

Connecting CAS to Vision One

1. Inventory Management->Email Account Inventory".

🖄 Inventory Management 🔺

Endpoint Inventory

Email Account Inventory

Network Inventory

Service Gateway Inventor...



2. 點選Get Started



3. mailbox數量越多,同步的時間會越久

4. 完成後於Email Account Inventory就選擇要XDR monitor的 mailbox

Trend Micro Vision One [™] Email Account Inventory	Manage Email Accounts	>
Manage Mailbox Sensors Active mailbox sensors: 3	Move mailboxes to the Selected Accounts list to automatically begin sending alerting. Removing a mailbox from the Selected Accounts list stops the activit	activity data to Trend Micro for state-of-the-art threat detection and y data collection and removes collected data.
	Available Users / Groups (3)	Selected Accounts
Users / Groups ¢	Search Q	绕 All Users/Groups X
ନ୍ତି All Lisers/Groups	All Users / Groups	
	・ 🗌 糸 All Users/Groups	
	・ 🗌 冬 All Company	
	→ │ 冷 Trend Micro TW Support	
	□ A hktmsupport	
	□ A TWBUSupport	
	□ A TWWTSupport	
4 © 2019 Trend Micro Inc.		

 CAS同時會有一個Default Exchange Online Policy ATP (For Trend Micro XDR Only), 但無法從CAS進行策略修改

Dashboard Advarced Threat Protection Data Loss Prevention Logs Quarantine Administration Add Delete Copy Run Manual Scan Internal Domains Priority O Policy Exchange Online Policies Blocked Lists for Exchange Online enabled Internal Domains Image: Comparity of the policy Policy Image: Comparity of the policy ATP Image: Comparity of the policy of the policy of the policy ATP (Monitor Only) Image: Comparity of the policy of the policy ATP (Monitor Only) Image: Comparity of the policy of the policy ATP (Monitor Only) Image: Comparity of the policy ATP (Monitor Only) Image: Comparity of the policy at the policy created for target Image: Comparity of the policy of the policy at the policy created for target Image: Comparity of the policy at the policy created for target Image: Comparity of the policy of the policy at the policy at the policy at the policy created for target Image: Comparity of the policy at the policy		Clou	d App Security
Add Delete Copy Run Manual Scan Internal Domains Priority Policy Exchange Online Policies Blocked Lists for Exchange Online enabled Image: Default Microsoft Exchange Online Policy ATP Image: Default Microsoft Exchange Online Policy ATP Image: Image: Image:	Dashboard	A	dvanced Threat Protection Data Loss Prevention Logs Quarantine Administration
Priority • Policy Exchange Online Policy Blocked Lists for Exchange Online enabled () Image: Construction of the policy of t	Add	•	Delete Copy Run Manual Scan Internal Domains
Exchange Online Policies Blocked Lists for Exchange Online enabled Image: Content of the conten	Priority	0	Policy
Image: Control of the control of th	Exchange (Online	e Policies Blocked Lists for Exchange Online enabled 🕕
1 Image: Comparison of the second			ON Default Microsoft Exchange Online Policy ATP
Image: Contract of the second seco	1		
2 TWBUSupport Test Image: Construction of the point of			OFF TWBUSupport
Image: Control Default Exchange Online Policy ATP (Monitor Only) BEFAULT POLICY: Works in monitor mode to scan targets and record detections only. All actions are fixed to PASS and not configurable. Image: Control Default Exchange Policy ATP 4 DEFAULT POLICY: Policy used if no other policy created for target Image: Control Default Exchange Online Policy ATP (For Trend Micro XDR Only) 5 Default Exchange Online Policy ATP (For Trend Micro XDR Only) 5 Default Exchange Online Policy ATP (For Trend Micro XDR Console to XDR. This policy cannot be changed manually. It sets all actions to Pass and has the lowest priority.	2		TWBUSupport Test
3 DEFAULT POLICY: Works in monitor mode to scan targets and record detections only. All actions are fixed to PASS and not configurable. 1 OFF Default Exchange Policy ATP 4 DEFAULT POLICY: Policy used if no other policy created for target 1 ON Default Exchange Online Policy ATP (For Trend Micro XDR Only) 5 DEFAULT POLICY: Policy used to connect Trend Micro XDR for threat visibility and investigation. After it is enabled, Cloud App Security sends email activity data of users specified in the Email Account Inventory app on the XDR console to XDR. This policy cannot be changed manually. It sets all actions to Pass and has the lowest priority.			OFF Default Exchange Online Policy ATP (Monitor Only)
Image: Control of the sector of the secto	3		DEFAULT POLICY: Works in monitor mode to scan targets and record detections only. All actions are fixed to PASS and not configurable.
4 DEFAULT POLICY: Policy used if no other policy created for target Image: Default Exchange Online Policy ATP (For Trend Micro XDR Only) 5 DEFAULT POLICY: Policy used to connect Trend Micro XDR for threat visibility and investigation. After it is enabled, Cloud App Security sends email activity data of users specified in the Email Account Inventory app on the XDR console to XDR. This policy cannot be changed manually. It sets all actions to Pass and has the lowest priority.			OFF Default Exchange Policy ATP
 Default Exchange Online Policy ATP (For Trend Micro XDR Only) DEFAULT POLICY: Policy used to connect Trend Micro XDR for threat visibility and investigation. After it is enabled, Cloud App Security sends email activity data of users specified in the Email Account Inventory app on the XDR console to XDR. This policy cannot be changed manually. It sets all actions to Pass and has the lowest priority. 	4		DEFAULT POLICY: Policy used if no other policy created for target
5 DEFAULT POLICY: Policy used to connect Trend Micro XDR for threat visibility and investigation. After it is enabled, Cloud App Security sends email activity data of users specified in the Email Account Inventory app on the XDR console to XDR. This policy cannot be changed manually. It sets all actions to Pass and has the lowest priority.			Default Exchange Online Policy ATP (For Trend Micro XDR Only)
	5		DEFAULT POLICY: Policy used to connect Trend Micro XDR for threat visibility and investigation. After it is enabled, Cloud App Security sends emai activity data of users specified in the Email Account Inventory app on the XDR console to XDR. This policy cannot be changed manually. It sets all actions to Pass and has the lowest priority.



如何將CAS從Vision One Disconnect

1. 至Manage Mailbox Sensors

6

Trend Micro Vision One [™] Email Account Inventory				
Manage Mailbox Sensors Active mailbox sensors: 3	Manage Email Accounts			x
Users / Groups ¢	Move mailboxes to the Selected Accounts list to automatically begin alerting. Removing a mailbox from the Selected Accounts list stops th	sending activity	y data to Trend Micro for state-of-the-art threat detectio collection and removes collected data.	on and
욨All Users/Groups	Available Users / Groups (3) Search Q. All Users / Groups \$?, All Users/Groups		Selected Accounts ନି: All Users/Groups	
2. 將所有Mailbox移除				
© 2019 Trend Micro Inc.			Save	

如何將CAS從Vision One Disconnect

• 顯示為No XDR sensors enable on mailboxes

	ن UTC+08:00
Manage Mailbox Sensors Active mailbox sensors: 0	Ν
Users / Groups 💲	Email address 💲
No XDR sensors enabl	led on mailboxes
Select mailboxes to enable XDR sensors. The sensor sends activity data dire	ectly to Trend Micro for state-of-the-art threat detection and alerting.
Manage Mailbo	

• CAS上的Policy也會disable

OFF Default Exchange Online Policy ATP (For Trend Micro XDR Only) DEFAULT POLICY: Policy used to connect Trend Micro XDR for threat visibility and investigation. After it is enabled, Cloud App Security sends email activity data of users specified in the Email Account Inventory app on the XDR console to XDR. This policy cannot be changed manually. It sets all actions to Pass and has the lowest priority.

All Users



5



如何將CAS從Vision One Reconnect

• 重新加回Mailbox

Aanage Email Accounts			
fove mailboxes to the Selected Accounts list to automatically begin lerting. Removing a mailbox from the Selected Accounts list stops th	sending activit ne activity data	v data to Trend Micro for state-of-the-art thre collection and removes collected data.	at detection and
Available Users / Groups (3)		Selected Accounts	
Search Q		糸 All Users/Groups	
All Users / Groups			
・ □ 糸 All Users/Groups			
			Save Cancel
end Micro Inc.			

