

Vision One[™] Apex One SaaS Onboarding

趨勢科技



Apex One SaaS initialize



瀏覽器開啟<u>https://manage.trendmicro.com/</u>, 並輸入設定的 帳密登入, 開始準備Apex One SaaS主控台流程:

🕖 Trend Micro Apex One™ 針對第一次使用準備您的主控台... 簡介 初始組態設定 佈建主控台 簡介 花幾分鐘時間設定您的主控台。完成後,您將能夠使用 主控台作為中樞來存取 Apex One 和 Apex One (Mac) 主控台。 開始使用



在<u>資料中心區域</u>務必選擇「東南亞」





等待一段時間後, 主控台準備完成就會自動開啟

針對第一次使用準備您的主控台... T 111 1 0 1 快速入門手冊 Х 簡介 初始組態設定 佈建主控台 開始使用視訊教學課程 ► 歡迎使用 Apex One as a Service。我們彙整了一些逐步視訊教學課程,以協助您開始使用這項產品。這些指南將協助您進行初始設定,並說明如何使用進階設定,以 及如何在新功能可用時立即使用它們。 造訪 Apex One 歡迎中心 2% Security Agent 下載 Active Directory 同步處理 *** 透過在每個端點上安裝 Apex One 和 Apex One (Mac) 代理程式,為 根據您現有的組織結構,將一或多部 Active Directory 伺服器與 Apex Windows 和 Mac 雷腦提供安全防護,來抵禦安全威魯。 Central 整合,以擴展及對應使用者/端點目錄。 深入瞭解 | 立即設定 深入瞭解 | 立即設定 正在準備伺服器... ▲ Apex One 伺服器和用戶端移轉 策略管理 诱過建立策略、選取目標及設定產品設定清單,來從單一管理主控台對受 Apex One SaaS 支援從執行版本 XG SP1 (或更新版本) 的內部部署 Apex 注意: 主控台準備就緒後將自動開啟, 且趨勢科技將傳送通知電子郵件到 grn me以讓您 管理產品和端點強制執行產品設定。 One 伺服器移轉伺服器和 Apex One 用戶端設定。 瞭解如何存取管理主控台。 ④ 您可以随時在主功能表中按一下「說明>快速入門手冊」來開啟快速入門手冊畫面。 關閉 為了確保所有客戶均能獲得最佳的資源配置, Trend Micro Apex One™ as a Service 實施了離線 Trend Micro Apex One™ 休眠政策。



之後就可以依照通知信中的URL開啟Apex One SaaS主控台

Trend Micro Apex One™ as a Service Web 主控台

發件人: no-reply@manage.trendmicro.com, 收件人: generations 時 間:

親愛的

您的 Trend Micro Apex One™ as a Service主控台已可供使用。按一下以下連結來存取您的 Web 主控台。

登入資訊

- URL : https://swjxrq.manage.trendmicro.com/WebApp/Login.aspx
- 使用者名稱:

注意:此為僅適用於您公司的 Web 主控台的特殊 URL。您可以將此 URL 加入書籤以便於存取。

為了確保所有客戶均能獲得最佳的資源配置, Trend Micro Apex One[™] as a Service 實施了離線 Trend Micro Apex One[™] 休眠政策。

注意:當您很長一段時間未登入服務,並且主控台未管理任何 Security Agent 時,趨勢科技會將 Apex One as a Service 歸類為離線。

順頌商祺, 趨勢科技團隊

此為自動產生的電子郵件,請勿回覆。如需詳細資訊,請造訪 Trend Micro eSupport。





Credits Activation



啟用 Vision One 授權

自行申請試用Vision One的話, 請點選通知信的「Activate Trial」 若是購買Vision One授權, 請點選電子授權書的「Activate Here」

Welcome to Trend Micro Vision One

發件人: connect@trendmicro.com, 收件人: guar the 間



Welcome to Trend Micro Vision OneTM

Your 60-day all-access trial begins today.

Activate Trial



啟用 Vision One 授權

請參照「建立CLP帳號及啟用 Product or Credit 授權的SOP」的 P.4~P.7設定:

https://trendmicro.sharepoint.com/:b:/s/TWBUtest/EcCGMLAU H1RIuo59OEtQgEwBb62QqOcpl6Zsx7Q77-levQ?e=MKj5hM

注意:一個CLP帳號視為一個公司行號,因此不建議多個管理 者建立各自的CLP帳號,也不要將所購買的各項產品授權分別 註冊到不同CLP帳號下。



啟用 Vision One 授權

Vision One授權啟用成功後,請點選藍框位置,進到Vision One



Trend Micro Vision One[™] is a threat operations platform offering advanced XDR capabilities across email, endpoints, servers, cloud workloads, and networks as well as Zero Trust applications, Mobile Security, and more.



登入 Vision One

接著看到初始化設定,下一步後,就可以看到Vision One console

Initial Configuration

Trend Micro Vision One will be provisioned in the following geographic region.

Region: Singapore

Next

One [™] Credit Usage		
The Samba Vu CVE-2021-44142 is a vulnerability that specific gap exists in the parsing of the I vulnerability to execute code in the root of being compromised by threat actors. Samba nrice to 4.13 cT that use the VES	Inerability: What is CVE-2021-44142 and How to Fix It allows remote attackers to execute arbitrary code on affected installations of Sam EA metadata in the server daemon smbd when opening a file. An attacker can abu context even without authentication. If left unpatched, affected systems could be CVE-2021-44142 is a remote code execution Samba vulnerability affecting all vei S module v/S. finil and configured to use trilit metadata-metable or full resources	ba. The ctivities on Set Up se this Set Set Up at risk rsions of
		file.
Maliciously Crafted File	Transfer Request to Samba Server Potential malicious (using Apple File Protocol) remote code execution	activities on Set U



Product Connector



連接 Apex One SaaS 到 Vision One

點選Connect Product, 選擇Apex One as a Service, 點選Save

0	Trend Micro	o Vision One™ Product Cor	nnector	Ī	~
	Connect				Connect Product ^
	Product	Connection status	Data center	Identifier 🛈	* Product name:
[ů]]			No product has been connected yet. Click C	connect to connect your fi	Select a product ^
Х			Conne	ect Product	Apex One as a Service
					Cloud App Security
					Cloud One - Workload Security
					Deep Discovery
					Network Security
					Deep Security Software
					TippingPoint Security Management System
					Trend Micro Web Security



連接 Apex One SaaS 到 Vision One

稍待片刻,就會看到Apex One SaaS增加在列表中:

O	Trend Micro Vision One™	M Product Connector		O	(UTC+00:00)	Ļ		
	Connect				>	(DR Da	ta Center: Sing	apore
	Product	Connection status	Data center	Identifier 🛈	Description	Ac	tion	
[ÿ]	Apex One as a Service	Connected	Singapore	(Taiwan)			Disconnect	
Х								



開啟Vision One主控台-方法一

登入<u>CLP</u>後,在Vision One項目的右方,點選「開啟主控台」

Customer Licensing Portal

▲ TM_TS_SMB ▼

產品/	/服務 公司 ▼	說明 ▼						
產品/	服務							
+提	供金鑰							
\$	產品/服務		\$ 作用中使用授權	◆ 使用	授權≑	到期日	•	處理行動
0	Trend Micro Visi	on One™		Free		2023/12/31		[】 開設主控台



開啟Vision One主控台-方法二

點選Apex One SaaS console的Vision One會出現錯誤是正常, 因為該捷徑需要搭配MxDR授權。

🥏 Trend Micro Apex Central™



\$	資訊中心	目錄	生政	<u>中</u> 入武易咨钮	同權	佔測	答理	────────────────────────	Trend Micro Vision One
摘	摘要 安全威脅調查		swjxrq.mai	nage.trendmicro.	.com 顯示			+	
			功能已關閉 無法透過單	-登入來登入 Trend N	dicro Vision	One。雲要	<u></u> 其他授權和	答	
嚴重安全威脅			理員帳號權限	业八 尔亚八 mend k 【。如需詳細資訊,請	情洽詢您的支	援人員。			勒索軟體防範
範圍	: 最近7天 >						確定		期間: 最近7天 ~

請透過此URL<u>https://portal.xdr.trendmicro.com</u>開啟Vision One





Install XDR Sensor



Windows 支援平台

- Desktop
 - Windows 10 (32/64-bit)
 - Windows 8.1 (32/64-bit)
 - Windows 7 (32/64-bit)
- Server
 - Windows Server 2019 (32/64-bit)
 - Windows Server 2016 (32/64-bit)
 - Windows Server 2012 / 2012 R2 (32/64-bit)
 - Windows Server 2008 R2 (32/64-bit)

- 最小需求: CPU:2 cores/ 記憶體:512 MB/硬碟可用空間:3 GB



Linux/Mac 支援平台

Linux

- Red Hat Enterprise Linux 6/7/8 (64-bit)
- Amazon Linux (64-bit)
- Amazon Linux 2 (64-bit)
- CentOS Linux 6/7/8 (64-bit)
- Ubuntu 16/18/20
- 建議規格:記憶體:5GB/硬碟可用空間:1GB
- Mac
- macOS High Sierra (10.13) and later
- 硬碟可用空間: 3 GB



登入Vision One > 切換到Endpoint Inventory





方法一:在El app(Endpoint Inventory)清單中勾選,並啟用。

Trend Micro Vision One [™] Endpoint Inventory					Enable XDR Sensor		×		
Endp	ooint List	Agent Installer			After enabling XDR capabilities on the following supported endpoints, the endpoints automatically start sending activity data to Trend Micro for state-of-the-art threat detection and alerting.				
Ċ	⊋ All		154	ত ি No f	Endpoint name	Operating system			
					L L	Windows 10	×		
En	able	emove X 2 sele	cted		1	Windows 10	×		
	4								
	Endpoir	nt name	IP addres	S					
9	Ţ		192.						
	Ţ		192.						
	Ţ		192.						
	Ţ	yWu	192.			Enable	Now (2) Cancel		
	Ţ	Х.	192.						



方法二: 運用分組概念, 對特定群組自動啟用XDR Sensor。 在Endpoint Groups中, 點選「加號」。





方法二:運用分組概念,對特定群組自動啟用XDR Sensor。 設定群組資訊,並選擇過濾端點的條件:

Endpoint Group			Endpoint name		~
Group name (for example, US or Finance	e)		CONTAINS	 Ente 	r string
Descriptions					OK Cancel
Target endpoints:	AND	Endpoint name		~	CONTAINS ~
+ Add criteria		Endpoint name			CONTAINS
		IP range			EQUALS
Preview endpoints	Save	Operating system			STARTS WITH
© 2020 Trand Miaro Inc					

MICRO

方法二:運用分組概念,對特定群組自動啟用XDR Sensor。 切換到Security Policies > Endpoint,選擇特定群組,即可設定是否啟用功能。











關於更多Vision One參考資訊,請查看<u>V1 KB main page</u>

