# Integrazione di AMP for Endpoints con Splunk

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Risoluzione dei problemi

## Introduzione

In questo documento viene descritto il processo di integrazione tra Advanced Malware Protection (AMP) e Splunk.

Contributo di Uriel Islas e Juventino Macias, a cura di Jorge Navarrete, Cisco TAC Engineers.

# Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza di:

- AMP for Endpoints
- API (Application Programming Interface)
- Splunk
- Utente amministratore su Splunk

#### Componenti usati

- AMP Public Cloud
- Istanza Splunk

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione

Passaggio 1. Passare alla console AMP (<u>https://console.amp.cisco.com</u>) e selezionare **Account>Credenziali API**, dove è possibile creare flussi di eventi.

API Credentials	View API Documentation
Collers	+ New API Credential

Passaggio 2. Per eseguire questa integrazione, selezionare la casella di controllo **Lettura e scrittura** come mostrato di seguito:

New API Credential	
Application name	calsias-amp
Scope Er A	Read-only     Read & Write     Able Command line     low API access to File Repository download audit logs
An API credential AMP for Endpoint with your endpoint Some of the input	with read and write scope can make changes to your s configuration that may cause significant problems ts. protections built into the AMP Console do not apply
to the API.	Cancel Create

**Nota:** Se si desidera raccogliere ulteriori informazioni sugli eventi, selezionare la casella **Abilita riga di comando** per ottenere i log di controllo generati dal repository dei file selezionare la casella **Consenti accesso API al repository dei file**.

Passaggio 3. Una volta creato il flusso di eventi, vengono visualizzati l'ID client e la chiave API richiesti in Splunk.

< API Key I	Details
3rd Party A	PI Client ID
	rafol2c390
API Key	
	\$3ddr817+wssr+43
API credentisis and password, a	API Client ID & API Key) will allow other programs to retrieve and modify your Clsco AMP for Endpoints data. It is functionally equivalent to a use and should be treated as such.
Delete the API c	redentials for an application if you suspect they have been compromised and create new ones.
Deleting API cre	dentials will lock out any clients using the old ones so make sure to update them to the new credentials.
Your API creden	tials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.
View API Docum	ventation .

Attenzione: queste informazioni non possono essere recuperate in alcun modo. In caso di perdita, è necessario creare una nuova chiave API.

Passaggio 4. Per integrare Splunk con AMP for endpoints, verificare che l'account **Admin** esista in Splunk.

splunk>enter	prise	
Usemanie	Password	Sign In
-O admin From this website		
*O mex-amp From this website	jed out. Log in to return	n to the system.
View Saved Logins		

Passaggio 5. Dopo aver eseguito l'accesso a Splunk, procedere al download di AMP da Splunk Apps.



Passaggio 6. Cercare Cisco Endpoint nel browser dell'app e installarlo (Cisco AMP for Endpoints Events Input).

splunk> Apps ~	Administrator V Messages V Settings V Activity V Help V Find
Browse More Apps	
cisco endpoint 🕲	Best Match Newest Popular 7 Apps
CATEGORY DevOps Security, Fraud & Compliance IT Operations Utilities Business Analytics IoT & Industrial Data	the cisco AMP for Endpoints CIM Add-On       Install         The Cisco AMP for Endpoints CIM Add-on provides a mechanism to map data from the Cisco AMP for Endpoints Event Input App for CIM compliant applications.       The add-on also provides additional workflow actions so security analysts can go straight from Splunk Events to the Cisco AMP for Endpoints console.
CIM VERSION 4.x 3.x	Category: Security, Fraud & Compliance   Author: Samson Nguyen   Downloads: 996   Released: 2 years ago   Last Updated: a year ago   View on Splunkbase
SUPPORT TYPE Developer Splunk	titie Cisco AMP for Endpoints Events Input
Not Supported  APP CONTENT  Inputs	The Cisco AMP for Endpoints Events Input provides a mechanism to create, update, and delete event streams in Cisco Advanced Malware Protection (AMP) for Endpoints via the API and index them in your Splunk® instance to make them searchable. All you need to do is provide your API host and credentials from your AMP for Endpoints account and specify the stream parameters. This app has been tested on Splunk v6.6.0 Less

Passaggio 7. Per completare l'installazione su Splunk, è necessario riavviare la sessione.



Passaggio 8. Dopo aver effettuato l'accesso in Splunk, fare clic su **Cisco AMP For Endpoints** sul lato sinistro della schermata.



Passaggio 9. Fare clic sull'etichetta Configuration nella parte superiore dello schermo.

splunk	enterprise	App: Clsco AMP for Endpoints Events Input •
Inputs	New Input	Configuration
Input	s	
Crea	te a New Input	
Retriev	ing inputs	

Passaggio 10. Digitare le credenziali API generate in precedenza dalla console AMP.

splunk	>enterprise	App: Cisco AMP for Endpoints Events Input *
Inputs	New Input	Configuration
Conf	iguration	
Global c	onfiguration for (	Cisco AMP for Endpoints events input
AMP fi	or Endpoints AF	PLAccess Configuration
AMP to	or Endpoints API	Host '
api.ar	mp.cisco.com	
Enter th	e address of the Ci	isco AMP for Endpoints API Server that the application will access for managing event streams. Please re
API CI	ent ID.*	
Enter th	e 3rd Party API Cile	ant ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope
API Ke	y *	
Enter th	e secret API key	
Save	Configuration	

**Nota:** L'area API Host potrebbe essere diversa in base al centro dati cloud a cui punta l'organizzazione:

Nord America: api.amp.cisco.com Europa: api.eu.amp.cisco.com APJC: api.apjc.amp.cisco.com Passaggio 11. Includere e salvare le credenziali API nella console Splunk per collegarle ad AMP.

splunk	>enterprise	App: Cisco AMP for Endpoints Events Input *
Inputs	New input	Configuration
Conf	iguration	
Global co	onfiguration for (	Cisco AMP for Endpoints events input
<b>()</b> Co	enfiguration succ	essfully saved
AMP fo	or Endpoints AF	Pl Access Configuration
AMP to	r Endpoints API	Host *
apilar	np.cisco.com	
Enter the	e address of the Ci	sco AMP for Endpoints API Server that the application will access for managing event streams. Please refer to the AMP for Endpoints API documentation for the correct hostname
API CIH	ent ID 1	
e36c1	12c3905be05ca	cb7
Enter the	e 3rd Party API CH	nt JD provided by AMP for Endpoints. Prease note that your API Client must have read and verice scope
API Key	y.*	
a68f	433e-bane-f620	J41c163#b
Enter the	é secrit API key	
Save	Configuration	

Passaggio 12. Tornare a Input per creare il flusso di eventi.

nputs New Input Configuration	
New Input	
Name *	
caislas	
Index	
main	2
In which index would you like the events to appear?	
Stream Settings	
Stream Name *	
caislas	
Event Types	
1	0
Groups	
Leave this field blank to return all Groups	÷ 🕞
Sauce	

**Nota:** Se si desidera ottenere tutti gli eventi per tutti i gruppi da AMP, lasciare vuoti i campi **Tipi di evento** e **Gruppi**.

Passaggio 13. Verificare che l'input sia stato creato correttamente.

nputs	
Create a New Input	
Name	Index
caislas	main

Nota: Questa integrazione non è ufficialmente supportata

## Risoluzione dei problemi

Se durante la creazione di un flusso di eventi tutti i campi sono disattivati, ciò potrebbe essere dovuto ad alcuni dei motivi seguenti:

nputs New input Consiguration	
New Input	
Name."	
0	
Index	
In which index would you like the events to appear?	
Stream Settings	
Stream Settings Stream Name *	
Stream Name *	
Stream Settings Stream Name * Event Types Leave this field blank to return all Event-types	
Stream Name * Event Types Leave this field blank to return all Event types Groups	Ş

- 1. Problemi di connettività: Verificare che l'istanza Splunk sia in grado di contattare l'host API
- 2. Host API: Verificare che l'host API configurato nel passaggio 10 corrisponda all'organizzazione AMP, in base al punto di riferimento dell'azienda.
- 3. Credenziali API: Verificare che la chiave API e l'ID client corrispondano a quelli configurati nel passaggio 3.
- 4. Flussi di eventi: Verificare che siano configurati meno di 4 flussi di eventi.