



Connecting Tipping Point to Vision One



Automated response for suspicious objects

(No need extra license)

啟用Third-Party Integration service

- 佈署好Service Gateway後，並註冊到Vision One後，啟用Third-Party Integration service。

The screenshot displays the Trend Micro Vision One™ interface. The top navigation bar includes the Trend Micro logo, the text 'Trend Micro Vision One™', and a 'Service Gateway Inventory' tab. On the right, there is a clock showing 'UTC+08:00', a notification bell with a red '1', and a user profile icon labeled 'TWTS_XDR'.

The left sidebar contains a list of navigation items: Security Posture, Assessment, Threat Intelligence, XDR, Zero Trust Secure Acc..., Search, Response Management, Mobile Security, and Inventory Management.

The main content area is divided into two panels. The left panel, titled 'Service Gateway Inventory', features a '+ Download Virtual Appliance' button and a table with the following data:

Service Gateway	Connection status	Connected endpoints	Upload
TWTS-SG (3.1.1.1)	Healthy	1	51.55 MB
localhost.localdomain (3.1.1.1)	Unhealthy	0	0 MB

The right panel, titled 'Service Gateway Settings', contains the following sections:

- TWTS-SG**
- Services**
 - ☒ ActiveUpdate ⓘ
 - ☒ Smart Protection Services ⓘ
 - ☒ Suspicious Object List Synchronization ⓘ
 - ☒ Third-Party Integration ⓘ (highlighted with a red box)
- Product Component Update**
 - ☒ Hourly
 - ☐ Every 15 minutes
- [Configure update sources](#)
- Service Gateway Update**

取得API Key

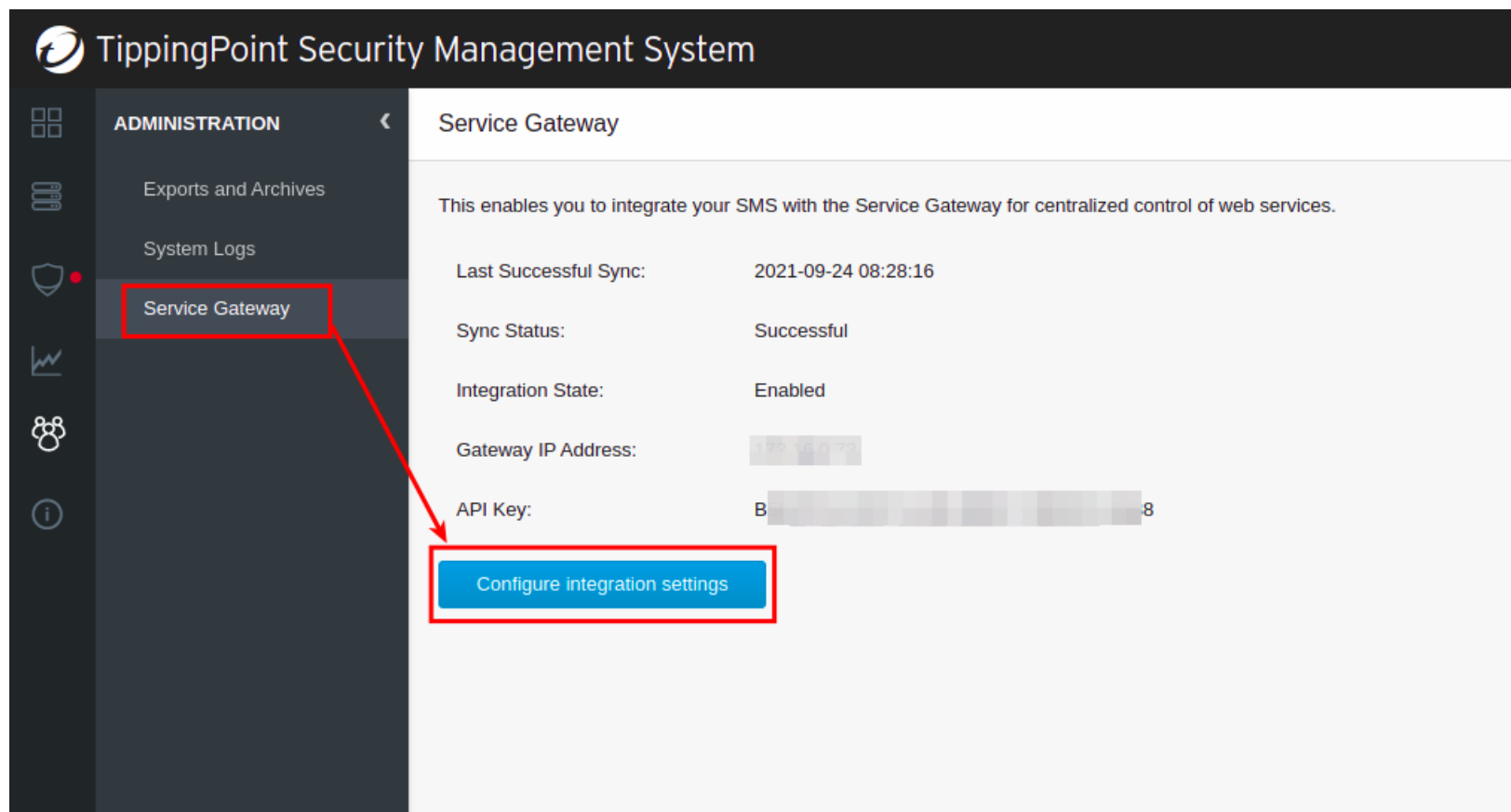
- 到Vision One 的 Inventory Management > Service Gateway Inventory 中，點選 Manage API Key 取得API Key。

The screenshot shows the Trend Micro Vision One interface. The top navigation bar includes the Trend Micro logo, the title 'Trend Micro Vision One™', and the current page 'Service Gateway Inventory'. The right side of the header shows the time 'UTC+08:00', a notification bell with a red '1', and the user profile 'TWTS_XDR'. The left sidebar contains navigation links for Security Posture, Assessment, Threat Intelligence, XDR, and Zero Trust Secure Acc... The main content area features a table with columns: Service Gateway, Connection status, Connected endpoints, Uploaded, Downloaded, Last connected, and Action. The table lists two entries: 'TWTS-SG' (Healthy) and 'localhost.localdomain' (Unhealthy). A red box highlights the 'Manage API Key' button in the top right corner of the main content area. An arrow points from this button to the 'API Key' dialog box on the right. The dialog box has a title 'API Key', a text input field containing a masked API key, a 'Change API Key' button, and a message: 'Suspicious Object List Synchronization requires the API key to authenticate connections between the connected Trend Micro products and Service Gateway.'

Service Gateway	Connection status	Connected endpoints	Uploaded	Downloaded	Last connected	Action
TWTS-SG ()	Healthy	1	51.55 MB	136.85 MB	Just now (2021-09-24 08:30:52)	⚙️ 🗑️
localhost.localdomain ()	Unhealthy	0	0 KB	0 KB	57d (2021-07-28 23:20:58)	⚙️ 🗑️

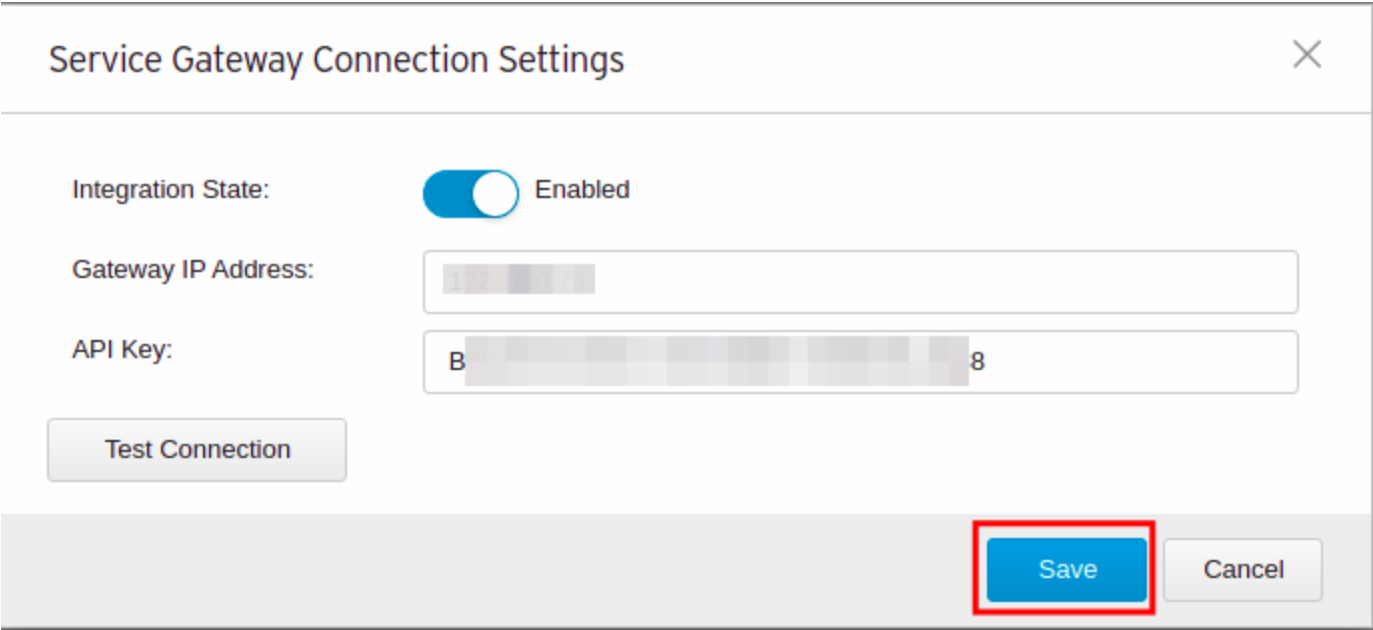
SMS設定Service Gateway

- 登入到 SMS Web Console, 點選到 ADMINISTRATION > Service Gateway, 點選 Configure integration settings



SMS設定Service Gateway

- 輸入Service Gateway IP及前步驟中，在Vision One上取得的API key，點選Save。



The image shows a 'Service Gateway Connection Settings' dialog box. It has a title bar with a close button (X). Inside, there are three main sections: 'Integration State' with a toggle switch set to 'Enabled'; 'Gateway IP Address' with a text input field containing '1'; and 'API Key' with a text input field containing 'B' followed by a masked area and '8'. Below these fields is a 'Test Connection' button. At the bottom right, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted with a red rectangle.

Service Gateway Connection Settings

Integration State: ☒ Enabled

Gateway IP Address:

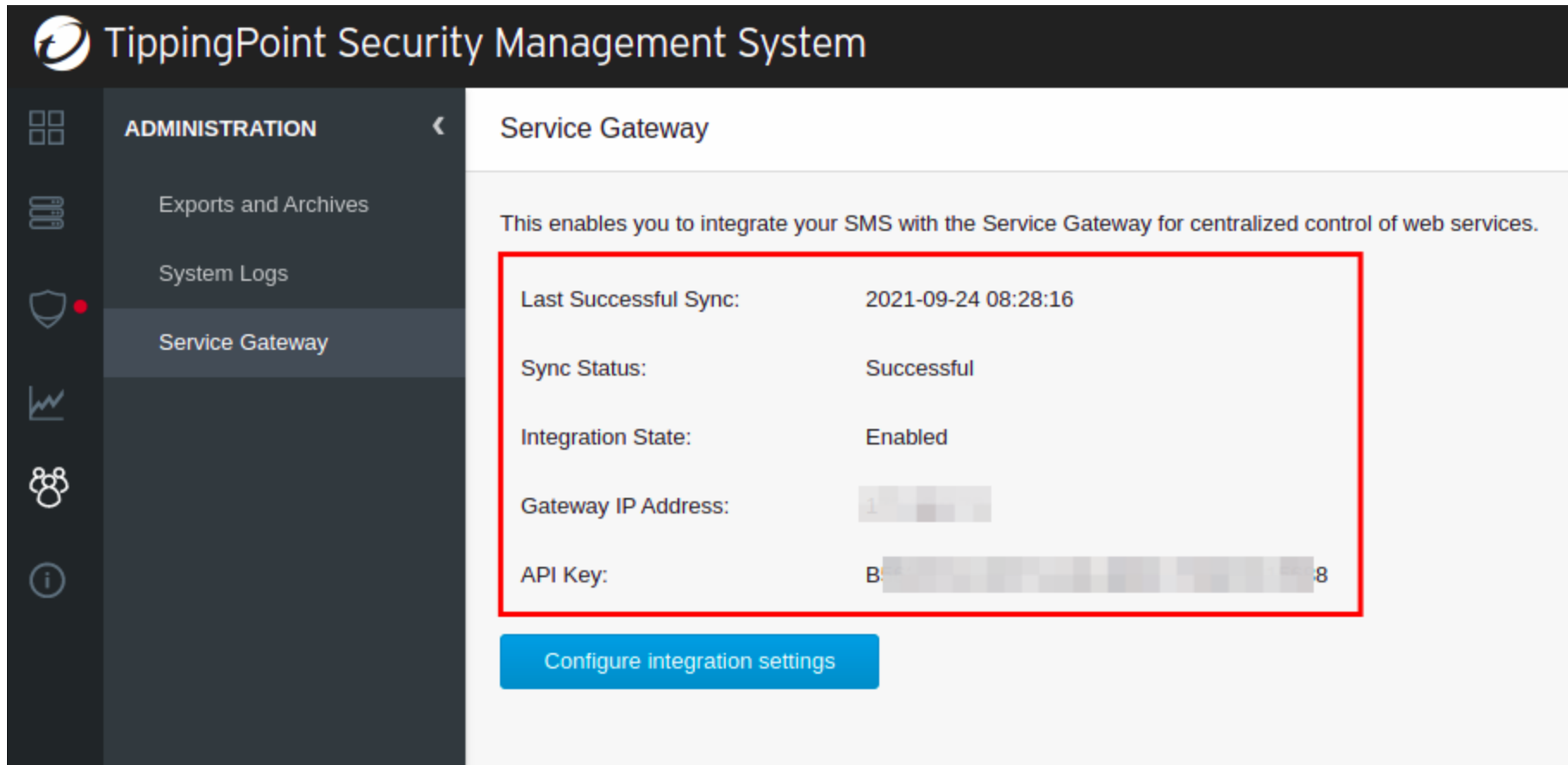
API Key:

Test Connection

Save Cancel

SMS設定Service Gateway

- 若成功，可在 SMS Web Console，點選到 ADMINISTRATION > Service Gateway中，看到 同步狀態。



TippingPoint Security Management System

ADMINISTRATION < Service Gateway

Exports and Archives

System Logs

Service Gateway

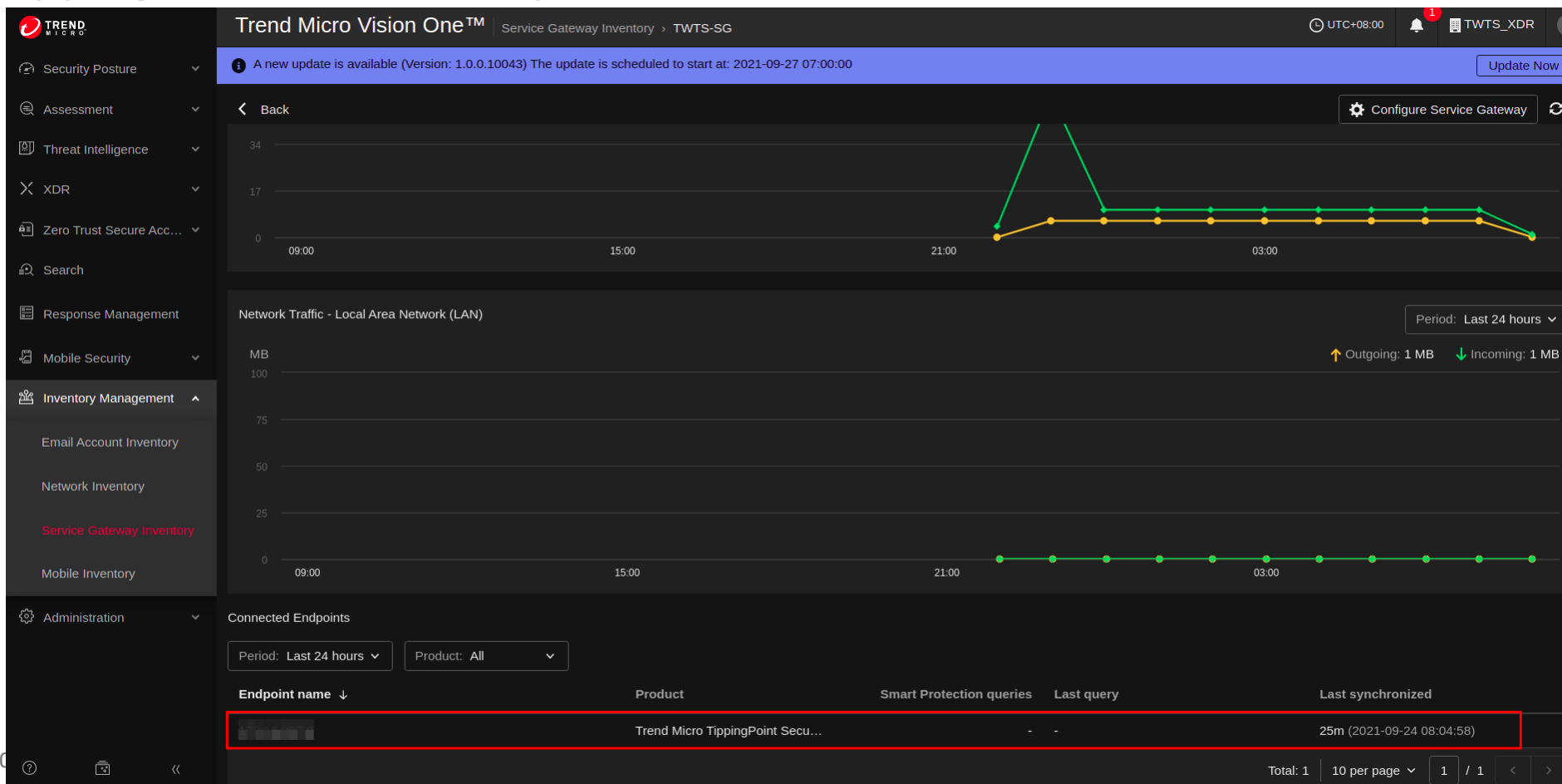
This enables you to integrate your SMS with the Service Gateway for centralized control of web services.

Last Successful Sync:	2021-09-24 08:28:16
Sync Status:	Successful
Integration State:	Enabled
Gateway IP Address:	[Redacted]
API Key:	B-[Redacted]-8

[Configure integration settings](#)

SMS設定Service Gateway

- 以及在Vision One 的 Inventory Management > Service Gateway Inventory 中看到Tipping Point回報的 Endpoint Name。



手動新增UDSO

- 再到Threat Intelligence > Suspicious Object Management > Suspicious Object List 中，新增UDSO。

Trend Micro Vision One™ Suspicious Object Management

UTC+08:00 TWTS_XDR

Suspicious Object List Exception List

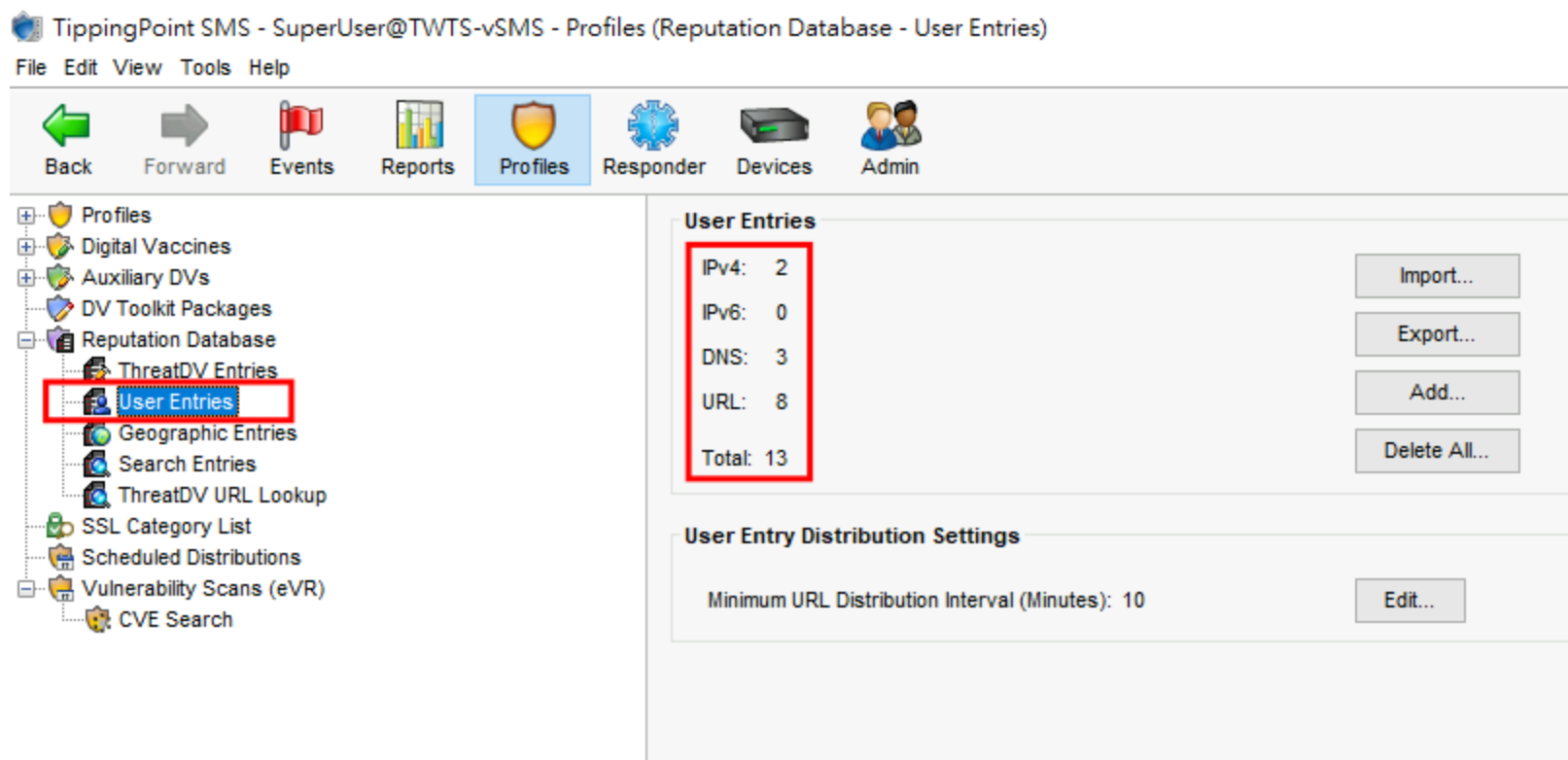
Applicable products: 2

+ Add Last updated: All Object type: All Source: All Object, Source details

☐	Object	Risk level	Action ⓘ	Expiration	Source	Source details	Last updated ↓
☐	wrs49.winshipway.com	High	Block / Quarantine	2021-10-23 23:31:26	Manual creation	Added manually	2021-09-23 23:31:...

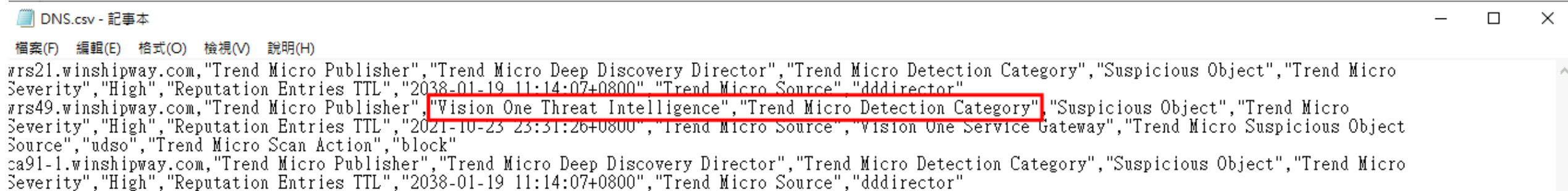
SMS 從Vision One同步UDSO

- 到SMS Client中，點選到Reputation Database > User Entries 中，可看到User Entries數量增加。



SMS 從Vision One同步UDSO

- 點選Export 匯出檢視，可看到是由"Trend Micro Publisher","Vision One Threat Intelligence" 所同步下來的。



```
DNS.csv - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
wrs21.winshipway.com,"Trend Micro Publisher","Trend Micro Deep Discovery Director","Trend Micro Detection Category","Suspicious Object","Trend Micro Severity","High","Reputation Entries TTL","2038-01-19 11:14:07+0800","Trend Micro Source","dddirector"
wrs49.winshipway.com,"Trend Micro Publisher","Vision One Threat Intelligence","Trend Micro Detection Category","Suspicious Object","Trend Micro Severity","High","Reputation Entries TTL","2021-10-23 23:31:26+0800","Trend Micro Source","Vision One Service Gateway","Trend Micro Suspicious Object Source","udso","Trend Micro Scan Action","block"
ca91-l.winshipway.com,"Trend Micro Publisher","Trend Micro Deep Discovery Director","Trend Micro Detection Category","Suspicious Object","Trend Micro Severity","High","Reputation Entries TTL","2038-01-19 11:14:07+0800","Trend Micro Source","dddirector"
```

Event Sharing

(Need XDR add on license for TP license)

環境確認

- Service Gateway需升級到 1.0.0.10051版本以上
- Vision One上有 XDR Add-On: TippingPoint Software的授權。

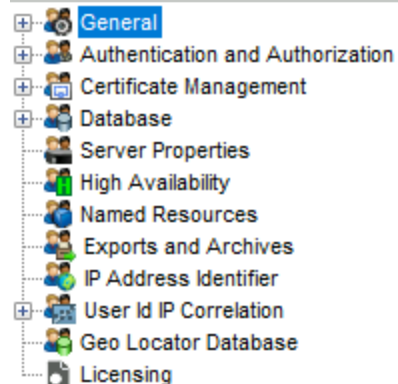
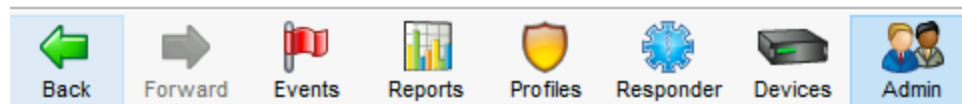
The screenshot displays the Trend Micro Vision One™ interface. On the left, a navigation menu includes 'Response Management', 'Mobile Security', 'Inventory Management', 'Email Account Inventory', 'Network Inventory', 'Service Gateway Inventory' (highlighted), 'Mobile Inventory', 'Administration', and 'Single Sign-On'. The main panel shows the 'Service Gateway Inventory' for endpoint 'TWTS-SG2'. It lists details such as 'Endpoint name: TWTS-SG2', 'IPv4 address', 'IPv6 address: fe80::...', 'Connection status: Healthy', and 'Last connected: 2021-10-07 16:55:15'. The 'Version: 1.0.0.10051' is highlighted with a red box. Below this, a 'Storage' bar shows '436.6 GB free (Total:459 GB)'. On the right, a 'Services' list includes 'ActiveUpdate', 'Smart Protection Services', 'Suspicious Object List synchronization', 'Third-party intelligence synchronization', and 'Log forwarding' (highlighted with a red box). A top banner shows a green checkmark and 'XDR Add-On: TippingPoint Software'.

環境確認

- SMS版本需更新至 5.5 Patch1 (5.5.0.204732.1)版本以上。

TippingPoint SMS - SuperUser@TWTS-vSMS - Admin (General)

File Edit View Tools Help



SMS Server

System Time: 2021/10/7 下午04時59分16秒 GMT+08:00
System Uptime: 0 years, 2 weeks, 0 days, 3 hrs, 42 mins, 11 secs

SMS Software

Current Version: 5.5.0.204732
Available for Download: None
Available for Install: None

SMS Patches

Currently Installed: 5.5.0.204732.1 [Release Notes...](#)
Available for Download: None
SMS Patch Notifications: ☒ Enabled

Authorized users only. All activity may be monitored and reported.
TippingPoint Technologies SMS (version 5.5.0.204732 (Patch 1))
TWTS-vSMS login:

SMS設定Service Gateway

- 在SMS Web Console中的 Administration > Service Gateway中，啟用 Event Sharing，並且成功連線到Service Gateway。

Service Gateway Connection Settings

Connection

Gateway IP Address:

API Key:

Suspicious Object

State: ☒ Enabled

Download Interval (minutes):

Event Sharing

State: ☒ Enabled

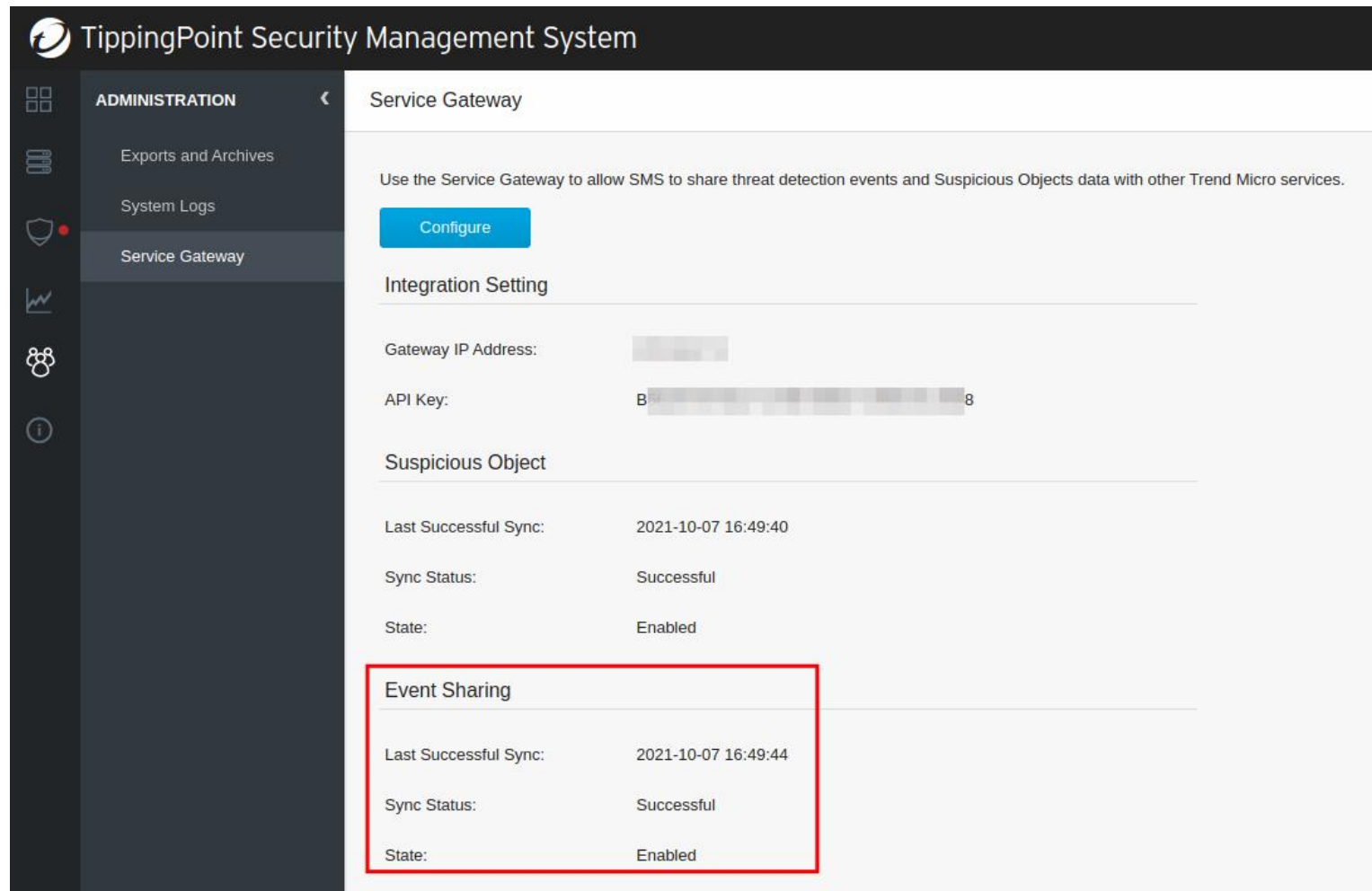
設定Service Gateway

- 在Vision One上, Service Gateway成功啟用Log Forwarding。
- 此功能在Service Gateway 1.0.0.10051版本以上才可啟用。

The screenshot displays the Trend Micro Vision One™ interface. On the left, the 'Inventory Management' menu is expanded, with 'Service Gateway Inventory' highlighted. The main panel shows the 'Service Gateway Inventory' for 'TWTS-SG2'. The 'Services' section lists several services, all of which are enabled (indicated by green checkmarks): 'ActiveUpdate', 'Smart Protection Services', 'Suspicious Object List synchronization', 'Third-party intelligence synchronization', and 'Log forwarding'. The 'Log forwarding' service is highlighted with a red box. On the right, the 'Service Gateway Settings' panel for 'TWTS-SG2' is shown, with the 'Log forwarding' toggle switch also highlighted by a red box. A red arrow points from the 'Log forwarding' toggle in the settings panel to the 'Log forwarding' service in the main panel. The 'Log forwarding' service is also highlighted with a red box. The 'Log forwarding' service is highlighted with a red box. The 'Log forwarding' service is highlighted with a red box.

設定Service Gateway

- 在SMS Web Console中，確認Event Sharing的狀態為成功Sync Event。



TippingPoint Security Management System

ADMINISTRATION <

- Exports and Archives
- System Logs
- Service Gateway

Service Gateway

Use the Service Gateway to allow SMS to share threat detection events and Suspicious Objects data with other Trend Micro services.

[Configure](#)

Integration Setting

Gateway IP Address: [Redacted]

API Key: B [Redacted] 8

Suspicious Object

Last Successful Sync: 2021-10-07 16:49:40

Sync Status: Successful

State: Enabled

Event Sharing

Last Successful Sync: 2021-10-07 16:49:44

Sync Status: Successful

State: Enabled

Vision One Search App 查詢

- 在Vision One的 Search App中, 可查詢到Tipping Point 的Detection Log

The screenshot displays the Trend Micro Vision One Search App interface. The left sidebar contains navigation options: Assessment, Threat Intelligence, XDR, Zero Trust Secure Acc..., Search (highlighted with a red box), Response Management, Mobile Security, and Inventory Management. The main panel shows the search results for 'pname:tipping'. A red box highlights the 'Search Method: Detections' dropdown. Below the search bar, a bar chart shows detection counts over time, with a peak around 16:48:30. The 'Matched events: 10' section displays a list of events, with the first event highlighted. The event details are shown in a table below.

act	Block
aggregatedCount	1
app	udp
deviceGUID	2cabea11-27e6-11eb-b282-abbfe1a0dd98
dpt	137
dst	192.168.254.208
dvchost	TWTS-440T
eventName	INTRUSION_DETECTION
interestedip	
logKey	761ace6a0e0302be04e0963a4d47788c55bab66a26cb48b100a5b95f059aa785
mpname	Trend Micro TippingPoint Security Management System
overSsl	0
pname	TippingPoint SMS