# Intégration d'AMP for Endpoints avec Splunk

## Contenu

Introduction Conditions préalables Conditions requises Components Used Configuration Dépannage

## Introduction

Ce document décrit le processus d'intégration entre Advanced Malware Protection (AMP) et Splunk.

Contribué par Uriel Islas and Juventino Macias, édité par Jorge Navarrete, Ingénieurs du TAC Cisco.

# Conditions préalables

#### **Conditions requises**

Cisco vous recommande de connaître :

- AMP pour les points terminaux
- API (Application Programming Interface)
- Épingler
- Utilisateur Admin sur Splunk

#### **Components Used**

- Cloud public AMP
- Instance Splunk

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configuration

Étape 1. Accédez à la console AMP (<u>https://console.amp.cisco.com</u>) et accédez à Comptes>Informations d'identification de l'API, où vous pouvez créer des flux d'événements.



Étape 2. Pour effectuer cette intégration, cochez la case **Lecture et écriture** comme indiqué cidessous :

New A	PI Credential	
	Application name	caisias-amp
	Scope	Read-only     Read & Write     Ible Command line
C Al Al W St	n API credential v MP for Endpoints ith your endpoints ome of the input p	with read and write scope can make changes to your configuration that may cause significant problems s.
to	the API.	Carical Create

**Note**: Si vous souhaitez collecter plus d'informations sur les événements, cochez la case **Activer la ligne de commande**, pour obtenir les journaux d'audit générés à partir du référentiel de fichiers, cochez la case **Autoriser l'accès API au référentiel de fichiers**.

Étape 3. Une fois que vous avez créé le flux d'événements, il affiche l'ID de client et la clé d'API requis sur Splunk.

< API Ke	/ Details
3rd Party	API Client ID
	#36012c390
API Key	
	\$3ddr#17-west+#27
API credents and passwor	is (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 d, and should be treated as such.
Delete the A	I credentials for an application if you suspect they have been compromised and create new ones,
Deleting API	credentials will lock out any clients using the old ones so make sure to update them to the new credentials.
Your API cree	dentials 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 Do	aumentalian

Attention : Ces informations ne peuvent être récupérées par aucun moyen, en cas de perte, une nouvelle clé d'API doit être créée.

Étape 4. Afin d'intégrer Splunk à AMP pour les terminaux, assurez-vous que l'**administrateur** du compte existe sur Splunk.

spiulik>enter	prise	
Usemame	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		

Étape 5. Une fois connecté à Splunk, téléchargez AMP à partir des applications Splunk.

splunk>			Administrator 🗸	Messages 🗸	Settings 🗸	Activity 🗸	Help 🗸	Find	
Apps 🗢	Explore Splunk Enterprise								×
Search & Reporting	Product Tours	Add Data		Explore Da	ta		Splunk	Appt Splunk App	s
+	New to Splunk? Take a tour to help you on your way.	Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.	Expl	ore data and define parses that da	e how Hunk ta.	cap	pps and add- abilities of Sp	ons extend the olunk Enterprise.	

Étape 6. Recherchez Cisco Endpoint sur le navigateur de l'application et installez-le (entrée d'événements Cisco AMP for Endpoints).

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	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	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	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

Étape 7. Un redémarrage de la session est nécessaire pour terminer l'installation sur Splunk.

Restart Required	×
You must restart Splunk Splunk Ente AMP for Endpoints Events Input.	rprise to complete installation of Cisco
Restart Later	Restart Now

Étape 8. Une fois connecté sous Splunk, cliquez sur **Cisco AMP For Endpoints** sur le côté gauche de l'écran.



Étape 9. Cliquez sur l'étiquette Configuration en haut de l'écran.

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

Étape 10. Tapez vos informations d'identification API précédemment générées à partir de la console AMP.

splunk	>enterprise	App: Cisco AMP for Endpoints Events Input +
Inputs	New Input	Configuration
Conf Global co	iguration	Cisco AMP for Endpoints events input
AMP fo	or Endpoints AF	PLAccess Configuration
AMP fo	r Endpoints APi	Host "
apiar	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 re
API CI	ent ID *	
Enter the	o 3rd Party API Cilo	In ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope
API Key	· *	
Enter the	a secret API key	
Save	Configuration	

**Note**: L'emplacement de l'hôte API peut être différent en fonction du data center cloud sur lequel pointe votre entreprise :

Amérique du Nord: api.amp.cisco.com Europe: api.eu.amp.cisco.com Étape 11. Incluez et enregistrez les informations d'identification API sur la console Splunk pour les lier à AMP.

splunk	>enterprise	App: Cisco AMP for Endpoints Events Input *
Inputs	New Input	Configuration
Conf	iguration	
Global c	configuration for	Cisco AMP for Endpoints events input.
0 0	onfiguration succ	cessfully saved
AMP f	or Endpoints Al	PI Access Configuration
AMP 6	or Endpoints API	Host *
apia	mp.cisco.com	
Enter th	ie address of the C	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 CI	ient ID 1	
e36c	12c3905be05ca	cb7
Eriter th	to 3rd Party API CH	nt ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope
API Ke	Y.*	
a68	433e-base-f620	041c1638b
Enter th	e secrit API key	
Sav	e Configuration	

Étape 12. Revenez à Entrée pour créer votre flux d'événements.

New Input	
Name *	
caislas	
Index	
main	~
In which index would you like the events to appear?	
In which index would you like the events to appear? Stream Settings	
In which index would you like the events to appear? Stream Settings Stream Name *	
In which index would you like the events to appear? Stream Settings Stream Name * caislas	
In which index would you like the events to appear? Stream Settings Stream Name * caislas Event Types	
In which index would you like the events to appear? Stream Settings Stream Name * caislas Event Types	
In which index would you like the events to appear? Stream Settings Stream Name * caislas Event Types [ Groups	

**Note**: Si vous voulez obtenir tous les événements pour tous les groupes à partir d'AMP, laissez vides les champs **Types d'événements** et **Groupes**.

	Étape	913.	Assurez-v	ous que	votre	entrée	a bien	été	créée.
--	-------	------	-----------	---------	-------	--------	--------	-----	--------

nputs	
Create a New Input	
Name	Inc
caislas	ma

Note: N'oubliez pas que cette intégration n'est pas officiellement prise en charge

### Dépannage

Si, pendant que vous créez un flux d'événements, tous les champs sont grisés, cela peut être dû à certaines des raisons suivantes :

Inputs	New Input	Configuration	
New	Input		
Name			
		0	
Index			
In which	index would you i	ke the events to appear?	
Stream	Settings		
Stream	Name *		
Event 1	ypes		
Leave this field blank to return all Event types			¢
Groups			
Leave this field blank to return all Groups			· · ·

- 1. Problèmes de connectivité: Assurez-vous que l'instance Splunk est en mesure de contacter l'hôte API
- 2. Hôte API : Assurez-vous que l'hôte API configuré à l'étape 10 correspond à votre organisation AMP, en fonction de l'emplacement de votre entreprise.
- 3. Informations d'identification de l'API : Assurez-vous que la clé API et l'ID client correspondent à ceux configurés à l'étape 3.
- 4. Flux d'événements : Vérifiez que moins de 4 flux d'événements sont configurés.