CloudOne Workload Security
註冊 VisionOne SOP

系統需求檢查

- 確保Workload Security Agent 版本至少v20.0.1559 或更高。
  - ➢ 檢查方式
    - Windows

      至新增移除應用程式，檢視DSA版本。
    - Linux

      使用terminal執行指令:

      rpm -qa|grep ds_agent

© 2020 Trend Micro Inc.

Firewall 需開通 FQDN URLs & Port

- **請先檢查、開通Firewall相關網路配置，確保Workload Security Agent 能對外Internet連線至下列TrendMicro CloudOne 及 Vision One 位置：**

  下列註冊地區以Singapore 為例 (其它區域請參閱此) :

  - *.workload.sg-1.cloudone.trendmicro.com:443
  - gateway-control.workload.sg-1.cloudone.trendmicro.com:443
  - gateway.workload.sg-1.cloudone.trendmicro.com:443
  - *.xdr.trendmicro.com:443
  - *.xbc.trendmicro.com:443
  - *.mgcp.trendmicro.com:443
  - *.manage.trendmicro.com:443
  - ak5ih4ev105f2-ats.iot.us-east-1.amazonaws.com
  - azrb5zzyvrkw6-ats.iot.us-east-1.amazonaws.com

© 2020 Trend Micro Inc.

Firewall 需開通 FQDN URLs & Port

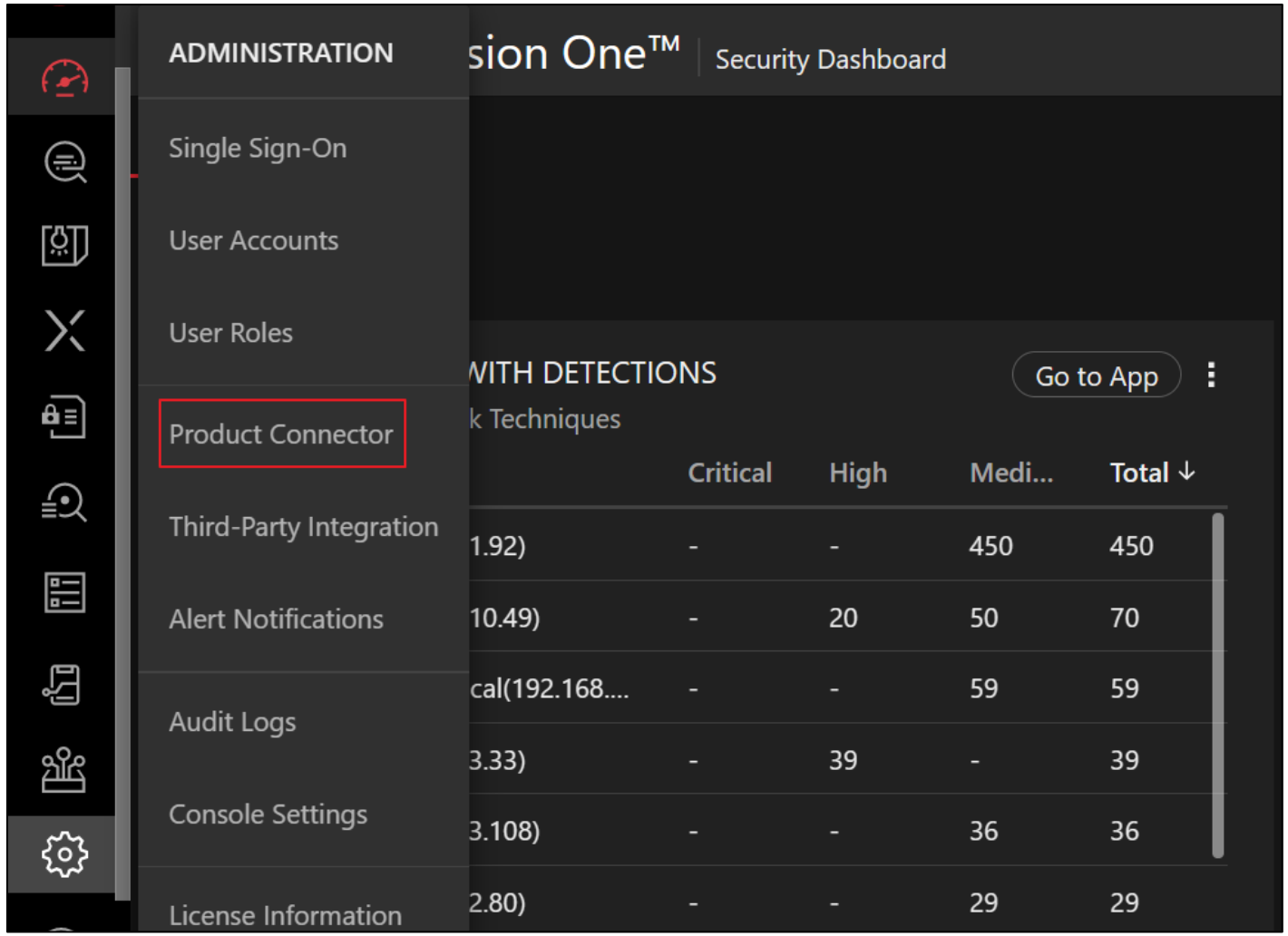
若你的防火牆配置不支援*.workload.<region>.cloudone.trendmicro.com格式，請個別允許訪運下列FQDN位置：

- workload.sg-1.cloudone.trendmicro.com
- agents.workload.sg-1.cloudone.trendmicro.com
- agents-001.workload.sg-1.cloudone.trendmicro.com
- agents-002.workload.sg-1.cloudone.trendmicro.com
- agents-003.workload.sg-1.cloudone.trendmicro.com
- agents-004.workload.sg-1.cloudone.trendmicro.com
- agents-005.workload.sg-1.cloudone.trendmicro.com
- agents-006.workload.sg-1.cloudone.trendmicro.com
- agents-007.workload.sg-1.cloudone.trendmicro.com
- agents-008.workload.sg-1.cloudone.trendmicro.com
- agents-009.workload.sg-1.cloudone.trendmicro.com
- agents-010.workload.sg-1.cloudone.trendmicro.com
- gateway.workload.sg-1.cloudone.trendmicro.com
- gateway-control.workload.sg-1.cloudone.trendmicro.com
- xdr-resp-gw.workload.sg-1.cloudone.trendmicro.com
- dsmim.workload.sg-1.cloudone.trendmicro.com
- relay.workload.sg-1.cloudone.trendmicro.com
- agent-comm.workload.sg-1.cloudone.trendmicro.com

© 2020 Trend Micro Inc.

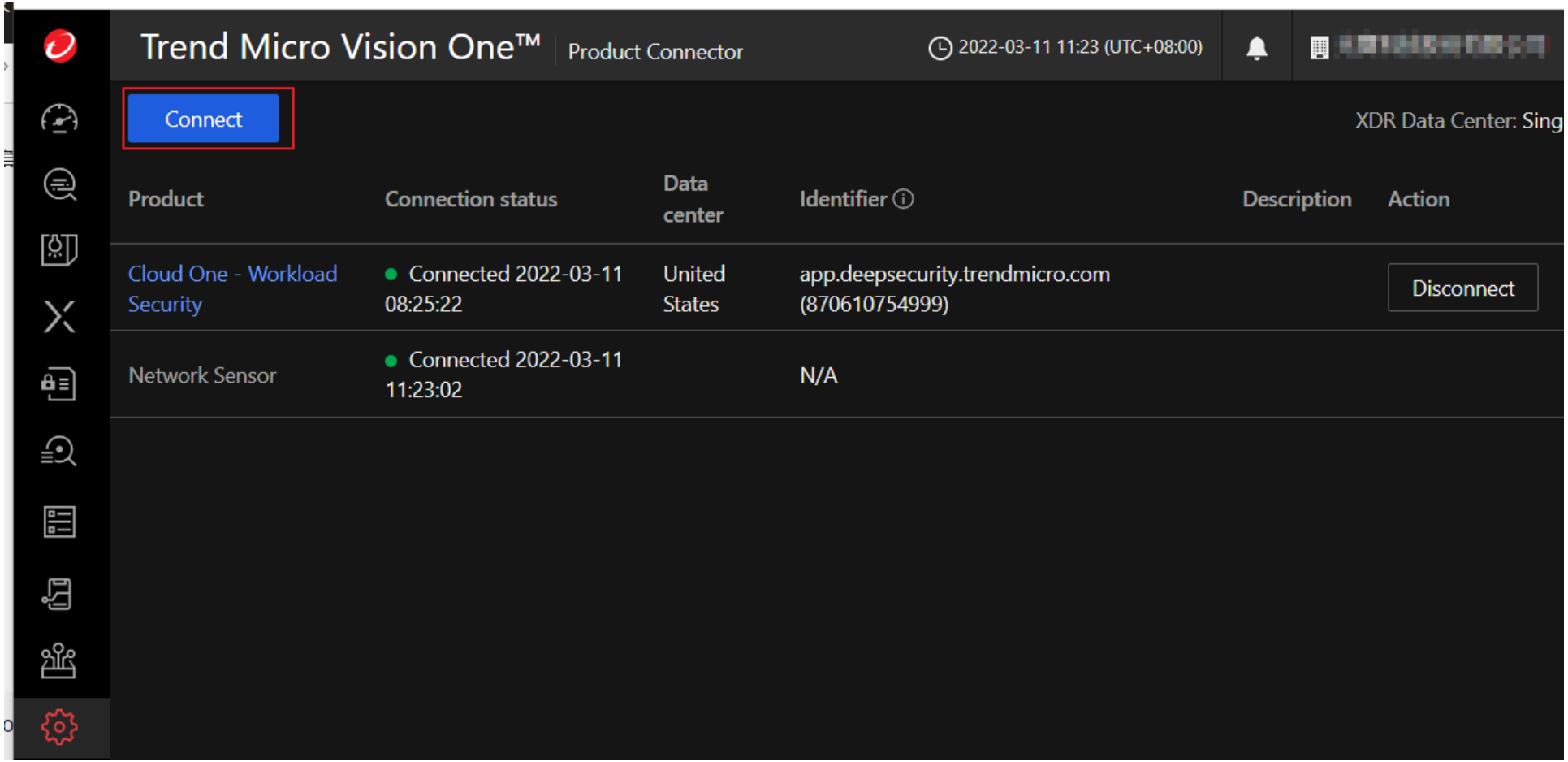
Workload Security 註冊 Trend Micro Vision One (XDR)

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



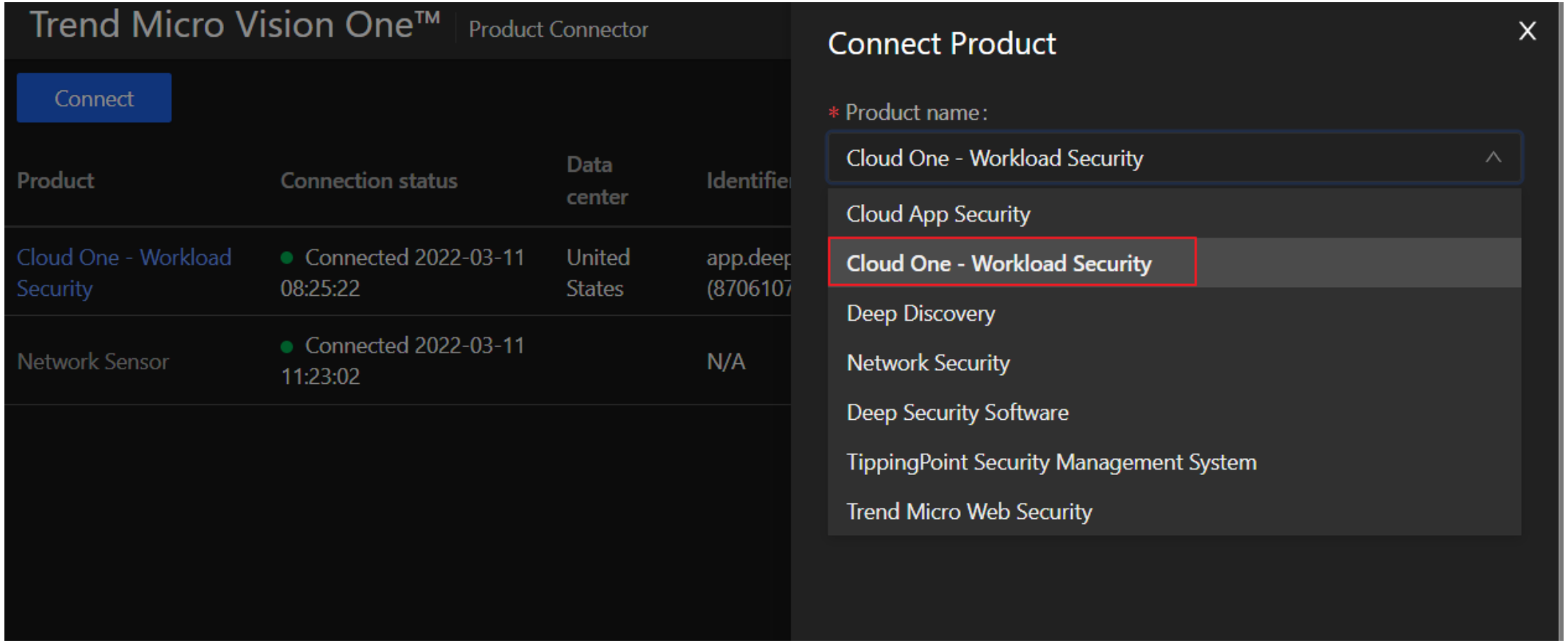
© 2020 Trend Micro Inc.

- 建立 Product Connector。點擊Connect



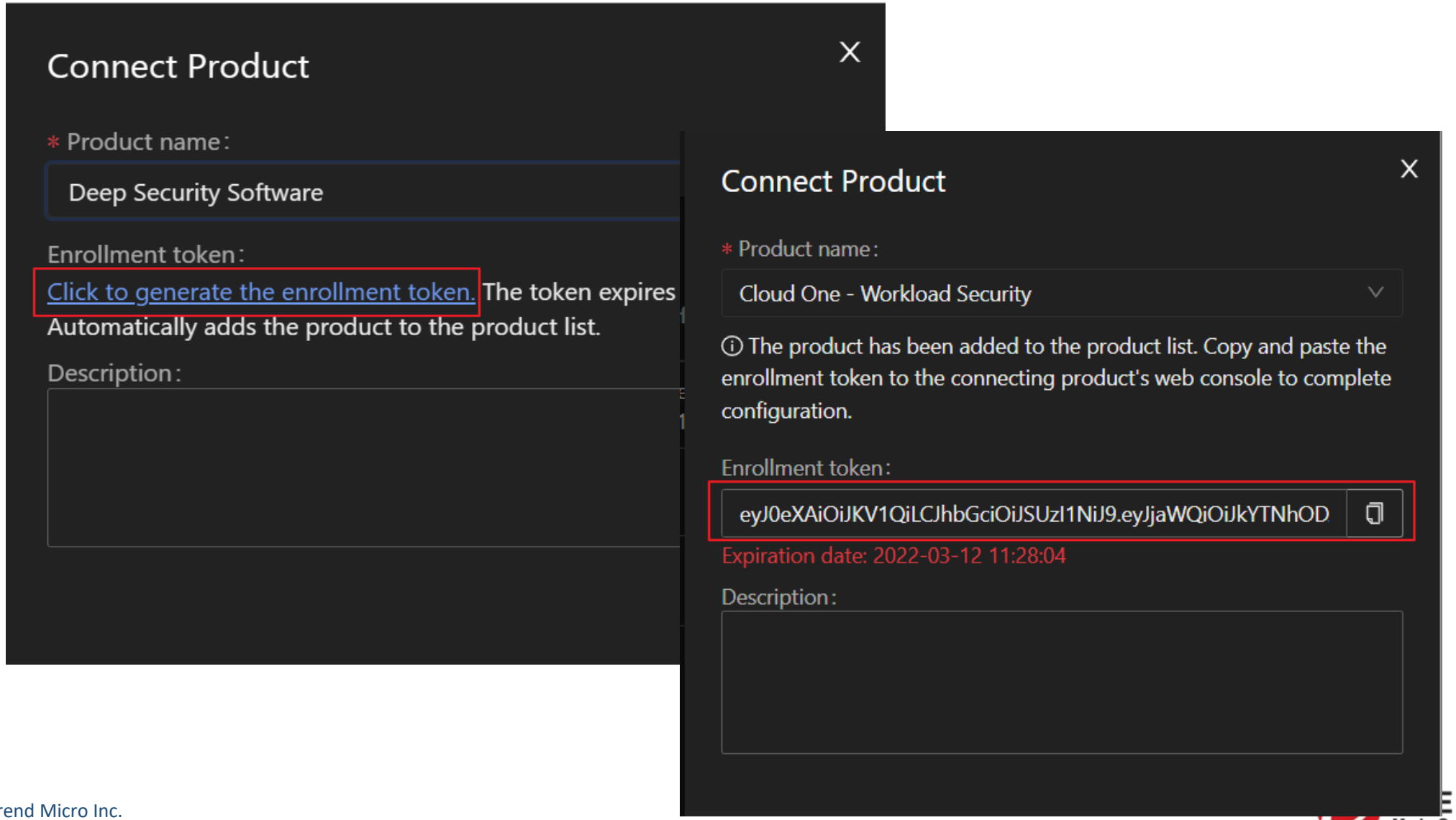
© 2020 Trend Micro Inc.

- 產品名稱選擇 Select Product： Workload Security



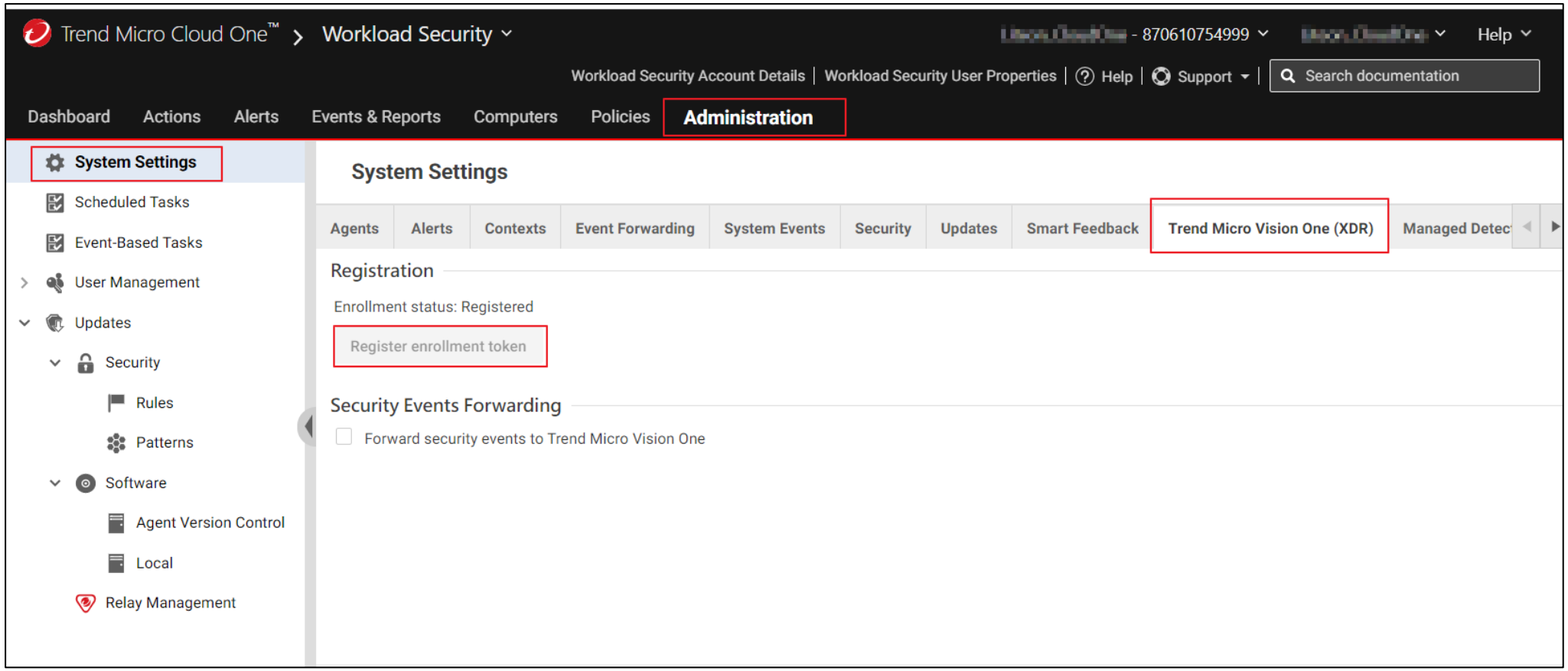
© 2020 Trend Micro Inc.

- 點擊Click Generate enrollment token並記錄保存token



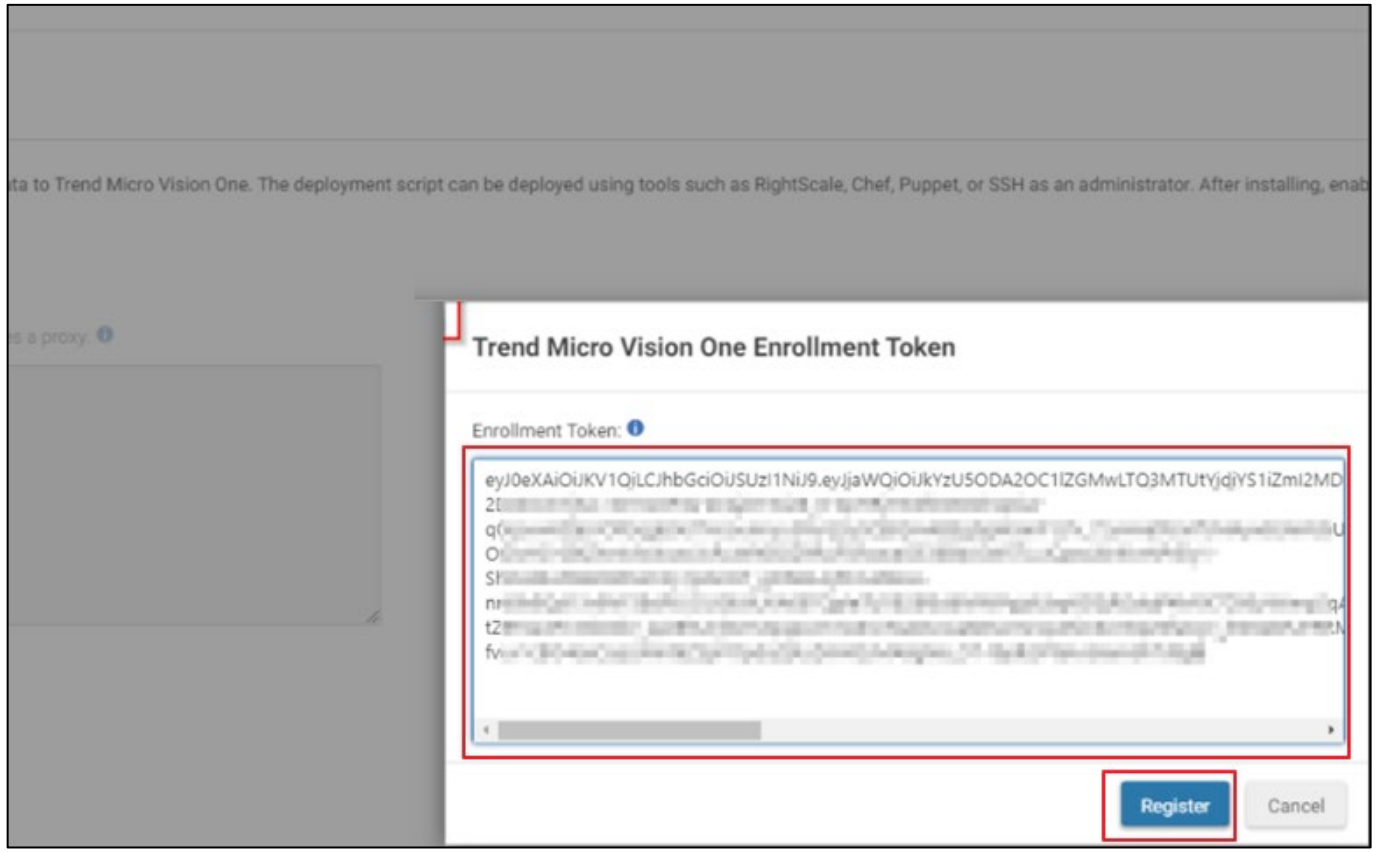
© 2020 Trend Micro Inc.

- 登入 Workload Security主控台，至 Administration > System Settings >頁籤 Trend Micro Vision One(XDR) > 點擊Registration Button



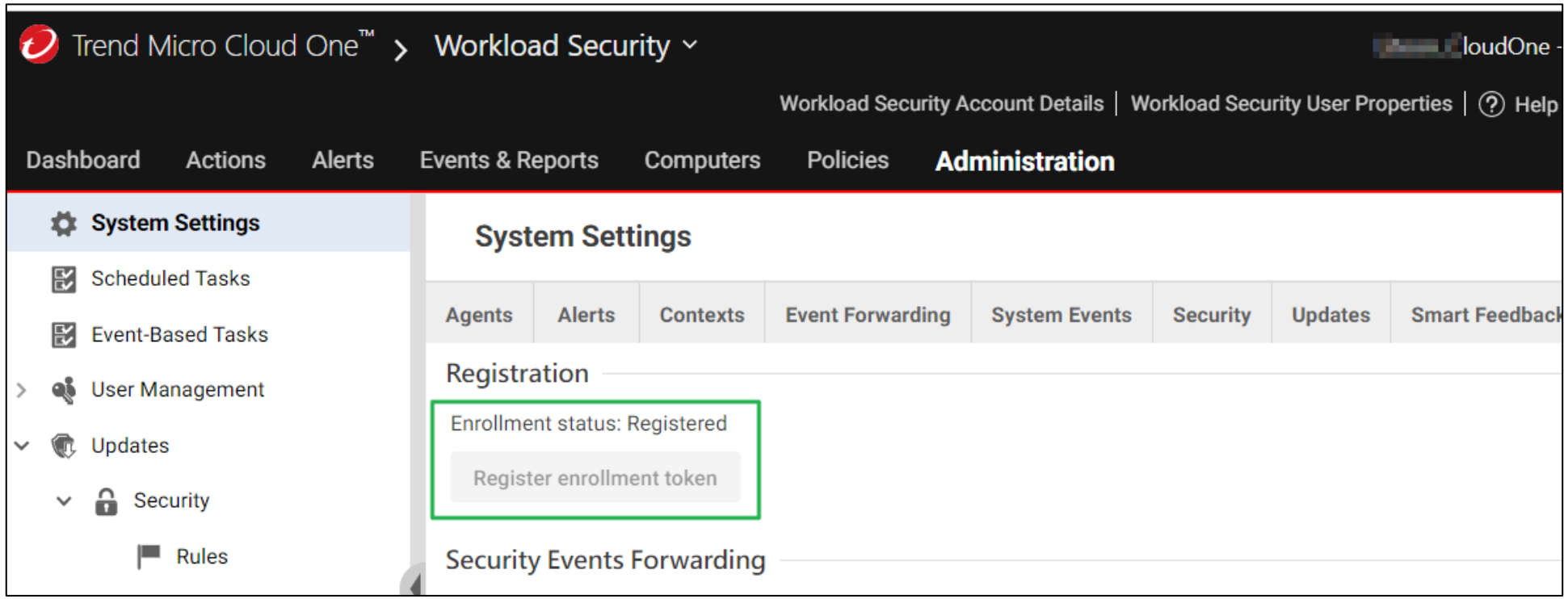
© 2020 Trend Micro Inc.

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



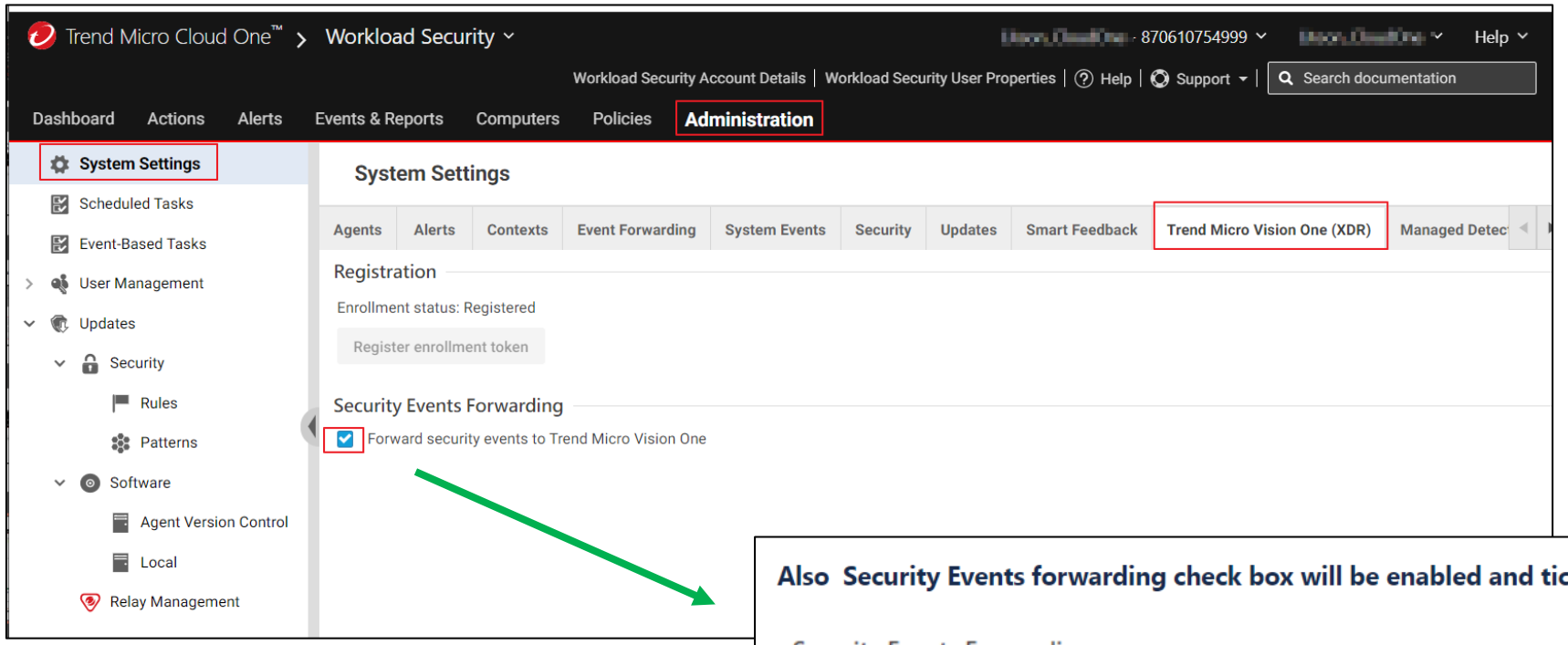
© 2020 Trend Micro Inc.

- 顯示Trend Micro Vision One 註冊成功

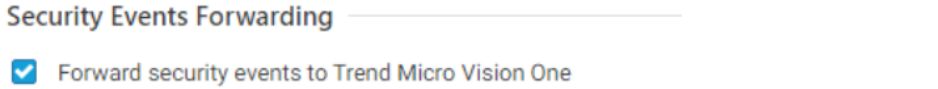


© 2020 Trend Micro Inc.

- 啟用[安全事件轉發]
  勾選Security Events Forwarding > Save



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).

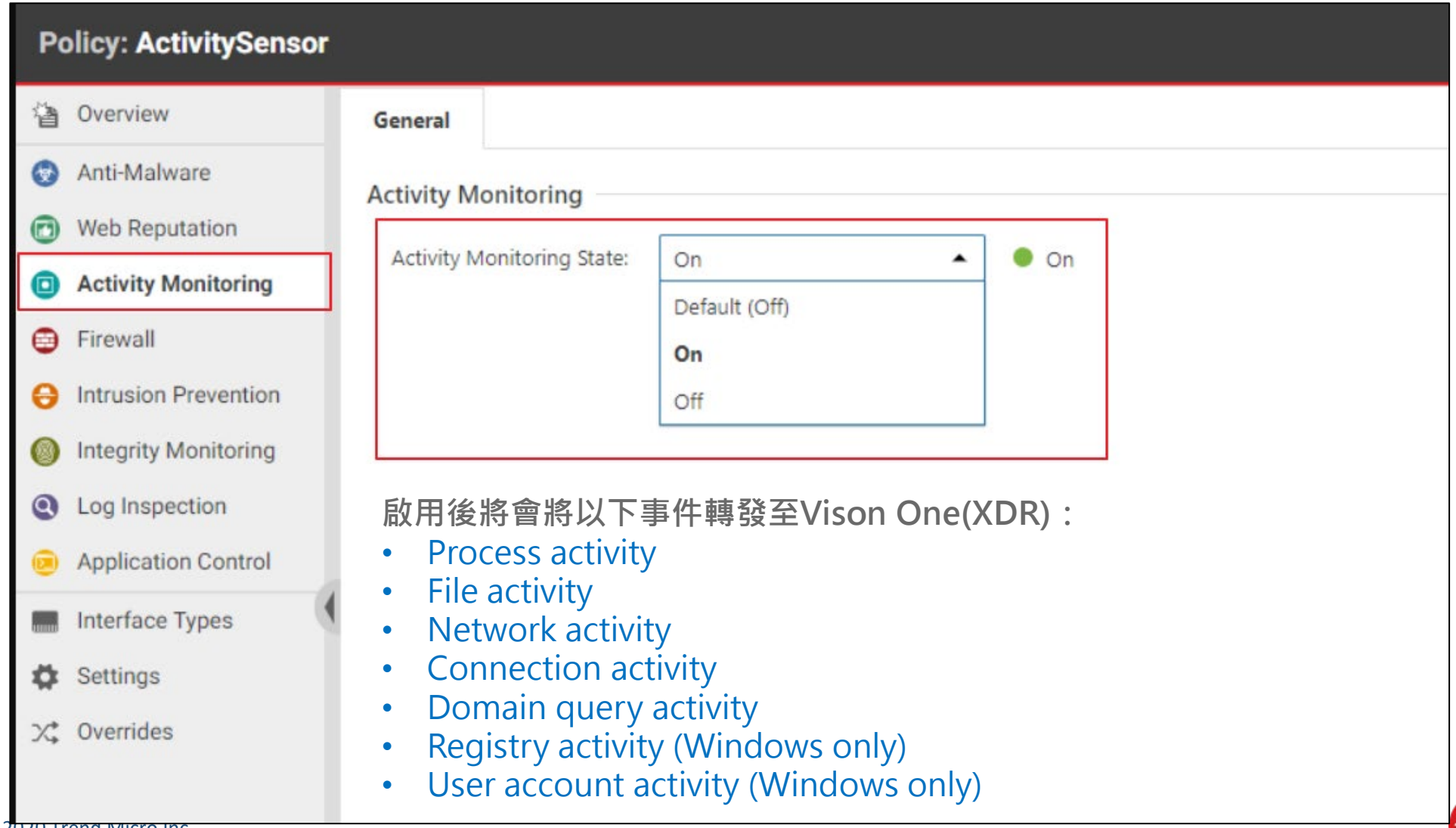
轉發將會包含以下模組事件：

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

© 2020 Trend Micro Inc.

- 啟用 [Activity Monitoring]
  至Policies > Activity Monitoring > General > On > Save

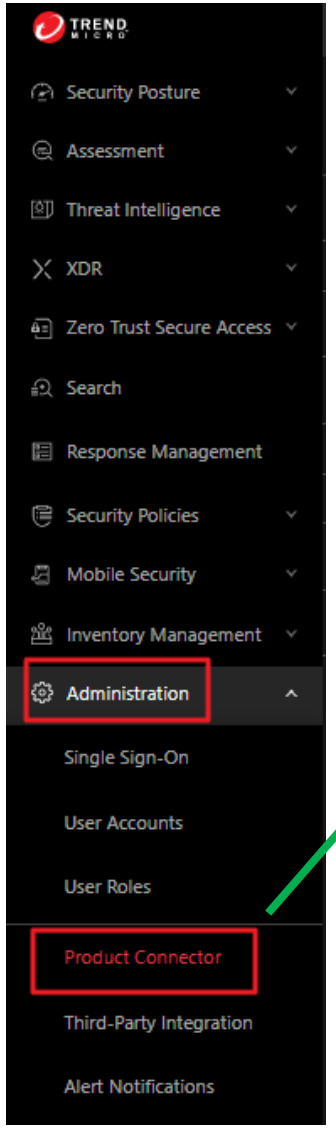
※Agent 版本必須至少 v20.0.0-1681或更高版本才能支援。

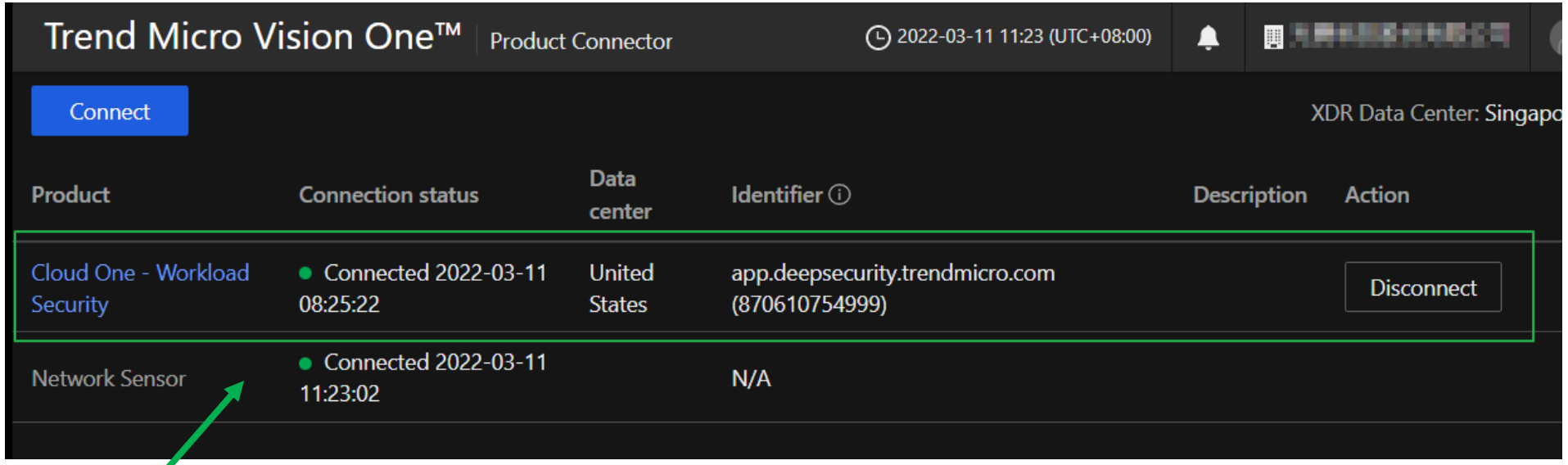


啟用後將會將以下事件轉發至Vison One(XDR)：

- Process activity
- File activity
- Network activity
- Connection activity
- Domain query activity
- Registry activity (Windows only)
- User account activity (Windows only)

© 2020 Trend Micro Inc.





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

註冊作業完成!

END

© 2020 Trend Micro Inc.