Deep Security (On-prem)

註冊VisionOne SOP

系統需求檢查

- 確保DSM版本至少v20.0.198 或更高。
  - ➢ 檢查方式
    - **Windows**

      以系統管理員身份執行powershell下列指令:

      & 'C:\Program Files\Trend Micro\Deep Security Manager\dsm_c.exe' -action versionget -software

    - **Linux**

      使用terminal執行下列指令:

      /opt/dsm/dsm_c -action versionget -software

Firewall 需開通 FQDN URLs & Port

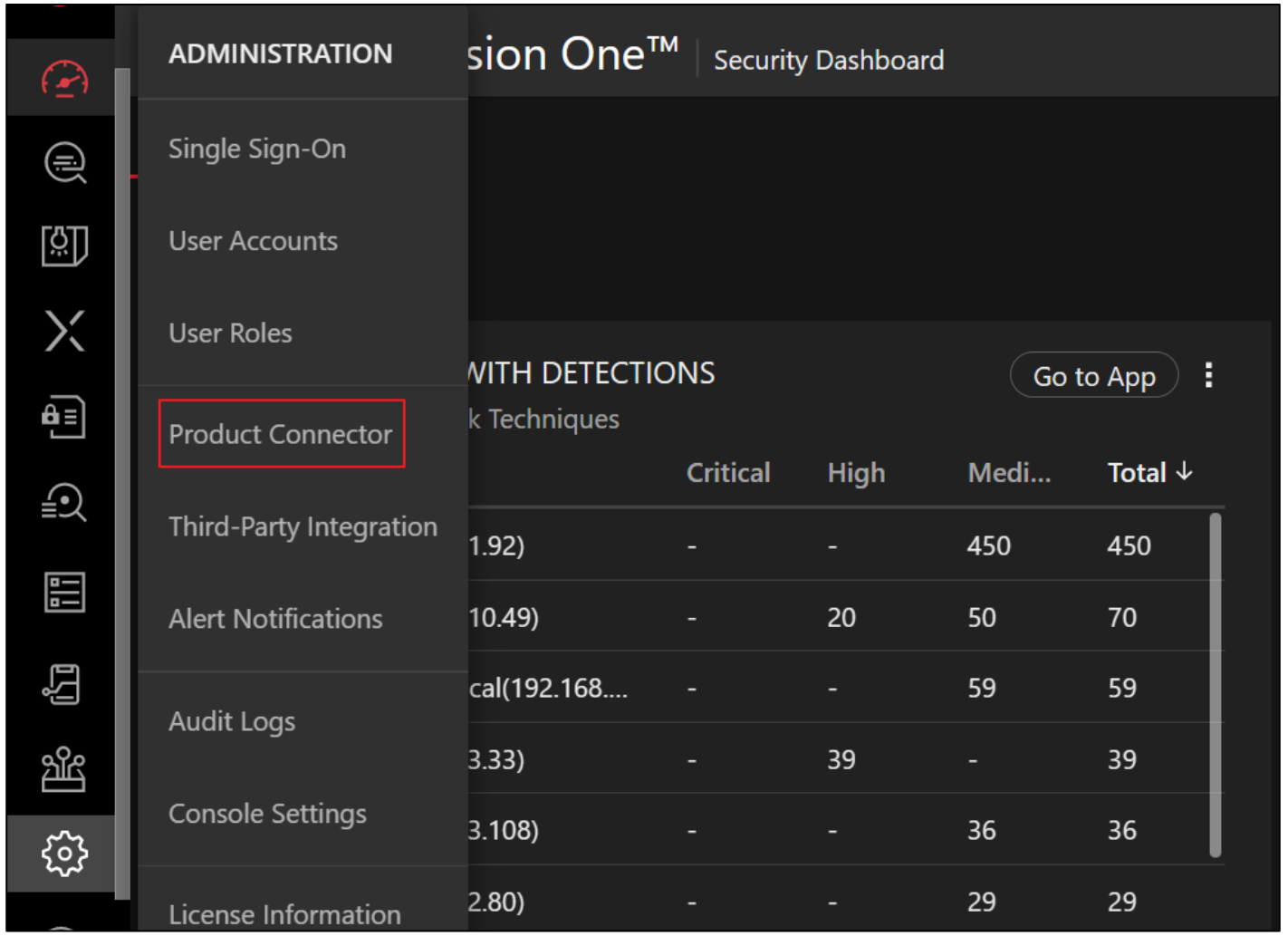
- **請先檢查、開通Firewall設備，確保DSM Server主機能對外Internet連線至下列TrendMicro Vision One 位置：**

*.xdr.trendmicro.com:443
*.xbc.trendmicro.com:443
*.mgcp.trendmicro.com:443
*.manage.trendmicro.com:443
xlogr-ue1.xdr.trendmicro.com:443
api.xdr.trendmicro.com:443
portal.xdr.trendmicro.com:443
tm.xdr.trendmicro.com:443
auth.xdr.trendmicro.com:443

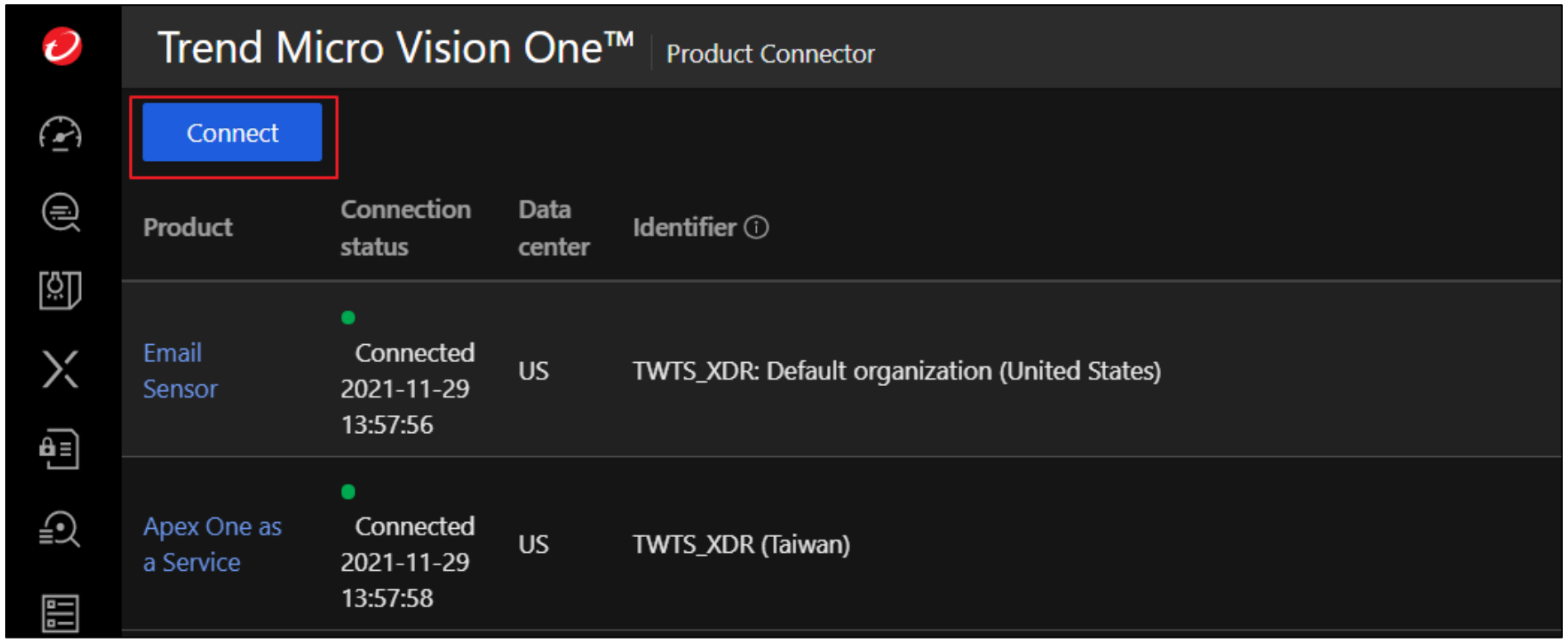
wb.xdr.trendmicro.com:443
assessment.xdr.trendmicro.com:443
xdr2-nabu-prod-ap.etdl.trendmicro.com:443
mxdr-us-prod.xdr.trendmicro.com:443
th-ue1.xdr.trendmicro.com:443
er-ue1.xdr.trendmicro.com:443
era-ue1.xdr.trendmicro.com:443

DSM 註冊 Trend Micro Vision One (XDR)

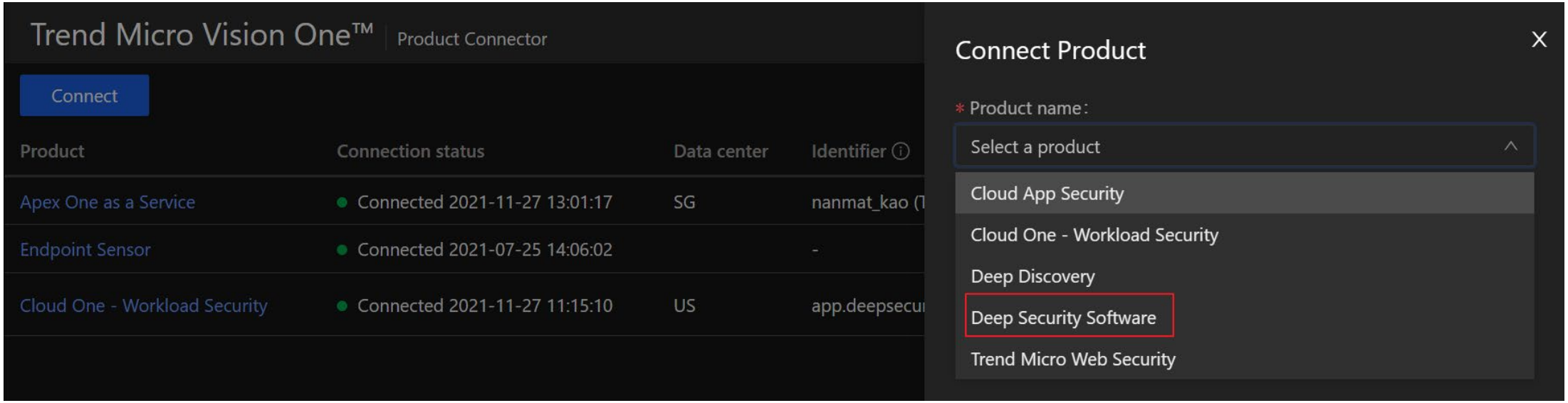
- 登入 TrendMicro Vision One console (ADMINISTRATION → Product Connector)



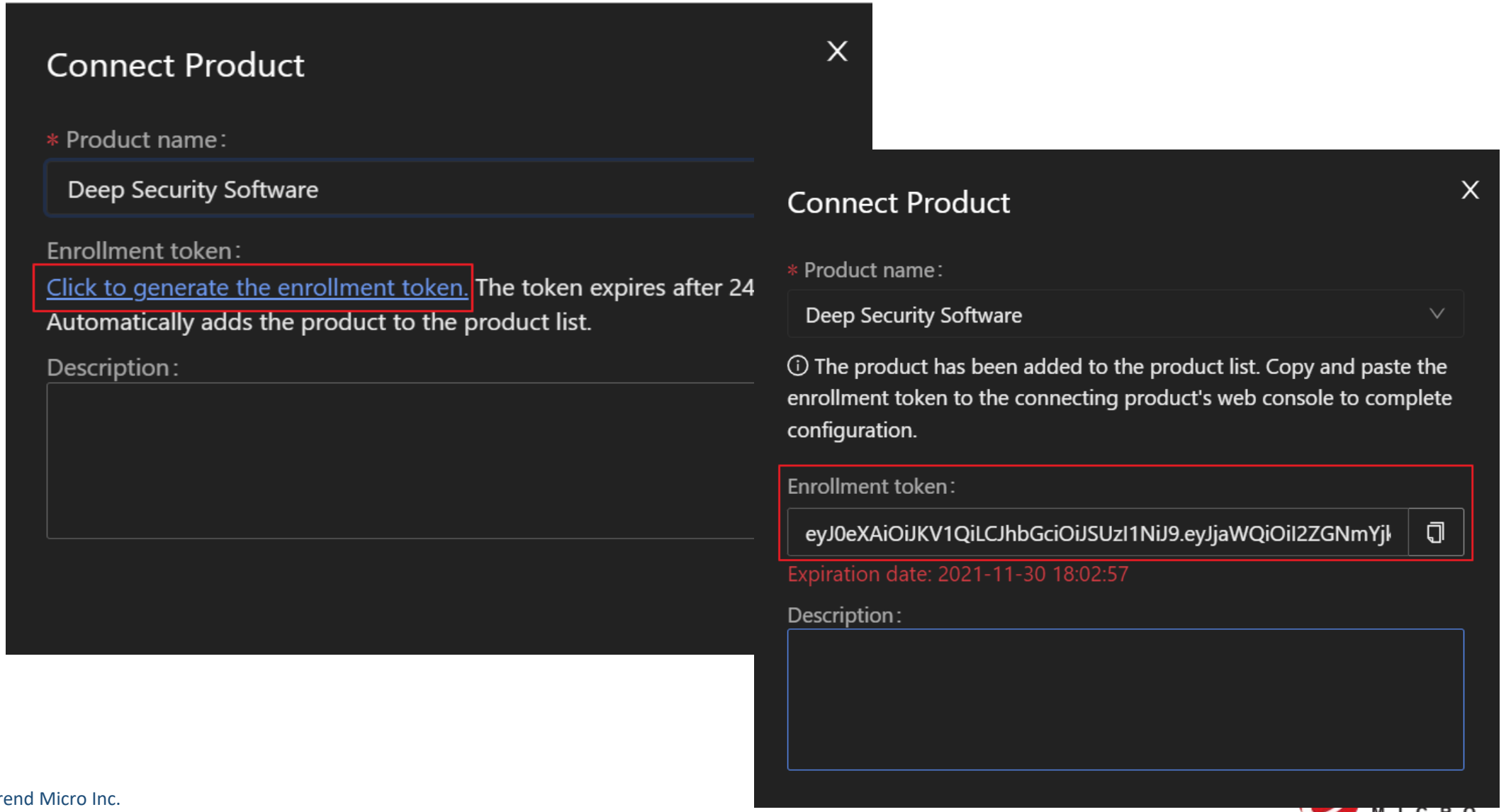
- 建立 Product Connector



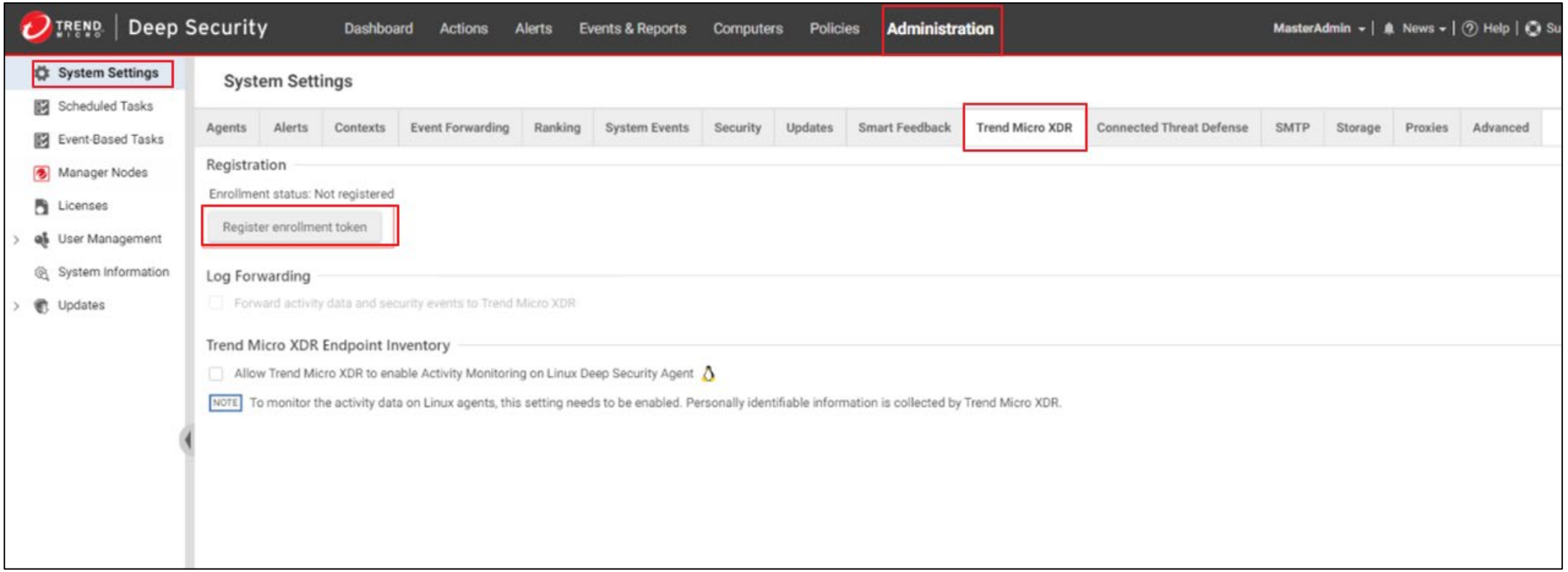
- 產品名稱選擇 Select Product：Deep Security Software



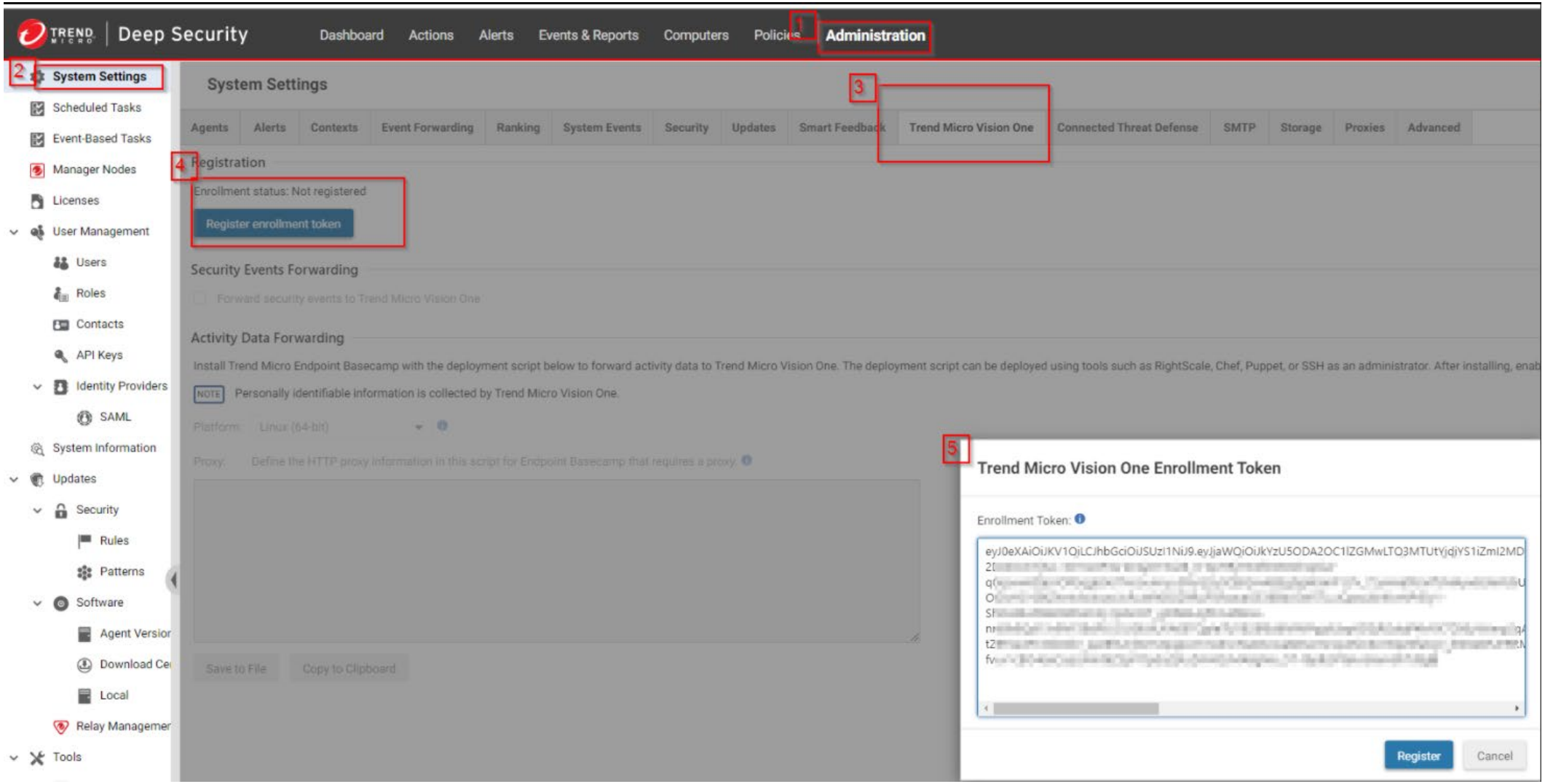
- 點擊Click Generate enrollment token並記錄保存JWT token



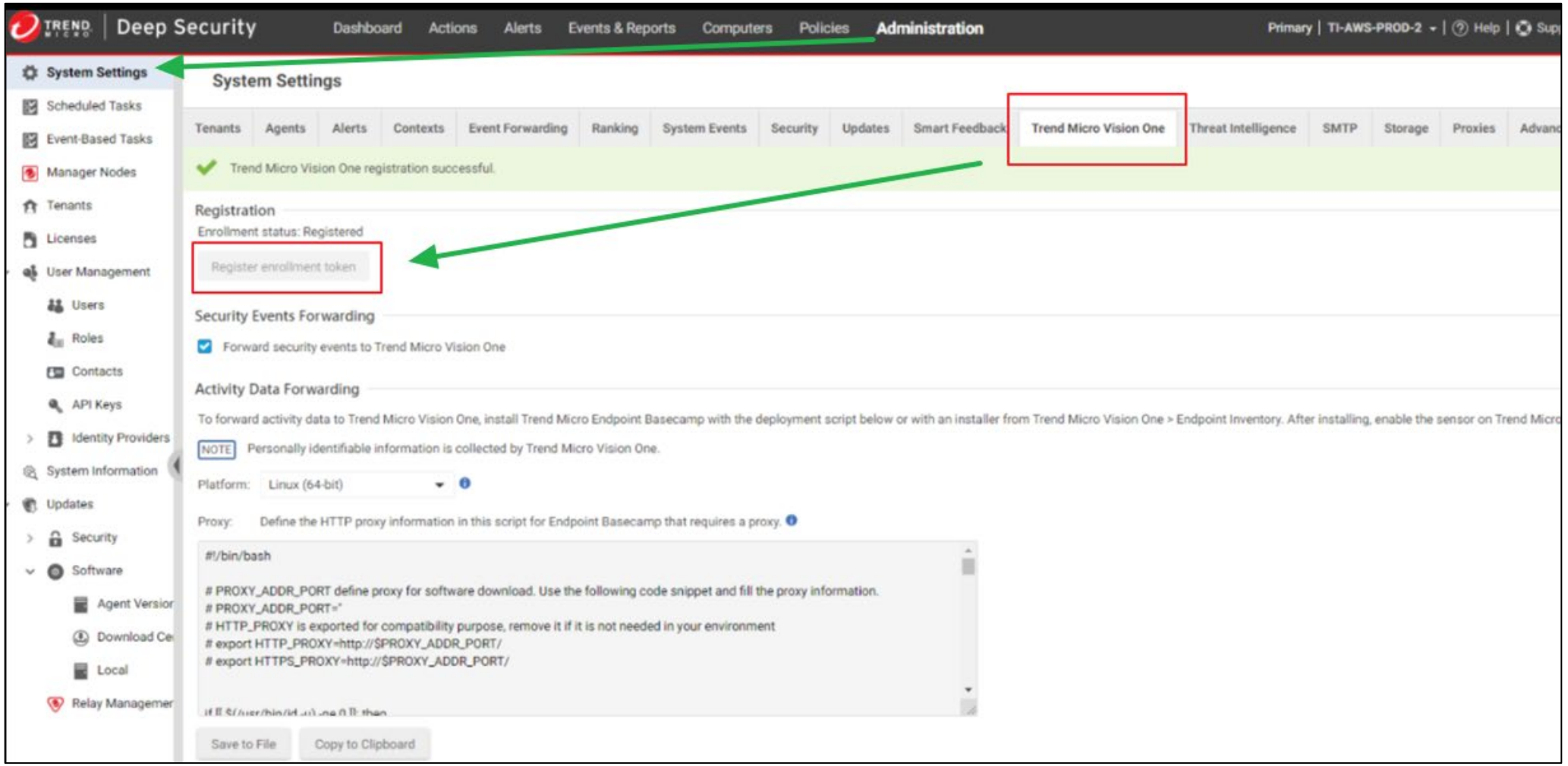
- 登入 DSM 主控台，至 Administration > System Settings >頁籤 Trend Micro Vision One > 點擊Registration Button



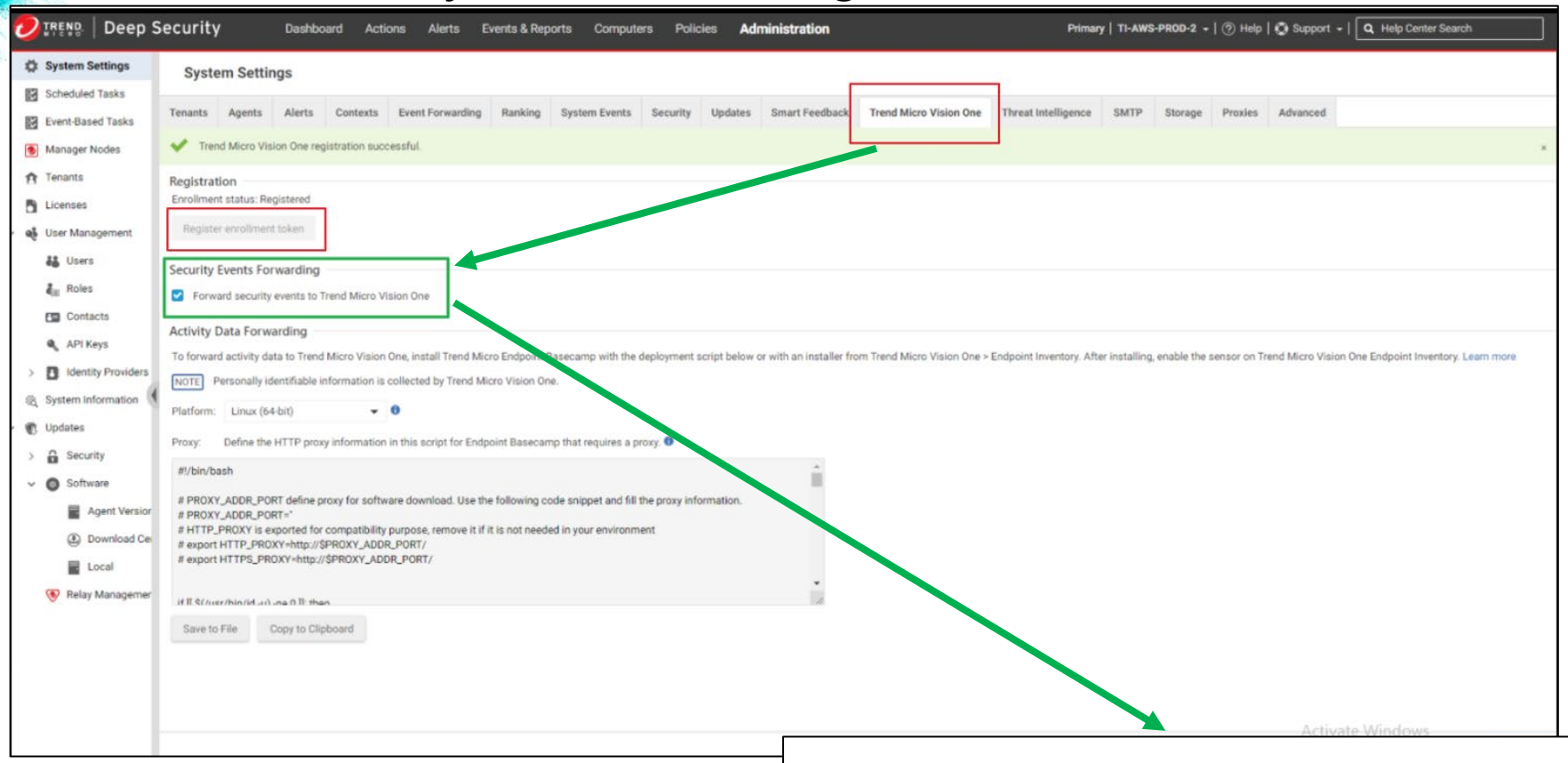
- 輸入貼上Vision One上取得的JWT token並點擊Register button.



- 顯示Trend Micro Vision One 註冊成功
  DSM主控台 > Administaion > System Settings > TrendMicro Vision One



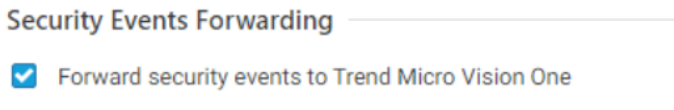
- 啟用[安全事件轉發]
  DSM主控台 > Administaion > System Settings > TrendMicro Vision One >
  勾選Security Events Forwarding > Save



轉發將會包含以下模組事件：

- Anti-Malware
- Web Reputation
- Integrity Monitoring
- Log Inspection
- Intrusion Prevention

Also Security Events forwarding check box will be enabled and ticked.



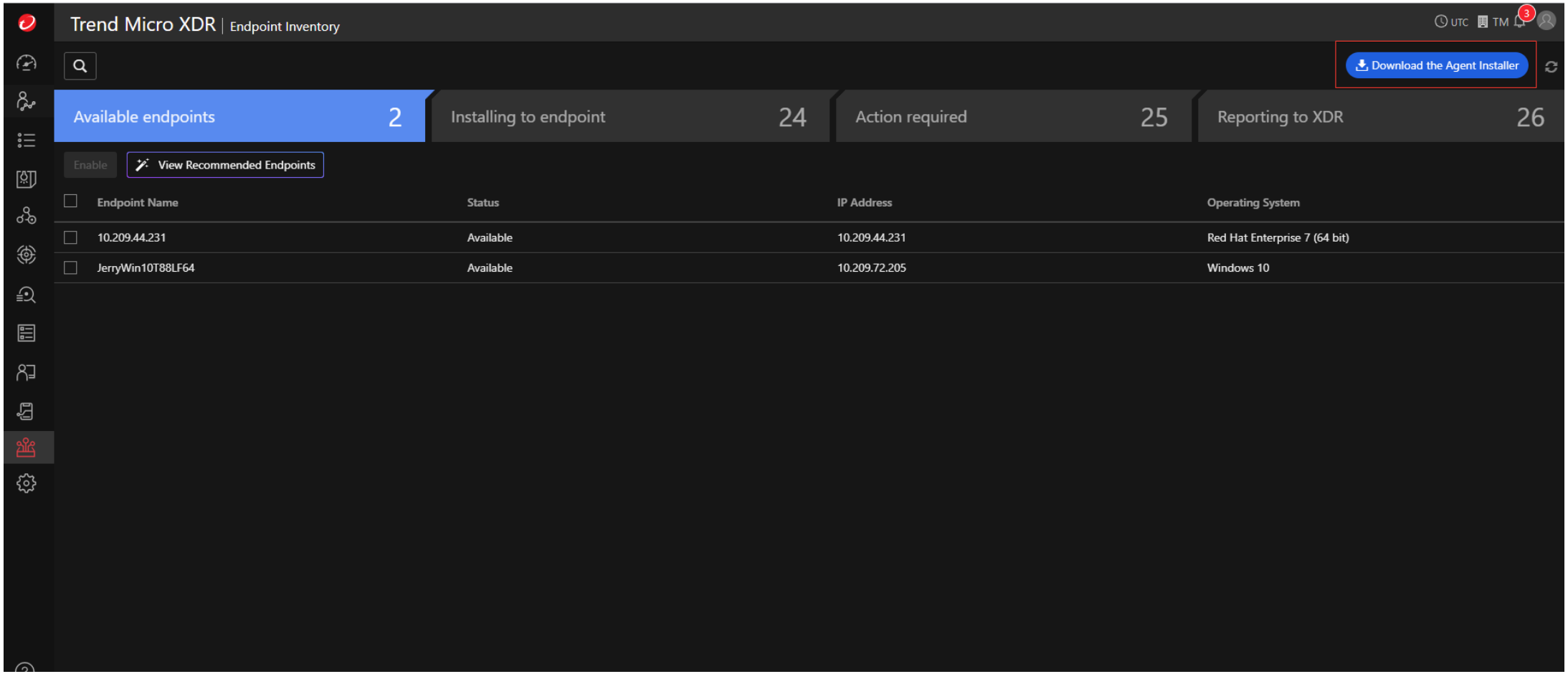
At this point Deep Security Manager is enrolled with Vision One for Detection modules events (IPS, IM, LI, WRS, AM).

- 至Vision One > Administation > Preduct Commector 檢視Deep Security software 連線狀態 (綠燈)

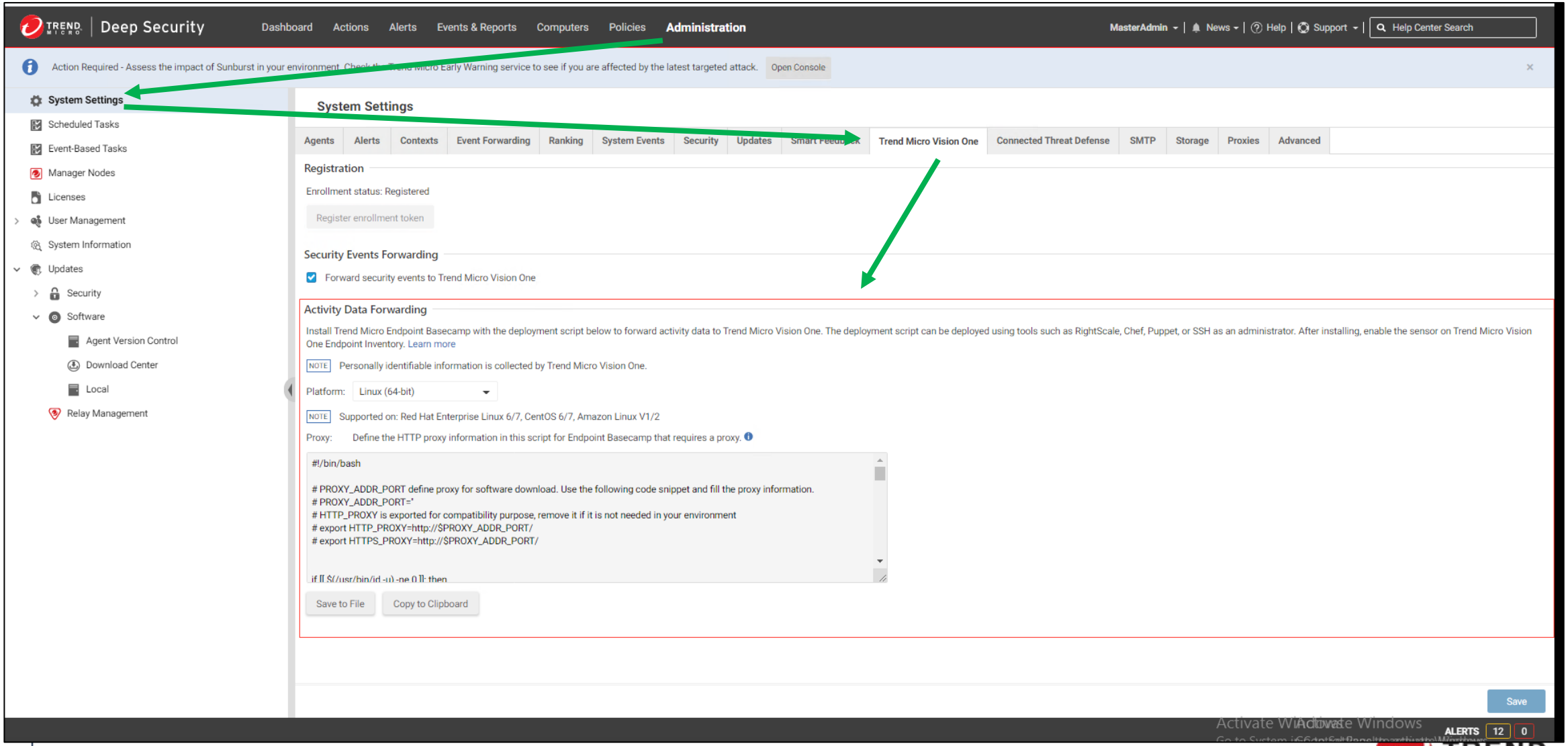
註冊作業完成!

END

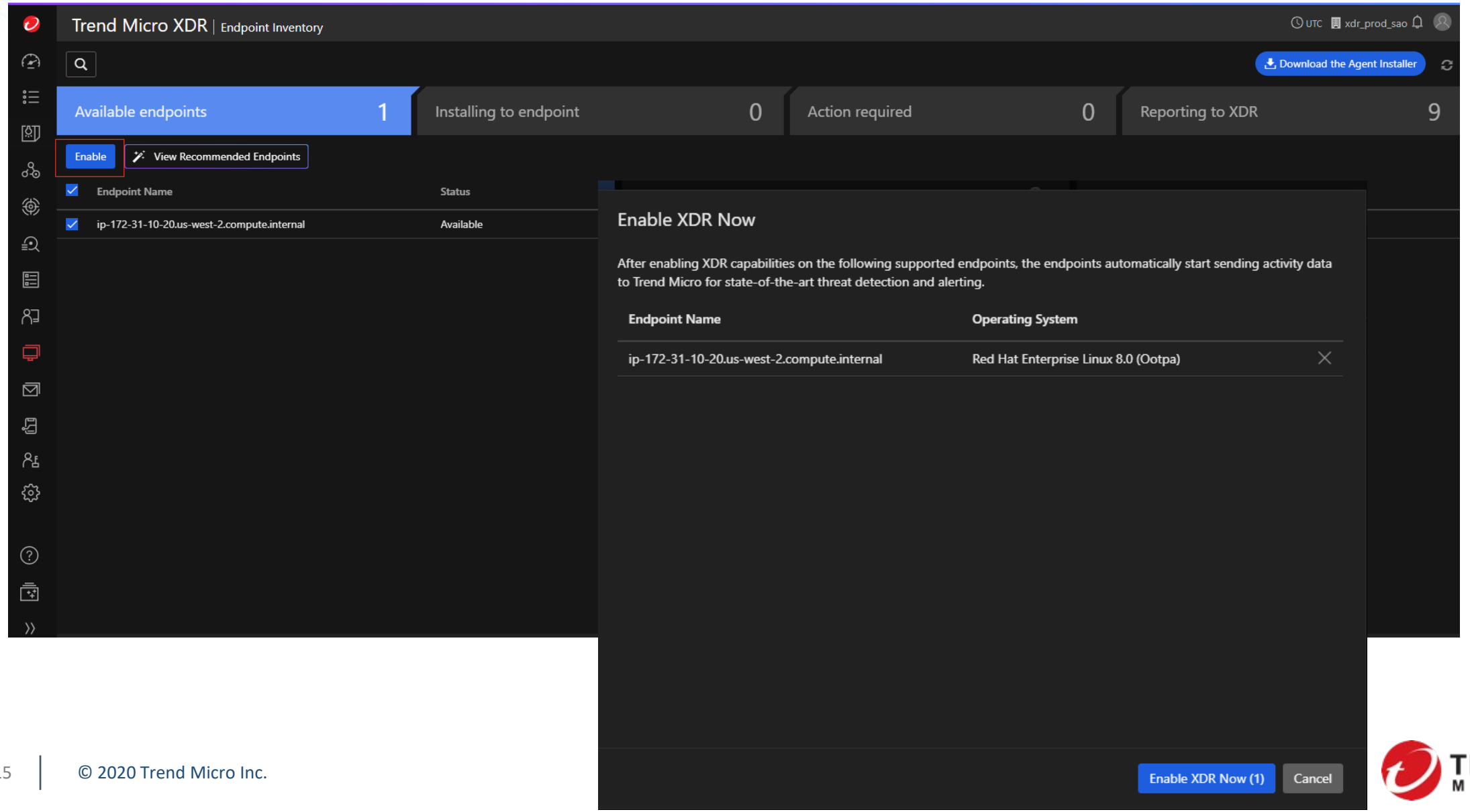
- 下載XDR(XBC) Agent 安裝 from Endpoint Inventory



- 從DSM主控台取得XDR(XBC) Agent佈署Script



- 於Vision One上管理頁面選取需啟用的端點，點選Enable Sensor > Enable XDR Now



- 啟動成功，將顯示Reporting to XDR successfully.