

eNitor Access System

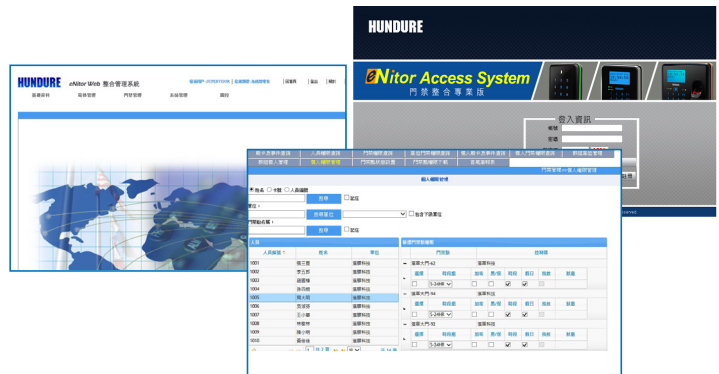
門禁整合專業版

■ 功能概述

- WEB系統架構，透過Windows Edge或Google Chrome等瀏覽器即可對設備進行管理、通行權限設定、卡機參數管理以及報表查詢等。
- 系統設備支援單機及階層式控制器架構，以TCP網路做資料傳輸。
- 採開放式架構設計，允許將設備的刷卡資料提供給其他系統應用。
- 能與消防系統連動，在發生火災時釋放指定位置的門鎖。
- 支援即時傳輸(Real-Time)及多點傳輸技術，可同時對多點傳送資料，24小時ON Line收集使用記錄及狀態事件。
- 電腦開機後自動執行資料接收、資料庫寫入以及資料異動同步。
- 以伺服器為母鐘自動對門禁控制器及讀卡機做時間校正。
- 系統登入提供帳號、密碼、圖形驗證碼的安全認證機制。
- 系統具帳號驗證與系統權限區分功能，可讓系統管理人員規劃系統內各階層與子系統的權限。
- 系統採MS SQL資料庫具自動備份及回存還原功能。

■ 基本資料

- 人員基本資料沒有筆數限制，支援.csv 檔或 .txt 檔案匯入功能。
- 可設定卡號停用日期到期時自動刪除人員進出權限。
- 人員群組定義功能，可以群組做批次新增與刪除人員權限。
- 人員基本資料查詢具有模糊比對搜尋功能。
- 提供API可與其他應用系統進行人員資料交換與串接。
- 可以月為單位搜尋顯示未曾刷卡的人員，清除冗員。
- 臨時卡發放功能可以設定臨時卡的使用起迄區間。



■ 門禁管理

◎ 門禁人員權限管理：

1. 系統可以選擇以群組單位或群組個人方式來大量設定人員權限。
2. 使用群組單位方式，可以指定部門/單位之人員，在某一時間下進出數個門禁點。
3. 使用群組個人方式，可以人員在某一時間下進出數個門禁點。
4. 使用群組單位或群組個人方式來授權時，在有人員新加入或人員離職時，系統都會自動設定權限取消或加入權限的動作。
5. 授權完成，系統在固定時間內會自動生效。

◎ 個人門禁權限管理：

1. 個人門禁授權乃針對個人對單一門禁點設定其進出時間、假日、是否密碼管制、是否使用指紋做判斷依據及設定黑名單。
2. 提供單日多組時段進出。
3. 授權完成，系統在固定時間內會自動生效。

◎ 門禁權限查詢，以門禁點查詢可以進出的人員，查詢結果可以匯出成Excel檔、HTML檔以及Text文字檔。

◎ 人員權限查詢，以人員查詢可以進出的門禁點，提供單位、姓名、編號、卡號等搜尋條件，查詢結果可以匯出成Excel檔、HTML檔以及Text文字檔。

◎ 刷卡及事件查詢：

1. 提供刷卡紀錄、硬體事件以及警報事件三種報表查詢功能。
2. 提供單位、姓名、人員編號、卡號、門禁點、事件名稱以及日期範圍等搜尋條件選擇。
3. 系統預設當年、當月、當周、當天四個快捷按鈕，方便快速搜尋，管理者仍可以自訂日期範圍做搜尋。
4. 提供4個欄位排序條件做選擇，可以選擇升序或降序排列。
5. 查詢結果可以匯出成Excel檔、HTML檔以及Text文字檔。
6. 管理人員可以查詢所有門禁點及單位人員的進出紀錄，系統操作員只能查詢自己所管理門禁點及單位人員的進出紀錄。

eNitor Access System

門禁整合專業版

◎ 門禁點狀態設置：

1. 門禁點可以選擇門禁或考勤用途，權限下載可以選擇自動或手動，選擇自動下載系統會自動將所有人及新增人員的刷卡權限下載至選擇的門禁點。
2. 設定各門禁點的通行時段及假日管制表。
3. 匯入/匯出各門禁點的通行名單。
4. 手動讀取或校正門禁控制器及讀卡機的日期、時間。
5. 設定各門禁點的常開不管制時區。
6. 對門禁點做遠端遙控開門（開鎖）/關門（閉鎖）。
7. 依安裝設備不同，可以對指定裝置設定連動條件。

◎ 門禁點權限下載，門禁權限由系統同步後自動下載至門禁控制器或讀卡機，系統另提供管理者可以手動選擇門禁點下載權限名單。

■ 系統管理

◎ 使用者管理：

1. 人員權限新增/修改管理控制權為最高管理者管理權限，可再分配其他管理角色的系統權限。
2. 管理者可區分三個角色，三種角色的功能權限可以由系統管理者做適當的變更及設定。
3. 員工查詢：提供員工註冊後上網查詢個人的刷卡記錄及門禁權限。
4. 使用者帳號設定初次使用可以使用系統預設密碼或自訂密碼，登入後再由使用者自行變更密碼。

◎ 使用者權限管理：

1. 系統可以對操作員或操作群組個別設定系統功能權限、單位管理權限、群組權限、門禁組權限以及門禁點權限。
2. 操作員帳號向下建立新帳號時，新帳號各功能權限受限於操作員帳號權限的範圍。
3. 系統權限功能，系統各功能項目都可以選擇是否授權帳號使用。
4. 單位權限功能，分配各帳號可以查詢、管理的單位。
5. 群組權限功能，管理員先建立操作群組設定各項權限範圍，然後再建立操作員帳號設定群組權限，快速完成帳號權限設定。
6. 門禁組權限功能，分配各帳號可以管理設定通行權限的門禁組。
7. 門禁點權限功能，分配各帳號可以管理設定通行權限的門禁點。

◎ 修改密碼，提供系統使用者可以自行修改登入密碼，但使用者無權修改帳號名稱。

◎ 裝置規劃：

1. 支援單機、控制器、指紋機、人臉辨識等多種設備，採TCP/IP通訊方式做資料傳輸。
2. 通訊方式設定完成後，系統可以偵測線上裝置，將已連線的裝置顯示供管理員快速建立與編輯。
3. 系統可以讀取控制器及卡機的參數，以便快速建立各項參數並儲存至資料庫做保存。

◎ 系統事件查詢：

1. 可以查詢門禁權限、單位資料、人員資料、門組定義、設備操作以及系統相關的各項歷史記錄。
2. 提供新增、更新、刪除、登錄等操作類型條件做搜尋。
3. 可以自行輸入日誌內容關鍵字做搜尋條件。
4. 可以自訂日期區間搜尋各項記錄。
5. 查詢結果可以匯出成Excel檔、HTML檔以及Text文字檔。

■ 應用系統(選購)

◎ 事件監控系統

1. 自訂監視點
2. 照片顯示
3. 警告事件提示
4. 自訂提示音效檔

◎ ModbusTCP

1. 支援Read傳送門位狀態及卡號與Write遠端控制門鎖

◎ Web 版圖控系統

1. 提供 Web 圖控顯示與控制功能
2. 支援 Microsoft Edge、Google Chrome
3. 可用任一電腦進行設備監控與管理
4. 可多台電腦同步監視，同步更新
5. 自訂監控點名稱、圖控畫面與監控底圖
6. 自訂監控點音效檔

7. 即時顯示監控點狀態
8. 可顯示告警位置及時間
9. 可遠端開門以及關閉警報
10. 求救偵測點 (EHU Sensor) 可以設定偵測時段自動佈防及撤防。

eNitor Access System

門禁整合專業版

■ 資安強化模組 (選購)

- 源碼掃描防護：在系統開發、更新與維護過程中，導入自動化原始碼安全檢測機制，避免常見漏洞並符合 OWASP Top 10 標準。
- 弱點掃描檢測：定期對系統平台與伺服器進行弱點掃描，輸出風險等級與修補建議報告，提前防範潛在攻擊。

■ 系統需求 (最低建議配置)

◎ 門禁伺服器硬體

- CPU：INTEL Xeon E-2334 3.4GHz (含)以上
- 記憶體：32GB DDR4-3200 ECC UDIMM (含)以上
- 硬碟：1TB SATA3 7200 rpm x 2
- SATA 控制器：INTEL C242；6 x SATA3 6Gb/s
- 連接埠：INTEL RSTe (Support Software RAID 0,1)
- 網路：2個 RJ45 網路介面
- 網路埠：TCP 4660、4661、3195、3196、9876、502，UDP 3195
- 儲存：DVD-RW (備份用，可免)

◎ 虛擬主機硬體

- CPU：4核心 (含)以上
- 記憶體：32GB (含)以上
- 容量：C：100GB(含)以上，D：200GB(含)以上(含資料庫備份所需空間)。
- 網路埠：4660、4661、3195、3196、9876、502，UDP 3195

◎ 管理工作站硬體

- CPU：Intel Core i7 Series 四核心處理器主頻3.0GHz以上
- 記憶體：32GB (含) 以上
- 硬碟容量：500GB 以上
- 網路：至少內建1組100/1000M網路RJ-45埠

◎ 門禁伺服器軟體

- 作業系統：Windows Server 2022
- 資料庫：MS SQL SERVER 2022

◎ 虛擬主機軟體

- 作業系統：Windows Server 2022
- 資料庫：MS SQL SERVER 2022

◎ 管理工作站軟體

- 作業系統：Windows 11以上
- 瀏覽器：Windows Edge或Google Chrome

■ 支援硬體

軟體支援的硬體請至官網查詢 <https://www.hundure.com/>
(產品資訊/軟體下載/硬體支援對照) 或掃描下列QRCode

