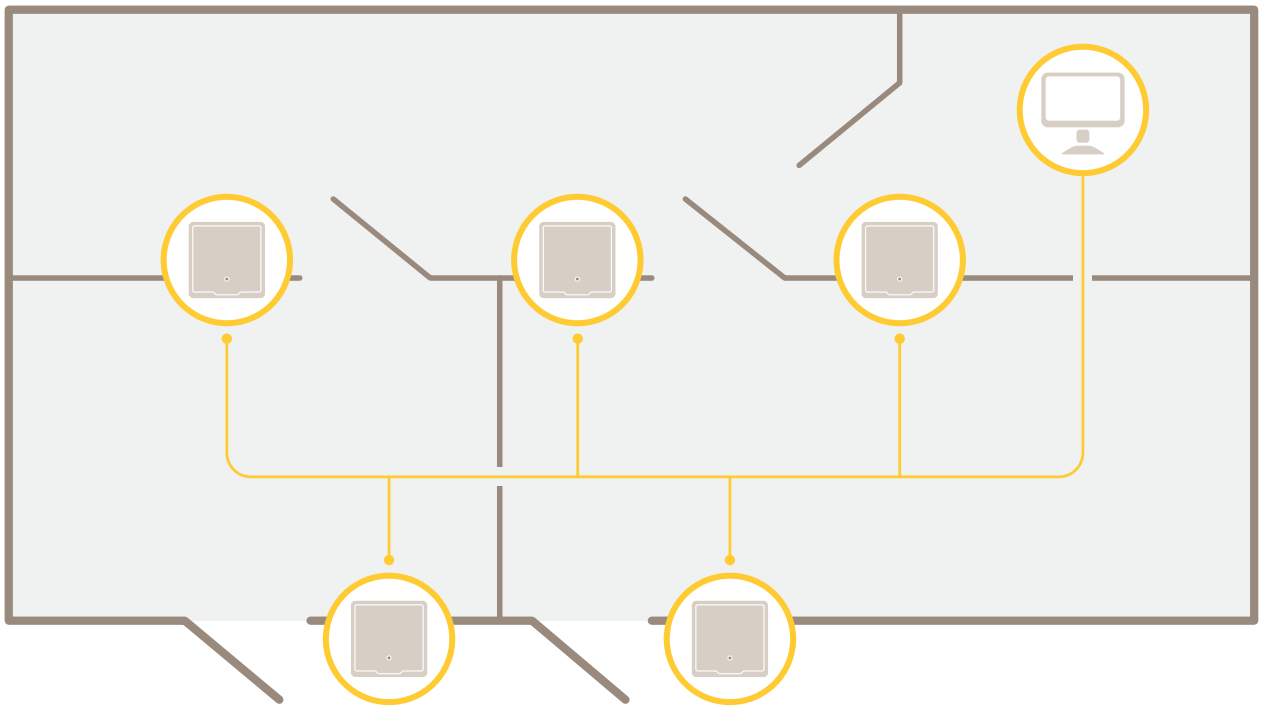
AXIS A1601 Network Door Controller

使用手冊

目錄

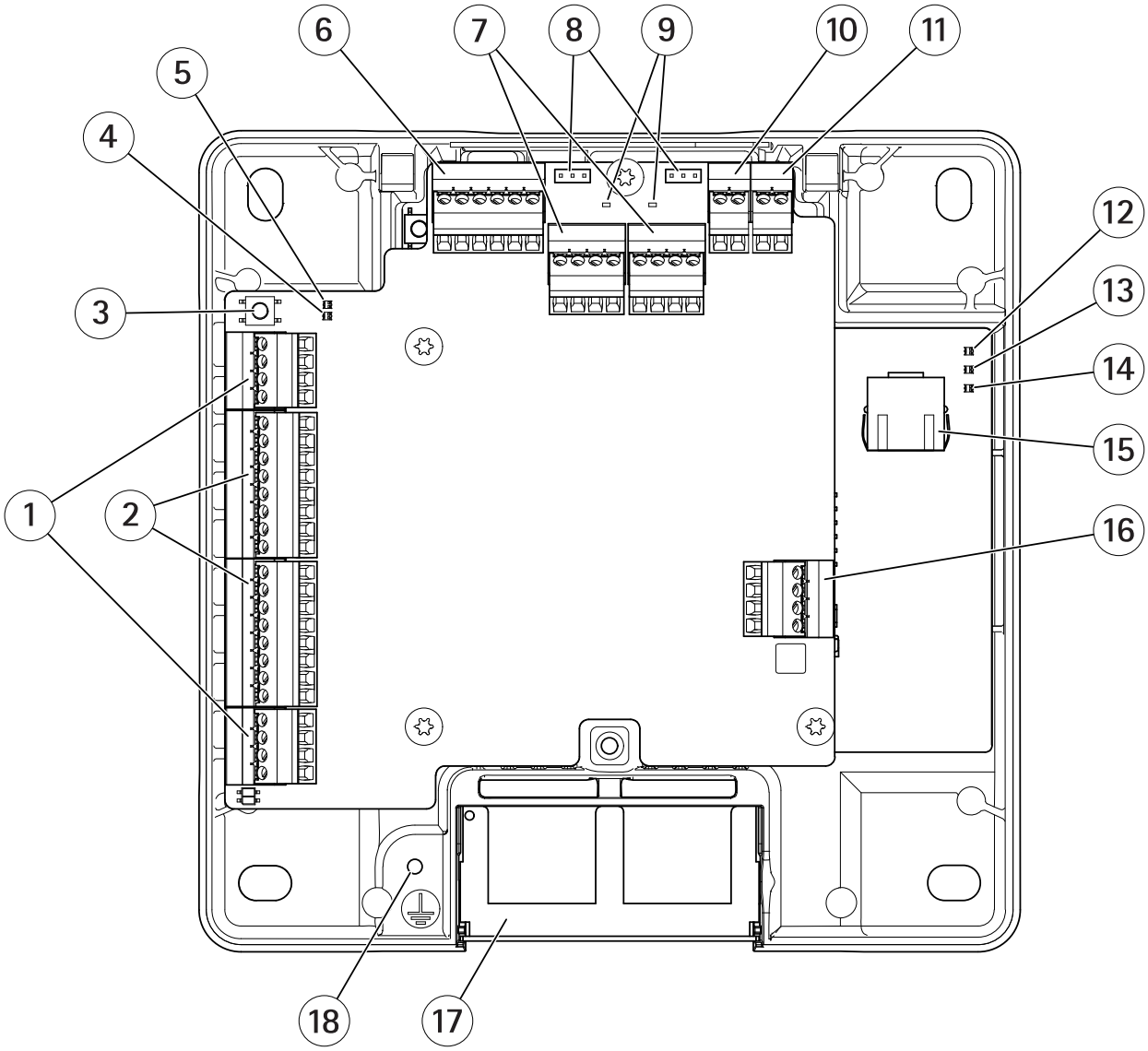
解決方案總覽



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

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

產品總覽



1 *(2x)*
2 *(2x)*
3
4 *讀卡機過電流 LED*
5 *繼電器過電流 LED*
6
7 *(2x)*
8 *繼電器跳線 (2x)*
9 *繼電器 LED (2x)*
10
11
12 *電源指示燈*
13 *狀態LED燈號*
14 *網路 LED*
15
16
17 *可反插纜線蓋*
18 *接地位置*

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*。

存取裝置

1. 開啟瀏覽器，然後輸入 Axis 裝置的 IP 位址或主機名稱。
   如果您不知道 IP 位址，請使用 AXIS IP Utility 或 AXIS Device Manager，在網路上尋找設備。
2. 輸入使用者名稱和密碼。如果您是第一次存取設備，則必須設定 root 密碼。請參考 。
3. 隨即在瀏覽器中開啟設備的網頁。啟始頁面稱為概觀頁面。

如何從網際網路存取產品

網路路由器可讓私人網路 (LAN) 上的產品共用單一網際網路連線。這是藉由將網路流量從私人網路轉發至網際網路來完成。

大多數路由器都已預先設定為阻止嘗試從公用網路 (網際網路) 存取私人網路 (LAN)。

如果 Axis 產品位於內部網路 (LAN)，而您想要從 NAT (網路位址轉譯器) 路由器的另一端 (WAN) 使用此產品時，請開啟 [NAT 周遊]。正確設定 NAT 周遊後，所有在 NAT 路由器中流向外部 HTTP 連接埠的 HTTP 流量都會轉發至產品。

如何開啟 NAT 周遊功能

- 前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)]。
- 按一下 [啟用]。
- 手動設定 NAT 路由器以允許從網際網路存取。

附註

- 在此情境中，「路由器」是指任何網路路由裝置，例如 NAT 路由器、網路路由器、網際網路閘道、寬頻路由器、寬頻分享裝置，或是像防火牆這樣的軟體。
- 若要讓 NAT 周遊功能運作，路由器必須支援 NAT 周遊。路由器也必須支援 UPnP®。

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。

如何設定 root 密碼

若要存取 Axis 產品，您必須設定預設管理員使用者 root 的密碼。這個設定可在初次存取產品時所開啟的 [設定 Root 密碼] 對話方塊中完成。

為了防止網路竊聽，可透過加密的 HTTPS 連線設定 root 密碼，這需要 HTTPS 憑證。HTTPS (基於 SSL 的超文本傳輸協定 (HTTP)) 是一種用於加密網頁瀏覽器與伺服器之間流量的通訊協定。HTTPS 憑證可確保加密的資訊交換。請參考 。

預設管理員使用者名稱 root 永久不變，無法刪除。如果遺失 root 的密碼，則必須將產品重設為出廠預設設定。請參考 。

若要設定密碼，請直接在對話方塊中輸入。

概觀頁面

產品網頁中的概觀頁面顯示有關門控制器名稱、MAC 位址、IP 位址和韌體版本的資訊。此頁面還可讓您識別網路上的門控制器。

初次存取 Axis 產品時，概觀頁面會提示您設定硬體、設定日期和時間滿以及設定網路設定。如需有關設定系統的詳細資訊，請參閱。

若要從產品的其他網頁返回概觀頁面，請按一下功能表列中的 [概觀]。

系統組態

若要開啟產品的設定頁面，請按一下 [概觀] 頁面右上角的 [設定]。

Axis 產品可由管理員進行設定。如需使用者和管理員的詳細資訊，請參閱。

組態設定 — 逐步進行

開始使用門禁管制系統之前，您必須完成下列設定步驟：

1. 如果英語不是您的第一語言，您可能會希望產品的網頁使用不同的語言。請參考 。
2. 設定日期和時間。請參考 。
3. 設定網路設定。請參考 。
4. 設定門控制器以及連接的裝置，例如讀卡機、門鎖和外出開關 (REX) 裝置。請參考 。
5. 驗證硬體連接。請參考 。
6. 設定卡片和格式。請參考 。

如需有關維護建議的詳細資訊，請參閱。

選取語言

產品網頁的預設語言是英文，但您可以切換到產品韌體中包含的任何語言。如需最新可用韌體的詳細資訊，請參閱 *www.axis.com*

您可以在任何產品的網頁中切換語言。

若要切換語言，請按一下語言下拉式清單 ，並選取語言。所有產品的網頁和說明頁面都是以選取的語言來顯示。

附註

- 切換語言時，日期格式也會變更為所選語言中常用的格式。資料欄位會顯示正確的格式。
- 如果將產品重設為出廠預設設定，產品的網頁就會切換回英文。
- 如果還原或重新啟動產品，或升級韌體，則產品的網頁仍將繼續使用所選語言。

設定日期和時間

若要設定 Axis 產品的日期和時間，請移至 [設定 > 日期和時間]。

您可以透過下列方式設定日期和時間：

- 從網路時間通訊協定 (NTP) 伺服器取得日期和時間。請參考 。
- 手動設定日期和時間。請參考 。
- 從電腦取得日期和時間。請參考 。

[目前控制器時間] 會顯示門禁控制器目前的日期和時間 (24 小時制)。

[系統選項] 頁面中也有提供相同的日期和時間選項。前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Date & Time (日期和時間)]。

從網路時間通訊協定 (NTP) 伺服器取得日期和時間

1. 移至 [設定 > 日期和時間。
2. 從下拉式清單選取 [時區]。
3. 如果您所在地區採用日光節約時間，請選取 [調整日光節約時間]。
4. 選項 [與 NTP 同步]。
5. 選取預設 DHCP 位址，或輸入 NTP 伺服器的位址。
6. 按一下Save。

與 NTP 伺服器同步時，由於資料是從 NTP 伺服器推送，因此日期和時間會持續更新。如需 NTP 的詳細資訊，請參閱。
如果使用 NTP 伺服器的主機名稱，您必須設定 DNS 伺服器。請參考 。

手動設定日期和時間

1. 移至 [設定 > 日期和時間。
2. 如果您所在地區採用日光節約時間，請選取 [調整日光節約時間]。
3. 選取 [手動設定日期和時間]。
4. 輸入所需的日期和時間。
5. 按一下Save。

手動設定日期和時間時，日期和時間會設定一次，並不自動更新。這表示，如果需要更新日期或時間，則必須手動進行變更，因為沒有與外部 NTP 伺服器的連線。

從電腦取得日期和時間

1. 移至 [設定 > 日期和時間。
2. 如果您所在地區採用日光節約時間，請選取 [調整日光節約時間]。
3. 選取 [手動設定日期和時間]。
4. 按一下 [立即同步並儲存]。

使用電腦時間時，日期和時間會與電腦時間同步一次，並不自動更新。這表示，如果您變更用於管理系統之電腦上的日期或時間，則應再次同步。

設定網路設定

若要設定基本網路設定，請移至 [設定 > 網路設定] 或 [設定 > 其他控制器組態 > 系統選項 > 網路 > TCP/IP > 基本]。

如需網路設定的詳細資訊，請參閱。

設定硬體

您可以先將讀卡機、門鎖及其他裝置連接至 Axis 產品，再完成硬體組態設定。不過，如果先完成硬體組態設定，連接裝置時就會更輕鬆。這是因為組態設定完成時會提供硬體接腳圖。硬體接腳圖是有關裝置與接腳連接方式的指南，可當做維護參考表使用。如需維護指示，請參閱。

如果是第一次設定硬體，請選擇下列其中一個方法：
- 匯入硬體組態設定檔。請參考 。
- 建立新的硬體組態。請參考 。

附註
如果產品的硬體先前未進行設定，或已遭刪除，概觀頁面的通知面板中有 [硬體組態] 可用。

如何匯入硬體組態設定檔

您可以匯入硬體組態設定檔，加快完成 Axis 產品的硬體組態設定。

您可以從一個產品匯出檔案，再將其匯入至其他產品，藉此建立同一個硬體組態的多個複本，無需一遍又一遍地重複相同的步驟。您還可以將匯出的檔案儲存為備份，並使用這些備份來還原先前的硬體組態。如需詳細資訊，請參閱 。

若要匯入硬體組態設定檔：
1. 移至 [設定 > 硬體組態]。
2. 按一下 [匯入硬體組態]，如果已經有硬體組態，則按一下 [重設並匯入硬體組態]。
3. 在出現的檔案瀏覽器對話方塊中，尋找並選取電腦上的硬體組態設定檔 (*.json)。

4. 按一下OK (確認)。

如何匯出硬體組態設定檔

您可以匯出 Axis 產品的硬體組態來建立同一個硬體設定的多個複本。您還可以將匯出的檔案儲存為備份，並使用這些備份來還原先前的硬體組態。

附註

樓層的硬體組態無法匯出。

無線門鎖設定不包含在硬體組態匯出中。

若要匯出硬體組態設定檔：

1. 移至 [設定 > 硬體組態]。
2. 按一下 [匯出硬件組態]。
3. 視瀏覽器而定，您可能需要瀏覽對話方塊來完成匯出。
   除非另有說明，匯出的檔案 (*.json) 會儲存在預設下載資料夾中。您可以在網頁瀏覽器的使用者設定中選取下載資料夾。

建立新的硬體組態

根據您的需求，按照說明進行操作：

-
-
-

如何建立沒有周邊設備的新硬體組態

1. 移至 [設定 > 硬體組態]，並按一下 [開始新的硬體組態設定]。
2. 輸入 Axis 產品的名稱。
3. 選取連接門的數量並按一下 [下一步]。
4. 根據您的需求設定門禁監控器 (門位置感應器) 和門鎖，然後按一下 [下一步]。如需有關可用選項的詳細資訊，請參閱。
5. 設定將會使用的讀卡機和 REX 裝置，然後按一下 [完成]。如需有關可用選項的詳細資訊，請參閱。
6. 按一下 [關閉]，或按一下連結以檢視硬體接腳圖。

如何設定門禁監控器和門鎖

選取新硬體組態中的門選項時，您可以設定門禁監控器和門鎖。

1. 如果要使用門禁監控器，請選取 [門禁監控器]，然後選取符合門禁監控器電路連接方式的選項。
2. 如果要門鎖在開門後立即上鎖，請選取 [開門後即取消準入時間]。
   如果想要延遲重新上鎖，請在 [重新上鎖時間] 中，以毫秒為單位設定延遲時間。
3. 指定門禁監控器時間選項，如果不使用門禁監控器，則指定上鎖時間選項。
4. 選取符合門鎖電路連接方式的選項。
5. 如果要使用鎖監控器，請選取 [鎖監控器]，然後選取符合鎖監控器電路連接方式的選項。
6. 如果來自讀卡機、REX 裝置和門禁監控器的輸入連線應受監控，請選取 [受監控的輸入]。
   如需詳細資訊，請參閱 。

附註

- 大多數門鎖、門禁監控器和讀卡機選項，都可以在不重設和啟動新硬體組態的情況下進行變更。移至 [設定 > 硬體重新設定]。
- 您可以將每個門控制器各連接一個鎖監控器。因此，如果您使用雙鎖門，則只有其中一個門鎖可以有門鎖監控器。如果兩扇門連接到同一個門控制器，則無法使用門鎖監視器。

關於門禁監控器和時間選項

有下列門禁監控器選項可用：

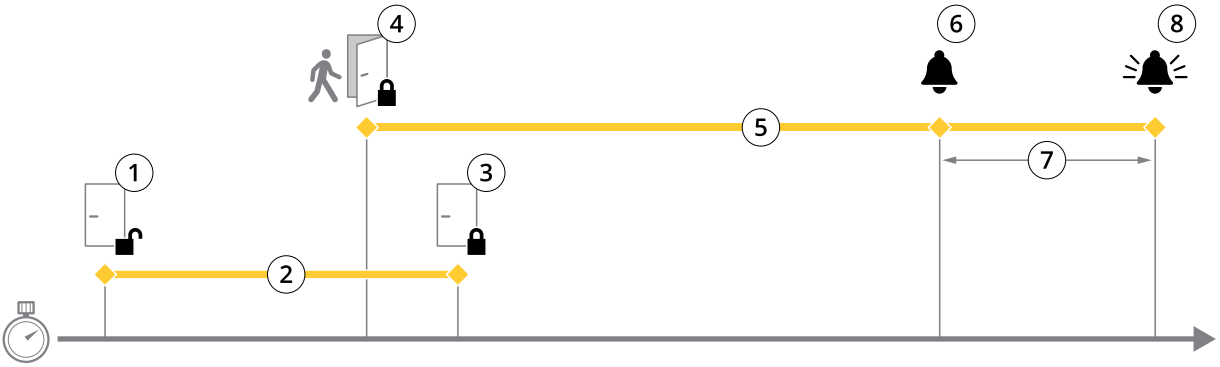
- 門禁監控器 — 預設會選取此選項。每扇門都有其本身的門禁監控器；例如，這些門禁監控器會在門口遭強行開啟或開啟時間過長時發出訊號。如果不使用門禁監控器，請取消選取。
- 開路 = 關門 — 如果門禁監控器電路常開，則選取此選項。當電路閉路時，門禁監控器會發出開門訊號。當電路開路時，門禁監控器會發出關門訊號。
- 開路 = 開門 — 如果門禁監控器電路常閉，則選取此選項。當電路開路時，門禁監控器會發出開門訊號。當電路閉路時，門禁監控器會發出關門訊號。
- 開門後取消準入時間 — 選取以防止尾隨通行。只要門禁監控器指示門已打開，鎖就會立即上鎖。

始終有下列門禁時間選項可用：

- 準入時間 — 設定授予進入權限後，門應保持解鎖狀態的秒數。門會保持解鎖狀態，直到門口開啟或已達設定時間為止。無論準入時間是否已過，門口關閉時都會上鎖。
- 長準入時間 — 設定授予進入權限後，門應保持解鎖狀態的秒數。長準入時間會覆寫已設定的準入時間，並針對選取長準入時間的使用者啟用。

選取 [門禁監控器] 以提供下列門禁時間選項：

- 門口開啟時間過長 — 設定允許門口保持開啟狀態的秒數。如果到達設定時間時門口仍然開啟，則會觸發門口開啟時間過長警報。設定動作規則，以設定門口開啟時間過長事件會觸發哪一個動作。
- 警報前時間 — 預報警是在達到 [門口開啟時間過長] 所設時間前觸發的警告訊號。這會通知管理員，並根據動作規則的設定方式，警告進入門口的人員必須關門以避免「門口開啟時間過長」警報響起。設定觸發「門口開啟時間過長」警報前的秒數，當時間一到，系統即應發出預警報警告訊號。若要停用預警報，請將警報前時間設定為 0。



1 *已授予進入權限 - 門鎖解鎖*
2 *準入時間*
3 *未採取任何動作 — 門鎖上鎖*
4 *已採取動作 (門已開啟) — 門鎖上鎖，或保持解鎖直到門關上*
5 *門口開啟時間過長*
6 *預警報響起*
7 *警報前時間*
8 *門口開啟時間過長警報響起*

如需有關如何設定動作規則的詳細資訊，請參閱。

關於門鎖選項

有下列門鎖電路選項可用：

- 繼電器 — 只能用於每個門控制器的一個鎖。如果有兩個門連接至門控制器，則繼電器只能用於第二個門的鎖。
- 無 — 僅適用於門鎖 2。如果只使用一個鎖，則選取此選項。

下列鎖監控器選項適用於單門組態：

- 鎖監控器 — 選取以提供鎖監控器控制。然後選取要監控的門鎖。鎖監控器只能用於雙鎖門，如果將兩個門連接至門禁控制器，則無法使用。

— 開路 = 上鎖 — 如果鎖監控器電路常閉，則選取此選項。當電路閉路時，鎖監控器會發出門口解鎖訊號。當電路開路時，鎖監控器會發出門口上鎖訊號。

— 開路 = 解鎖 — 如果鎖監控器電路常開，則選取此選項。當電路開路時，鎖監控器會發出門口解鎖訊號。當電路閉路時，鎖監控器會發出門口上鎖訊號。

如何設定讀卡機和 REX 裝置

在新的硬體組態中設定門禁監控器和門鎖時，您可以設定讀卡機和外出開關 (REX) 裝置。

1. 如果要使用讀卡機，請選取讀卡機，然後選取符合讀卡機通訊協定的選項。
2. 如果會使用按鈕、感應器或推門把手等 REX 裝置，請選取核取方塊，然後選取符合 REX 裝置電路連接方式的選項。
   如果 REX 訊號對開門沒有影響 (例如，對有機械把手或推手的門而言)，請選取 [REX 不解開門鎖]。
3. 如果將多個讀卡機或 REX 裝置連接到門控制器，請再次執行前兩個步驟，使每個讀卡機或 REX 裝置都有正確的設定。

關於讀卡機和 REX 裝置選項

有下列讀卡機選項可用：

- Wiegand — 選取以用於使用 Wiegand 通訊協定的讀卡機。然後選取讀卡機支援的 LED 控制。含單 LED 控制的讀卡機通常會在紅色與綠色燈號之間切換。具有雙 LED 控制的讀卡機使用不同電線控制紅色和綠色 LED。這表示這兩個 LED 可彼此獨立運作。當兩個 LED 都亮起時，指示燈呈琥珀色。請參閱製造商所提供有關讀卡機支援何種 LED 控制的資訊。
- OSDP，RS485 半雙工 — 選取以用於含半雙工支援的 RS485 讀卡機。請參閱製造商所提供有關讀卡機支援哪個通訊協定的資訊。

有下列 REX 裝置選項可用：

- 低態啟動 — 如果啟動 REX 裝置會使電路閉路，則選取此選項。
- 高態啟動 — 如果啟動 REX 裝置會使電路開路，則選取此選項。
- REX 不解開門鎖 — 如果 REX 訊號對開門沒有影響 (例如，對有機械把手或推手的門而言)，則選取此選項。只要使用者在準入時間內開門，就不會觸發門口遭強行開啟報警。如果使用者啟動 REX 裝置時應自動將門口解鎖，則取消選取。

附註

大多數門鎖、門禁監控器和讀卡機選項，都可以在不重設和啟動新硬體組態的情況下進行變更。移至 [設定 > 硬體重新設定]。

如何使用受監控的輸入

受監控的輸入會回報門禁控制器與門禁監控器之間的連接狀態。如果連接中斷，則啟動事件。

若要使用受監控的輸入：

1. 在所有使用的受監控輸入上安裝線路終端電阻器。請參閱上的連接圖。
2. 移至 [設定 > 硬體重新設定]，並選取 [啟用受監控的輸入]。您也可以在進行硬體組態設定時啟用受監控的輸入。

關於受監控的輸入相容性

下列功能支援受監控的輸入：

- 門禁監控器。請參考 。

如何為無線門鎖建立新的硬體組態

1. 移至 [設定 > 硬體組態]，並按一下 [開始新的硬體組態設定]。
2. 輸入 Axis 產品的名稱。
3. 在周邊設備清單中，選取無線閘道器的製造商。
4. 如果要連接有線門，請選取 [1 道門] 核取方塊，並按一下 [下一個]。如果沒有包含任何門，請按一下 [完成]。
5. 視您取得的鎖製造商而定，根據其中一項進行操作：
   - ASSA Aperio：按一下連結以檢視硬體接腳圖，或按一下 [關閉]，然後移至 [設定 >硬體重新設定] 以完成設定，請參閱
   - SmartIntego：按一下連結以檢視硬體接腳圖，或按一下 [按一下這裡選取無線閘道器並設定門] 以完成組態設定，請參閱。

新增 Assa Aperio™ 門和裝置

將無線門新增至系統之前，需要使用 Aperio PAP (Aperio 編程應用程式工具)，與連接的 Assa Aperio 通訊中心配對。

若要新增無線門：

1. 移至 [設定] > [硬體重新設定]。
2. 在 [無線門和裝置] 下方，按一下 [新增門]。
3. 在 [門名稱] 欄位中：輸入描述性名稱。
4. 在 [門鎖] 下的 [ID] 欄位中：輸入要新增的裝置的六字元長度位址。此裝置位址會列印在產品標籤上。
5. (選擇性) 在 [門位置感應器] 底下：選擇 [內建門位置感應器] 或 [外部門位置感應器]。

附註

如果使用外部門位置感應器 (DPS)，請先確定 Aperio 門鎖裝置支援門把手狀態偵測，再進行其設定。

6. (選擇性) 在 [門位置感應器] 下的 [ID] 欄位中：輸入要新增的裝置的六字元長度位址。此裝置位址會列印在產品標籤上。
7. 按一下 [Add (新增)]。

如何使用電梯控制 (AXIS A9188) 來建立新的硬體組態

重要

建立硬體組態之前，您需要在 AXIS A9188 Network I/O Relay Module 繼電器模組中新增使用者。移至 A9188 網頁介面 > [偏好設定 > 其他裝置組態 > 基本設定 > 使用者 > 新增 > 使用者設定]。

附註

每個 Axis Network Door Controller 網路門禁控制器最多可以配置 2 個 AXIS 9188 Network I/O Relay Module 繼電器模組

1. 在門禁控制器的網頁中，移至 [設定 > 硬體組態]，並按一下 [開始新的硬體組態設定]。
2. 輸入 Axis 產品的名稱。
3. 在周邊設備清單中，選取 [電梯控制] 以包含 AXIS A9188 Network I/O Relay Module，然後按一下 [下一個]。
4. 輸入所連接讀卡機的名稱。
5. 選取要使用的讀卡機通訊協定，並按一下 [完成]。
6. 按一下 [網路周邊設備] 以完成組態設定，請參閱，或按一下連結以移至硬體接腳圖。

如何新增和設定網路周邊設備

重要

- 設定網路周邊設備之前，您必須在 AXIS A9188 Network I/O Relay Module 繼電器模組中新增使用者。移至 AXIS A9188 網頁介面 > [偏好設定 > 其他裝置組態 > 基本設定 > 使用者 > 新增 > 使用者設定]。
- 不要再新增其他 AXIS A1001 Network Door Controller 網路門禁控制器做為網路周邊設備。

1. 移至 [設定 > 網路周邊設備] 以新增裝置
2. 在 [探索到的裝置] 底下尋找您的裝置。
3. 按一下 [新增此裝置]
4. 輸入裝置名稱。
5. 輸入 AXIS A9188 使用者名稱和密碼。
6. 按一下 [Add (新增)]。

附註

您可在 [手動新增裝置] 對話方塊中輸入 MAC 位址或 IP 位址，以手動方式新增網路周邊設備。

重要

如果要刪除排程，請先確定網路 I/O 繼電器模組並未使用該排程。

如何設定網路周邊設備中的 I/O 和繼電器

重要

設定網路周邊設備之前，您需要在 AXIS A9188 Network I/O Relay Module 繼電器模組中新增使用者。移至 AXIS A9188 網頁介面 > [偏好設定 > 其他裝置組態 > 基本設定 > 使用者 > 新增 > 使用者設定]。

1. 移至 [設定 > 網路周邊設備]，並按一下 [新增的裝置] 列。
2. 選擇要設定為樓層的 I/O 和繼電器。
3. 按一下 [設定為樓層] 並輸入名稱。
4. 按一下 [Add (新增)]。

驗證硬體連接

在硬體安裝與設定完成時，以及在門禁控制器生命週期中的任何時候，您都可以驗證連接的門禁監控器、網路 I/O 繼電器模組、門鎖及讀卡機的功能。

若要驗證組態設定並存取驗證控制項，請移至 [設定 > 硬體連接驗證]。

驗證會控制門

- 門狀態 — 驗證門禁監控器、門禁警報和門鎖的目前狀態。按一下 [取得目前狀態]。
- 上鎖 — 手動觸發門鎖。主要鎖和次要鎖 (如果有) 都會受到影響。按一下 [上鎖] 或 [解鎖]。
- 上鎖 — 手動觸門鎖以授予進入權限。只有主要鎖會受影響。按一下 [準入]。
- 讀卡機：反饋 — 驗證讀卡機對不同命令的反饋，例如聲音和 LED 訊號。選取命令並按一下 [測試]。可用的反饋類型取決於讀卡機。如需詳細資訊，請參閱 。另請參閱製造商的說明書。
- 讀卡機：防竄改 — 取得有關上一次竄改嘗試的資訊。第一次竄改嘗試會在安裝讀卡機時留下。按一下 [取得上次竄改]。
- 讀卡機：刷卡 — 取得有關上次刷卡或讀卡機所接受使用者其他類型認證載具 (Token) 的資訊。按一下 [取得上次認證]。
- REX — 取得有關上次按下外出開關 (REX) 裝置的資訊。按一下 [取得上次 REX]。

驗證控制樓層

- 樓層狀態 — 驗證樓層門禁的目前狀態。按一下 [取得目前狀態]。
- 樓層上鎖和解鎖 — 手動觸發樓層準入。主要鎖和次要鎖 (如果有) 都會受到影響。按一下 [上鎖] 或 [解鎖]。
- 樓層準入 — 手動授予暫時進入樓層的權限。只有主要鎖會受影響。按一下 [準入]。
- 電梯讀卡機：反饋 — 驗證讀卡機對不同命令的反饋，例如聲音和 LED 訊號。選取命令並按一下 [測試]。可用的反饋類型取決於讀卡機。如需詳細資訊，請參閱 。另請參閱製造商的說明書。
- 電梯讀卡機：防竄改 — 取得有關上一次竄改嘗試的資訊。第一次竄改嘗試會在安裝讀卡機時留下。按一下 [取得上次竄改]。
- 電梯讀卡機：刷卡 — 取得有關上次刷卡或讀卡機所接受使用者其他類型認證載具 (Token) 的資訊。按一下 [取得上次認證]。
- REX — 取得有關上次按下外出開關 (REX) 裝置的資訊。按一下 [取得上次 REX]。

設定卡片和格式

門禁控制器有一些預先定義的常用卡片格式，您可以依原樣使用，或視需要進行修改。您也可以建立自訂卡片格式。每種卡片格式都有一組有關如何組織卡片中所儲存資訊的不同規則 (欄位對應)。您可以藉由定義卡片格式，告訴系統如何解譯控制器從讀卡機取得的資訊。如需有關讀卡機支援哪些卡片格式的詳細資訊，請參閱製造商的說明書。

若要啟用卡格式：

1. 移至 [設定 > 設定卡片和格式]。
2. 選取一個或多個與已連接讀卡機所用卡片格式相符的卡片格式。

若要建立新的卡片格式：

1. 移至 [設定 > 設定卡片和格式]。
2. 按一下 [新增卡片格式]。
3. 在 [新增卡片格式] 對話方塊中，輸入卡片格式的名稱、描述和位元長度。請參考 。
4. 按一下 [新增欄位對應]，並在欄位中輸入所需的資訊。請參考 。
5. 若要新增多個欄位對應，請重複上一個步驟。

若要展開 [Card formats (卡片格式)] 清單中的項目，並檢視卡片格式說明和欄位對映，請按一下 。

若要編輯卡片格式，請按一下 ,255mm,sfx)="graphics:graphic64E1E98F15D44930541DD4F04C65FA89"，並視需要變更卡片格式說明和欄位對映。然後按一下 [儲存]。

若要刪除 [Edit card format (編輯卡片格式)] 或 [Add card format (新增卡片格式)] 對話方塊中的欄位對映，請按一下 ,255mm,sfx)="graphics:graphic474F43E0E3E4CB8D5531B942646F70FD"

若要刪除卡片格式，請按一下 ,255mm,sfx)="graphics:graphic474F43E0E3E4CB8D5531B942646F70FD"。

重要

- 如果門控制器配置了至少一個讀卡機，您只能啟用和停用卡片格式。請參閱和。
- 兩種位元長度相同的卡片格式無法同時啟用。例如，如果您已定義兩種 32 位元卡片格式「格式 A」和「格式 B」，而您啟用了「格式 A」，就無法在不停用「格式 A」的情況下啟用「格式 B」。
- 如果沒有啟用任何卡片格式，則可以使用 [僅限記憶卡 raw] 和 [記憶卡 raw 和 PIN 碼] 識別類型來識別卡片並授予使用者進入權限。但是不建議這樣做，因為不同的讀卡機製造商或讀卡機設定會產生不同的記憶卡 raw 資料。

卡片格式說明

- 名稱 (必填) — 輸入描述性名稱。
- 描述 — 視需要輸入其他資訊。此資訊只有在 [編輯卡片格式] 和 [新增卡片格式] 對話方塊。
- 位元長度 (必填) — 輸入卡片格式的位元長度。這必須是介於 1 和 1000000000 之間的數字。

欄位對應

- 名稱 (必填) — 輸入不留空格的欄位對映名稱，例如 `OddParity`。
  常見欄位對應的範例包括：
  - `Parity` — 同位位元用於錯誤偵測。同位位元通常會加在二進制代碼字串的開頭或結尾，並指示位元數是偶數還是奇數。
  - `EvenParity` — 偶數同位位元確保字串中有偶數個位元。值為 1 的位元會納入計數。如果計數已經是偶數，則將同位位元值設定為 0。如果計數為奇數，則將偶數同位位元值設定為 1，使總計數為偶數。
  - `OddParity` — 奇數同位位元確保字串中有奇數個位元。值為 1 的位元會納入計數。如果計數已經是奇數，則將奇數同位位元值設定為 0。如果計數為偶數，則數同位位元值設定為 1，使總計數為奇數。
  - `FacilityCode` — 設施代碼有時用於驗證認證載具 (Token) 是否與有序的最終使用者認證批次相符。在舊版門禁管制系統中，設施代碼用於降級驗證，允許已用相符監控地點編碼之認證批次中的每個員工進入。此欄位對應名稱 (區分大小寫) 是讓產品根據設施代碼進行驗證所需的名稱。
  - `CardNr` — 卡號或使用者 ID 是門禁管制系統中最常驗證的內容。此欄位對應名稱 (區分大小寫) 是讓產品根據卡號進行驗證所需的名稱。
  - `CardNrHex` — 卡號二進制資料會在產品中編碼為十六進制小寫數字。這主要用於排解為什麼沒有從讀卡機取得預期卡號的疑難。
- Range (必填) — 輸入欄位對應的位元範圍，例如 1、2-17、18-33 和 34。
- Encoding (必填) — 選取每個欄位對應的編碼類型。
  - BinLE2Int — 二進制資料依位元組由小到大的位元順序編碼為整數數字。整數即表示這需要的是非負整數 (沒有小數)。位元組由小到大的位元順序意味著第一個位元的值最小 (最低有效位元)。
  - BinBE2Int — 二進制資料依位元組由大到小的位元順序編碼為整數數字。整數即表示這需要的是非負整數 (沒有小數)。位元組由大到小的位元順序意味著第一個位元的值最大 (最高有效位元)。
  - BinLE2Hex — 二進制資料依位元組由小到大的位元順序編碼為十六進制小寫數字。十六進位系統，也稱為 16 進制系統，由 16 個獨特符號組成：數字 0—9 及字母 a—f。位元組由小到大的位元順序意味著第一個位元的值最小 (最低有效位元)。
  - BinBE2Hex — 二進制資料依位元組由大到小的位元順序編碼為十六進制小寫數字。十六進位系統，也稱為 16 進制系統，由 16 個獨特符號組成：數字 0—9 及字母 a—f。位元組由大到小的位元順序意味著第一個位元的值最大 (最高有效位元)。
  - BinLEIBO2Int — 二進制資料依照與 BinLE2Int 相同的方式進行編碼，但會在取出欄位對應進行編碼之前，依照多位元組序列中的反向位元組順序來讀取記憶卡 raw 資料。
  - BinBEIBO2Int — 二進制資料的編碼方式與 BinBE2Int 的相同，但會在取出欄位對應進行編碼之前，依照多位元組序列中的反向位元組順序來讀取記憶卡 raw 資料。

如需有關您的卡片格式使用哪個欄位對應的資訊，請參閱製造商的說明書。

設定服務

[設定] 頁面中的 [設定服務] 用於存取可與門控制器搭配使用之外部服務的設定。

SmartIntego

SmartIntego 是增加門控制器所能處理之門數量的無線解決方案。

SmartIntego 先決條件

繼續進行 SmartIntego 設定之前，需要滿足下列先決條件：

- 必須建立 csv 檔案。csv 檔案包含有關 SmartIntego 解決方案中所用 GatewayNode 和門的資訊。此檔案是在 SimonsVoss 合作夥伴提供的獨立軟體中所建立。
- SmartIntego 的硬體組態已經完成設定，請參閱。

附註

- SmartIntego 設定工具必須是版本 2.1.6452.23485
  組建 2.1.6452.23485 (8/31/2017 1:02:50 PM) 或更新的版本。
- SmartIntego 不支持進階加密標準 (AES)，因此必須在 SmartIntego 設定工具中加以停用。

如何設定 SmartIntego

附註

- 確定已滿足列出的先決條件。
- 為了更清楚顯示電池狀態，請移至 [設定] > [設定事件和警報記錄]，然後新增 [門 — 電池報警] 或 [IdPoint — 電池警報] 做為警報。
- 門禁監控器設定來自匯入的 CSV 檔案。在一般安裝中，您不需要變更此設定。

1. 按一下 [瀏覽...]、選取 csv 檔案，然後按一下 [上傳檔案]。
2. 選取 GatewayNode 並按一下 [下一步]。
3. 新組態的預覽會出現。視需要停用門禁監控器。
4. 按一下 [設定]。
5. 組態中所包含的門的概觀會出現。按一下 [設定] 以個別設定每個門。

如何重新設定 SmartIntego

1. 按一下頂端功能表中的 [設定]。
2. 按一下 [設定服務] > [設定]。
3. 按一下 [重新設定]。
4. 按一下 [瀏覽...]、選取 csv 檔案，然後按一下 [上傳檔案]。
5. 選取 GatewayNode 並按一下 [下一步]。
6. 新組態的預覽會出現。視需要停用門禁監控器。

附註

門禁監控器設定來自匯入的 CSV 檔案。在一般安裝中，您不需要變更此設定。

7. 按一下 [設定]。
8. 組態中所包含的門的概觀會出現。按一下 [設定] 以個別設定每個門。

維護指示

為保持門禁管制系統執行順暢，Axis 建議對門禁管制系統 (門控制器以及連接的裝置) 進行定期維護。

每年至少進行一次維護。建議進行的維護程序包括但不限於下列步驟：

- 確保門禁控制器與外部裝置之間的所有連接都穩固。
- 驗證所有的硬體連接。請參考 。

- 驗證系統 (包括連接的外部裝置) 是否正確運作。

— 刷卡，測試讀卡機、門和門鎖。

— 如果系統包含 REX 裝置、感應器或其他裝置，也要加以測試。

— 如果已啟動，請測試防竄改警報。

如果上述任何步驟的結果都指出故障或意外行為：

— 使用適當的設備測試電線的訊號，並檢查電線或纜線是否有任何損壞情形。

— 更換所有已損壞或故障的纜線和電線。

— 更換纜線和電線之後，就重新驗證所有的硬體連接。請參考 。

- 如果門控制器表現的行為不如預期，請參閱和以取得更多資訊。

事件設定

系統中發生的事件 (例如，使用者刷卡或 REX 裝置啟動時發生的事件) 會記錄在事件記錄中。

- 檢視事件記錄。請參考 。
- 匯出事件記錄。請參考 。
- 設定事件記錄。請參考 。

檢視事件記錄

若要檢視記錄的事件，請移至 [事件記錄]。

若要展開事件記錄中的項目並檢視事件詳細資料，請按一下 ▶。

將過濾器套用至事件記錄，尋找特定事件會變得更輕鬆。若要過濾清單，請選取一個或多個事件記錄過濾器，然後按一下 [套用過濾器]。如需詳細資訊，請參閱 。

身為管理員，您對某些事件可能比對其他事件更感興趣。因此，您可以選擇要記錄哪些事件。如需詳細資訊，請參閱 。

事件記錄過濾器

您可以選取下列其中一個或多個過濾器來縮小事件記錄的範圍：

- 使用者 — 過濾與所選使用者相關的事件。
- 門與樓層 - 過濾與特定門或樓層相關的事件。
- 主題 — 根據事件類型進行過濾。
- 日期和時間 — 依據日期和時間範圍過濾事件記錄。

設定事件記錄

[設定事件記錄] 頁面可讓您定義哪些事件應予記錄。

事件記錄選項

若要定義哪些事件應包含在事件記錄中，請移至 [設定 > 設定事件記錄]。

有下列選項可用於記錄事件：

- 不記錄 — 停用事件記錄。事件不會記入事件記錄或包含在其中。
- 為所有來源記錄 — 啟用事件記錄。事件會記錄下來，並包含在事件記錄中。

如何設定動作規則

事件頁面可讓您設定 Axis 產品，使其在發生不同事件時執行動作。一組定義如何和何時觸發動作的條件即稱為動作規則。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。

如需可用觸發器和動作的詳細資訊，請參閱產品的內建說明。

此範例說明如何設定動作規則，以便在門口遭強行開啟時啟動輸出埠。

1. 移至 [設定 > 其他控制器組態 > 系統選項 > 接埠和裝置 > I/O 連接埠]。
2. 從所需的 [I/O 連接埠類型] 下拉式清單選取 [輸出]，並輸入 [名稱]。
3. 選取 I/O 連接埠的 [正常狀態]，然後按一下 [儲存]。
4. 前往 [事件 > 動作規則]，並按一下 [新增]。
5. 從 [觸發器] 下拉式清單選取 [門]。
6. 從下拉式清單選取 [門禁警報]。

7. 從下拉式清單中選取所需的門。
8. 從下拉式清單選取 [門口遭強行開啟]。
9. (選擇性) 選取 [排程] 和 [附加條件]。請見下文。
10. 在 [動作] 下方，從 [類型] 下拉式清單選取 [輸出埠]。
11. 從 [連接埠] 下拉式清單選取所需的輸出埠。
12. 設定 [作用中] 狀態。
13. 選取 [持續時間] 和 [之後轉為相反狀態]。然後輸入動作所需的持續時間。
14. 按一下OK (確認)。

若要在動作規則中使用多個觸發器，請選取 [附加條件]，然後按一下 [新增] 以加入額外的觸發器。使用附加條件時，所有的條件都必須符合才能觸發動作。

為了避免重複觸發動作，可以設定 [至少等待] 時間。以小時、分鐘和秒為單位，輸入動作規則再次啟動前的間隔時間，如果這段時間未滿，則應忽略觸發器。

如需詳細資訊，請參閱產品的內建說明。

如何新增接收者

此產品可以傳送訊息來通知接收者有關事件和警報的資訊。但是您必須先定義一個或多個接收者，才能讓產品傳送通知訊息。如需可用選項的詳細資訊，請參閱。

若要新增接收者：

1. 移至 [設定 > 其他控制器組態 > 事件 > 接收者]，然後按一下 [新增]。
2. 輸入描述性名稱。
3. 選取接收者類型。
4. 輸入接收者類型所需的資訊。
5. 按一下 [測試] 以測試與接收者的連線。
6. 按一下OK (確認)。

如何設定電子郵件收件者

可以選取其中一個列出的電子郵件供應商，或指定使用的 (例如，公司電子郵件伺服器使用的) SMTP 伺服器、連接埠和驗證，來設定電子郵件收件者。

附註

部分電子郵件供應商設有安全過濾器，可防止使用者接收或檢視大量附件，或接收排程的電子郵件和類似訊息。檢查電子郵件供應商的安全性政策，以避免發生傳遞問題和電子郵件帳戶鎖定。

若要使用其中一個列出的供應商來設定電子郵件收件者：

1. 移至 [事件 > 接收者]，然後按一下 [新增]。
2. 輸入名稱，並從 [類型] 清單選取 [電子郵件]。
3. 在 [收件者] 欄位中輸入要將電子郵件傳送到的電子郵件地址。使用逗號分隔多個地址。
4. 從 [供應商] 清單選取電子郵件供應商。
5. 輸入電子郵件帳戶的使用者 ID 和密碼。
6. 按一下 [測試] 以傳送測試電子郵件。

例如，要使用公司電子郵件伺服器來設定電子郵件收件者，請依照上述指示操作，但選取 [使用者定義] 做為 [供應商]。輸入電子郵件地址以顯示為 [寄件者] 欄位中的傳送者。選取 [進階設定]，並指定 SMTP 伺服器位址、連接埠和驗證方法。(選擇性) 選取 [使用加密] 以透過加密的連線傳送電子郵件。可以使用 Axis 產品中提供的憑證來驗證伺服器憑證。如需有關如何上傳憑證的詳細資訊，請參閱。

如何建立排程

預約排程可以當做動作規則觸發器或附加條件使用。如下所述，使用其中一個預先定義的排程，或建立新的排程。

若要建立新的排程：

1. 移至 [設定 > 其他控制器組態 > 事件 > 排程]，然後按一下 [新增]。
2. 輸入描述性名稱，以及每日、每週、每月或每年排程所需的資訊。
3. 按一下OK (確認)。

若要在動作規則中使用排程，請從 [動作規則設定] 頁面的 [排程] 下拉式清單中選取排程。

如何設定循環週期

循環週期用於重複觸發動作規則，例如每 5 分鐘或每小時一次。

若要設定循環週期：

1. 移至 [設定 > 其他控制器組態 > 事件 > 接收者]，然後按一下 [循環週期]。
2. 輸入描述性名稱和循環模式。
3. 按一下OK (確認)。

若要在動作規則中使用循環週期，請先從 [動作規則設定] 頁面的 [觸發器] 下拉式清單中選取 [時間]，然後從第二個下拉式清單選取循環模式。

若要修改或移除循環週期，請選取 [循環週期清單] 中的循環週期，然後按一下 [修改] 或 [移除]。

讀卡機反饋

讀卡機使用 LED 和蜂鳴器向使用者 (進入門或嘗試進入門的人) 發送反饋訊息。門控制器可以觸發幾則反饋訊息，有些是在門控制器中預先設定，大多數讀卡機都有支援。

讀卡機有不同的 LED 行為，但通常都會使用紅色、綠色和琥珀色的不同恒亮燈號與閃爍燈號序列。

讀卡機還可以使用單音蜂鳴器，藉由不同序列的短與長蜂鳴器訊號來發送訊息。

下表顯示門禁控制器中預先設定的事件，這些事件可觸發讀卡機反饋及其一般讀卡機反饋訊號。AXIS 讀卡機的反饋訊號會在 AXIS 讀卡機隨附的安裝指南中做說明。

[事件]	Wiegand 雙 LED	Wiegand 單 LED	OSDP	蜂鳴器模式	狀態
閒置[1]	關閉	紅色	紅色	無訊息	一般
要求輸入PIN	閃爍紅色/綠色	閃爍紅色/綠色	閃爍紅色/綠色	兩短嗶聲	需要 PIN
授予存取權	綠色	綠色	綠色	嗶聲	已允許進入
已拒絕進入	紅色	紅色	紅色	嗶聲	已拒絕進入

上述以外的反饋訊息必須是由用戶端 (例如門禁管理系統) 透過 VAPIX® 應用程式開發介面所設定，該用戶端支援此功能並使用可提供所需訊號的讀卡機。如需詳細資訊，請參閱門禁管理系統開發商和讀卡機製造商提供的使用者資訊。

1. 當門關閉且門上鎖時進入閒置狀態。

系統選項

安全

使用者

使用者存取控制預設為啟用狀態，並且可在 [設定 > 其他控制器組態 > 系統選項 > 安全性 > 使用者] 底下進行設定。管理員可以提供使用者名稱和密碼來設定其他使用者。

使用者清單會顯示授權使用者和使用者群組 (存取層級)：

- 管理員可以存取所有設定而不受限制。管理員可以新增、修改和移除其他使用者。

附註

請注意，選取 [加密和未加密] 選項時，網頁伺服器會對密碼進行加密。這是新裝置或已重設為出廠預設設定之裝置的預設選項。

在 [HTTP/RTSP 密碼設定] 下方，選取要允許的密碼類型。如果有不支援加密的檢視用戶端，或如果您已升級韌體，而現有用戶端支援加密但需要重新登入並已設定為使用此功能時，您可能需要允許未加密的密碼。

ONVIF

ONVIF 是一個開放式產業論壇，旨在提供並推廣標準化介面，讓 IP 型實體保全產品可以有效互通。

您只要建立使用者，就會自動啟用 ONVIF 通訊。使用者名稱和密碼適用於所有與產品相關的 ONVIF 通訊。如需詳細資訊，請參閱 *www.onvif.org*

IP 位址過濾

IP 位址過濾可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Security (安全性) > IP Address Filter (IP 位址過濾)] 頁面上啟用。啟用後，就會允許或拒絕列出的 IP 位址存取 Axis 產品。從清單選取 [允許] 或 [拒絕]，然後按一下 [套用] 以啟用 IP 位址過濾。

管理員可以最多將 256 個 IP 位址項目新增至清單 (單一項目可以包含多個 IP 位址)。

HTTPS

HTTPS (安全超文本傳輸協定，也就是基於 SSL 的 HTTP) 是一種提供加密瀏覽的網頁通訊協定。使用者和用戶端也能使用 HTTPS 來驗證所存取設備的正確性。HTTPS 提供的安全等級一般認為適用於大多數商業交易。

Axis 產品可以設定成會在管理員登入時要求使用 HTTPS。

若要使用 HTTPS，必須先安裝 HTTPS 憑證。前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Security (安全性) > Certificates (憑證)] 以安裝和管理憑證。請參考 。

若要在 Axis 產品上啟用 HTTPS：

1. 移至 [設定 > 其他控制器組態 > 系統選項 > 安全性 > HTTPS]
2. 從已安裝的憑證清單中選取 HTTPS 憑證。
3. (選擇性) 按一下 [密碼]，並選擇要用於 SSL 的加密算法。
4. 設定不同使用者群組的 [HTTPS 連線政策]。
5. 按一下 [儲存] 即可啟用設定值。

若要透過所需的通訊協定存取 Axis 產品，請在瀏覽器的網址欄位中輸入 `https://` 代表 HTTPS 協定，以及 `http://` 代表 HTTP 協定。

HTTPS 連接埠可在 [系統選項 > 網路 > TCP/IP > 進階] 頁面下進行變更。

IEEE 802.1X

IEEE 802.1X 是一種連接埠型網路存取控制 (Network Admission Control) 的標準，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，必須對裝置進行驗證。驗證是由驗證伺服器 (通常為 RADIUS 伺服器) 執行，例如 FreeRADIUS 和 Microsoft Internet Authentication Server 即是。

在 Axis 實作中，Axis 產品和驗證伺服器使用 EAP-TLS (可延伸的驗證通訊協定 - 傳輸層安全性)，透過數位憑證來識別本身的身分。憑證由憑證授權單位 (CA) 提供。您需要：

- 用於對驗證伺服器進行驗證的 CA 憑證。
- 用於驗證 Axis 產品的 CA 簽署的用戶端憑證。

若要建立和安裝憑證，請前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Security (安全性) > Certificates (憑證)]。請參考 。

若要允許產品存取受 IEEE 802.1X 保護的網路：

1. 移至 [設定 > 其他控制器組態 > 系統選項 > 安全性 > IEEE 802.1X]。
2. 從已安裝的憑證清單中選取 [CA 憑證] 和 [用戶端憑證]。
3. 在 [設定] 下方，選取 EAPOL 版本，並提供與用戶端憑證相關聯的 EAP 身分識別。
4. 勾選方塊以啟用 IEEE 802.1X，並按一下 [儲存]。

附註

若要讓驗證正常運作，Axis 產品中的日期和時間設定必須與 NTP 伺服器同步。請參考 。

憑證

憑證會用來驗證網路上的裝置。一般應用程式會包含加密的網頁瀏覽功能 (HTTPS)、透過 IEEE 802.1X 進行網路保護，以及透過電子郵件等方式提供通知訊息。可搭配 Axis 產品使用的憑證有兩種：

伺服器/用戶端憑證 - 用於驗證 Axis 產品。伺服器/用戶端憑證可以自我簽署，或由憑證授權單位 (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 - 可在 Axis 產品連線至受 IEEE 802.1X 保護的網路的情況下驗證對等的憑證，例如驗證伺服器的憑證。Axis 產品隨附數個預先安裝的 CA 憑證。

附註

- 如果將產品重設為出廠預設值，則除了預先安裝的 CA 憑證以外，所有的憑證都會遭到刪除。
- 如果將產品重設為出廠預設值，則會重新安裝所有已遭刪除的預先安裝 CA 憑證。

如何建立自我簽署的憑證

1. 前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Security (安全性) > Certificates (憑證)]。
2. 按一下 [建立自我簽署的憑證] 並提供所需的資訊。

如何建立和安裝 CA 簽署的憑證

1. 建立自我簽署的憑證，請參閱。
2. 前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Security (安全性) > Certificates (憑證)]。
3. 按一下 [建立憑證簽署要求] 並提供所需的資訊。
4. 複製 PEM 格式的要求，並傳送至您選擇的 CA。
5. 傳回已簽署的憑證時，按一下 [安裝憑證] 並上傳憑證。

如何安裝額外的 CA 憑證

1. 前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Security (安全性) > Certificates (憑證)]。
2. 按一下 [安裝憑證] 並上傳憑證。

網路

基本 TCP/IP 設定

Axis 產品支援 IP 版本 4 (IPv4) 和 IP 版本 6 (IPv6)。

Axis 產品可以透過下列方式取得 IP 位址：

- 動態 IP 位址 — 預設會選取 [透過 DHCP 取得 IP 位址]。這表示 Axis 產品已設定為透過動態主機設定通訊協定 (DHCP) 自動取得 IP 位址。
  DHCP 可讓網路管理員集中管理並自動化 IP 位址指派。
- 固定 IP 位址 — 若要使用固定 IP 位址，請選取 [使用下列 IP 位址]，並指定 IP 位址、子網路遮罩和預設路由器。然後按一下 [儲存]。

只有在使用動態 IP 位址通知時才應啟用 DHCP，如果 DHCP 可以更新 DNS 伺服器，就可以透過名稱 (主機名稱) 存取 Axis 產品。

如果啟用了 DHCP 但無法存取產品，請執行 AXIS IP Utility 以在網路中搜尋連接的 Axis 產品，或者將產品重設為出廠預設設定，然後重新執行安裝。如需有關如何重設為出廠預設設定的詳細資訊，請參閱。

AXIS 影像代管系統 (AVHS)

與 AVHS 服務搭配使用的 AVHS，可讓您輕鬆且安全地從任何位置透過網際網路存取控制器管理和記錄。如需有關尋找當地 AVHS 服務供應商的詳細資訊和說明，請前往 www.axis.com/hosting

AVHS 設定可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP IP > Basic (基本)] 底下進行設定。預設會啟用適合連線至 AVHS 服務的可能情況。若要停用，請清除 [啟用 AVHS] 方塊。

單鍵啟用 - 按住產品的控制按鈕 (請參閱) 約 3 秒鐘，以透過網際網路連線至 AVHS 服務。註冊後，就會啟用 [永遠]，而且 Axis 產品會與 AVHS 服務保持連線。如果產品未在按下按鈕後 24 小時內註冊，則產品會中斷與 AVHS 服務的連線。

永遠 - Axis 產品將會不斷嘗試透過網際網路連線至 AVHS 服務。註冊後，產品就會與服務保持連線。當產品已安裝，但不方便或無法使用單鍵安裝時，可以使用此選項。

附註

AVHS 支援取決於服務供應商的訂閱可用性。

AXIS 網際網路動態 DNS 服務

AXIS 網際網路動態 DNS 服務會指派主機名稱，以方便存取產品。如需更多資訊，請參閱 *www.axiscam.net*

若要向 AXIS 網際網路動態 DNS 服務註冊 Axis 產品，請前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Basic (基本)]。在 [服務] 下方，按一下 AXIS 網際網路動態 DNS 服務的 [設定] 按鈕 (需要存取網際網路)。隨時都可以移除產品目前在 AXIS 網際網路動態 DNS 服務中註冊的網域名稱。

附註

AXIS 網際網路動態 DNS 服務需要 IPv4。

進階 TCP/IP 設定

DNS 組態

DNS (網域名稱服務) 提供主機名稱的 IP 位址轉譯。DNS 設定可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)] 底下進行設定。

選取 [透過 DHCP 取得 DNS 伺服器位址]，以使用 DHCP 伺服器所提供的 DNS 設定。

若要進行手動設定，請選取 [使用下列 DNS 伺服器位址]，並指定下列資料：

網域名稱 - 輸入網域以搜尋 Axis 產品所使用的主機名稱。可以使用分號來分隔多個網域。主機名稱永遠為完整網域名稱的第一部分；例如，`myserver` 是完整網域名稱 `myserver.mycompany.com` 的主機名稱，其中 `mycompany.com` 是網域名稱。

主要/次要 DNS 伺服器 - 輸入主要和次要 DNS 伺服器的 IP 位址。次要 DNS 伺服器是可選的，如果沒有主要 DNS 伺服器可用，則使用該伺服器。

NTP 組態

NTP (網路時間通訊協定) 用於同步網路中裝置的時鐘時間。NTP 設定可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)] 底下進行設定。

選取 [透過 DHCP 取得 NTP 伺服器位址]，以使用 DHCP 伺服器所提供的 NTP 設定。

若要進行手動設定，請選取 [使用下列 NTP 伺服器位址]，並輸入 NTP 伺服器的主機名稱或 IP 位址。

主機名稱組態

您可以使用主機名稱而不使用 IP 位址來存取 Axis 產品。主機名稱通常與指派的 DNS 名稱相同。主機名稱可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)] 底下進行設定。

選取 [透過 IPv4 DHCP 取得主機名稱] 以使用在 IPv4 上執行的 DHCP 伺服器所提供的主機名稱。

選取 [使用主機名稱] 手動設定主機名稱。

選取 [啟用動態 DNS 更新]，使得只要 Axis 產品的 IP 位址變更，就動態更新本機 DNS 伺服器。如需詳細資訊，請參閱線上說明 。

連結本機 IPv4 位址

[連結本機位址] 預設為啟用狀態，並且會將額外的 IP 位址指派給 Axis 產品，這可用來從區域網路中同一區段上的其他主機存取產品。該產品可以同時具有連結本機 IP 以及靜態或 DHCP 提供的 IP 位址。

此功能可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)] 底下加以停用。

HTTP

Axis 產品所使用的 HTTP 連接埠可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)] 底下進行變更。除了預設設定 (也就是 80) 之外，還可以使用任何在 1024-65535 範圍內的連接埠。

HTTPS

Axis 產品所使用的 HTTPS 連接埠可在 [設定 > 其他控制器組態 > 系統選項 > 網路 > TCP/IP > 進階] 底下進行變更。除了預設設定 (也就是 443) 之外，還可以使用任何在 1024-65535 範圍內的連接埠。

若要啟用 HTTPS，請前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Security (安全性) > HTTPS]。如需更多資訊，請參閱 。

IPv4 的 NAT 周遊 (連接埠對應)

網路路由器可讓私人網路 (LAN) 上的裝置共用單一網際網路連線。這是藉由將網路流量從私人網路轉發至「外部」(即網際網路) 來完成。由於大多數路由器都已預先設定為阻止嘗試從公用網路 (網際網路) 存取私人網路 (LAN)，因此提高了私人網路 (LAN) 的安全性。

當 Axis 產品位於內部網路 (LAN)，而您想要讓產品可從 NAT 路由器的另一端 (WAN) 存取時，請使用 NAT 周遊。正確設定 NAT 周遊後，所有在 NAT 路由器中流向外部 HTTP 連接埠的 HTTP 流量都會轉發至產品。

NAT 周遊可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)] 底下進行設定。

附註

- 若要讓 NAT 周遊功能運作，路由器必須支援此功能。路由器也必須支援 UPnP®。
- 在此情境中，路由器是指任何網路路由裝置，例如 NAT 路由器、網路路由器、網際網路閘道、寬頻路由器、寬頻分享裝置，或是像防火牆這樣的軟體。

啟用/停用 - 啟用後，Axis 產品將嘗試透過 UPnP 在您的網路中設定 NAT 路由器的連接埠對映。請注意，必須在產品中啟用 UPnP (請參閱 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > UPnP])。

使用手動選取的 NAT 路由器 - 選取此選項可手動選擇 NAT 路由器，並在欄位中輸入路由器的 IP 位址。如果未指定路由器，產品就會自動搜尋網路上的 NAT 路由器。如果找到多個路由器，則選擇預設路由器。

備用 HTTP 連接埠 - 選取此選項可手動定義外部 HTTP 連接埠。輸入 1024—65535 範圍內的連接埠。如果連接埠欄位空白或包含預設設定 (也就是 0)，則會在啟用 NAT 周遊時自動選擇連接埠號碼。

附註

- 即使 NAT 周遊已停用，還是可以使用或啟用備用 HTTP 連接埠。如果您的 NAT 路由器不支援 UPnP，而您需要在 NAT 路由器中手動設定連接埠轉發時，這會很有用。
- 如果您嘗試手動輸入已在使用中的連接埠，則自動選擇其他可用的連接埠。
- 自動選擇連接埠後，連接埠會顯示在此欄位中。若要變更此設定，請輸入新的連接埠號碼，並按一下 [儲存]。

FTP

Axis 產品中執行的 FTP 伺服器支援上傳新韌體、使用者應用程式等檔案。FTP 伺服器可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > TCP/IP > Advanced (進階)] 底下加以停用。

RTSP

Axis 產品中執行的 RTSP 伺服器允許連線中用戶端啟動事件串流。RTSP 連接埠號碼可在 [設定 > 其他控制器組態 > 系統選項 > 網路 > TCP/IP > 進階] 底下進行變更。預設連接埠為 554。

附註

如果停用 RTSP 伺服器，則事件串流將無法使用。

SOCKS

SOCKS 是網路 Proxy 通訊協定。Axis 產品可以設定為使用 SOCKS 伺服器連線至防火牆或 Proxy 伺服器另一端的網路。如果 Axis 產品位於防火牆後面的網路，並且需要將通知、上傳項目、警報等內容傳送至區域網路以外的目的地 (例如網際網路)，則此功能相當實用。

SOCKS 可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > SOCKS] 底下進行設定。如需詳細資訊，請參閱線上說明。

QoS (服務品質)

QoS (服務品質) 保證網路上所選流量的指定資源達到特定等級。QoS 感知網路透過控制應用程式所能使用的頻寬量，決定處理網路流量的優先順序，並提供更高的網路可靠性。

QoS 設定可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > QoS] 底下進行設定。使用 DSCP (差異化服務代碼點) 值，Axis 產品可以標記事件/警報流量和管理流量。

SNMP

簡易網路管理通訊協定 (SNMP) 允許遠端管理網路裝置。SNMP 群體是執行 SNMP 的設備和管理站群組。群體名稱用於辨識群組。

若要啟用和設定 Axis 產品中的 SNMP，請前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > SNMP] 頁面。

根據所需的安全等級，選取要使用的 SNMP 版本。

Axis 產品使用設陷，在發生重要事件或狀態變更時將訊息傳送至管理系統。勾選 [啟用設陷]，然後輸入應傳送設陷訊息的 IP 位址，以及應接收訊息的設陷社群。

附註

如果 HTTPS 已啟用，則應停用 SNMP v1 和 SNMP v2c。

Axis 產品使用 SNMP v1/v2 設陷，在發生重要事件或狀態變更時將訊息傳送至管理系統。勾選 [啟用設陷]，然後輸入應傳送設陷訊息的 IP 位址，以及應接收訊息的設陷社群。

您可以使用下列設陷：

- 冷啟動
- 暖啟動
- 上行連結
- 驗證失敗

SNMP v3 提供加密和安全密碼。若要與 SNMP v3 搭配使用設陷，必須有 SNMP v3 管理應用程式。

若要使用 SNMP v3，必須啟用 HTTPS，請參閱。若要啟用 SNMP v3，請勾選方塊並提供初始使用者密碼。

附註

初始密碼只能設定一次。如果密碼遺失，則必須將 Axis 產品重設為出廠預設值，請參閱。

UPnP

Axis 產品包含對 UPnP® 的支援。UPnP 預設為啟用狀態，而且支援此通訊協定的作業系統及用戶端會自動偵測該產品。

UPnP 可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > UPnP] 底下加以停用。

Bonjour

Axis 產品包含對 Bonjour 的支援。Bonjour 預設為啟用狀態，而且支援此通訊協定的作業系統及用戶端會自動偵測該產品。

Bonjour 可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Network (網路) > Bonjour] 底下加以停用。

連接埠和裝置

I/O埠

輔助連接器提供四個可設定的輸入埠和輸出埠，用於連接外部裝置。

外部連接器提供兩個可設定的輸入埠和輸出埠，用於連接外部裝置。

您可以在 [設定 > 其他控制器組態 > 系統選項 > 連接埠和裝置 > I/O 埠] 底下設定 I/O 埠。選取連接埠方向 ([輸入] 或 [輸出])。您可以為連接埠提供描述性名稱，而其 [正常狀態] 則可設定為 [開路] 或 [接地電路]。

連接埠狀態

[系統選項 > 連接埠和裝置 > 連接埠狀態] 頁面上的清單會顯示產品輸入埠和輸出埠的狀態。

維護

Axis 產品提供多項維護功能。這些功能可在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Maintenance (維護)] 底下找到。

如果 Axis 產品表現的行為不如預期，請按一下 [重新啟動] 執行正確的重新啟動。這對目前任何設定都不造成影響。

附註

重新啟動會清除伺服器報告中的所有項目。

按一下 [重新還原]，將大多數設定重設為出廠預設值。下列設定不受影響：

- 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
- 系統時間
- IEEE 802.1X 設定

按一下 [預設]，將所有設定 (包括 IP 位址) 都重設為出廠預設值。此按鈕應謹慎使用。還可以使用控制按鈕將 Axis 產品重設為出廠預設值，請參閱。

如需韌體升級的詳細資訊，請參閱。

支援

支援概觀

如果您需要技術協助，[Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Support (支援) > Support Overview (支援概觀)] 頁面有提供故障排除及聯絡資訊的相關資訊。

另請參閱 。

系統概觀

若要取得 Axis 產品狀態及設定的概觀，請移至 [設定 > 其他控制器組態 > 系統選項 > 支援 > 系統概觀]。可在其中找到的資訊包括韌體版本、IP 位址、網路和安全性設定、事件設定以及最近的記錄項目。

記錄與報告

[Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Support (支援) > Logs & Reports (記錄與報告)] 頁面會產生對系統分析和故障排除有用的記錄與報告。如果要聯絡 Axis 支援，請提供伺服器報告與您的問題。

系統記錄 - 提供有關系統事件的資訊。

存取記錄 - 列出所有存取產品失敗的事件。存取記錄也可以設定為列出所有與產品的連線 (見下文)。

檢視伺服器報告 - 在快顯視窗中提供有關產品狀態的資訊。存取記錄會自動包含在伺服器報告中。

下載伺服器報告 - 建立 .zip 檔案，其中包含 UTF—8 格式的完整伺服器報告文字檔。選取 [包含即時影像的快照] 選項，以包含產品即時影像的快照。聯絡支援人員時，請務必附上伺服器報告 .zip 檔案。

參數清單 - 顯示產品的參數以及其目前的設定。這可能會在故障排除或聯絡 Axis 支援時派上用場。

連線清單 - 列出目前正在存取媒體串流的所有用戶端。

當機報告 - 產生包含除錯資訊的存檔。報告需要幾分鐘才能產生。

系統及存取記錄的記錄層級是在 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Support (支援) > Logs & Reports (記錄與報告) > Configuration (組態)] 底下進行設定。存取記錄可以設定為列出所有與產品的連線 (選取 [嚴重]、[警告] 和 [資訊])。

進階

指令碼

編寫指令碼可讓有經驗的使用者自訂和使用他們自己的指令碼。

注意

使用不當可能會造成意想不到的行為，並與 Axis 產品失去聯繫。

Axis 強烈建議，除非您了解後果，否則不要使用此功能。Axis 支援對於自訂指令碼的問題，不提供協助。

若要開啟指令碼編輯器，請前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Advanced (進階) > Scripting (指令碼)]。如果指令碼造成問題，請將產品重設為出廠預設設定，請參閱。

如需詳細資訊，請參閱 *www.axis.com/developer*

檔案上傳

檔案 (例如網頁和影像) 可以上傳至 Axis 產品，並當做自訂設定使用。若要上傳檔案，請前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > System Options (系統選項) > Advanced (進階) > File Upload (檔案上傳)]。

上傳的檔案可透過 `http://<ip address>/local/<user>/<file name>` 來存取，其中 `<user>` 是上傳檔案的選定使用者群組 (管理員)。

故障排除

重設為出廠預設設定

重要

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

若要將產品重設為出廠預設設定：

1. 將產品斷電。
2. 按住控制按鈕，同時重新接通電源。請參考 。
3. 繼續按住控制按鈕 25 秒，直到狀態 LED 指示燈第二次變成琥珀色。
4. 放開控制按鈕。當狀態LED指示燈轉變成綠色時，即完成重設程序。產品已重設為出廠預設設定。如果網路中沒有可用的 DHCP 伺服器，預設的 IP 位址會是 `192.168.0.90`。
5. 使用安裝與管理軟體工具來指派 IP 位址、設定密碼，並存取產品。

您也可以透過網頁介面將參數重設為出廠預設值。前往 [Setup (設定) > Additional Controller Configuration (其他控制器組態) > Setup (設定) > System Options (系統選項) > Maintenance (維護)]，然後按一下 [Default (預設)]。

如何檢查目前的韌體

韌體是決定網路裝置所具功能的軟體。對問題進行疑難排解時，首先要採取的其中一項行動就是檢查目前的韌體版本。最新版本可能包含解決特定問題的修正檔案。

Axis 產品目前的韌體版本會顯示在 [概觀] 頁面中。

如何升級韌體

重要

- 您的經銷商保留收取任何可歸因於使用者升級錯誤所產生維修費用的權利。
- 升級韌體時會儲存預先設定和自訂的設定 (假如新韌體中有提供這些功能)，但並非必然發生，Axis Communications AB 對此概不承擔責任。
- 如果您安裝先前的韌體版本，此後就必須將產品還原為出廠預設設定。

附註

- 完成升級程序之後，產品會自動重新啟動。如果在升級後手動重新啟動產品，即使您認為升級可能已失敗，仍請稍待 5 分鐘。
- 由於使用者、群組、認證及其他資料的資料庫會在韌體升級後更新，因此初次啟動可能需要幾分鐘才能完成。所需時間取決於資料量。
- 當您使用最新韌體升級 Axis 產品時，產品會獲得最新的可用功能。升級韌體之前，請務必閱讀每個新版本所提供的升級指示和版本資訊。

1. 將最新的韌體檔案下載到您的電腦，檔案可從 *www.axis.com/support* 免費取得
2. 移至產品網頁中的 [設定 > 其他控制器組態 > 系統選項 > 維護]。
3. 在 [升級伺服器] 下方，按一下 [選擇檔案]，並在電腦上找到檔案。
4. 如果您希望產品在升級後自動還原為出廠預設設定，請勾選 [預設] 核取方塊。
5. 按一下 [升級]。
6. 等待約 5 分鐘，讓產品進行升級並重新啟動。然後清除網頁瀏覽器的快取。
7. 存取產品。

徵兆、可能原因和補救動作

升級韌體時發生問題

韌體升級失敗	如果韌體升級失敗，則產品會重新載入之前的韌體。檢查韌體檔案並重試。

設定 IP 位址時發生問題

使用 ARP/Ping 時	重新嘗試安裝。IP 位址必須在產品接通電源後兩分鐘內設定。確定 Ping 長度已設定為 408。如需相關指示，請參閱產品頁面上的安裝指南，網址為 *axis.com*。
產品位於不同的子網路	如果用於產品的 IP 位址以及存取產品所用電腦的 IP 位址位在不同的子網路，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 產品與網路的連接。執行 Ping 命令 (在命令/DOS 視窗中，輸入 `ping` 以及產品的 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，然後重新安裝產品。 • 如果您收到：`Request timed out`，這表示此 IP 位址可供 Axis 產品使用。檢查所有接線，然後重新安裝產品。
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 產品中的固定 IP 位址。這表示，如果另一個產品也使用同一個預設的固定 IP 位址，則存取該產品可能會發生問題。

無法從瀏覽器存取產品

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`。 如果遺失使用者 root 的密碼，則必須將產品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，在網路上尋找產品。使用產品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，請參閱產品頁面 (axis.com) 上的*如何指派 IP 位址及存取您的裝置*文件
使用 IEEE 802.1X 時的憑證錯誤	若要讓驗證正常運作，Axis 產品中的日期和時間設定必須與 NTP 伺服器同步。請參考 。

產品可在本機加以存取，但無法從外部存取

路由器組態	若要設定路由器讓資料流量可以傳入至 Axis 產品，請啟用 NAT 周遊功能，此功能會嘗試自動設定路由器以允許存取 Axis 產品，請參閱。路由器必須支援 UPnP®。
防火牆保護	向網路管理員洽詢網際網路防火牆。
需要預設路由器	從 [設定 > 網路設定] 或 [設定 > 其他控制器組態 > 系統選項 > 網路 > TCP/IP > 基本] 中檢查是否需要設定路由器設定。

規格

有 UL 標示的文字僅適用於 UL 293 或 UL 294 安裝。

LED 指示燈

LED	彩色	指示
網路	綠色	常亮表示已連線到 100 MBit/s 網路。閃爍表示有網路活動。
	黃色	常亮表示已連線到 10 MBit/s 網路。閃爍表示有網路活動。
	熄滅	無網路連線。
狀態	綠色	綠燈常亮表示正常操作。
	黃色	在啟動和還原設定時保持常亮。
	紅色	緩慢閃爍表示升級失敗。
電源	綠色	正常運作。
	黃色	升級韌體時綠色/琥珀色交替閃爍。
繼電器過電流	紅色	短路或偵測到過電流時常亮。
	熄滅	正常運作。
讀卡機過電流	紅色	短路或偵測到過電流時常亮。
	熄滅	正常運作。
繼電器	綠色	繼電器啟動。[2]
	熄滅	繼電器未啟用。

附註

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

按鈕

控制按鈕

控制按鈕用於：
- 將產品重設為出廠預設設定。請參考 。

接頭

網路接頭

支援增強型乙太網路供電 (PoE+) 的 RJ45 乙太網路接頭。

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

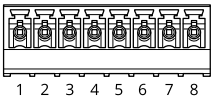
讀卡機接頭

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

2. *COM* 連到 *NO* 時繼電器啟動。

兩個讀卡機連接埠之間共用指定的功率輸出值。這表示會為所有連接至門控制器的讀卡機保留 486 mA (12 V DC)。

在產品網頁中選取要使用的通訊協定。



對 RS485 進行設定

功能	針腳	附註	規格
DC 接地 (GND)	1		0 V DC
DC 輸出（+12 V）	2	為讀卡機供電。	12 V DC，最大 486 mA (兩個讀卡機合計)
RX/TX	3—4	全雙工：RX。半雙工：RX/TX。	
TX	5—6	全雙工：TX。	
可設定 (輸入或輸出)	7—8	數位輸入 — 連接到接腳 1 以啟用，或浮接 (不連接) 以停用。	0 到最大 30 V DC
		數位輸出 — 如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。	0 到最大 30 V DC，漏極開路，100 mA

重要

- 讀卡機由控制器供電時，最多可支援的纜線長度達 200 公尺 (656 英呎)。
- 讀卡機不由控制器供電時，若電纜符合1條AWG 24，120歐姆阻抗電屏雙絞線的要求，讀卡機允許數據線最長可達 1000 公尺（3280.8 英尺）：

對 Wiegand 進行設定

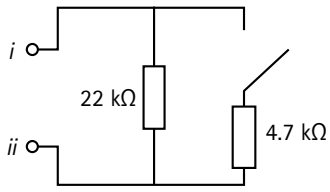
功能	針腳	附註	規格
DC 接地 (GND)	1		0 V DC
DC 輸出（+12 V）	2	為讀卡機供電。	12 V DC，最大 486 mA (兩個讀卡機合計)
D0	3		
D1	4		
O	5—6	數位輸出，漏極開路	
可設定 (輸入或輸出)	7—8	數位輸入 — 連接到接腳 1 以啟用，或浮接 (不連接) 以停用。	0 到最大 30 V DC
		數位輸出 — 如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。	0 到最大 30 V DC，漏極開路，100 mA

重要

- 讀卡機由控制器供電時，最多可支援的纜線長度達 150 公尺 (500 英呎)。
- 讀卡機不由控制器供電時，若電纜符合AWG 22的要求，讀卡機允許數據線最長可達 150 公尺（500 英尺）。

受監控的輸入

若要使用受監控的輸入，請根據下圖安裝線路終端電阻器。



i 輸入

ii 0 V DC (-)

UL：受監控的輸入未經 UL 評估用於防止入室盜竊。只有門禁監控器和 REX 支援使用線路終端電阻器進行監控。

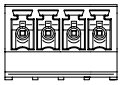
附註

建議使用雙絞線和屏蔽線。將屏蔽裝置連接至 0 V DC。

門組接頭

兩組用於門禁監控裝置的 4 針接線端子 (數位輸入)。

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



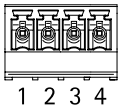
功能	針腳	附註	規格
DC 接地	1, 3		0 V DC
輸入	2, 4	用於與門禁監視器通訊。 數位輸入監督式輸入：分別連到 PIN 1 或 3 啟動，浮接（不連線）停用。	0 到最大 30 V DC

重要

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

繼電器接頭

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



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

繼電器電源跳線

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

這可用於連接 GND 與 NO 之間或 GND 與 NC 針腳之間的鎖。

電源	最大功率，於 12 V DC[3]	最大功率，於 24 V DC[3]
DC IN	1600 mA	800 mA
PoE	800 mA	400 mA

注意

如果門鎖無極性，建議您加裝一個外接續流二極體。

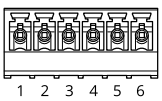
輔助連接器

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

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

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

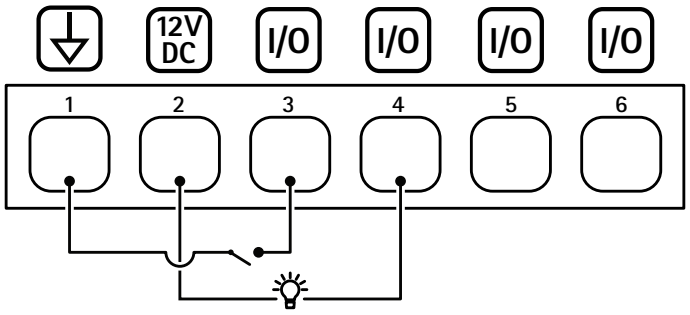
6 針接線端子



功能	針腳	附註	規格
DC 接地	1		0 V DC
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 V DC 最大負載 = 每個 I/O 各 50 mA
可設定 (輸入或輸出)	3—6	數位輸入 — 連接到接腳 1 以啟用，或浮接 (不連接) 以停用。	0 到最大 30 V DC

3. 電力由兩個繼電器及*AUX I/O 12 V DC*共享。

		數位輸出 — 作用中時，內部會連接到針腳 1 (DC 接地)，非作用中時為浮接 (不連接)。如果用於電感性負載 (例如繼電器)，請連接一個二極體與負載並聯，以防止瞬態電壓。如果使用內部 12 V DC 輸出 (針腳 2)，則每個 I/O 都可以驅動 12 V DC、50 mA (最大) 外部負載。如果將漏極開路連接與外部電源供應器搭配使用，則 I/O 可以管理 0—30 V DC、100 mA 的 DC 電源。	0 到最大 30 V DC，漏極開路，100 mA

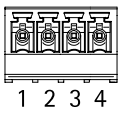


1 *DC 接地*
2 *DC 輸出 12 V*
3 *I/O 設定為輸入*
4 *I/O 設定為輸出*
5 *可設定的 I/O*
6 *可設定的 I/O*

外部連接器

用於外部裝置的 4 針接線端子，例如玻璃破碎偵測器或火災探測器。

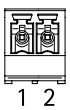
UL：接頭未經 UL 防盜火警用評估。



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

電源接頭

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



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

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

備用電池輸入連接器

適用於內建充電器的備用方案。12 V DC 輸入。

UL：接頭未經 UL 評估。

重要

使用電池輸入時，必須串聯外接 3A 慢熔保險絲。

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

安全資訊

危險等級

⚠ 危險
表示如果不避免，此危險情況會導致死亡或嚴重傷害。

⚠ 警告
表示如果不避免，此危險情況可能導致死亡或嚴重傷害。

⚠ 小心
表示如果不避免，此危險情況可能導致輕度或中度傷害。

注意
表示如果不避免，此情況可能導致財產損壞。

其他訊息等級

重要
表示是產品正常運作所不可缺少的重要資訊。

附註
表示是能充分發揮產品功能的實用資訊。

網頁介面

在網頁瀏覽器中輸入該設備的 IP 位址，就可連上該設備的網頁介面。

附註

本節內容僅適用於搭配 AXIS Camera Station Secure Entry 韌體的 AXIS A1601 Network Door Controller 網路門禁控制器。

顯示或隱藏主功能表。

存取版本須知。

存取產品說明。

變更語言。

設定淺色或深色主題。

使用者功能表包含：

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

內容功能表包含：

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

狀態

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 OS 版本和序號等資訊。

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

裝置

警報

設備位移：開啟以在偵測到設備移動時觸發系統警報。

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

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

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

周邊設備

讀卡機

新增讀卡機：按一下可新增讀卡機。

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

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

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

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

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

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

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

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

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

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

無線鎖

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

附註

您必須將 AH30 通訊集線器安裝在安全側。

連接通訊集線器：按一下可連接無線鎖。

升級

升級讀卡機：按一下可升級讀卡機軟體。只有在支援的讀卡機上線時才能升級。

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

系統

時間和地點

日期和時間

時間格式取決於網路瀏覽器的語言設定。

附註

我們建議您將該設備的日期和時間與 NTP 伺服器同步。

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

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

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

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

附註

系統在所有錄影、記錄和系統設定中使用該日期和時間設定。

網路

IPv4

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

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

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

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

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

附註

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

IPv6

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

主機名稱

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

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

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

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

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

DNS 伺服器

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

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

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

附註

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

HTTP 和 HTTPS

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

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

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

附註

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

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

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

[Certificate (憑證)]：選取憑證來為設備啟用 HTTPS。

網路發現協定

[Bonjour®]：啟用此選項可允許在網路上自動搜尋。

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

[UPnP®]：啟用此選項可允許在網路上自動搜尋。

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

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

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

單鍵雲端連線

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

[Allow O3C (允許 O3C)]：

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

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

[Host (主機)]：輸入 Proxy 伺服器的位址。

[Port (連接埠)]：輸入用於存取的連接埠號碼。

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

[Authentication method (驗證方法)]：

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

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

SNMP

簡易網路管理通訊協定 (SNMP) 允許遠端管理網路裝置。

[SNMP]：選取要使用的 SNMP 版本。

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

附註

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

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

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。

安全

憑證

憑證會用來驗證網路上的裝置。裝置支援兩種類型的憑證：

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

支援以下格式：

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

重要

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

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

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

⋮ 內容功能表包含：

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

[Secure keystore (安全金鑰儲存區)ⓘ]：

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

[網路存取控制和加密]

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

憑證

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

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

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

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

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

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

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

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

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

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

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

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

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

防止暴力破解

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

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

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

防火牆

防火牆：開啟以啟動防火牆。

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

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

+ 新規則：按一下可建立規則。

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

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

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

自訂簽署的 AXIS OS 憑證

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

[安裝]：按一下以安裝憑證。安裝軟體之前需要先安裝憑證。

內容功能表包含：

- [Delete certificate (刪除憑證)]：刪除憑證。

帳戶

帳戶

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

[Account (帳戶)]：輸入唯一的帳戶名稱。

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

[Repeat password (再次輸入密碼)]：再次輸入相同的密碼。

[Privileges (權限)]：

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

內容功能表包含：

[Update account (更新帳戶)]：編輯帳戶特性。

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

MQTT

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

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

您可以在 *AXIS OS 知識庫*中深入了解 MQTT。

ALPN

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

MQTT 客戶

[Connect (連線)]：開啟或關閉 MQTT 用戶端。

[Status (狀態)]：顯示 MQTT 用戶端目前的狀態。

中介者

[Host (主機)]：輸入 MQTT 伺服器的主機名稱或 IP 位址。

[Protocol (協定)]：選取要使用的通訊協定。

[Port (連接埠)]：輸入連接埠號碼。

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

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

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

[Password (密碼)]：輸入使用者名稱的密碼。

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

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

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

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

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

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

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

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

連線訊息

指定是否要在建立連線時送出訊息。

[Send message (傳送訊息)]：開啟以傳送訊息。

[Use default (使用預設)]：關閉以輸入您自己的預設訊息。

[Topic (主題)]：輸入預設訊息的主題。

[Payload (承載)]：輸入預設訊息的內容。

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

[QoS]：變更封包流的 QoS 層。

最終聲明訊息

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

[Send message (傳送訊息)]：開啟以傳送訊息。

[Use default (使用預設)]：關閉以輸入您自己的預設訊息。

[Topic (主題)]：輸入預設訊息的主題。

[Payload (承載)]：輸入預設訊息的內容。

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

[QoS]：變更封包流的 QoS 層。

MQTT 發佈

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

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

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

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

[+ Add condition (新增條件)]：按一下可新增條件。

[Retain (保留)]：定義要傳送為保留的 MQTT 訊息。

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

[QoS]：選取 MQTT 發佈所需的服務品質等級。

MQTT 訂閱

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

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

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

[Subscription type (訂閱類型)]：

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

[QoS]：選取 MQTT 訂閱所需的服務品質等級。

配件

I/O埠

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

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

連接埠

[Name (名稱)]：編輯文字以重新命名該連接埠。

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

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

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

附註

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

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

記錄檔

報表和紀錄

報告

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

記錄檔

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

網路追蹤

重要

網路追蹤檔案可能包含機密資訊，例如憑證或密碼。

網路追蹤檔案可以記錄網路上的活動，協助您針對問題進行疑難排解。

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

遠端系統日誌

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

[+ Server (伺服器)]：按一下可新增伺服器。

[Host (主機)]：輸入伺服器的主機名稱或 IP 位址。

[Format (格式化)]：選取要使用的 Syslog 訊息格式。

- 安迅士
- RFC 3164
- RFC 5424

[Protocol (協定)]：選取要使用的通訊協定：

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

[Port (連接埠)]：編輯連接埠號碼以使用不同的連接埠。

[Severity (嚴重性)]：選取要在觸發時要傳送的訊息。

[Type (類型)]：選擇您想要傳送的日誌類型。

測試伺服器設定：在儲存設定之前，向所有伺服器發送測試訊息。

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

維護

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

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

重要

還原後僅會儲存的設定是：

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

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

附註

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

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

升級時，您可以在三個選項之間進行選擇：

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

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

T10125657_zh_tw

2025-11 (M14.3)