)]：選取所需的字型大小。
  - — [Appearance (外觀)]：選取文字顏色和背景顏色，例如黑色背景中的白色文字 (預設值)。
  - — ：選取影像中的浮水印位置，或按一下並拖曳浮水印，將其在即時影像中移動。
- [Image (影像)]：選擇顯示疊加在影像串流上的靜態影像。您可以使用 .bmp、.png、.jpeg 或 .svg 檔案。
  若要上傳影像，請按一下 [Manage images (管理影像)]。上傳影像之前，您可以選擇：
  - — [Scale with resolution (隨著解析度縮放)]：選取此選項可自動縮放浮水印影像，以符合影像解析度。
  - — [Use transparency (使用透明度)]：選取此選項並輸入表示該顏色的 RGB 十六進位值。請使用格式 RRGGBB。十六進位值的範例：FFFFFF 代表白色、000000 代表黑色、FF0000 代表紅色、6633FF 代表藍色，而 669900 則代表綠色。僅適用於 .bmp 影像。
- [Scene annotation (場景標註)]：選取此選項可在影像串流中顯示維持在相同位置的文字浮水印，即使攝影機向另一個方向水平移動或傾斜也是如此。您可以選擇僅在特定變焦程度內顯示浮水印。
  - — ：按一下可新增日期修飾詞 `%F` 以顯示 yyyy-mm-dd。
  - — ：按一下可新增時間修飾詞 `%X` 以顯示 hh:mm:ss (24 小時制時鐘)。
  - — [Modifiers (修飾詞)]：按一下可選取清單中任一顯示的修飾詞，將其新增至文字方塊。例如，`%a` 會顯示星期幾。
  - — [Size (大小)]：選取所需的字型大小。
  - — [Appearance (外觀)]：選取文字顏色和背景顏色，例如黑色背景中的白色文字 (預設值)。
  - — ：選取影像中的浮水印位置，或按一下並拖曳浮水印，將其在即時影像中移動。浮水印將被儲存並保留在該位置的水平移動和傾斜座標中。
  - — [Annotation between zoom levels (%) (變焦程度 (%) 之間的標註)]：設定浮水印將顯示在其中的變焦程度。
  - — [Annotation symbol (標註符號)]：選取當攝影機不在設定的變焦程度內時顯示的符號而不是浮水印。
- [Streaming indicator (串流指示燈)]：選取此選項可顯示疊加在影像串流上的動畫。即使場景不含任何位移，此動畫也能指示影像串流正在直播。

- [Appearance (外觀)]：選取動畫顏色和背景顏色，例如透明背景上的紅色動畫 (預設值)。
- [Size (大小)]：選取所需的字型大小。
- ：選取影像中的浮水印位置，或按一下並拖曳浮水印，將其在即時影像中移動。

- [Widget: Linegraph (小部件：折線圖)]：顯示測量值如何隨時間變更的圖表。
  - [Title (標題)]：輸入小部件的標題。
  - [Overlay modifier (浮水印修改)]：選取浮水印修改作為資料來源。如果您建立了 MQTT 浮水印，它們將位於清單的末端。
  - ：選取影像中的浮水印位置，或按一下並拖曳浮水印，將其在即時影像中移動。
  - [Size (大小)]：選取浮水印的大小。
  - [Visible on all channels (可在所有頻道上顯示)]：關閉以僅在您目前選取的頻道上顯示。開啟以在所有啟用中的頻道上顯示。
  - [Update interval (更新間隔)]：選擇資料更新之間的時間。
  - [Transparency (透明度)]：設定整個浮水印的透明度。
  - [Background transparency (背景透明度)]：僅設定浮水印背景的透明度。
  - [Points (點)]：開啟此選項以在資料更新時為圖表線條新增點。
  - X 軸
    - [Label (標籤)]：輸入 x 軸的文字標籤。
    - [Time window (時間窗口)]：輸入資料視覺化的時間長度。
    - [Time unit (時間單位)]：輸入 x 軸的時間單位。
  - Y 軸
    - [Label (標籤)]：輸入 y 軸的文字標籤。
    - [Dynamic scale (動態比例)]：開啟以讓比例自動根據資料值調整。關閉以手動輸入固定比例的值。
    - [Min alarm threshold (最小警報界限)] 和 [Max alarm threshold (最大警報界限)]：這些值將為圖表新增水平參考線，以便更容易看到資料值何時變得過高或過低。

- [Widget: Meter (小部件：測量儀表)]：顯示柱狀圖，該柱狀圖顯示最近測量的資料值。
  - [Title (標題)]：輸入小部件的標題。
  - [Overlay modifier (浮水印修改)]：選取浮水印修改作為資料來源。如果您建立了 MQTT 浮水印，它們將位於清單的末端。
  - ：選取影像中的浮水印位置，或按一下並拖曳浮水印，將其在即時影像中移動。
  - [Size (大小)]：選取浮水印的大小。
  - [Visible on all channels (可在所有頻道上顯示)]：關閉以僅在您目前選取的頻道上顯示。開啟以在所有啟用中的頻道上顯示。
  - [Update interval (更新間隔)]：選擇資料更新之間的時間。
  - [Transparency (透明度)]：設定整個浮水印的透明度。
  - [Background transparency (背景透明度)]：僅設定浮水印背景的透明度。
  - [Points (點)]：開啟此選項以在資料更新時為圖表線條新增點。
  - Y 軸

- [Label (標籤)]：輸入 y 軸的文字標籤。
- [Dynamic scale (動態比例)]：開啟以讓比例自動根據資料值調整。關閉以手動輸入固定比例的值。
- [Min alarm threshold (最小警報界限)] 和 [Max alarm threshold (最大警報界限)]：這些值將為柱狀圖新增水平參考線，以便更容易看到資料值何時變得過高或過低。

隱私遮罩

：按一下可建立新的隱私遮蔽。

[Privacy masks x/32 (隱私遮蔽 x/32)]：按一下此標題列可變更所有隱私遮蔽的顏色，或永久刪除所有隱私遮蔽。

[Cell size (方格大小)]： 如果選擇馬賽克顏色，隱私遮蔽會以畫素圖案顯示。使用滑桿變更像素大小。

[Mask x (遮罩 x)]：按一下單一遮罩名稱/編號可重新命名、停用或永久刪除該遮罩。

[Use zoom level (使用縮放比例)]：開啟後，只有在達到建立時的縮放等級才會顯示此隱私遮蔽。縮小影像會再次隱藏遮罩。

聲音

設備設定

[Input (輸入)]：開啟或關閉音訊輸入。顯示輸入的類型。

[Input type (輸入類型)]：選取輸入類型，例如，內部麥克風輸入還是線路輸入。

[Power type (電源類型)]：選取輸入的電源類型。

[Apply changes (套用變更)]：套用您的選擇。

[Echo cancellation (回音消除)]：開啟此選項可消除雙向通訊期間的回音。

[Separate gain controls (個別增益控制)]：開啟以分別調整不同輸入類型的增益。

[Automatic gain control (自動增益控制)]：開啟此選項可動態調整增益以適應聲音中的變化。

[Gain (增益)]：使用滑桿變更增益。按一下麥克風圖示可靜音或取消靜音。

[Output (輸出)]：顯示輸出的類型。

[Gain (增益)]：使用滑桿變更增益。按一下喇叭圖示可靜音或取消靜音。

[Automatic volume control (自動音量控制)]：開啟可讓裝置根據環境雜訊等級自動動態調整增益。自動音量控制會影響所有音訊輸出，包括線路和電話線圈。

串流

[Encoding (編碼)]：選取要用於輸入來源串流的編碼。您只能在開啟音訊輸入時選擇編碼。如果已關閉音訊輸入，請按一下 [Enable audio input (啟用音訊輸入)]，以開啟音訊輸入。

錄影檔案

按一下可過濾錄影內容。

From (從)：顯示特定時間點之後完成的錄影。

To (到)：顯示直到特定時間點的錄影。

[Source (來源)]：顯示錄影內容根據的來源。該來源是指感應器。

[Event (事件)]：顯示錄影內容根據的事件。

[Storage (儲存)]：顯示錄影內容根據的儲存類型。

[Ongoing recordings (持續錄影中)]：顯示裝置上所有進行中的錄影。

開始在裝置上錄影。

選擇要儲存到哪一個儲存設備。

停止在裝置上錄影。

[Triggered recordings (觸發的錄影)] 將在手動停止或裝置關閉時結束。

[Continuous recordings (連續錄影)] 將繼續，直到手動停止。即使裝置已關閉，當裝置重新啟動時也會繼續錄影。

播放錄影。

停止播放錄影。

顯示或隱藏有關錄影的資訊和選項。

[Set export range (設定匯出範圍)]：如果只要匯出部分錄影，請輸入時間範圍。請注意，如果您工作的時區與設備所在的時區不同，則時間範圍以設備的時區為準。

[Encrypt (加密)]：選取此選項以設定匯出錄影的密碼。沒有密碼就無法開啟匯出的檔案。

按一下可刪除錄影。

[Export (匯出)]：匯出全部或部分錄影。

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。
  - [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+) (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

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 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。
- [Viewer (觀看者)]：可存取：
  - 觀看並拍下影像串流的快照。
  - 觀看並匯出錄影。
  - 水平轉動、上下轉動和變焦；使用 [PTZ account (PTZ 帳戶)] 存取。

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 (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。

儲存

網路儲存裝置

[Ignore (忽略)]：開啟以忽略網路儲存空間。

[Add network storage (新增網路儲存空間)]：按一下以新增可儲存錄影資料的網路共享硬碟。

- [Address (位址)]：輸入主機伺服器 (通常是 NAS (網路附加儲存)) 的 IP 位址或主機名稱。建議您將主機設定為使用固定 IP 位址 (而非 DHCP，因為動態 IP 位址可能會改變)，或者您使用 DNS。我們不支援 Windows SMB/CIFS 名稱。
- [Network share (網路共享硬碟)]：輸入主機伺服器上的共享位置名稱。多部 Axis 設備可以使用同一個網路共享空間，因為每個設備都有專屬的資料夾。
- [User (使用者)]：如果伺服器需要登入，請輸入使用者名稱。若要登入特定網域伺服器，請輸入 `DOMAIN\username`。
- [Password (密碼)]：如果伺服器需要登入，請輸入密碼。
- [SMB version (SMB 版本)]：選取要連線至 NAS 的 SMB 儲存通訊協定版本。如果選取 [Auto (自動)]，則裝置會嘗試交涉取得其中一個安全版本 SMB：3.02、3.0 或 2.1。選取 1.0 或 2.0 以連線至不支援更新版本的舊版 NAS。您可以在*這裡*閱讀更多資訊，進一步了解 Axis 裝置中的 SMB 支援。
- [Add share without testing (無需測試即可新增共享)]：選取此選項時，即使在連線測試過程中發現錯誤，也能新增網路共享硬碟。錯誤可能是，例如，伺服器需要密碼，但是您沒有輸入密碼。

[Remove network storage (移除網路儲存空間)]：按一下可卸載、解除綁定和移除網路共享的連接。這會移除網路共享的所有設定。

[Unbind (解除綁定)]：按一下可解除綁定網路共享硬碟並中斷連線。
[Bind (綁定)]：按一下可綁定並連結網路共享硬碟。

[Unmount (卸載)]：按一下可卸載網路共享。
[Mount (裝載)]：按一下可裝載網路共享硬碟。

[Write protect (寫入保護)]：開啟可停止寫入網路共享硬碟，並保護錄影不會遭到移除。您無法格式化受寫入保護的網路共享硬碟。

[Retention time (保留時間)]：選取保留錄影內容的時間長短，以便限制舊錄影內容的數量，或遵循關於資料儲存方面的法規。如果網路儲存空間已滿，則會在選取的時間段經過之前，移除舊的錄影資料。

工具

- [Test connection (測試連線)]：測試與網路共享硬碟的連線。
- [Format (格式化)]：例如，當您需要快速清除所有資料，請格式化網路共享。CIFS 是可用的檔案系統選項。

[Use tool (使用工具)]：按一下以啟用選取的工具。

內建儲存空間

重要

有遺失資料和損毀錄影內容的風險。當設備執行中時，請勿取出 SD 卡。請在移除前卸載 SD 卡。

[Unmount (卸載)]：按一下可安全地移除 SD 卡。

[Write protect (寫入保護)]：啟用這個選項可停止寫入 SD 卡，並保護錄影不被移除。您無法格式化受寫入保護的 SD 卡。

[Autoformat (自動格式化)]：開啟此選項可自動格式化新插入的 SD 卡。此功能會將檔案系統格式化成 ext4。

[Ignore (忽略)]：開啟此選項可停止將錄影內容儲存於 SD 卡。忽略 SD 卡，裝置不再辨識是否存在卡片。此設置僅適用於管理員。

[Retention time (保留時間)]：選取保留錄影內容的時間長短，以便限制舊錄影內容的數量，或遵從資料儲存法規。當 SD 記憶卡已滿時，它會在保留時間尚未到期之前刪除舊的錄影。

工具

- [Check (檢查)]：檢查 SD 記憶卡上的錯誤。
- [Repair (修復)]：修復檔案系統中的錯誤。
- [Format (格式化)]：格式化 SD 記憶卡，以更改檔案系統並刪除所有資料。您只能將 SD 記憶卡格式化為 ext4 檔案系統。您需要第三方供應商的 ext4 驅動程式或應用程式，才能存取 Windows® 中的檔案系統。
- [Encrypt (加密)]：使用此工具格式化 SD 卡，並且啟用加密功能。這會刪除所有儲存在 SD 記憶卡上的資料。您儲存在 SD 記憶卡上的所有新資料都會加密。
- [Decrypt (解密)]：使用此工具格式化 SD 記憶卡，毋需加密。這會刪除所有儲存在 SD 記憶卡上的資料。您儲存在 SD 記憶卡上的所有新資料都不會加密。
- [Change password (變更密碼)]：變更加密 SD 卡所需的密碼。

[Use tool (使用工具)]：按一下以啟用選取的工具。

[Wear trigger (磨損觸發)]：為要觸發動作的 SD 卡磨損級別設定一個值。磨損級別範圍 0—200%。全新 SD 卡的磨損級別為 0%。磨損級別為 100% 表示該 SD 卡已接近其預期壽命。磨損級別達到 200% 時，SD 卡發生故障的風險很高。我們建議將磨損觸發定在 80—90% 之間。這使您有時間下載任何錄影，並在 SD 卡可能磨損之前及時更換。磨損觸發允許您設定一個事件，並在磨損級別達到您的設定值時收到通知。

串流設定檔

串流格式是一個會影響影像串流的設定群組。您可以在不同情況下使用串流格式，例如：在建立事件並使用規則錄影時使用。

[Add stream profile (新增串流格式)]：按一下以建立新增的串流格式。

[Preview (預覽)]：預覽使用所選取串流格式設定的影像串流。當您變更頁面上的設定時，預覽會更新。如果您的設備有不同的觀看區域，您可以在影像左下角的下拉式清單中變更觀看區域。

[Name (名稱)]：為您的設定檔新增名稱。

[Description (說明)]：新增設定檔的說明。

[Video codec (影片轉碼器)]：選取應套用於設定檔的影片轉碼器。

[Resolution (解析度)]：如需此設定的說明，請參閱。

[Frame rate (影格速率)]：如需此設定的說明，請參閱。

[Compression (壓縮)]：如需此設定的說明，請參閱。

[Zipstream (Zipstream 智能影像壓縮)]：如需此設定的說明，請參閱。

[Optimize for storage (最佳化以儲存)]：如需此設定的說明，請參閱。

[Dynamic FPS (動態 FPS)]：如需此設定的說明，請參閱 。

[Dynamic GOP (動態圖片群組 (GOP))]：如需此設定的說明，請參閱 。

[Mirror (鏡像)]：如需此設定的說明，請參閱。

[GOP length (GOP 長度)]：如需此設定的說明，請參閱。

[Bitrate control (傳輸率控制)]：如需此設定的說明，請參閱。

[Include overlays (包含浮水印)]：選取要包含的浮水印類型。如需如何新增浮水印的資訊，請參閱。

[Include audio (包含音訊)]：如需此設定的說明，請參閱。

ONVIF

ONVIF 帳戶

ONVIF (Open Network Video Interface Forum) 是全球性介面標準，方便終端使用者、整合商、專家顧問和製造商利用網路影像技術可能帶來的潛在價值。ONVIF 使不同廠商產品之間可以互通、提高配置彈性、協助降低成本，並實現具備未來性的系統。

建立一個 ONVIF 帳戶時，就會自動啟用 ONVIF 通訊。使用帳戶名稱和密碼與設備進行所有 ONVIF 通訊。如需更多資訊，請參閱 *axis.com* 上的 Axis 開發人員社群

[+ Add accounts (新增帳戶)]：按一下可新增一個新的 ONVIF 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。

[Role (角色)]：

- [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。
  - 新增應用程式。
- [Media account (媒體帳戶)]：僅允許存取影像串流。

⋮ 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。

ONVIF 媒體設定檔

ONVIF 媒體設定檔包含一組可用來變更媒體串流設定的組態。您可以使用自己的一組組態建立新的設定檔，或使用預設的設定檔進行快速設定。

[+ Add media profile (新增媒體設定檔)]：按一下可新增新的 ONVIF 媒體設定檔。

[Profile name (設定檔名稱)]：新增媒體設定檔的名稱。

[Video source (影像來源)]：選取組態的影像來源。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態。下拉式清單中的組態對應於裝置的影像頻道，包括多分割串流、觀看區域及虛擬頻道。

[Video encoder (影像編碼器)]：選擇組態的影像編碼格式。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態，並調整編碼設定。下拉式清單中的組態作為影像編碼器組態的識別碼/名稱。選取使用者 0 至 15，以便套用您的設定，或如果您想要為特定編碼格式使用預設設定，則請選擇其中一名預設使用者。

附註

啟用裝置中的音訊，以取得選取音訊來源和音訊編碼器組態的選項。

[Audio source (音訊來源)]：選取組態的音訊輸入來源。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態，並調整音訊設定。下拉式清單中的組態對應於裝置的音訊輸入。如果裝置有一個音訊輸入，則為 user0。如果裝置有數個音訊輸入，清單中將會有其他使用者。

[Audio encoder (音訊編碼器)]：選擇組態的音訊編碼格式。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態，並調整音訊編碼設定。下拉式清單中的組態作為音訊編碼器組態的識別碼/名稱。

[Audio decoder (音訊解碼器)]：選取組態的音訊解碼格式。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態，並調整設定。下拉式清單中的組態作為組態的識別碼/名稱。

[Audio output (音訊輸出)]：選取組態的音訊輸出格式。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態，並調整設定。下拉式清單中的組態作為組態的識別碼/名稱。

[Metadata (軌跡資料)]：選取要包括在組態內的軌跡資料。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態，並調整軌跡資料設定。下拉式清單中的組態作為軌跡資料組態的識別碼/名稱。

[PTZ]：選取組態的 PTZ 設定。

- [Select configuration (選取組態)]：從清單選取使用者定義的組態，並調整 PTZ 設定。下拉式清單中的組態對應於支援 PTZ 的裝置影像頻道。

[Create (建立)]：按一下以儲存您的設定並建立設定檔。

[Cancel (取消)]：按一下取消組態，並清除所有設定。

[profile_x]：按一下設定檔名稱，以開啟並編輯預設設定檔。

分析軌跡資料

RTSP 軌跡資料生產器

查看和管理串流軌跡資料的資料頻道及其使用的頻道。

附註

這些設定適用於使用 ONVIF XML 的 RTSP 軌跡資料串流。此處所做的變更不會影響軌跡資料視覺化頁面。

[Producer (產生器)]：採用即時串流協定 (RTSP) 傳送軌跡資料的資料頻道。

[Channel (頻道)]：用於從產生器發送軌跡資料的頻道。開啟以啟用軌跡資料串流。由於相容性或資源管理原因而關閉。

偵測器

聲音偵測

每個音訊輸入都可使用這些設定。

[Sound level (聲級)]：將聲級調整為從 0 到 100 的值，其中 0 級最敏感，100 級最不敏感。設定聲級時，使用活動指示燈做為判斷準則。建立事件時，您可以使用聲級做為條件。您可以選擇在聲級高於、低於或超過設定值時觸發動作。

撞擊偵測

[Shock detector (撞擊偵測器)]：開啟此選項可在設備受物件撞擊或遭竄改時產生警報。

[Sensitivity level (靈敏度等級)]：移動滑桿調整設備應據以產生警報的靈敏度等級。低值表示裝置僅在撞擊力量強大時才會發出警報。高值表示即使只是輕微的竄改，設備也會發出警報。

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)。

邊際對邊際

配對

配對讓您可以使用相容的 Axis 設備，彷彿其為主設備的一部分。

[+ Add (新增)]：新增要配對的設備。

[Discover devices (發現設備)]：按一下以在網路上尋找設備。網路掃描完成後，將顯示可用設備清單。

附註

清單會顯示所有找到的 AXIS 設備，而不只是可以配對的設備。

只能找到啟用 Bonjour 的設備。若要啟用設備的 Bonjour，請開啟設備的網頁介面，然後前往 [System (系統) > Network (網路) > Network discovery protocols (網路發現協定)]。

附註

已配對的設備將顯示資訊圖示。將滑鼠指標懸停在圖示上，可取得有關已啟用配對的資訊。

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。

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

[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。
- 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。

深入瞭解

調色板

為幫助人眼區分熱顯像中的細節，您可以對顯像套用調色板。調色板中的顏色是人工建立的偽色，強調溫差。

本產品有多種調色板可供選擇。如果操作者觀看影像串流，您可以選擇任何調色板。如果影像串流僅由應用程式使用，請選取白熱調色板。

浮水印

浮水印會疊加在影像串流上。其作用是在錄影期間或是產品安裝和設定期間提供額外的資訊，像是時間戳記。您可以新增文字或影像。

影像串流指示燈是另一種類型的浮水印。向您顯示即時畫面影像串流是在直播。

串流和儲存

影像壓縮格式

根據您的觀看需求和網路屬性來決定使用哪一個壓縮方法。可用的選項包括：

Motion JPEG

附註

為確保支援 Opus 音訊轉碼器，Motion JPEG 串流永遠都是透過 RTP 傳送。

Motion JPEG (或 MJPEG) 是由一系列個別 JPEG 影像組成的數位影像序列。這些影像接著在足以建立呈現不斷更新位移之串流的速率下顯示並更新。為了讓觀看者感知位移影像，速率必須至少為每秒 16 張畫面影格。完整位移影像可在每秒 30 (NTSC) 或 25 (PAL) 張影格的速率下感知得到。

Motion JPEG 串流使用的頻寬量相當大，但可提供出色影像畫質，並存取串流中包含的每一幀畫面。

H.264 或 MPEG-4 Part 10/AVC

附註

H.264 是經授權使用的技術。Axis 產品包含一份 H.264 觀看用戶端授權。禁止另外安裝其他未經授權的用戶端複本。若要購買額外的授權，請聯絡您的 Axis 經銷商。

與 Motion JPEG 格式相比，H.264 可在不影響影像畫質的情況下將使用影像檔案大小縮減 80% 以上，而與舊版 MPEG 格式相比，則縮減高達 50%。這意味著影像檔案所需的網路頻寬和儲存空間更少。或者從另一方面看，在特定的傳輸率下，可以取得更高的影像畫質。

H.265 或 MPEG-H Part 2/HEVC

與 H.264 相比，H.265 可在不影響影像畫質的情況下，縮減超過 25% 的數位影像檔案大小。

附註

- H.265 是經授權使用的技術。Axis 產品包含一份 H.265 觀看用戶端授權。禁止另外安裝其他未經授權的用戶端複本。若要購買額外的授權，請聯絡您的 Axis 經銷商。
- 大多數網頁瀏覽器都不支援 H.265 解碼，因此攝影機在其網頁介面中不支援此選項。您可以改用支援 H.265 解碼的影像管理系統或應用程式。

影像、串流和串流格式設定相互關聯的情形？

[Image (影像)] 索引標籤包含影響產品所有影像串流的攝影機設定。如果變更此索引標籤中的某些設定，就會立即影響所有影像串流和錄製內容。

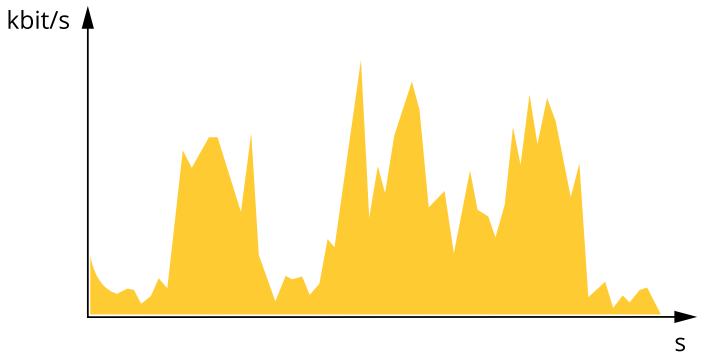
[Stream (串流)] 索引標籤包含影像串流的設定。如果向產品要求提供影像串流，但未指定解析度或影格張數等設定時，您將會看到這些設定。變更 [Stream (串流)] 索引標籤中的設定時，並不影響進行中的串流，但會在您啟動新串流時產生作用。

[Stream profiles (串流格式)] 設定會覆寫 [Stream (串流)] 索引標籤中的設定。如果您要求具有特定串流格式的串流，則串流會包含該串流格式的設定。如果未指定串流格式就要求提供串流，或是要求產品中不存在的串流格式，則串流會包含 [Stream (串流)] 索引標籤中的設定。

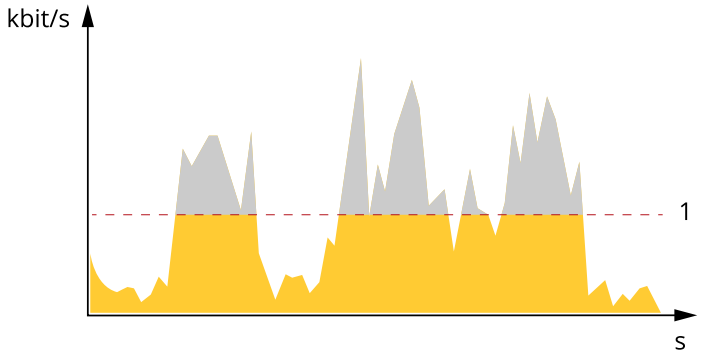
位元速率控制

傳輸率控制可幫助您管理影像串流的頻寬消耗。

可變位元傳輸率(VBR)
變動傳輸率允許頻寬消耗依照場景中的活動程度變動。活動愈多，需要的頻寬愈大。您可以憑藉變動位元速率保證穩定的影像畫質，但您需要確定有餘裕的儲存空間。



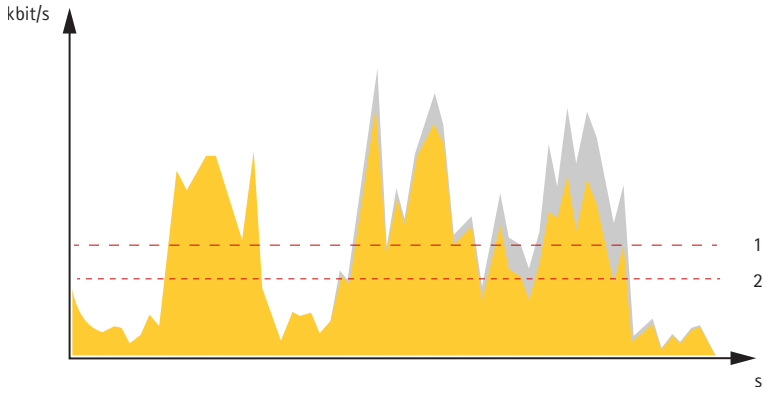
最大位元傳輸率 (MBR)
最大傳輸率讓您設定確定目標傳輸率來處理系統的傳輸率限制。當瞬時傳輸率保持在指定的目標傳輸率以下時，您可能會看到影像畫質或影格張數下降。您可以選擇優先處理影像畫質或影格張數。建議您將目標傳輸率設定為高於預期傳輸率的值。這讓您在場景中有高度活動時，有餘地運作。



1 目標位元速率

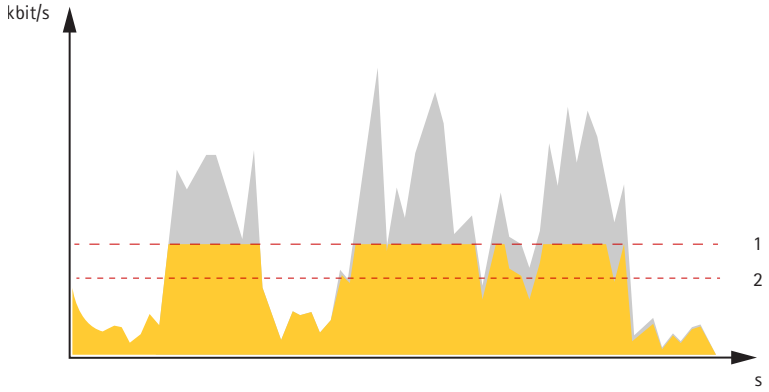
平均傳輸率 (ABR)
平均傳輸率會在更長的時段自動調整。這樣您就可以滿足指定的目標，並根據可用儲存空間提供最佳影像畫質。與靜態場景相比，有很多活動的場景會有更高的傳輸率。如果您在活動量大的場景中使用平均傳輸率選項，您更有可能獲得比較好的影像畫質。調整影像畫質達到指定的目標傳輸率時，您可以定義儲存指定時間長度的影像串流 (存留時間) 所需的總儲存空間。以下列其中一個方法指定平均傳輸率設定：

- 若要計算估計儲存需求，請設定目標傳輸率和保留時間。
- 若要根據可用的儲存空間及所需的保留時間計算平均傳輸率，請使用目標傳輸率計算工具。



1 目標位元速率
2 實際平均傳輸率

您還可以開啟最大位元速率，並在平均傳輸率選項中指定目標傳輸率。



1 目標位元速率
2 實際平均傳輸率

分析和應用程式

利用分析和應用程式，您可以更加善用您的 Axis 設備。AXIS Camera Application Platform (ACAP) 是一個開放式平台，可讓第三方開發適用於 Axis 設備的分析及其他應用程式。應用程式可以預先安裝在設備上，可供免費下載或支付授權費。

若要尋找 Axis 分析和應用程式的使用手冊，請前往 *help.axis.com*。

附註

- 數個應用程式可以同時執行，但有些應用程式可能會彼此不相容。在並行情況下執行時，特定組合的應用程式可能需要過高的處理能力或記憶體資源。部署前，請先確認應用程式可以一起運作。

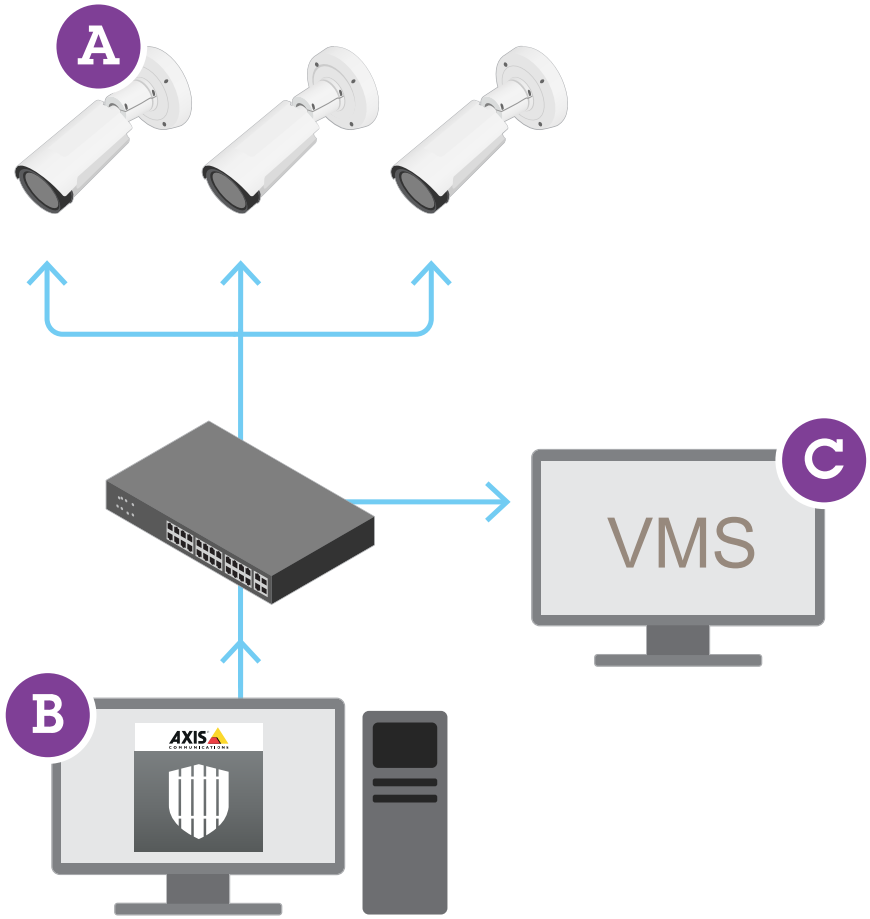
AXIS Perimeter Defender

AXIS Perimeter Defender是周圍監控保全的應用程式。適合需要透過可靠的入侵偵測系統來強化實體門禁控制系統的高度安全警戒周邊防護使用。

AXIS Perimeter Defender 主要設計用於所謂的無菌區防護，例如沿著標記邊界的圍欄。無菌區一詞是指人們不應該在的區域。

在室外環境中使用 AXIS Perimeter Defender 可以：

- 偵測移動的人。
- 偵測移動的車輛，而不區分車輛類型。



此攝影機可以在校準模式、AI 模式或兩種模式的組合下執行應用程式。如果您選擇僅在 AI 模式下執行，攝影機安裝更加靈活，您無需校準攝影機。

AXIS Perimeter Defender 由桌面介面 (B) 組成，您可以從該介面在攝影機 (A) 上安裝和設定應用程式。然後您可以將系統設定為向影像管理軟體 (C) 傳送警報。

AXIS Perimeter Defender PTZ Autotracking是AXIS Perimeter Defender應用程式的外掛程式，使用相同的桌面介面。使用該外掛程式，您可以將固定視覺或熱顯像攝影機與 Axis Q-line PTZ 攝影機配對。然後，您可以使用固定攝影機維持對場景的連續偵測覆蓋，同時 PTZ 攝影機會自動追蹤，並讓您更近距離地檢視偵測到的物件。

重要

AXIS Perimeter Defender PTZ Autotracking 需要校準固定和 PTZ 攝影機。

AXIS Perimeter Defender 提供以下類型的情境：

- 入侵：當有人車進入地面自訂區域時（無論方向軌跡）觸發警報。
- 徘徊：當有人車停留在地面上自訂區域超過自訂秒數時觸發警報。
- 穿越：當有人車通過地面自訂的兩塊以上區域時觸發警報。
- 條件：當有人車未先經過地面指定區域即進入地面另一塊自訂區域時觸發警報。

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*。

TPM 模組

TPM (信賴平台模組) 是一個提供密碼編譯功能的元件，可保護資訊免遭未經授權的存取。此元件永遠處於啟動狀態，您無法變更其中任何設定。

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。

您可以使用 AXIS Device Manager 同時升級多台設備。請前往 *axis.com/products/axis-device-manager* 進一步了解。

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...` 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`，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*。

串流問題

多點傳送 H.264 只能由本機用戶端存取	檢查路由器是否支援多點傳送，或者是否需要設定用戶端與裝置之間的路由器設定。您可能需要增加 TTL (存留時間) 值。
用戶端未顯示多點傳送 H.264	洽詢您的網路管理員，確認 Axis 裝置使用的多點傳送位址對您的網路有效。 洽詢網路管理員，以了解是否有阻止檢視的防火牆。
H.264 影像的呈現效果差	確定您的顯示卡使用最新的驅動程式。通常可以從製造商的網站下載最新的驅動程式。
影格張數低於預期	• 請參考 。 • 減少在用戶端電腦上執行的應用程式數量。 • 限制同時觀看者的人數。 • 洽詢網路管理員，以了解是否有足夠的頻寬可用。 • 降低影像解析度。 • 每秒最大影格數取決於 Axis 裝置的電源頻率 (60/50 Hz)。
無法在即時影像中選取 H.265 編碼	網頁瀏覽器不支援 H.265 解碼。使用支援 H.265 解碼的影像管理系統或應用程式。

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。

效能考量

當您設定系統時，務必要考量各項設定和情況對效能的影響。有一些因素會影響所需頻寬量 (傳輸率)，也有其他因素會影響影格張數，而某些因素則會同時影響這兩者。如果 CPU 的負載達到上限，這也會影響影格張數。

以下是最重要的考量因素：

- 高影像解析度或降低壓縮等級會導致影像包含更多資料，進而影響頻寬。
- 在 GUI 中旋轉影像可能會增加產品的 CPU 負載。

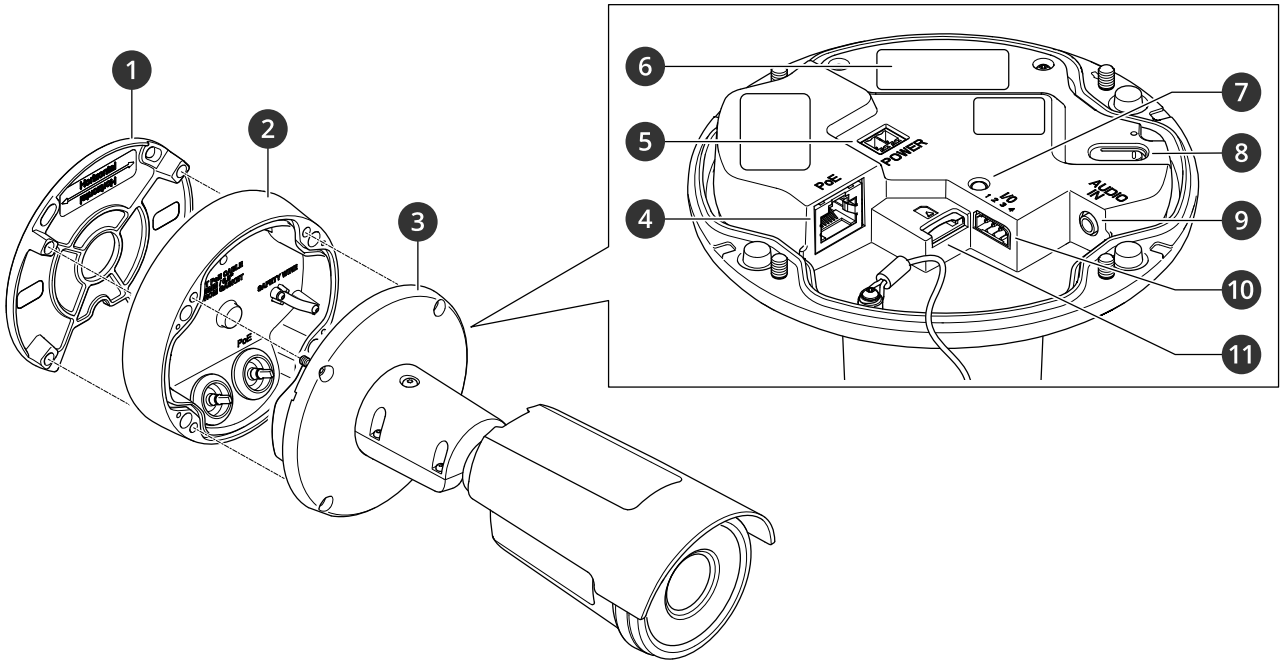
- 大量 Motion JPEG 用戶端或單點傳送 H.264/H.265/AV1 用戶端的存取會影響頻寬。
- 不同用戶端同時檢視不同串流 (解析度、壓縮) 會影響影格張數和頻寬。
  盡可能使用相同的串流以維持高的影格張數。串流格式可用於確保串流是相同的。
- 同時存取具有不同編解碼器的影像串流會影響影格速率和頻寬。為了獲得最佳效能，請使用具有相同編碼解碼器的串流。
- 密集使用事件設定會影響產品的 CPU 負載，進而影響影格張數。
- 使用 HTTPS 可能會降低影格張數，尤其是在串流傳輸 Motion JPEG 時。
- 由於基礎設施不佳而導致的網路密集使用會影響頻寬。
- 在效能不佳的用戶端電腦上檢視會降低所感知的效能，並影響影格張數。
- 同時執行多個 AXIS Camera Application Platform (ACAP) 應用程式可能會影響影格張數和整體效能。
- 使用調色板會影響產品的 CPU 負載，進而影響影格張數。

聯絡支援人員

如需更多協助，請前往 *axis.com/support*。

規格

產品總覽



1 *安裝支架*
2 *連接蓋*
3 *攝影機裝置*
4 *網路接頭 (PoE)*
5 *電源接頭*
6 *零件編號 (P/N) 和序號 (S/N)*
7 *狀態 LED 指示燈*
8 *控制按鈕*
9 *音訊接頭*
10 *I/O 連接端子*
11 *SD 記憶卡插槽*

LED 指示燈

狀態LED燈號	指示
熄滅	連線和正常操作。
綠色	連線和正常操作。
黃色	啟動過程中保持常亮。在升級設備軟體或重設為出廠預設值時閃爍。
琥珀色/紅色	琥珀色/紅色交替閃爍表示無網路連線或連線中斷。
紅色	設備軟體升級失敗。

SD 卡插槽

注意

- 有損壞 SD 卡的風險。插入或取出 SD 卡時，請勿使用銳利的工具、金屬物件或用力過大。請用手指插入和取出卡片。
- 有遺失資料和損毀錄影內容的風險。先透過設備的網頁介面卸載 SD 卡，再將卡片取出。產品正在執行時，請勿取出 SD 卡。

此設備支援 microSD/microSDHC/microSDXC 卡。

如需有關 SD 卡的建議，請參閱 *axis.com*。

microSD、microSDHC 和 microSDXC 標誌是 SD-3C LLC 的商標。microSD、microSDHC 和 microSDXC 是 SD-3C, LLC 在美國和/或其他國家/地區的商標或註冊商標。

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，請按下並放開按鈕，然後等待狀態 LED 燈號閃爍綠色三次。

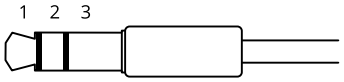
接頭

網路接頭

支援乙太網路供電 (PoE) 的 RJ45 乙太網路接頭。

音訊接頭

- 音訊輸入 — 適用於數位麥克風、類比單聲道麥克風或線路輸入單聲道訊號的 3.5 mm 輸入 (使用立體聲訊號的左聲道)。



音訊輸入

1 尖端接點	2 環狀接點	3 套管接點
非平衡麥克風 (含或不含駐極體電源) 或線路輸入	駐極體電源 (如果選用)	接地
數位訊號	環形供電 (如果選用)	接地

I/O 連接端子

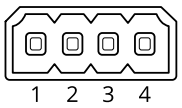
將 I/O 連接端子搭配外部裝置結合位移偵測、事件觸發和警報通知等功能使用。除了0 VDC參考點和電源 (12 VDC 輸出) 以外，I/O 連接端子也會提供連線介面：

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。

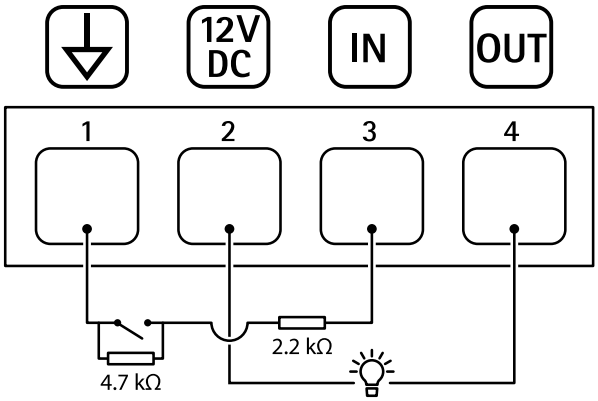
數位輸出 - 用於連接繼電器和 LED 等外接式設備。連接的設備可透過 VAPIX® 應用程式開發介面、事件或設備網頁介面加以啟動。

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 = 25 mA
數位輸入或受監控的輸入	3	連接到針腳 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 VDC
數位輸出	4	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

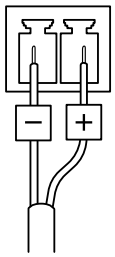
範例:



1 *DC 接地*
2 *DC 輸出 12 V，最大 25 mA*
3 *受監控的輸入*
4 *數位輸出*

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。



T10167107_zh_tw

2024-11 (M18.2)

© 2021 – 2024 Axis Communications AB