

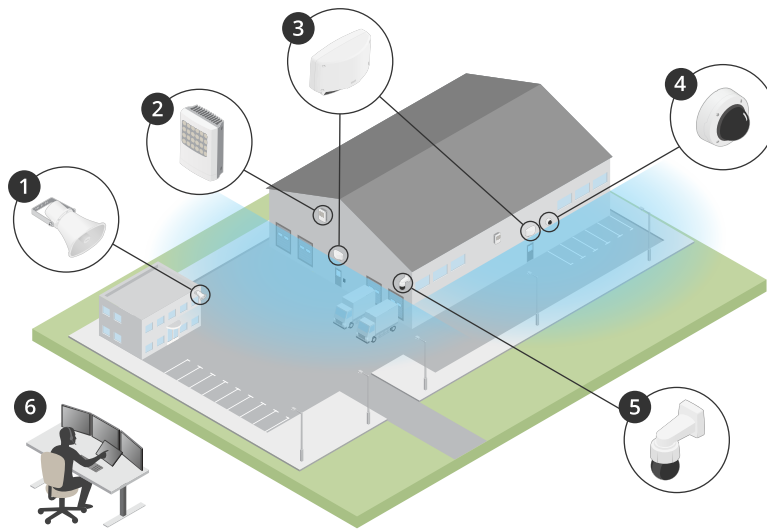
AXIS D2110-VE Security Radar

目錄

解決方案總覽.....	4
雷達設定檔.....	4
產品安裝位置	4
涵蓋區域	5
區域監控設定檔.....	6
安裝多部雷達	6
在同一個共存區安裝 2-3 個雷達	6
在同一個共存區安裝 4-6 個雷達	6
區域安裝範例	7
區域偵測範圍	9
區域監控使用案例.....	10
道路監控設定檔.....	12
道路安裝範例	12
道路偵測範圍	12
道路監控使用案例.....	12
開始使用	14
在網路上尋找裝置.....	14
瀏覽器支援	14
開啟設備的網頁介面.....	14
建立管理員帳戶	14
安全密碼	14
網頁介面概觀	15
設定您的設備.....	16
設定安裝高度	16
校準參考地圖	16
設定偵測區域.....	17
新增情境.....	17
新增不包含區域.....	18
將誤報減至最少	18
觀看和錄製影像	19
減少頻寬和儲存空間	19
設定網路儲存空間	19
錄製並觀看影片.....	20
使用雷達控制 PTZ 攝影機.....	20
使用內建雷達自動追蹤服務控制 PTZ 攝影機.....	20
使用 AXIS Radar Autotracking for PTZ 控制 PTZ 攝影機.....	21
設定事件規則	21
觸發動作.....	21
當機殼打開時觸發通知.....	21
在偵測到位移時用攝影機錄影.....	22
偵測到位移時開燈	22
如果有人使用金屬物體遮住雷達，請傳送電子郵件.....	23
網頁介面	24
狀態.....	24
雷達.....	25
設定	25
串流.....	26
地圖校準.....	27
不包含區域.....	28
情境.....	29
浮水印	30
雷達 PTZ 自動追蹤	32
錄影檔案	33

應用程式	34
系統	34
時間和地點	34
網路	36
安全	39
帳戶	44
事件	46
MQTT	50
儲存	53
串流設定檔	55
ONVIF	56
偵測器	58
配件	59
邊際對邊際	59
記錄檔	61
一般設定	62
維護	63
維護	63
疑難排解	64
驗證您的安裝	65
驗證雷達的安裝	65
驗證雷達	65
完成驗證	66
深入瞭解	67
串流和儲存	67
影像壓縮格式	67
位元速率控制	67
規格	69
產品總覽	69
.....	69
LED 指示燈	69
.....	70
SD 卡插槽	70
按鈕	70
控制按鈕	70
接頭	70
網路接頭	70
網路連接器 (PoE 輸出)	70
I/O 連接端子	71
電源接頭	71
繼電器接頭	72
清潔設備	73
故障排除	74
重設為出廠預設設定	74
檢查目前的 AXIS 作業系統版本	74
升級 AXIS 作業系統	74
技術問題、線索和解決方式	74
效能考量	76

解決方案總覽



- 1 C1310-E 擴音喇叭
- 2 門控制器
- 3 D2110-VE Security Radar
- 4 固定式半球型攝影機
- 5 PTZ攝影機
- 6 監控中心

雷達設定檔

附註

若要使用雷達設定檔，您的裝置必須執行韌體版本 10.11 或更高版本。移至 以更新您的韌體。

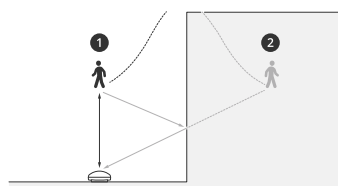
使用手冊是設定來協助您根據您對雷達的期望來使用雷達。AXIS D2110-VE Security Radar 有兩個設定檔：

- 區域監控設定檔可追蹤以低於 55 公里/小時 (34 mph) 的速度移動的大小物體
- 道路監控設定檔可追蹤以最高 105 公里/小時 (65 mph) 的速度移動的車輛

本使用手冊中不屬於區域監控設定檔或道路監控設定檔的任何資訊，對這兩種設定檔都通用，無論您使用哪一個設定檔都可以參照。

產品安裝位置

- 雷達用於監控開放區域。涵蓋區域內的任何實體物體 (如牆壁、柵欄、樹或大灌木) 都會在其後面產生盲點 (雷達陰影)。
- 將雷達安裝在穩定的桿子上，或牆上沒有其他物體或裝置的位置。距離雷達左側和右側 1 公尺 (3 英呎) 內的物體會反射無線電波，進而影響雷達的效能。
- 視野中的金屬物件會引起反射，進而影響雷達執行分類的的能力。



- 1 實際偵測
- 2 反射的偵測 (鬼影軌跡)

有關如何處理反射物件的資訊，請參閱。

- 如果要在同一個共存區安裝兩個以上的雷達，請參閱。

涵蓋區域

AXIS D2110—VE 的水平區域涵蓋範圍為 180°。偵測範圍對應於人類的 5600 公尺² (61000 英呎²) 和車輛的 11300 公尺² (122000 英呎²)。

附註

當雷達安裝在 3.5—4 公尺 (11—13 英呎) 時，適用最佳區域涵蓋率。安裝高度會影響雷達下方盲點的大小。

區域監控設定檔

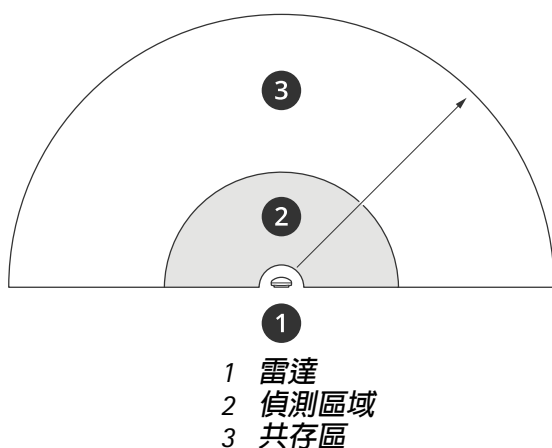
區域監控設定檔已針對偵測移動時速最高 55 公里 (34 英里) 的物件最佳化。此設定檔允許您偵測無論是人、車輛或未知的物體。可以將規則設定為在偵測到任何這些物件時觸發動作。若要追蹤高速行駛的車輛，請使用。

安裝多部雷達

您可以安裝多個雷達來覆蓋區域，例如建築物的周圍或圍欄外的暫存區。

並存

當您在同一個共存區內放置兩個以上的雷達時，來自區域內雷達的無線電波會造成干擾並影響性能。共存區半徑為 350 公尺 (380 碼)。



附註

共存區中雷達的性能也會受到環境和/或雷達朝向柵欄、建築物或鄰近雷達的方向的影響。

在同一個共存區安裝 2-3 個雷達

當您將兩個或三個雷達放在同一個共存區時，您需要在設備介面中定義相鄰雷達的數量。這有助於提高雷達的性能並避免干擾。

1. 前往 [雷達 > 設定 > 共存]。
2. 選取相鄰雷達的數量。

請參閱以了解有關安裝多個雷達的範例。

在同一個共存區安裝 4-6 個雷達

附註

從韌體版本 11.3 開始，可以選擇在同一共存區安裝多達六個雷達。

當您在同一共存區安裝四到六個雷達時，首先設定相鄰雷達的數量，然後將每個雷達新增至一個群組中。從安裝最遠的雷達開始，例如最左邊的雷達。將雷達以三個為一群組新增，並將彼此距離最近的雷達新增至同一群組中。

群組內的雷達將相互同步以最佳化性能並避免相互干擾。

1. 前往 [雷達 > 設定 > 共存]。
2. 設定相鄰雷達數量為 [3—5]。
3. 為您的雷達選取一個群組。



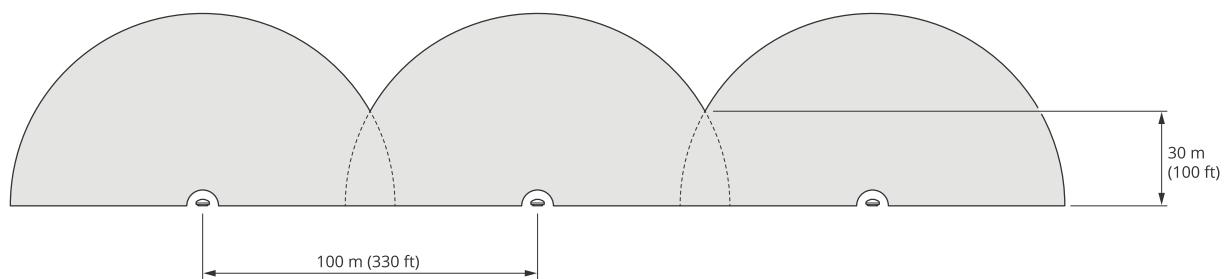
這是一個如何將並排安裝在同一共存區的多個雷達分組的範例。

請參閱以了解有關安裝多個雷達的更多範例。

區域安裝範例

使用多個雷達建立虛擬圍籬

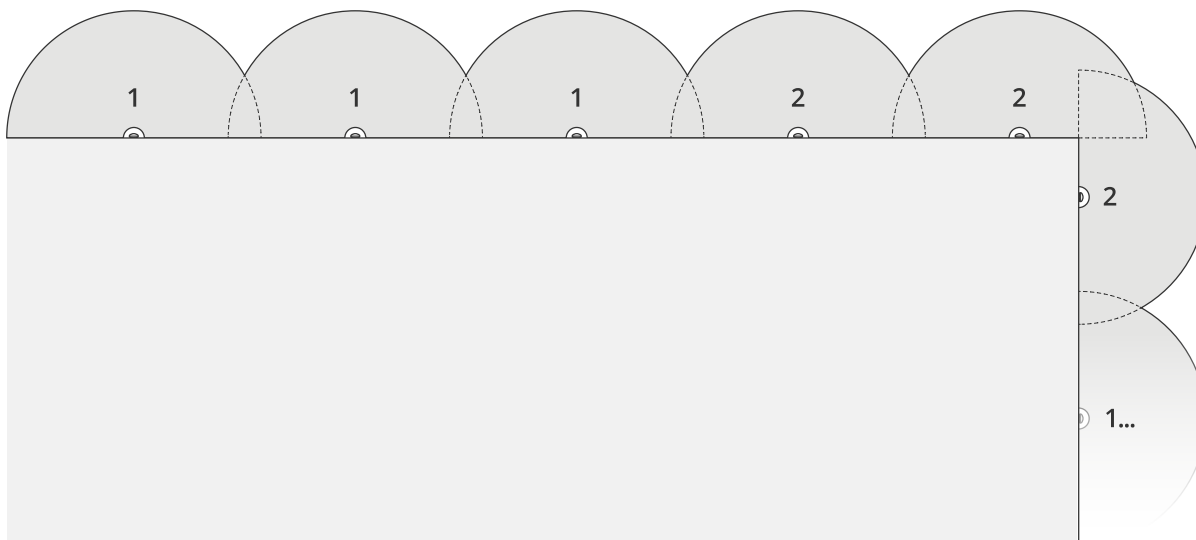
如要建立虛擬圍籬，例如沿著建築物或圍繞建築物，您可以並排放置多個雷達。我們建議以 100 公尺 (330 英尺) 間距放置。



當您在同一共存區安裝兩個以上雷達時，為避免干擾，請在設備介面中設定相鄰雷達的數量。此外，當您安裝三個以上的雷達時，請將每個雷達新增至一個群組中。



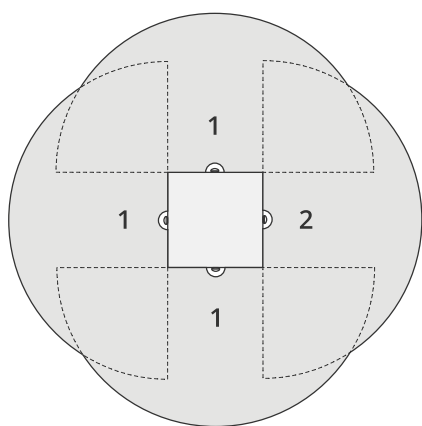
您也可以調整虛擬圍籬以覆蓋角落，如本例所示。



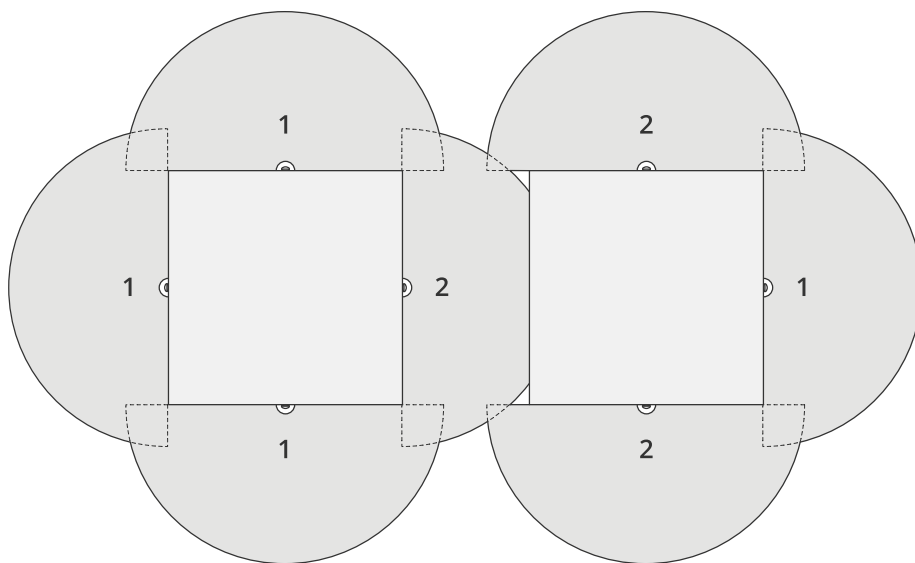
請參閱以了解有關鄰近雷達和群組的更多資訊。

涵蓋建築物周圍區域

若要涵蓋建築物周圍區域，應在建築物牆壁上面朝外放置雷達。如果您在同一個共存區放置三個以上的雷達，請在設備介面中設定相鄰雷達的數量，並將每個雷達新增至一個群組中，如本例所示。



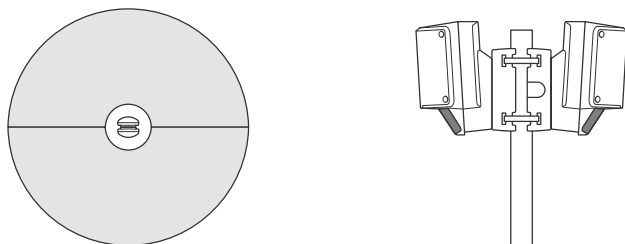
您也可以涵蓋多個建築物的周圍區域。



請參閱以了解有關鄰近雷達和群組的更多資訊。

涵蓋空曠區域

若要涵蓋大型空曠區域，可使用兩個桿架將兩個雷達背靠背放置。

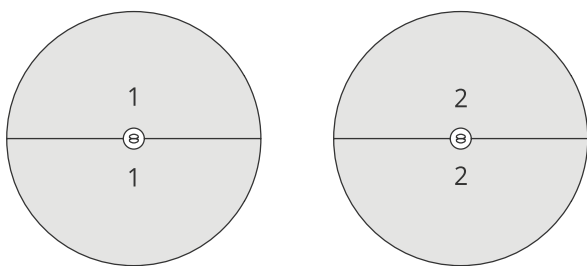


您可以使用一部雷達的 PoE 輸出為第二部雷達供電，但無法以這種方式連接第三部雷達。

附註

當雷達由 60 W 中跨器 (midspan) 供電時，會啟用雷達上的 PoE 輸出。

如果需要在同一個共存區內背對背安裝多台雷達，可在設備介面設定相鄰雷達的數量，將每個雷達新增至一個群組內，避免相互干擾。這是一個範例，說明如何在背靠背安裝中對雷達進行分組。



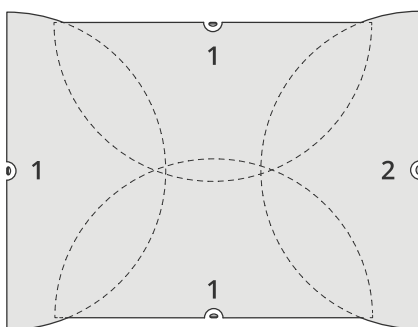
請參閱以了解有關鄰近雷達和群組的更多資訊。

相對安裝多個雷達

一般來說，不建議安裝超過三個雷達，因為這會增加雷達之間相互干擾的風險。但是，在某些特定領域，這可能是必要的。例如，如果你想涵蓋一個足球場，你就不能把雷達放在場地中間。

如果安裝三個以上的雷達並彼此面對，則一個雷達與另一個雷達之間的最小距離需要為 40 公尺 (130 英尺)。在設備介面中設定相鄰雷達的數量，並將每個雷達新增至一個群組也尤為重要。這將有助於提高雷達的性能。

這是一個如何將涵蓋一個區域的四個雷達分組的範例。



請參閱以了解有關鄰近雷達和群組的更多資訊。

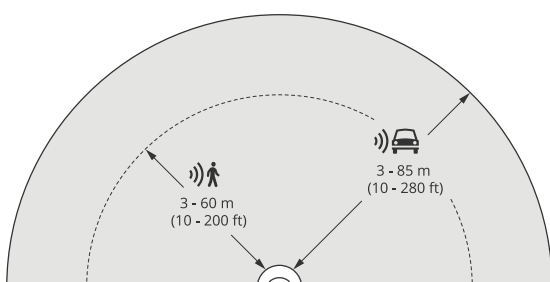
區域偵測範圍

偵測範圍是可追蹤到物體，並觸發警報的距離。它是從近偵測限制 (可以在離裝置多近的位置偵測) 到遠偵測限制 (可以在離裝置多遠的位置偵測)。

區域監控設定檔已針對人員偵測進行最佳化，但具備 +/- 2 公里/小時 (1.24 英里/小時) 的速度準確度，因此仍可讓您追蹤移動時速最高 55 公里 (34 英里) 的車輛和其他物件。

安裝在最佳安裝高度時，偵測範圍為：

- 偵測人體時為 3—60 公尺 (10—200 英尺)
- 偵測車輛時為 3—85 公尺 (10—280 英尺)



附註

- 如果您將雷達安裝在不同的高度，請在校準雷達時，在產品網頁中輸入實際安裝高度。
- 偵測範圍會受到場景的影響。
- 偵測範圍會受到相鄰雷達的影響。
- 偵測範圍會受到物件類型的影響。

在以下條件測量偵測範圍：

- 範圍是沿著接地而測量的。
- 物體是一個身高 170 公分 (5 英尺 7 英吋) 的人。
- 那個人筆直走到雷達前面。
- 當人進入偵測區域時會測量這些值。
- 雷達靈敏度設定為中等。

安裝高度	傾斜 0°	傾斜 10°	傾斜 20°
2.5 公尺 (8.2 英尺)	3.0—60 公尺 (9.8—197 英尺)	不建議	不建議
3.5 公尺 (11 英尺)	3.0—60 公尺 (9.8—197 英尺)	不建議	不建議
4.5 公尺 (15 英尺)	4.0—60 公尺 (13—197 英尺)	不建議	不建議
5.5 公尺 (18 英尺)	7.5—60 公尺 (25—197 英尺)	不建議	不建議
6.5 公尺 (21 英尺)	7.5—60 公尺 (25—197 英尺)	5.5—60 公尺 (18—197 英尺)	不建議
8 公尺 (26 英尺)	不建議	9—60 公尺 (30—197 英尺)	7.5—30 公尺 (25—98 英尺)
10 公尺 (33 英尺)	不建議	15—60 公尺 (49—197 英尺)	9—35 公尺 (30—115 英尺)
12 公尺 (39 英尺)	不建議	23—60 公尺 (75—197 英尺)	13—38 公尺 (43—125 英尺)
14 公尺 (36 英尺)	不建議	27—60 公尺 (89—197 英尺)	17—35 公尺 (56—115 英尺)
16 公尺 (52 英尺)	不建議	不建議	25—50 公尺 (82—164 英尺)

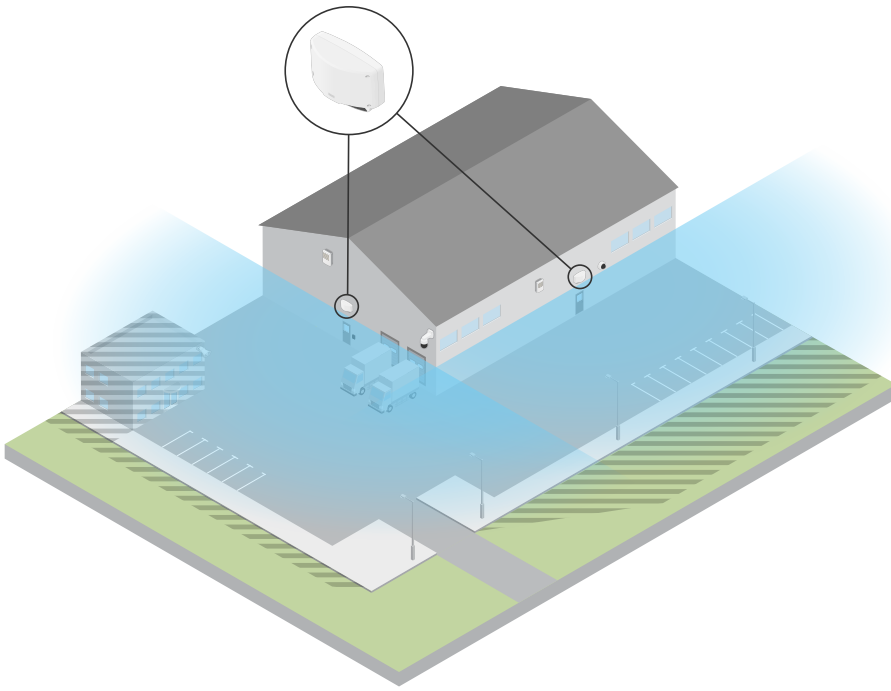
區域監控使用案例

游泳池區域涵蓋範圍

幾個小時之後，公共游泳池發生了一連串入侵事件。由於該交易屬私人性質，業主不得安裝視訊監控系統。他們選擇安裝雷達，並將其設定於區域監控設定檔。雷達安裝在建築物上，涵蓋整個游泳池及其周邊大部分區域。當在 20:00 關門休息，以及在 06:00 開門營業之間偵測到人體時，會觸發喇叭發出警告。

涵蓋建築物周圍場地

一家化工廠透過使用雷達涵蓋敏感建築物周邊的區域，為其系統增加了另一層安全保障。安全系統已經包括攝影機、熱顯像網路攝影機及門控制器。雷達可以觸發事件，促使攝影機追蹤入侵者、放大和記錄活動。與熱顯像攝影機連結的閃光信標會觸發閃光，以便入侵者知道該區域受到保護。門控制器可以限制門禁。雷達可幫助防禦系統在入侵者到達敏感建築物之前，便早已開始行動。



涵蓋大片空曠區域

一家小型購物中心外的停車場發生下班後車輛闖入事件變多了。他們一次只排一名保全值班，但他們認為需要加強夜間安全，又不想增加雇用員工成本。他們決定安裝兩個安全雷達，在區域監控設定檔中背對背安裝，使其能涵蓋整個停車場。雷達設定為向值班保全人員發出可疑行為警報，以方便他們到現場勘查。他們還可以安裝一個由雷達觸發的號角喇叭，以播放可阻止小偷的警報。

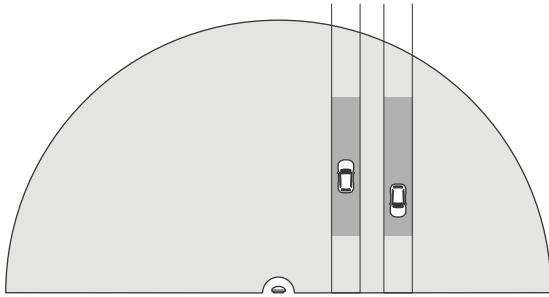
道路監控設定檔

[道路監控設定檔] 最適用於在市區、封閉區域和郊區道路上，追蹤移動速度高達 105 公里/小時 (65 mph) 的車輛。此模式不應用於偵測人體或其他類型的物體。若要追蹤車輛以外的物件，請在中使用雷達。

道路安裝範例

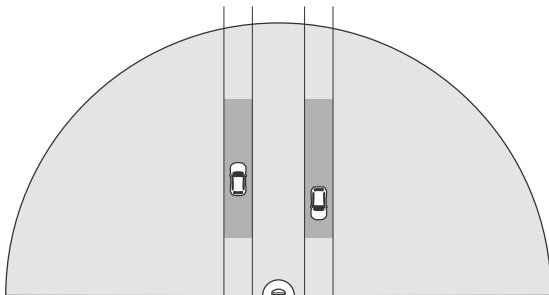
路旁安裝

若要監控沿路行駛的車輛，您可以將雷達安裝在路邊。雷達將提供 10 公尺 (32 英尺) 的橫向覆蓋距離。



道路中心安裝

這種安裝方式需要一個穩定的位置。雷達可以安裝在道路中間的柱子上，也可以安裝在道路上方的橋樑上。雷達將提供兩側 10 公尺 (32 英尺) 的橫向覆蓋距離。進行中心安裝時，雷達會覆蓋更寬的橫向距離。



附註

我們建議將雷達安裝在適合道路監控設定檔的 3 公尺 (10 英尺) 和 8 公尺 (26 英尺) 之間的高度。

道路偵測範圍

偵測範圍是可追蹤到物體，並觸發警報的距離。它是從近偵測限制 (可以在離裝置多近的位置偵測) 到遠偵測限制 (可以在離裝置多遠的位置偵測)。

此設定檔針對車輛偵測進行最佳化，並在監控車輛以 105 公里/小時 (65 mph) 移動時產生 ± 2 公里/小時 (1.24 mph) 的速度準確度。

雷達安裝在最佳安裝高度時的偵測範圍：

- 25—70 公尺 (82—229 英尺) 用於以 60 公里/小時 (37 mph) 行駛的車輛。
- 30—60 公尺 (98—196 英尺) 用於以 105 公里/小時 (65 mph) 行駛的車輛。

道路監控使用案例

管制低速區域車輛

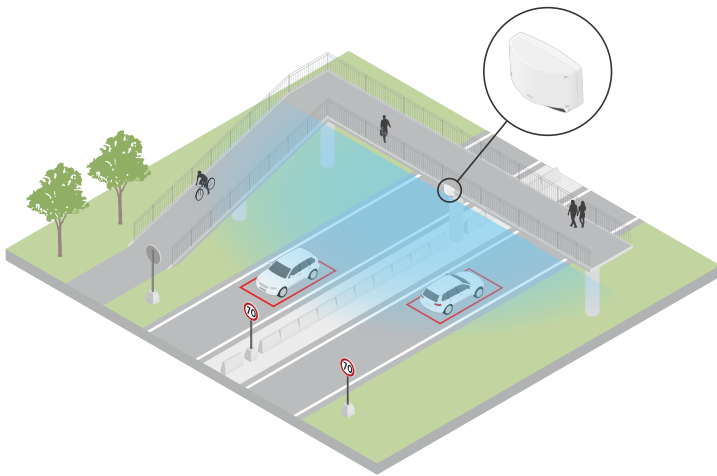
某工業園區中，在兩個倉庫之間的一條冗長道路上安裝雷達，目的是為了實施 60 公里/小時 (37 mph) 的車速限制。在道路監控設定檔中，雷達可以偵測到其偵測區域內超出該速限的車輛。偵測到後，會觸發一個事件，並向駕駛人和管理員傳送電子郵件通知。該提醒有助於提高速限遵守率。

封閉道路上不該出現的車輛

一條通往舊採石場的小路已經封閉，但曾有人舉報有車輛在路上行駛，於是當局便在該採石場安裝安全雷達道路監控設定檔。雷達安裝在路旁，涵蓋了道路的整個寬度。每當有車輛進入情境時，雷達就會觸發一個閃爍的信標，警告駕駛人離開道路。它還會向安全小組傳送訊息，以便在必要時派遣一個單位前來。

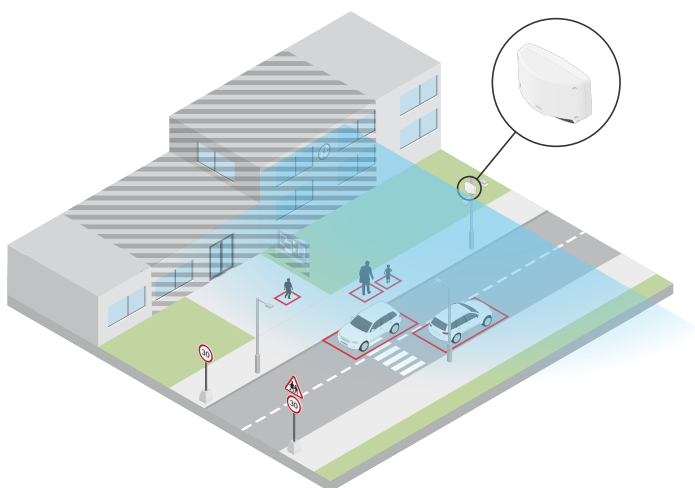
道路上的速度感知

一條穿越小鎮的道路曾發生過一些超速事件。為了強制實施速限 70 公里/小時 (43 mph)，交通管制局已經在橫跨馬路的一座橋上，在道路監控設定檔中安裝了安全雷達。這使他們能夠偵測車輛的行駛速度，並監控何時應該將相關單位駐紮在這條路上以控制交通。



人車安全

某學校的職員已經找出兩個需要解決的安全問題。他們曾在上學期間遇過不速之客闖入校園，以及車輛違規駛入校外 20 公里/小時 (12 mph) 低速區域。雷達安裝在人行道旁邊的一根柱子上，並選擇使用，讓雷達能夠追蹤以低於 55 公里/小時 (34 mph) 以下速度移動的人員和車輛。這有助於學校職員在上課期間追蹤進進出出的人員，同時還能在過往車輛開得太快時觸發喇叭警告行人。



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

*不完全支援。如果您遇到影像串流問題，請使用其他瀏覽器。

開啟設備的網頁介面

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

有關設備網頁介面中的所有控制項和選項的說明，請參閱。

建立管理員帳戶

首次登入設備必須建立管理員帳戶。

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

重要

設備沒有預設帳戶。如果您遺失了管理員帳戶的密碼，則必須重設設備。請參考。

安全密碼

重要

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

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

為了保護您的資料，我們強烈建議您採取以下措施：

- 使用至少包含 8 個字元的密碼，最好是由密碼產生器所建立。

- 不要洩露密碼。
- 定期變更密碼，至少一年變更一次。

網頁介面概觀

這段影片為您提供設備網頁介面的概觀。



若要觀賞此影片，請前往本文件的網頁版本。

Axis 裝置網頁介面

設定您的設備

設定安裝高度

在網頁介面中設定雷達的安裝高度。這樣能協助雷達正確偵測和測量經過的物件速度。

使地面到雷達的高度測量結果盡可能準確。對於表面不平坦的場景，設定代表場景中平均高度的值。

1. 前往 [雷達 > 設定 > 一般]。
2. 在 [安裝高度] 下設定高度。

校準參考地圖

上傳參考地圖將使您更容易看到偵測到的物件移動。您可以使用顯示雷達涵蓋範圍的平面圖或航拍照片。校準地圖，使雷達涵蓋範圍符合地圖的位置、方向和比例，您也可以放大地圖，以便檢視雷達涵蓋範圍的特定區域。

您可以使用設定輔助逐步，引導您逐步完成地圖校準，也可以個別編輯每個設定。

Use the setup assistant (使用設定輔助)：

1. 前往 [雷達 > 地圖校準]。
2. 按一下 [Setup assistant (設定輔助)]，然後依照指示進行。

若要移除已上傳的地圖及您已新增的設定，請按一下 [Reset calibration (重設校準)]。

Edit each setting individually (個別編輯每個設定)：

調整每個設定後，地圖將逐漸校準。

1. 前往 [Radar (雷達) > Map calibration (地圖校準) > Map (地圖)]。
2. 選取您要上傳的影像，或將其拖放到指定區域。
若要重複使用包含目前水平移動及縮放設定的地圖影像，請按一下 [Download map (下載地圖)]。
3. 在 [旋轉地圖] 下，使用滑動調整桿將地圖旋轉到定點。
4. 前往 [Scale and distance on a map (地圖上的比例尺和距離)]，然後按一下地圖上的兩個預定點。
5. 從 [Distance (距離)] 下，在您已新增到地圖中的兩點之間新增實際距離。
6. 前往 [Pan and zoom map (水平移動和縮放地圖)]，您可以用按鈕水平移動地圖影像，也可以放大和縮小地圖影像。

附註

縮放功能不會改變雷達的涵蓋範圍。縮放後，即使部分涵蓋範圍超出顯示畫面，雷達仍會偵測整個涵蓋範圍內的移動物件。若要排除偵測到的移動，唯一的方法是新增不包含區域。如需詳細資訊，請參閱。

7. 前往 [Radar position (雷達位置)]，您可以用按鈕在地圖上移動或旋轉雷達位置。

若要移除已上傳的地圖及您已新增的設定，請按一下 [Reset calibration (重設校準)]。



若要觀賞此影片，請前往本文件的網頁版本。

影片展示如何校正 Axis 雷達或雷達影像融合攝影機中的參考地圖範例。

設定偵測區域

若要決定偵測位移的位置，您可以新增一個或多個偵測區域。以不同區域觸發不同動作。

區域分兩種類型：

- [情境] (前稱為包含區域) 是移動物件觸發規則的區域。預設的情境域符合雷達涵蓋的整個區域。
- [不包含區域] 是忽略移動物件的區域。如果情境內的某些區域會觸發大量不需要的警報，請使用不包含區域。

新增情境

情境是觸發條件以及場景和偵測設定的組合，您可以藉此在事件系統中建立規則。如果您想為場景的不同部分建立不同的規則，請新增情境。

新增情境：

1. 前往 [雷達 > 情境]。
2. 按一下 [新增情境]。
3. 輸入情境的名稱。
4. 選取是否要觸發在區域中移動或跨越過一或兩條線的物件。

觸發在一個區域中移動的物件：

1. 選取 [區域內移動]。
2. 按 [Next (下一步)]。
3. 選取應包含在情境中的類型。
使用滑鼠移動和塑造區域，使其涵蓋雷達影像或參考地圖所需的部分。
4. 按 [Next (下一步)]。
5. 新增偵測設定。
1. 在 [忽略瞬間消失物件] 下方新增秒數，直到觸發。
2. 在 [觸發物件類型] 下方選取要觸發的物件類型。
3. 在 [限速] 下方新增速度限制範圍。
6. 按 [Next (下一步)]。
7. 在 [最短觸發持續時間] 下方設定警報的最短持續時間。
8. 按一下 Save (儲存)。

物件越線時觸發：

1. 選取 [跨越線]。
2. 按 [Next (下一步)]。
3. 在場景中定位線。
請使用滑鼠移動和塑造線條。
4. 如果要變更偵測方向，請開啟 [變更方向]。
5. 按 [Next (下一步)]。
6. 新增偵測設定。
 - 6.1. 在 [忽略瞬間消失物件] 下方新增秒數，直到觸發。
 - 6.2. 在 [觸發物件類型] 下方選取要觸發的物件類型。
 - 6.3. 在 [限速] 下方新增速度限制範圍。
7. 按 [Next (下一步)]。
8. 在 [最短觸發持續時間] 下方設定警報的最短持續時間。
預設值設定為 2 秒。如果您希望情境在每次物件越過線時觸發，請將持續時間降低至 0 秒。
9. 按一下 Save (儲存)。

物件跨越兩條線時觸發：

1. 選取 [跨越線]。
2. 按 [Next (下一步)]。
3. 若要使物件跨越兩條線以觸發警報，請開啟 [需要跨越兩條線]。
4. 在場景中定位線。
請使用滑鼠移動和塑造線條。
5. 如果要變更偵測方向，請開啟 [變更方向]。
6. 按 [Next (下一步)]。
7. 新增偵測設定。
 - 7.1. 在 [越過之間的最大時間] 下方設定跨越第一條線和第二條線之間的時間限制。
 - 7.2. 在 [觸發物件類型] 下方選取要觸發的物件類型。
 - 7.3. 在 [限速] 下方新增速度限制範圍。
8. 按 [Next (下一步)]。
9. 在 [最短觸發持續時間] 下方設定警報的最短持續時間。
預設值設定為 2 秒。如果您希望情境在每次物件跨越過兩條線時觸發，請將持續時間降低至 0 秒。
10. 按一下 Save (儲存)。

新增不包含區域

不包含區域是忽略移動物件的區域。新增要忽略的不包含區域，例如路邊搖曳的樹葉。您也可以新增不包含區域，以忽略雷達反射材質 (例如金屬柵欄) 導致的鬼影軌跡。

新增一個不包含區域：

1. 前往 [雷達 > 不包含區域]。
2. 按一下 [新增不包含區域]。
使用滑鼠移動和塑造區域，使其涵蓋雷達畫面或參考地圖所需的部分。

將誤報減至最少

如果您發現誤報過多，您可以篩選出某些類型的移動或物體、變更涵蓋範圍，或調整偵測靈敏度。查看那些設定最適合您的環境。

- 調整雷達的偵測靈敏度：
前往 [雷達 > 設定 > 偵測]，並選取較低的 [偵測靈敏度]。這會降低誤報的風險，但也可能導致雷達錯過一些移動。
靈敏度設定會影響所有區域。
 - [Low (低)]：當區域內有大量金屬物件或大型車輛時，請採用此靈敏度。雷達需要更長的時間來追蹤物體，並進行分類。這會縮減偵測範圍，尤其是對於快速移動的物體更是如此。
 - [Medium (中)]：此為預設設定。
 - [High (高)]：在開闊的區域中且雷達前方沒有金屬物件時，使用此靈敏度。這將會增加人體的偵測範圍。
- 修改情境並排除區域：
如果情境中包含金屬牆等堅硬表面，則可能會產生反射，導致對單一實體物件進行多次偵測。您可以修改情境的形狀，或新增忽略情境某些部分的排除區域。如需詳細資訊，請參閱和。
- 觸發跨越兩條線而不是一條線的物件：
如果跨越線的情境包括擺動物件或四處走動的動物，則存在物件碰巧跨越線並觸發誤報的風險。在這種情況下，您可以將情境設定為僅在物件跨越兩條線時觸發。如需詳細資訊，請參閱。
- 過濾移動：

- 前往 [雷達 > 設定 > 偵測]，並選取 [忽略擺動物件]。此項設定會盡量減少涵蓋區域內因樹木、灌木叢及旗桿而產生的誤報。
- 前往 [雷達 > 設定 > 偵測]，並選取 [忽略小型物件]。此項設定可在區域監控設定檔中使用，並盡量減少涵蓋區域內小型物件 (例如貓和兔子) 的誤報。
- 過濾時間：
 - 前往 [雷達 > 情境]。
 - 選取情境，然後按一下  以修改其設定。
 - 在 [觸發前的秒數] 下選取較高的值。這是從雷達開始追蹤物件到可以觸發警報的延遲時間。計時器在雷達首次偵測到物件時開始計時，而非在物件進入場景中的指定區域時開始計時。
- 過濾物體類型：
 - 前往 [雷達 > 情境]。
 - 選取情境，然後按一下  以修改其設定。
 - 若要避免觸發特定物件類型，請取消選取不應在此情境中觸發事件的物件類型。

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

減少頻寬會導致影像中的細節遺失。

1. 前往 [雷達 > 串流]。
2. 按一下即時影像中的 。
3. 選取 [Video format (影像格式) H.264]。
4. 前往 [雷達 > 串流 > 一般]，並增加 [壓縮] 值。

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

直接從雷達錄製影像

1. 前往 [雷達 > 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 。

使用雷達控制 PTZ 攝影機

可以使用來自雷達的物件相關位置資訊，讓 PTZ 攝影機追蹤物件。有兩種方法可以這麼做：

- 將 PTZ 攝影機和雷達安裝得過於靠近時，即適合使用此內建選項。
- 想要使用多部 PTZ 攝影機和雷達追蹤物件時，即適合使用 Windows 應用程式。

附註

使用 NTP 伺服器可同步攝影機、雷達和 Windows 電腦上的時間。如果時鐘不同步，您可能會遇到追蹤延遲或鬼影軌跡的情況。

使用內建雷達自動追蹤服務控制 PTZ 攝影機

內建雷達自動追蹤服務會建立邊際對邊際的解決方案，其中雷達直接控制 PTZ 攝影機。它支援所有 Axis PTZ 攝影機。

附註

您可以使用內建雷達自動追蹤服務，將一台雷達與一台 PTZ 攝影機連線。如需使用一台以上的雷達或 PTZ 攝影機的設定，請使用 AXIS Radar Autotracking for PTZ。更多資料請參閱。

本說明解說如何將雷達與 PTZ 攝影機配對、如何校準設備，以及如何設定物件追蹤。

開始之前：

- 透過在雷達中設置不包含區域來定義關注區域並避免不必要的警報。確保排除具有雷達反射材料或擺動物件 (如樹葉) 的區域，以防止 PTZ 攝影機追蹤不相關的物件。如需說明，請參閱。

將雷達與 PTZ 攝影機配對：

1. 前往 [系統 > 邊際對邊際 > PTZ 配對]。
2. 輸入該 PTZ 攝影機的 IP 位址、使用者名稱和密碼。
3. 按一下 [Connect (連線)]。
4. 按一下 [設定雷達自動追蹤]，或前往 [雷達 > 雷達 PTZ 自動追蹤]，以設定雷達自動追蹤。

校準雷達和 PTZ 攝影機：

5. 前往 [雷達 > 雷達 PTZ 自動追蹤]。
6. 若要設定攝影機的安裝高度，請前往 [攝影機安裝高度]。
7. 若要水平移動 PTZ 攝影機，使攝影機與雷達指向相同方向，請前往 [水平移動對齊]。
8. 如果您需要調整傾斜，以補償傾斜的地面，請前往 [地面傾斜偏移量] 並新增偏移量 (度)。

設定 PTZ 追蹤：

9. 前往 [追蹤]，選取是否要追蹤人員、車輛和/或未知物件。

10. 若要使用 PTZ 攝影機開始追蹤物體，請開啟 [追蹤]。
追蹤功能會自動放大一個物體或一群物體，使這些物體仍在攝影機的畫面中。
11. 如果您預期會有多個無法容納在攝影機畫面中的物件，請開啟 [物件切換]。
有了此設定，雷達會優先處理要追蹤的物件。
12. 若要決定每個物件的追蹤秒數，請設定 [物件停留時間]。
13. 若要讓 PTZ 攝影機在雷達不再追蹤任何物體時返回原點位置，請開啟 [返回原點]。
14. 若要決定 PTZ 攝影機從追蹤物件最後已知位置返回原點前的時間，請設定 [返回原點逾時]。
15. 若要微調 PTZ 攝影機的變焦，請調整滑桿上的變焦。

使用 AXIS Radar Autotracking for PTZ 控制 PTZ 攝影機

AXIS Radar Autotracking for PTZ 是可以在追蹤物件時處理不同設定的伺服器解決方案：

- 使用一個雷達控制若干部 PTZ 攝影機。
- 使用若干部雷達控制一部 PTZ 攝影機。
- 使用若干部雷達控制若干部 PTZ 攝影機。
- 當安裝在同一區域的不同位置時，可使用一部雷達控制一部 PTZ 攝影機。

應用程式相容於一組特定的 PTZ 攝影機。如需詳細資訊，請參閱 axis.com/products/axis-radar-autotracking-for-ptz#compatible-products。

如需如何設定應用程式的資訊，請下載應用程式並查看使用手冊。如需詳細資訊，請參閱 axis.com/products/axis-radar-autotracking-for-ptz/support。

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。

當機殼打開時觸發通知

此範例說明如何設定在設備外罩或外殼打開時發出的電子郵件通知。

新增電子郵件接收者：

1. 前往 [系統 > 事件 > 接收者]，並按一下 [新增接收者]。
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：

9. 移至 [系統 > 事件 > 規則]，並按一下 [新增規則]。
10. 輸入規則名稱。
11. 在條件清單中，選取 [外殼開啟]。
12. 在動作清單中，選取 [傳送通知至電子郵件]。
13. 從清單中選取接收者。
14. 輸入電子郵件的主旨和訊息。
15. 按一下 Save (儲存)。

在偵測到位移時用攝影機錄影

本範例說明如何設定雷達和攝影機，以便在雷達偵測到位移前五秒鐘開始錄製到 SD 卡，並在一分鐘後停止。

連接裝置：

1. 將纜線從雷達上的 I/O 輸出，連接攝影機上的 I/O 輸入。

設定雷達的 I/O 連接埠：

2. 前往 [系統 > 配件 > I/O 埠]，將 I/O 埠設定為輸出，並選取正常狀態。

在雷達中建立規則：

3. 前往 [System (系統) > Events (事件)]，並新增規則。
4. 輸入規則名稱。
5. 從條件清單中的 [雷達位移] 下，選取情境。
如要設定場景，請參閱。
6. 從動作清單中選取 [當規則作用時切換 I/O]，然後選取連接到攝影機的連接埠。
7. 按一下 Save (儲存)。

設定攝影機的 I/O 連接埠：

8. 前往 [系統 > 配件 > I/O 埠]，將 I/O 埠設定為輸入，並選取正常狀態。

在攝影機中建立規則：

9. 前往 [System (系統) > Events (事件)]，並新增規則。
10. 輸入規則名稱。
11. 從條件清單中選取 [數位輸入使用中]，然後選取應該觸發規則的連接埠。
12. 從動作清單中選取 [錄影]。
13. 從儲存選項清單中選取 [SD 卡]。
14. 選取現有的串流格式，或建立新的串流格式。
15. 將警報前暫存設定為 5 秒。
16. 將警報後暫存設定為 1 分鐘。
17. 按一下 Save (儲存)。

偵測到位移時開燈

當入侵者進入偵測區域時，開燈會有嚇阻效果，也能改善視覺攝影機錄製的影像畫質。

本範例說明如何設定雷達和照明燈，以便雷達偵測到位移時開啟照明燈，並在一分鐘後關閉。

連接裝置：

1. 透過雷達上的中繼埠，將其中一個照明燈纜線連接到電源插座。在電源供應器和照明燈之間，直接連接另一條纜線。

設定雷達的中繼埠：

2. 前往 [系統 > 配件 > I/O 埠] 並選取 [開路] 作為中繼埠的正常狀態。

在雷達中建立規則：

3. 前往 [System (系統) > Events (事件)]，並新增規則。
4. 輸入規則名稱。
5. 從條件清單中的 [雷達位移] 下，選取情境。
如要設定場景，請參閱。
6. 從動作清單中選取 [切換 I/O 一次]，並選取中繼埠。
7. 選取 [作用中]。
8. 設定 [持續期間]。
9. 按一下 Save (儲存)。

如果有人使用金屬物體遮住雷達，請傳送電子郵件

此範例說明在有人使用如金屬鋁箔或金屬板等金屬物體遮住雷達，以干擾雷達運作時，如何建立傳送電子郵件通知的規則。

附註

自 AXIS OS 11.11 起，已提供建立雷達防竄改事件規則的選項。

新增電子郵件接收者：

1. 前往 [系統 > 事件 > 接收者]，並按一下 [新增接收者]。
2. 輸入接收者的名稱。
3. 選取 [Email (電子郵件)]。
4. 輸入電子郵件要傳送到的電子郵件地址。
5. 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。
6. 若要傳送測試電子郵件，請按一下 [Test (測試)]。
7. 按一下 Save (儲存)。

建立規則：

8. 前往 [System (系統) > Events (事件)]，並新增規則。
9. 輸入規則名稱。
10. 從狀況清單中，在 [設備狀態] 下，選取 [雷達資料失敗]。
11. 在 [原因] 下，選取 [防竄改]。
12. 從動作清單，在 [通知] 下，選取 [向電子郵件傳送通知]。
13. 選取您建立的接收者。
14. 輸入電子郵件的主旨和訊息。
15. 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

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。

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。

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。

雷達

設定

一般

雷達傳輸：使用此選項可完全關閉雷達模組。

Channel (頻道) ⓘ：如果您遇到多台設備相互干擾的問題，最多可為相互靠近的四台設備選取相同的頻道。對於大多數設備而言，選取 [自動] 可讓設備自動交涉要使用哪個頻道。

[安裝高度]：輸入產品的安裝高度。

附註

在輸入安裝高度時，請盡可能精確。這有助於設備在影像的正確位置上將雷達偵測視覺化。

並存

[相鄰雷達數量]：選取安裝在同一共存區內的相鄰雷達的數量。這將有助於避免干擾。共存半徑為 350 公尺 (1148 英尺)。

- 0—1: 如果您在同一共存區安裝一到兩個雷達，請選取此選項。
- 2: 如果您在同一共存區安裝三個雷達，請選取此選項。
- 3—5: 如果您在同一共存區安裝四到六個雷達，請選取此選項。
 - [群組]：選取一個群組 ([群組 1] 或者 [群組 2]) 為你的雷達。這也有助於避免干擾。我們建議您在每個群組中新增三個雷達，並將距離最近的雷達新增至同一群組中。



如需詳細資訊，請參閱。

偵測

[偵測靈敏度]：選取雷達應有的靈敏度。數值越高，偵測範圍越大，但誤報風險也越高。靈敏度越低會減少誤報的次數，但可能會縮短偵測範圍。

[雷達設定檔]：選取適合您關注區域的設定檔。

- [區域監控]：追蹤在開放區域中以較低速度移動的大型和小型物件。
 - Ignore stationary rotating objects (忽略靜止旋轉物件) ：開啟可最大程度地減少由旋轉移動的靜止物件 (例如：風扇或渦輪機) 引起的誤報。
 - [忽略小型物件]：開啟以盡量減少小型物件 (例如：貓或兔子) 的誤報。
 - [忽略擺動物件]：開啟以將來自擺動物件 (例如：樹木、灌木叢或旗桿) 的誤報減至最低。
- [道路監控]：追蹤在市區和郊區道路上高速行駛的車輛
 - Ignore stationary rotating objects (忽略靜止旋轉物件) ：開啟可最大程度地減少由旋轉移動的靜止物件 (例如：風扇或渦輪機) 引起的誤報。
 - [忽略擺動物件]：開啟以將來自擺動物件 (例如：樹木、灌木叢或旗桿) 的誤報減至最低。

檢視

[Information legend] (資訊圖例)：開啟以顯示包含雷達可以偵測和追蹤的物件類型的圖例。拖放以移動資訊圖例。

[區域不透明度]：選取涵蓋區域的不透明或透明程度。

[網格不透明度]：選取網格的不透明或透明程度。

[色彩配置]：選取用於雷達視覺化的主題。

Rotation (旋轉) ：選取雷達影像的偏好方向。

物件視覺化

[軌跡存留期]：選取被追蹤物件的軌跡可以在雷達畫面中顯示多久。

[Icon style] (圖示樣式)：選取雷達畫面中被追蹤物件的圖示樣式。對於普通三角形，選取 [三角形]。對於代表性符號，選取 [符號]。無論樣式如何，圖示都將指向被追蹤物件的移動方向。

[顯示資訊和圖示]：選取被追蹤物件的圖示旁邊要顯示哪些資訊：

- [物件類型]：顯示雷達偵測到的物件類型。
- [分類機率]：顯示雷達對物件分類之正確性的確定程度。
- [速度]：顯示物件移動的速度。

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。

[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。

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。

地圖校準

使用地圖校準上傳和校準參考地圖。校準後會產生以適當比例顯示雷達涵蓋範圍的參考地圖，這將使您更容易看到物件的移動。

設定輔助：按一下可開啟設定輔助，引導您逐步完成校準。

Reset calibration (重設校準)：按一下即可移除目前地圖影像及地圖上的雷達位置。

地圖

[上傳地圖]：選取或拖放您要上傳的地圖影像。

Download map (下載地圖)：按一下可下載地圖。

旋轉地圖：使用滑動調整桿旋轉地圖影像。

地圖上的比例尺和距離

照射距離：在您已新增到地圖中的兩點之間新增距離。

水平移動和縮放地圖

[Pan (水平移動)]：按一下按鈕，即可水平移動地圖影像。

變焦：按一下按鈕，即可放大或縮小地圖影像。

Reset pan and zoom (重設水平移動和縮放)：按一下即可移除水平移動及縮放設定。

雷達位置

位置：在地圖上按一下按鈕，即可移動雷達。

[旋轉]：在地圖上按一下按鈕，即可旋轉雷達。

不包含區域

不包含區域是忽略移動中物件的區域。如果情境內的某些區域會觸發大量不需要的警報，請使用不包含區域。



：按一下此選項可建立新的不包含區域。

若要修改不包含區域，請在清單中選取它。

[追蹤經過的物件]：開啟以追蹤穿過不包含區域的物件。經過的物件保留其軌跡 ID，並且在整個區域中都是可見的。不會追蹤出現在不包含區域內的物件。

[區域形狀預設]：選取不包含區域的初始形狀。

- [覆蓋一切]：選取設定覆蓋整個雷達覆蓋區域的不包含區域。
- [重設為方塊]：選取在覆蓋區域的中間放置一個矩形不包含區域。

若要修改區域形狀，請拖放線上的任意點。若要移除某個點，請以滑鼠右鍵按一下該點。

情境

情境是觸發條件以及場景和偵測設定的組合。



：按一下此選項可建立新的情境。您最多可以建立 20 個情境。

[觸發條件]：選取觸發警報的條件。

- [區域內移動]：選取是否希望情境在某個區域中移動物件時觸發。
- 跨越線：選取是否希望場景在物件跨越一條線或兩條線時觸發。

[場景]：定義場景中移動物件會觸發警報的區域或線路。

- 對於 [區域內移動]，選取形狀預設之一來修改區域。
- 對於 [跨越線]，將線拖放到場景中。若要在該線上建立更多點，請按一下並拖曳該線上的任何位置。若要移除某個點，請以滑鼠右鍵按一下該點。
 - [需要跨越兩條線]：如果情境觸發警報之前物件必須跨過兩條線，則開啟。
 - [變更方向：] 如果您希望情境在物件從另一個方向跨過線時觸發警報，則開啟。

[偵測設定]：為情境定義觸發條件。

- 對於 [區域內移動]：
 - [忽略瞬間消失物件]：設定從雷達偵測到物件到情境觸發警報的延遲 (以秒為單位)。這有助於減少誤報。
 - [觸發物件類型]：選取您希望情境觸發的物件類型 (人、車輛、未知)。
 - [限速]：觸發以特定範圍內的速度移動的物件。
 - [轉換]：選取是否要在高於或低於設定速度限制的速度時觸發。
- 對於 [跨越線]：
 - [忽略瞬間消失物件]：設定從雷達偵測到物件到情境觸發動作的延遲 (以秒為單位)。這有助於減少誤報。此選項不適用於跨越兩條線的物件。
 - [越過之間的最大時間]：設定跨越第一條線和第二條線之間的最長時間。此選項僅適用於跨越兩條線的物件。
 - [觸發物件類型]：選取您希望情境觸發的物件類型 (人、車輛、未知)。
 - [限速]：觸發以特定範圍內的速度移動的物件。
 - [轉換]：選取是否要在高於或低於設定速度限制的速度時觸發。

[警報設定]：定義警報的標準。

- [最短觸發持續時間]：設定觸發警報的最短持續時間。

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)  - ：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) 

- [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。

雷達 PTZ 自動追蹤

將雷達與 PTZ 攝影機配對以使用雷達自動追蹤。若要建立連接，請前往 [系統 > 邊際對邊際]。

設定初始設定：

[攝影機安裝高度]：從地面到安裝 PTZ 攝影機高度的距離。

水平移動對齊：水平移動 PTZ 攝影機，使其與雷達指向相同的方向。按一下 PTZ 攝影機的 IP 位址以進行存取。

儲存水平移動偏移量：按一下以儲存水平移動對齊。

地面傾斜偏移量：使用地面傾斜偏移來微調攝影機的傾斜。如果地面傾斜或未水平架設攝影機，攝影機可能會在追蹤物體時瞄準過高或過低。

[完成]：按一下以儲存設定並繼續設定。

設定 PTZ 自動追蹤：

追蹤：選取是否要追蹤人員、車輛和/或未知物件。

追蹤：開啟此選項以使用 PTZ 攝影機開始追蹤物件。追蹤功能會自動放大一個物體或一群物體，使這些物體仍在攝影機的畫面中。

物件切換：如果雷達偵測到多個物件無法容納在 PTZ 攝影機的畫面，PTZ 攝影機會追蹤雷達排定優先順序最高的物件，並忽略其他物件。

物件停留時間：決定 PTZ 攝影機應追蹤每個物件多少秒數。

[返回原點]：開啟此選項使 PTZ 攝影機在雷達不再追蹤任何物件時返回原點位置。

[返回原點逾時]：決定 PTZ 攝影機從追蹤物件最後已知位置返回原點前的時間。

變焦：使用滑桿微調 PTZ 攝影機的變焦。

[重新設定安裝]：按一下可清除所有設定並返回初始設定。

錄影檔案

[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。



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。

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 NTP KE servers) (自動日期和時間 (手動 NTP 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 NTP KE servers (手動 NTP 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。

區域設定

設定要用於所有系統設定的測量制度。

[Metric (m, km/h) (公制 (公尺、公里/小時))]：選取以公尺測量距離，並且以每小時公里測量速度。

[U.S. customary (ft, mph) (慣用美制 (英尺、英里/小時))]：選取以英尺測量距離，並且以每小時英里測量速度。

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實性的 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) - [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

Firewall (防火牆)：打開啟動防火牆。

[Default Policy (預設政策)]：請選擇防火牆對於規則外連線請求的處理方式。

- ACCEPT (允許)：允許所有與設備的連接。該選項是預設的。
- DROP (置放)：封鎖裝置的所有連線。

若要對預設原則設定例外，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。

+ New rule (新增規則)：按一下可建立規則。

規則類型：

- FILTER (過濾)：選擇允許或封鎖定義中匹配條件的裝置連線。
 - [Policy (政策)]：選擇防火牆Accept (接受) 或Drop (置放) 規則。
 - IP範圍：選擇指定允許或封鎖的位址範圍。在Start和End 中使用 IPv4/IPv6 。
 - [IP address (IP 位址)]：輸入要允許或封鎖的位址。使用 IPv4/IPv6 或 CIDR 格式。
 - [Protocol (協定)]：選擇要允許或傳輸的網路協定 (TCP、UDP 或兩者)。若選擇傳輸協定，還須指定連接埠。
 - MAC：輸入要允許或封鎖的設備網卡號碼。
 - 連接埠範圍：選擇指定允許或封鎖的連接埠範圍。將它們加入Start 和End 中。
 - [Port (連接埠)]：輸入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：選擇要允許或封鎖的流量類型。
 - UNICAST：從單一發送者傳送至單一接收者的流量。
 - BROADCAST：從單一發送者傳送至網路上所有設備的流量。
 - MULTICAST：從一個以上傳送者傳送至一個以上接收者的流量。
- LIMIT：選擇接受符合規則中定義標準的裝置連線，但套用限制，減少過量流量。
 - IP範圍：選擇指定允許或封鎖的位址範圍。在Start和End 中使用 IPv4/IPv6 。
 - [IP address (IP 位址)]：輸入要允許或封鎖的位址。使用 IPv4/IPv6 或 CIDR 格式。
 - [Protocol (協定)]：選擇要允許或傳輸的網路協定 (TCP、UDP 或兩者)。若選擇傳輸協定，還須指定連接埠。
 - MAC：輸入要允許或封鎖的設備網卡號碼。
 - 連接埠範圍：選擇指定允許或封鎖的連接埠範圍。將它們加入Start 和End 中。
 - [Port (連接埠)]：輸入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：選擇要允許或封鎖的連線類型。
 - 期間：選擇Amount相關時段。
 - 數量：設定裝置在所設Period內允許的最大連線次數。上限為 65535 。
 - Burst：在所設Period (期間) 內，輸入允許超過設定Amount (數量) 一次的連線數量。一旦達到這個數量，就只允許在設定期間內受所設額度限制。
 - 流量類型：選擇要允許或封鎖的流量類型。
 - UNICAST：從單一發送者傳送至單一接收者的流量。
 - BROADCAST：從單一發送者傳送至網路上所有設備的流量。
 - MULTICAST：從一個以上傳送者傳送至一個以上接收者的流量。

測試規則：按一下以測試所設規則。

- 測試時間 (秒)：設定測試規則的時間限制。
- 回復：在測試規則前，按一下，將防火牆還原到之前的狀態。

- 套用規則：按一下啟動規則而不測試。不建議這樣做。

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)]：無法存取變更任何設定。

⋮

內容功能表包含：

[Update account (更新帳戶)]：編輯帳戶特性。

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

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) 

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。

用戶端憑據授予設定

[Admin claim (管理者申請)]：輸入管理者角色的值。

Verification URI (驗證URI)：輸入 API 端點驗證的網頁連結。

[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。

[Save (儲存)]：按一下儲存值。

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。

偵測器

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) 

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。

[Audio pairing (音訊配對)] 允許您與網路喇叭或麥克風配對。配對後，網路喇叭會作為音訊輸出設備運作，您可以播放音訊檔案並透過攝影機傳輸聲音。網路麥克風會接收周圍區域的聲音，並將其用作音訊輸入設備，可用於媒體串流和錄音。

重要

若要與影像管理軟體 (VMS) 搭配使用，必須先將攝影機與喇叭或麥克風配對，然後再將攝影機新增至 VMS。

當您在事件規則中使用網路配對的音訊設備，並將「聲音偵測」作為條件和「播放聲音檔」作為操作時，請在事件規則中設定「在動作之間等待 (hh:mm:ss)」限制。這將幫助您避免在捕捉麥克風從揚聲器拾取音訊時進行循環偵測。

[ Add (新增)]：新增要配對的設備。

發現裝置：按一下尋找網路上的設備。網路掃描完成後，會列出可用設備。

附註

清單會顯示所有找到的 AXIS 裝置，而非只有可配對裝置。

只有啟用Bonjour的設備才能找到。若要啟用設備的Bonjour，請開啟設備的網頁介面，並前往 System (系統) > Network (網路) > Network discovery protocols (網路發現協定)。

附註

已配對的設備會顯示資訊圖示。將滑鼠懸停在圖示上會顯示已啟動的配對資訊。

若要從清單中配對裝置，請按一下 。

[Select pairing type (選擇配對類型)]：從下拉式清單中選取。

[Speaker pairing (揚聲器配對)]：選取要配對的網路喇叭。

[Microphone pairing (麥克風配對) ]：選取要配對的麥克風。

[Address (位址)]：輸入網路喇叭的主機名稱或 IP 位址。

[Username (使用者名稱)]：輸入使用者名稱。

[Password (密碼)]：輸入使用者的密碼。

[Close (關閉)]：按一下清除所有欄位。

[Connect (連線)]：按一下以建立與要配對的設備的連接。

[PTZ 配對] 允許您將雷達與 PTZ 攝影機配對以使用自動追蹤。雷達 PTZ 自動追蹤使 PTZ 攝影機根據雷達提供的有關物件位置的資訊來追蹤物件。

[ Add (新增)]：新增要配對的設備。

發現裝置：按一下尋找網路上的設備。網路掃描完成後，會列出可用設備。

附註

清單會顯示所有找到的 AXIS 裝置，而非只有可配對裝置。

只有啟用Bonjour的設備才能找到。若要啟用設備的Bonjour，請開啟設備的網頁介面，並前往 System (系統) > Network (網路) > Network discovery protocols (網路發現協定)。

附註

已配對的設備會顯示資訊圖示。將滑鼠懸停在圖示上會顯示已啟動的配對資訊。

若要從清單中配對裝置，請按一下 。

[Select pairing type (選擇配對類型)]：從下拉式清單中選取。

[Address (位址)]：輸入 PTZ 攝影機的主機名稱或 IP 位址。

[Username (使用者名稱)]：輸入 PTZ 攝影機的使用者名稱。

[Password (密碼)]：輸入 PTZ 攝影機的密碼。

[Close (關閉)]：按一下清除所有欄位。

[Connect (連線)]：按一下以建立與 PTZ 攝影機的連接。

[設定雷達自動追蹤]：按一下以開啟和設定自動追蹤。您也可以前往 [雷達 > 雷達 PTZ 自動追蹤] 進行設定。

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。

[Type (類型)]：選擇要傳送的日誌類型。

測試伺服器設定：在儲存設定之前，先傳送測試訊息到所有伺服器。

[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) 

[Calibration (校正) 

[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)]。

驗證您的安裝

驗證雷達的安裝

附註

此測試可幫助您在目前條件下驗證您的安裝。日常安裝效能可能會受到場景變化的影響。

雷達安裝好後隨即可用，但我們建議您在開始使用前先行驗證。這可以幫助您識別安裝中的任何問題，或管理場景中的物體 (例如樹木和反射面)，進而提高雷達的準確性。

第一，先在嘗試驗證前。

在以下情況執行驗證是正確做法：

- 場景中有您想要排除的物體，以便這些區域可以包含某些物體，例如植被或金屬表面。
- 您將雷達與 PTZ 攝影機配對，並想要設定 [雷達自動追蹤]。
- 雷達安裝高度已變更。

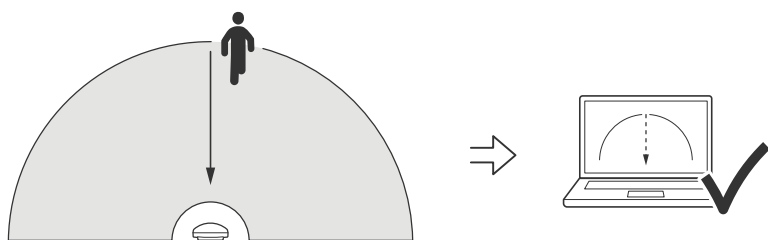
驗證雷達

確認沒有錯誤偵測

1. 檢查偵測區域是否沒有人類活動。
2. 等待幾分鐘，以確保雷達未偵測到偵測區內的任何靜態物件。
3. 如果沒有不需要的偵測，您可以略過步驟 4。
4. 如果有不需要的偵測，請自如何過濾掉某些類型的移動或物件、變更涵蓋範圍或調整中的偵測靈敏度。

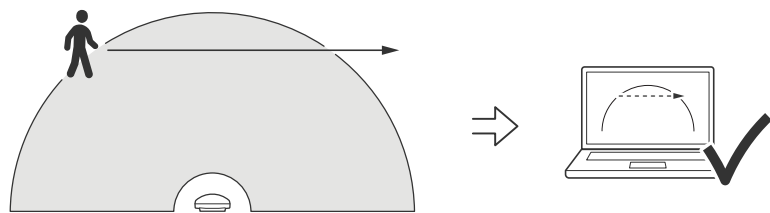
當從前方接近雷達時，請檢查正確的符號和行進方向

1. 進入雷達的網頁介面，並記錄工作階段。如需幫助，請前往。
2. 從雷達前方 60 公尺 (197 英呎) 處開始直接朝雷達走去。
3. 檢查雷達網頁介面中的工作階段。當您被偵測到時，應該會出現人體分類的符號。
4. 確認雷達的網頁介面顯示正確的行進方向。



當從側邊接近雷達時，請檢查正確的符號和行進方向

1. 進入雷達的網頁介面，並記錄工作階段。如需幫助，請前往。
2. 從雷達外 60 公尺 (197 英呎) 處開始直接穿過雷達涵蓋區域。
3. 確認雷達的網頁介面顯示人體分類的符號。
4. 確認雷達的網頁介面顯示正確的行進方向。



建立一個類似於下表的表格，以協助您記錄驗證的資料。

測試	通過/未通過	註解
1.當該區域清理乾淨後，檢查是否有不需要的偵測		
2a.確認當從前方接近雷達時，是否偵測到正確的「人類」符號		
2b.從前方接近雷達時，確認行進方向正確		
3a.確認當從側邊接近雷達時，是否偵測到正確的「人類」符號		
3b.當從側邊接近雷達時，確認行進方向正確		

完成驗證

成功完成驗證的第一部分後，應該執行以下測試來完成驗證程序。

1. 確保您已設定雷達，並已按照說明操作。
2. 若要進一步驗證，請新增並校準參考地圖。
3. 當偵測到適當的物件時，將雷達設定為觸發。根據預設，[觸發前的秒數] 設定為兩秒，但如有需要，可在網頁介面中變更此設定。
4. 當偵測到適當的物件時，將雷達設定為記錄資料。
相關說明，請參閱。
5. 將 [軌跡存留期] 設定為一小時，這樣就可以安全地超出您離開座位、在監控區域周遭走動，並返回座位所需的時間。[軌跡存留期] 是將軌跡保留在雷達的即時影像中達所設定的時間，等您完成驗證，就可以停用。
6. 沿著雷達涵蓋區域的邊界行走，並確定系統的尾隨軌跡與您行走的路線相符。
7. 如果您對驗證結果不滿意，請重新校準參考地圖，並重複驗證。

深入瞭解

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

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

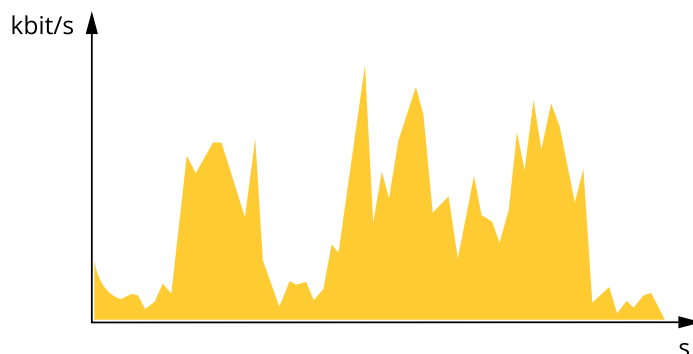
- H.265 是經授權使用的技術。Axis 產品包含一份 H.265 觀看用戶端授權。禁止另外安裝其他未經授權的用戶端複本。若要購買額外的授權，請聯絡您的 Axis 經銷商。
- 大多數網頁瀏覽器都不支援 H.265 解碼，因此攝影機在其網頁介面中不支援此選項。您可以改用支援 H.265 解碼的影像管理系統或應用程式。

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。

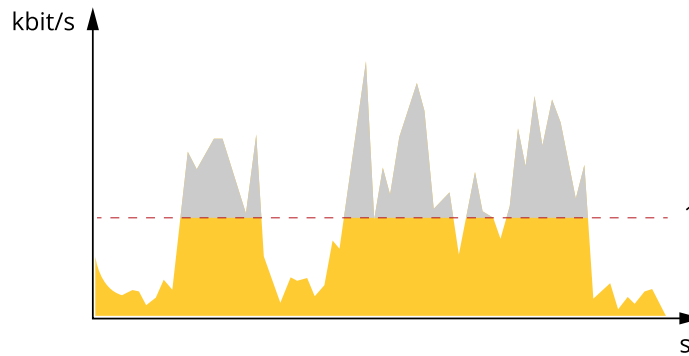
可變位元傳輸率(VBR)

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。

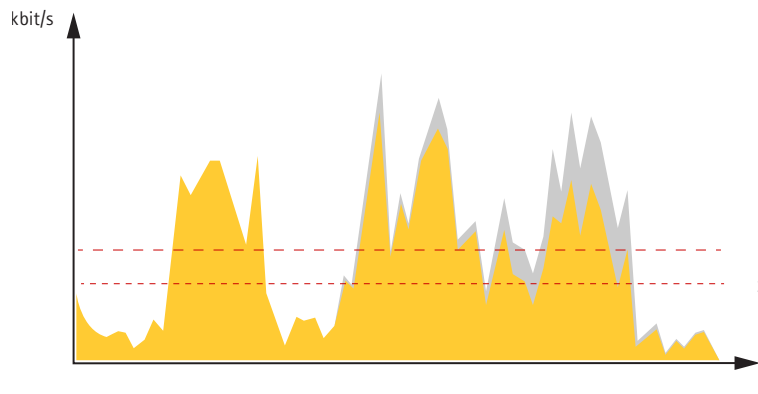


1 目標位元速率

平均傳輸率 (ABR)

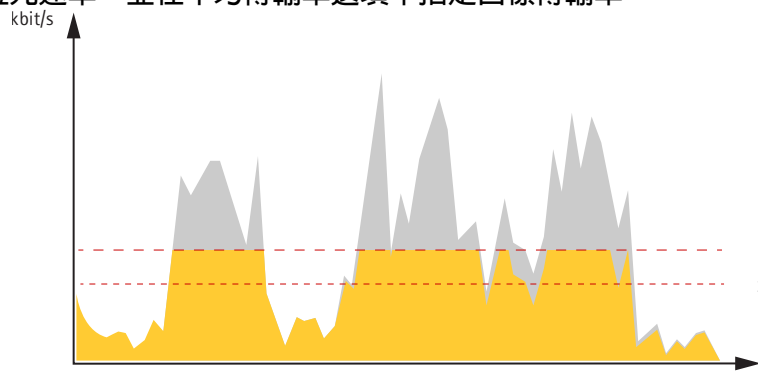
平均傳輸率會在更長的時段自動調整。這樣您就可以滿足指定的目標，並根據可用儲存空間提供最佳影像畫質。與靜態場景相比，有很多活動的場景會有更高的傳輸率。如果您在活動量大的場景中使用平均傳輸率選項，您更有可能獲得比較好的影像畫質。調整影像畫質達到指定的目標傳輸率時，您可以定義儲存指定時間長度的影像串流 (存留時間) 所需的總儲存空間。以下列其中一個方法指定平均傳輸率設定：

- 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

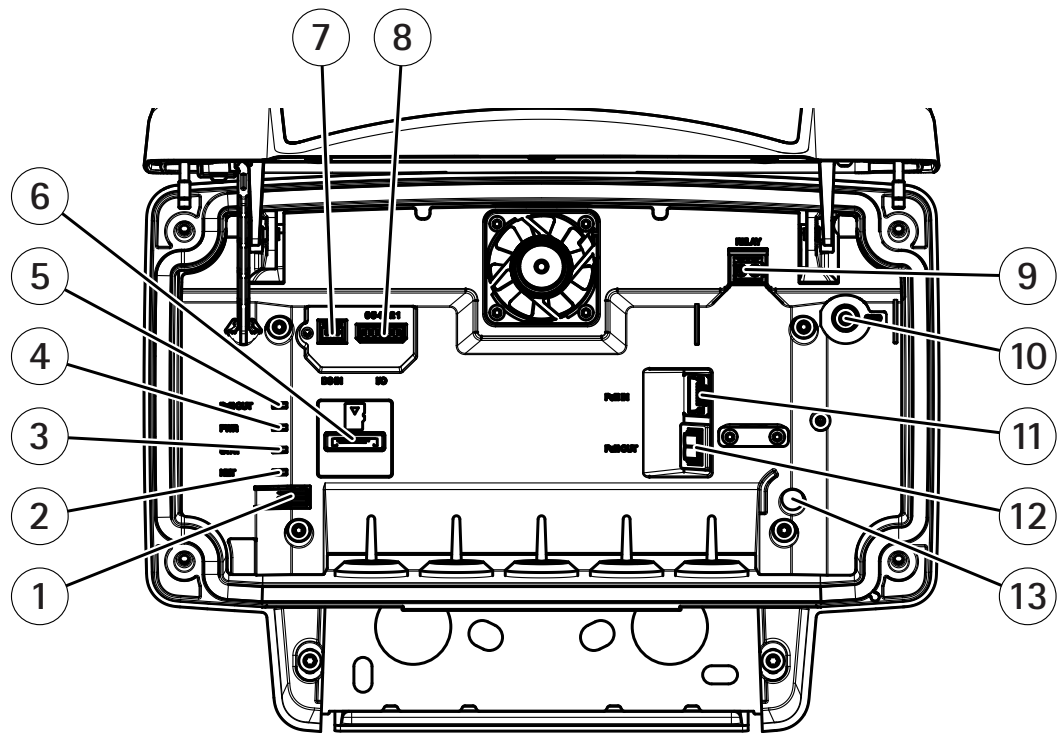
您還可以開啟最大位元速率，並在平均傳輸率選項中指定目標傳輸率。



1 目標位元速率
2 實際平均傳輸率

規格

產品總覽



- 1 控制按鈕
- 2 網路 LED
- 3 狀態LED燈號
- 4 電源指示燈
- 5 PoE 輸出 LED
- 6 microSD 卡插槽
- 7 電源接頭 (DC)
- 8 I/O 連接端子
- 9 繼電器接頭
- 10 接地螺絲
- 11 網路連接器 (PoE 輸入)
- 12 網路連接器 (PoE 輸出)
- 13 侵入警報感應器

有關技術規格的資訊，請參閱。

LED 指示燈

狀態LED燈號	指示
綠色	綠燈常亮表示正常操作。

網路 LED	指示
綠色	常亮表示已連線到 100 Mbit/s 網路。閃爍表示有網路活動。
黃色	常亮表示已連線到 10 Mbit/s 網路。閃爍表示有網路活動。
熄滅	無網路連線。

電源指示燈	指示
綠色	正常運作。

PoE 輸出 LED	指示
熄滅	PoE 輸出已關閉
綠色	PoE 輸出已開啟

SD 卡插槽

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

如需控制按鈕位置，請參閱。

控制按鈕用於：

- 將產品重設為出廠預設設定。請參考。
- 連線到 AXIS Video Hosting System (影像代管系統) 服務。請參考。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

支援增強型乙太網路供電 (PoE+) 的 RJ45 乙太網路接頭。

▲ 小心

裝置損壞風險。不要同時使用 PoE 和 DC 為裝置供電。

網路連接器 (PoE 輸出)

乙太網路供電 IEEE 802.3at Type 2，最大功率 30W

使用此連接器為另一個 PoE 設備供電，例如攝影機、家用喇叭或第二個 Axis 雷達。

附註

當雷達由 60 W 中跨器 (乙太網供電 IEEE 802.3bt，Type 3) 供電時，啟用 PoE 輸出。

附註

如果雷達由 30 W 中跨器 (midspan) 或直流電源供電，則停用 PoE 輸出。

附註

PoE 輸出和 PoE 輸入的結合產生乙太網路電纜總長度上限 100 公尺。您可以使用 PoE 延伸器來增加長度。

附註

如果連接的 PoE 設備需要超過 30 W，可以在雷達的 PoE 輸出連接埠和設備之間新增一個 60 W 的中跨器 (midspan)。此中跨器 (midspan) 將為設備供電，而安全雷達將提供乙太網路連線。

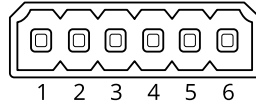
I/O 連接端子

將 I/O 連接端子搭配外部設備結合事件觸發和警報通知等功能使用。除了 0 VDC 參考點和電源 (DC 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。

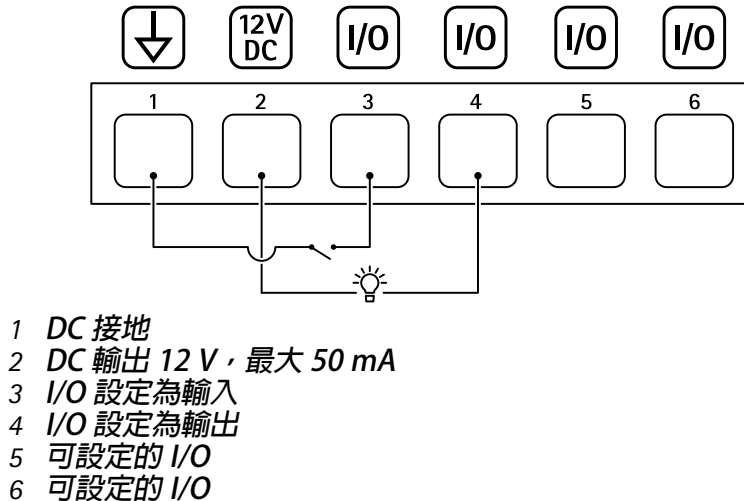
數位輸出 - 用於連接繼電器和 LED 等外接式設備。連接的設備可透過 VAPIX® 應用程式開發介面、事件或設備網頁介面加以啟動。

6 針接線端子



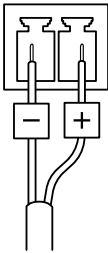
功能	針腳	附註	規格
DC 接地	1		0 VDC
DC 輸出	2	 可用於電源輔助設備。 注意：此接腳只能當做電源輸出使用。	12 VDC 最大負載 = 50 mA
可設定 (輸入或輸出)	3—6	數位輸入 — 連接到接腳 1 以啟用，或浮接 (不連接) 以停用。	0 到最大 30 VDC
		數位輸出 — 作用中時，內部會連接到針腳 1 (DC 接地)，非作用中時為浮接 (不連接)。如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。	0 到最大 30 VDC，漏極開路，100 mA

範例：



電源接頭

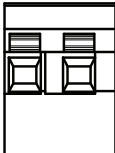
2 針接線端子，用於 DC 電源輸入。使用符合安全額外低電壓 (SELV) 的限功率電源 (LPS)，可以是額定輸出功率限制在 ≤ 100 W 或額定輸出電流限制在 ≤ 5 A 的電源。



▲ 小心

裝置損壞風險。不要同時使用 PoE 和 DC 為裝置供電。

繼電器接頭



▲ 小心

針對繼電器接頭使用單芯線。

功能	規格
類型	常開
額定值	24 V DC/5 A
與其他電路隔離	2.5 kV

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)]。

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... 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。

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所需頻寬量 (傳輸率) 的影響。

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。

T10145149_zh_tw

2025-06 (M31.2)

© 2020 – 2025 Axis Communications AB