

Deep Security (On-prem)

註冊VisionOne SOP



● 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



DSM 註冊 Trend Micro Vision One (XDR)

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

	ADMINISTRATION	sion One [™]	M Security	v Dashboard			
	Single Sign-On						
[ġ]]	User Accounts						
Х	User Roles				(-		
₽≣	Product Connector	k Techniques	DINS	Go t	Go to App		
<u>_</u>			Critical	High	Medi	Total ↓	
-~	Third-Party Integration	1.92)			450	450	
	Alert Notifications	10.49)		20	50	70	
Ę		cal(192.168			59	59	
ഫ്പ്	Audit Logs	3.33)		39		39	
રંજે	Console Settings	3.108)			36	36	
	License Information	2.80)	-	-	29	29	



• 建立 Product Connector

O									
	Connect								
	Product	Connection status	Data center	Identifier ()					
	Email Sensor	Connected 2021-11-29 13:57:56	US	TWTS_XDR: Default organization (United States)					
<u>କ</u> ଜ୍ଞା	Apex One as a Service	Connected 2021-11-29 13:57:58	US	TWTS_XDR (Taiwan)					



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

Trend Micro Vision O	NeTM Product Connector	Connect Product			
Connect				* Product name:	
Product	Connection status	Data center	Identifier ()	Select a product	^
Apex One as a Service	Connected 2021-11-27 13:01:17	SG	nanmat_kao (1	Cloud App Security	
Endpoint Sensor	Connected 2021-07-25 14:06:02			Cloud One - Workload Security	
Cloud One - Workload Security	Connected 2021-11-27 11:15:10	115	ann deensecui	Deep Discovery	
cloud one - workloud security		05	app.accpsecu	Deep Security Software	
				Trend Micro Web Security	



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

Connect Product

* Product name:

Deep Security Software

Enrollment token:

<u>Click to generate the enrollment token.</u> The token expires after 24 Automatically adds the product to the product list.

Description:

Connect Product

* Product name:

Х

Deep Security Software

① The product has been added to the product list. Copy and paste the enrollment token to the connecting product's web console to complete configuration.

Enrollment token:

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJjaWQiOiI2ZGNmYjł

Expiration date: 2021-11-30 18:02:57

Description:



ດີ

Х

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

🔊 TREND Deep S	Security Dashboard Actions Alerts Events & Reports Computers Policies Administration	MasterAdmin - 🌲 News - 🕐 Help 🔕 Su							
Scheduled Tasks	System Settings								
Event-Based Tasks	Agents Alerts Contexts Event Forwarding Ranking System Events Security Updates Smart Feedback Trend Micro XDR Connected Threat Defense	SMTP Storage Proxies Advanced							
Manager Nodes Licenses	Enrollment status: Not registered								
User Management System Information	Register enrollment token								
> C Updates	Forward activity data and security events to Trend Micro XDR								
	Trend Micro XDR Endpoint Inventory								
	Allow Trend Micro XDR to enable Activity Monitoring on Linux Deep Security Agent To monitor the activity data on Linux agents, this setting needs to be enabled. Personally identifiable information is collected by Trend Micro XDR.								
(



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

0	TREND Deep S	Security Dashboard Actions Alerts Events & Reports Computers Policies Administration	
2	System Settings	System Settings 3	
×	Scheduled Tasks		
E	Event-Based Tasks	Agents Alerts Contexts Event Forwarding Ranking System Events Security Updates Smart Feedback Trend Micro V	Vision One Connected Inreat Defense SMTP Storage Proxies Advanced
3	Manager Nodes	4 Registration	
Ð	Licenses	Enrollment status: Not registered	
~ 🤹	User Management	Register enrollment token	
	👪 Users	Security Events Forwarding	
	Roles	Forward security events to Trend Micro Vision One	
	Contacts	Activity Data Economica	
	🔍 API Keys	Install Trend Micro Endpoint Basecamp with the deployment script below to forward activity data to Trend Micro Vision One. The deployment script can	the deployed using tools such as RightScale. Chef. Pugnet, or SSH as an administrator, After installing, enable
~	Identity Providers	NOTE Personally identifiable information is collected by Trend Micro Vision One	and a block and a second s
	SAML	Pietform: Linux (64-bit) + 0	
6	System Information	5	
~ ©	Updates	Proxy. Deline the MTTP proxy intermation in this script for Endpoint basecamp that requires a proxy.	Trend Micro Vision One Enrollment Token
~	Security		Enrollment Token:
	Rules		evJ0eXAiOiJKV1OiLC/hbGciOiJSUzI1NiJ9.evJiaWOiOiJkYzU5ODA2OC1IZGMwLTO3MTUtYidiYS1iZmI2MD
	Patterns		21
~	Software		
	Agent Versior		n: 12
	Download Cer	Save to File Copy to Clipboard	from discussion and a state of a device of the second state of the second state of
	Local		4
	📀 Relay Managemer		
~ X	Tools		Register Cancel



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

🕖 IREND Deep S	Security Dashboard Actions Alerts Events & Reports Computers Policies Administration	Primary TI-AV	vs-prod-2 - ⑦ Help	🔘 Sup
 System Settings Scheduled Tasks Event-Based Tasks 	System Settings Tenants Agents Alerts Contexts Event Forwarding Ranking System Events Security Updates Smart Feedback Trend Micro Vision One Threat is	Intelligence SMTP	Storage Proxies	Advanc
 Manager Nodes Tenants Licenses User Management Users 				
 Roles Contacts API Keys Identity Providers System Information Updates 	 Forward security events to Trend Micro Vision One Activity Data Forwarding To forward activity data to Trend Micro Vision One, install Trend Micro Endpoint Basecamp with the deployment script below or with an installer from Trend Micro Vision One > Endpoint II NOTE Personally identifiable information is collected by Trend Micro Vision One. Platform: Linux (64-bit) Other Content on Conte	Inventory. After installin	ng, enable the sensor on Tre	end Micro
 Security Software Agent Version Download Cei Local Relay Managemer 	Proxy: Define the HTTP proxy information in this script for Endpoint Basecamp that requires a proxy. #/bin/bash # PROXY_ADDR_PORT define proxy for software download. Use the following code snippet and fill the proxy information. # PROXY_ADDR_PORT=" # HTTP_PROXY is exported for compatibility purpose, remove it if it is not needed in your environment. # export HTTP_PROXY=http://\$PROXY_ADDR_PORT/ # export HTTPS_PROXY=http://\$PROXY_ADDR_PORT/ # export HTTPS_PROXY_HTTPS_PROXY_ADDR_PORT/ # export HTTPS_PROXY_HTTPS_PROXY_HTTPS_HTT			



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





	8	10.13.07		
Micko	د مصر End	Inoint Connected		
Security Posture	Sen	Isor 2020-10-13		
	- \$\$	10.23.50		
🖄 Threat Intelligence 🗸 🗸	Tip	pingPoint Connected	172.16.207.8	Disconnect
XDR v	?	08:10:04		
€ Zero Trust Secure Access ∨	The Dee	ep Security Connected	https://172.16.250.164:4119	Disconnect
≣£ Search	>>	18:20:14	(172.16.250.164;1eb000000;5e0:7556:220:e042;%eff0;2001:0:2651:762C2C44;9e01:2370;558;1eb00000;2C44;9e01:2370;558%net1;1eb0000000;5e1e;ac10;1a44%net2)	
🗐 Response Management		1		
Security Policies				
🖉 Mobile Security 🗸 🗸				
避 Inventory Management ∨			云Vision One > Administration > Draduct Commo	ctor
Administration ^		•	主VISION ONE > Aummistation > Preduct Comme 检询Doop Socurity coftware 油炉毕能 (妈感)	clor
Single Sign-On			120元Deep Security Software 建級M忽(級燈)	
User Accounts				
User Roles			計皿作業点式	
Product Connector			就MIF未元パ!	
Third-Party Integration				
Alert Notifications			EIND	



• 下載XDR(XBC) Agent 安裝 from Endpoint Inventory

0	Trend Micro XDR Endpoint Inventory						🕓 итс 🔳 тм 🔑 😣
(\underline{P})	Q					🛃 Down	nload the Agent Installer
م چہ !!!	Available endpoints	2 Installing to endpoint	24	Action required	25	Reporting to XDR	26
<u>[ي]</u>	Enable View Recommended Endpoints						
	Endpoint Name	Status		IP Address		Operating System	
<u>ش</u>	10.209.44.231	Available		10.209.44.231		Red Hat Enterprise 7 (64 bit)	
ঞ	JerryWin10T88LF64	Available		10.209.72.205		Windows 10	
£ €							
87							
Ţ							
ŝ							
6							

從DSM主控台取得XDR(XBC) Agent佈署Script

🕗 IREND Deep Security 🛛 🛛	ashboard Actions Alerts Events & Reports Computers Policies Administration MasterAdmin - 🏚 News - 🕐 Help 🔇 Support - 🔍 Help Center Search
Action Required - Assess the impact of Sunburst in y	our environment. Check the Tester which a Early Warning service to see if you are affected by the latest targeted attack. Open Console
 Action Required - Assess the impact of Sundurst in y System Settings Scheduled Tasks Event-Based Tasks Manager Nodes Licenses User Management System Information Updates System Information Software Agent Version Control Download Center Local Relay Management 	Set in the control is all water to be any wate
	Save
	Activate WiAdbwede Windows
© 2020 Trend Micro Inc.	

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

2	Trend Micro XDR Endpoint Inventory						🛇 UTC 📕 xdr_prod_sao 🇘 🔗
Ð	Q						Download the Agent Installer
≣: ⊓©]	Available endpoints 1	Installing to endpoint	0	Action required	0	Reporting to XDR	9
ر مې	Enable View Recommended Endpoints						
۲	Endpoint Name	Status					
<u>.</u>	ip-172-31-10-20.us-west-2.compute.internal	Available	Enable XDR Now				
			After enabling XDR capabiliti to Trend Micro for state-of-tl	es on the following supported ne-art threat detection and ale	d endpoints, the endpoints a erting.	utomatically start sending activ	vity data
RJ			Endpoint Name		Operating System		
Ģ			ip-172-31-10-20.us-west-2	.compute.internal	Red Hat Enterprise Linux	8.0 (Ootpa)	×
\square							
Ţ							
14							
ŝ							
?							
 *+							
$\rangle\rangle$							
15	© 2020 Trend Micro Inc.					Enable XDR Now (1)	Cancel

REND

R O

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

Extend	xtend your XDR coverage to include your Office 365 mailboxes for correlated detection and investigation.									
0	Trend Micro XDR Endpoint Inventory		(りUTC 📕 xdr_prod_sao 🇘 🙎						
(\underline{P})	٩						t Do	wnload the Agent Installer		
:≡	Available endpoints	0	Installing to endpoint	0	Action required	0	Reporting to XDR	10		
٦ مې										
۲	Endpoint Name	Status		Last reported	IP Addres	SS	Operating System			
~	DESKTOP-35DOG1Q	Reporti	ng to XDR	2020-11-25T07:20:32.000Z	192.168.1	54.224	Windows 10			
<u>≦</u> عک	DESKTOP-6AE7QL6	Reporti	ng to XDR	2020-11-10T07:50:33.000Z	192.168.1	63.188	Windows 10			
	DESKTOP-MJV704U	Reporti	ng to XDR	2020-11-25T07:21:53.000Z	10.209.93	.6	Windows 10			
83	ER-PD20H2X86	Reporti	ng to XDR	2020-11-25T07:23:29.000Z	10.209.17	9.111	Windows 10			
	HA_19H1X86	Reporti	ng to XDR	2020-11-25T07:20:32.000Z	192.168.3	.131	Windows 10			
	ip-172-31-10-20.us-west-2.compute.internal	Reporti	ng to XDR	2020-11-24T09:04:01.000Z	172.31.10	.20	Red Hat Enterprise L	inux 8.0 (Ootpa)		
\square	ip-172-31-7-98.us-west-2.compute.internal	Reporti	ng to XDR	2020-11-25T07:19:48.000Z	172.31.7.9	98	Amazon Linux 2			
ŗ	ip-172-31-9-194.us-west-2.compute.internal	Reporti	ng to XDR	2020-11-24T15:01:23.000Z	172.31.9.1	194	CentOS Linux 8 (Core	e)		
۶.	localhost	Reporti	ng to XDR	2020-11-24T10:19:16.000Z	10.209.93	.5	Red Hat Enterprise L	inux		
- <u>-</u>	localhost	Reporti	ng to XDR	2020-11-25T07:20:53.000Z	10.209.93	.5	Red Hat Enterprise L	inux		
503										

? ||;+

