# Guida all'integrazione di SecureX con Advanced Malware Protection (AMP) for Endpoints

## Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Configurazione](#)
[Genera le credenziali API nella console AMP](#)
[Abilitare la barra multifunzione SecureX nella console AMP](#)
[Integrazione del modulo AMP for Endpoints in SecureX](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Il client API non dispone dell'accesso in scrittura [403]](#)
[Errore: Chiave API o ID client sconosciuto [401]](#)
[Guida video](#)

## Introduzione

Questo documento descrive il processo richiesto per integrare e verificare Cisco SecureX con Cisco Advanced Malware Protection (AMP) for Endpoints.

Contributo di Yeraldin Sanchez e Uriel Torres, a cura di Jorge Navarrete, Cisco TAC Engineers.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AMP for Endpoints
- Navigazione di base nella console SecureX
- Virtualizzazione delle immagini opzionale

### Componenti usati

- AMP for Endpoints Console versione 5.4.2020804
- Account amministratore AMP for Endpoints
- SecureX Console versione 1.54
- Account amministratore SecureX
- Microsoft Edge versione 84.0.522.52

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.

# Premesse

Cisco Advanced Malware Protection (AMP) for Endpoints è una parte fondamentale della piattaforma di sicurezza degli endpoint ed è implementato come strumento di prevenzione e indagine che supporta le funzioni di rilevamento e/o risposta per i dispositivi Windows, MacOS, Linux, Android e iOS. Il modulo AMP for Endpoints fornisce 5 tessere.

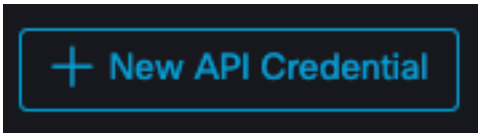
- **Compromessi rilevati da AMP:** Una serie di metriche che riepiloga i compromessi rilevati da AMP
- **Riepilogo computer AMP: un set di metriche che riepiloga lo stato dei computer AMP**
- **Riepilogo AMP: un set di metriche che riepiloga il rilevamento e la risposta AMP**
- **Quarantene AMP: Set di metriche che riepiloga le quarantene AMP in base al tempo**
- **Tattiche ATT&CK MITER Rilevate da AMP: un set di metriche che riepiloga le tattiche ATT&CK MITER rilevate da AMP**

# Configurazione

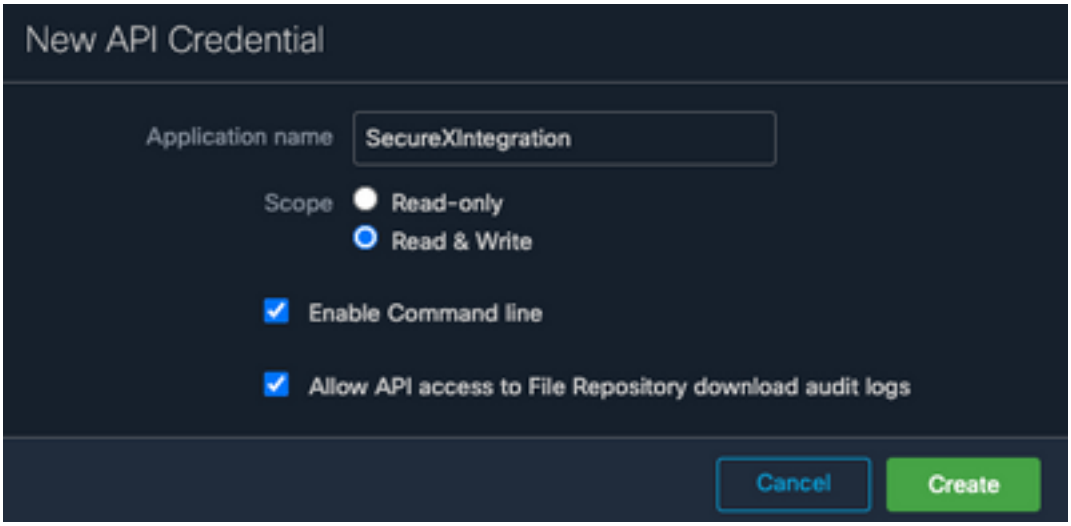
## Genera le credenziali API nella console AMP

Nella console AMP vengono create nuove credenziali API.

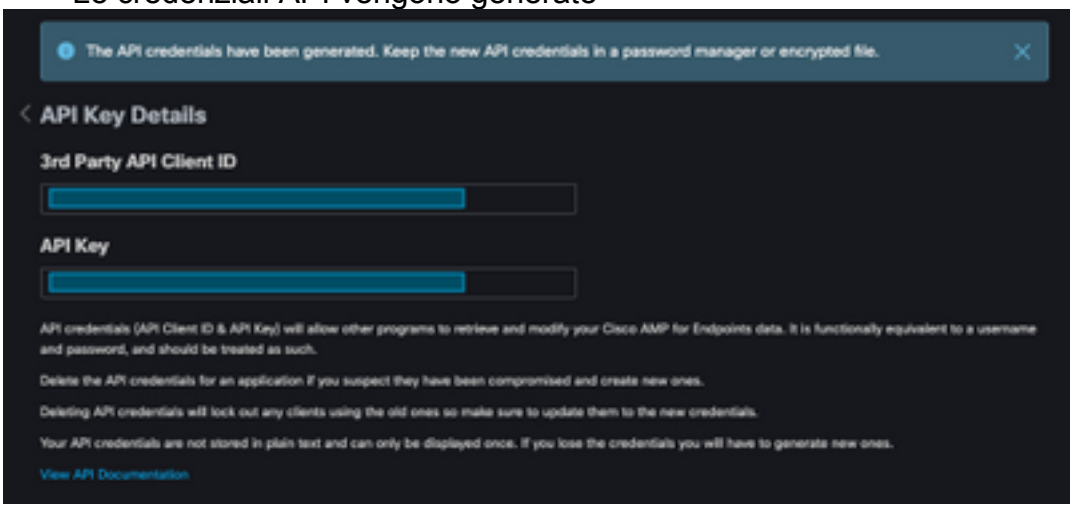
- Accedere alla console AMP con privilegi di amministratore
- In AMP Console passare ad **Account > Credenziali API**
- Fare clic su **New API Credential**




- Denominazione applicazione
- Selezionare **Lettura e scrittura**
- Selezionare **Abilita riga di comando** e **Consenti accesso API al repository dei file per scaricare i log di controllo**
- Fare clic su **Crea**




- Le credenziali API vengono generate

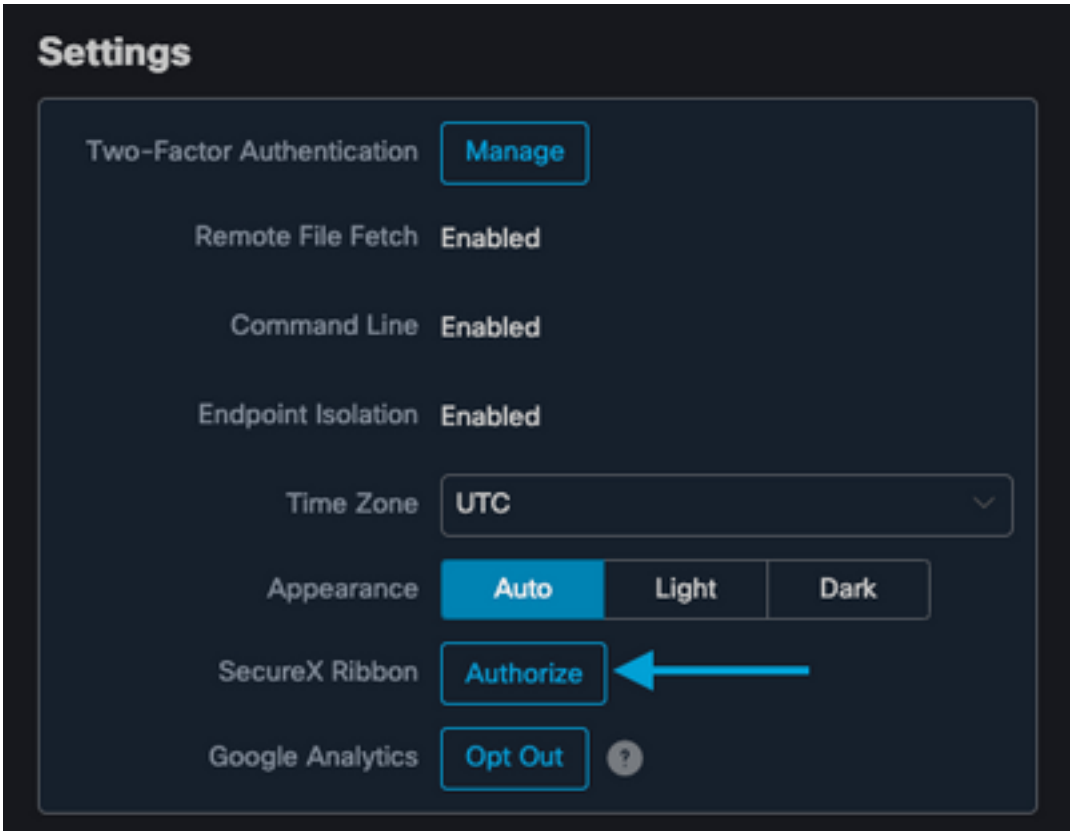



**Nota:** Queste informazioni sono disponibili solo in questa finestra. Salvare le credenziali in un file di backup.

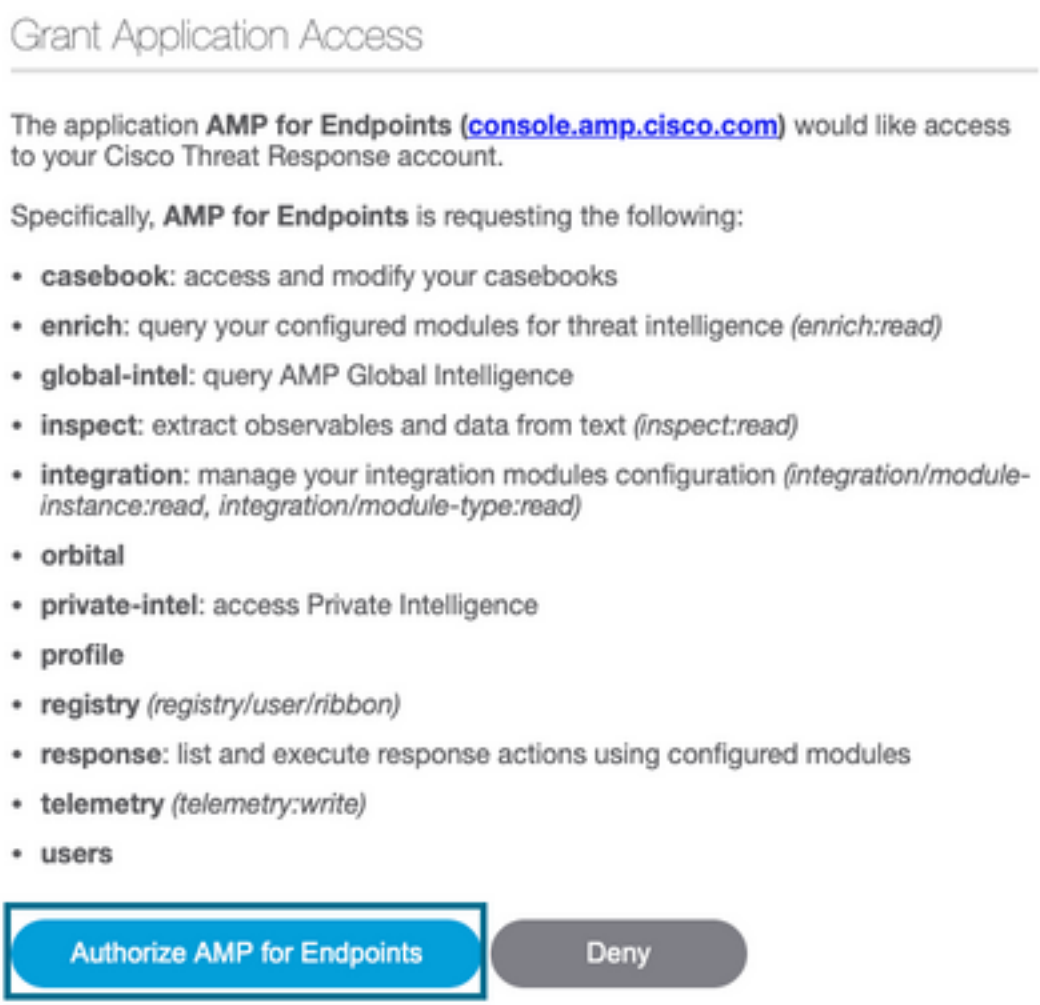
## Abilitare la barra multifunzione SecureX nella console AMP

SecureX è una console centralizzata e una serie distribuita di funzionalità che unificano la visibilità, consentono l'automazione, accelerano i flussi di lavoro di risposta agli incidenti e migliorano la ricerca di minacce. Queste funzionalità distribuite sono presentate sotto forma di applicazioni (app) e strumenti nella barra multifunzione SecureX, che può essere abilitata nella console AMP.

- Accedere a SecureX
- Sulla console AMP
- Selezionare **Account > Utenti >** Fare clic sull'**utente**
- Nella casella **Impostazioni** fare clic su **Autorizza** barra multifunzione SecureX

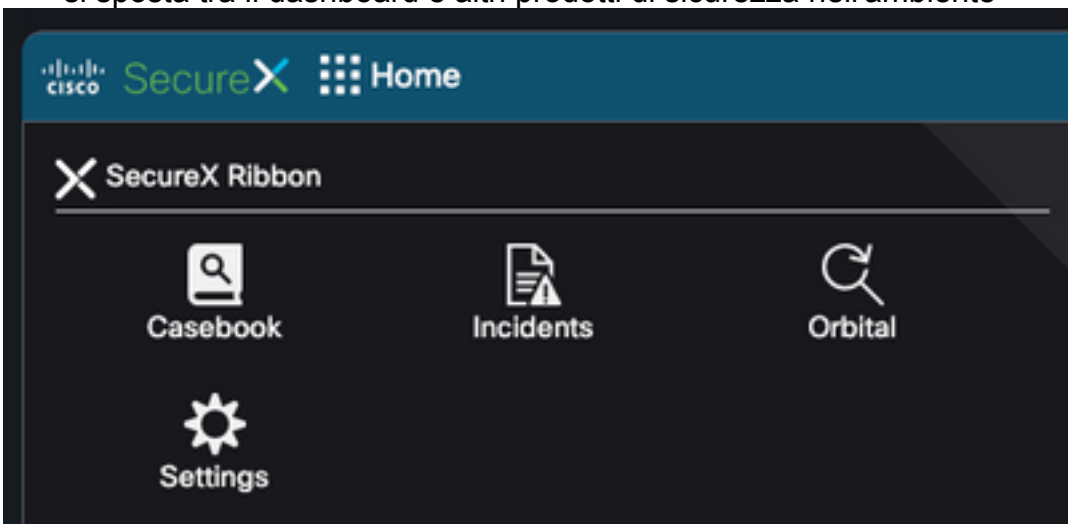



- Viene eseguito il reindirizzamento alla risposta alla minaccia SecureX
- Fare clic su **Autorizza AMP for Endpoints**




- La barra multifunzione si trova nella parte inferiore della pagina e viene mantenuta quando ci

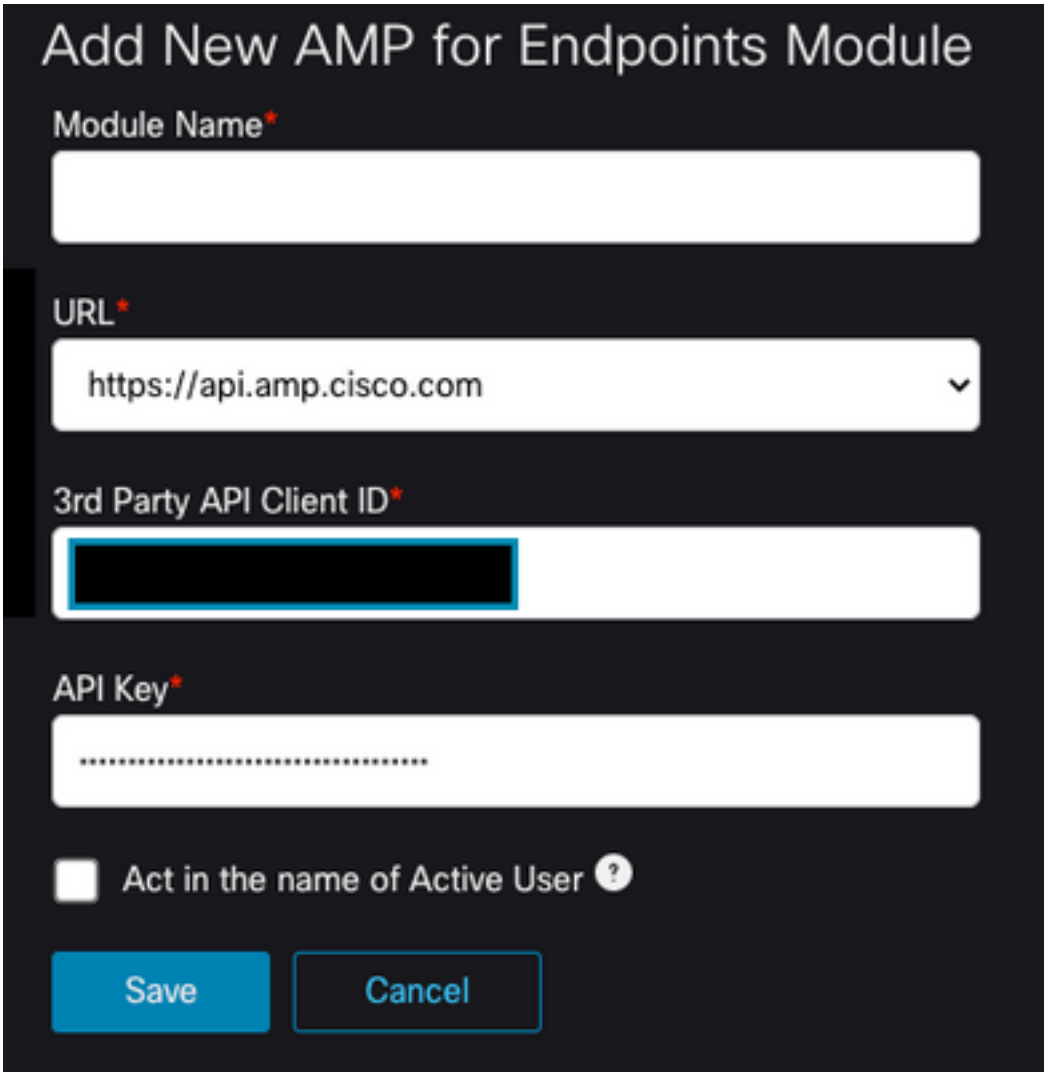
si sposta tra il dashboard e altri prodotti di sicurezza nell'ambiente




## Integrazione del modulo AMP for Endpoints in SecureX

Il modulo AMP for Endpoints consente di analizzare e identificare più file con contesto dalle integrazioni tra i prodotti di sicurezza. Fornisce informazioni dettagliate sugli endpoint e i dispositivi interessati, inclusi indirizzi IP, SO e GUID AMP.

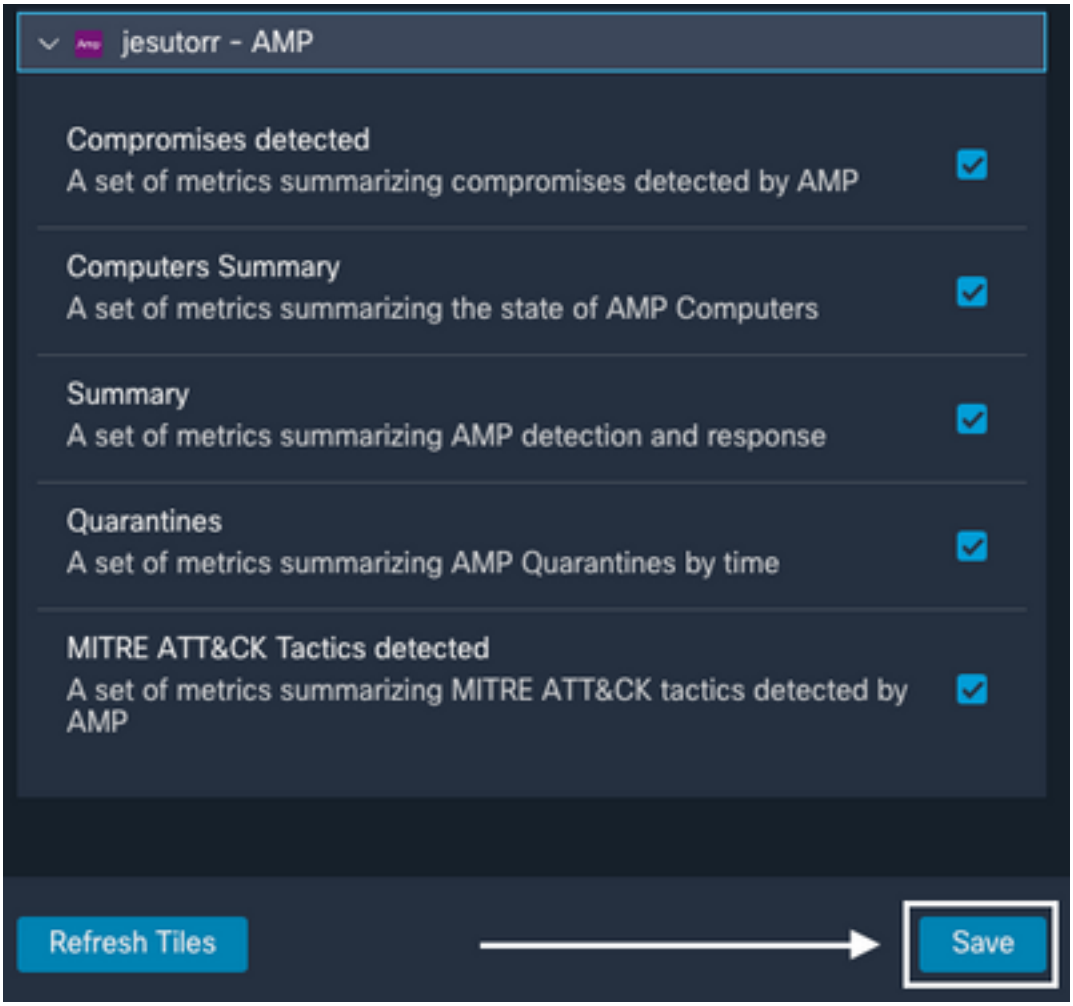
- Su console SecureX passare a **Integrations > Fare clic su Add New Module**
- Selezionare il modulo **AMP for Endpoints**, quindi fare clic su **Add New Module**
- Assegnare un nome al modulo
- Selezionare AMP Cloud
- Le credenziali API raccolte in precedenza vengono immesse in **ID client** e **chiave API di terze parti**




## Verifica

Verificare che le informazioni della console AMP siano visualizzate nel dashboard SecureX.

- In SecureX passare a **Dashboard**
- Fare clic su **Nuovo dashboard** e denominarlo
- Selezionare il modulo AMP generato in precedenza
- Selezionare i riquadri, per questa guida tutti sono aggiunti
- Fare clic su Salva.




- Selezionare l'intervallo di **tempo** e verificare se i dati di AMP sono visualizzati in SecureX

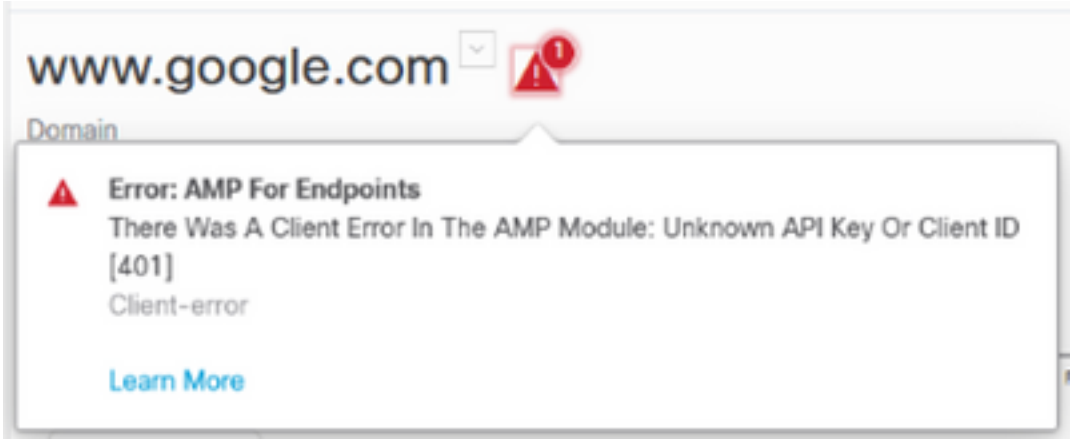

# Risoluzione dei problemi

## Il client API non dispone dell'accesso in scrittura [403]

L'integrazione SecureX - AMP for Endpoints richiede API **Read & Write** AMP for Endpoints. In caso contrario, viene visualizzato un messaggio di errore come mostrato nell'immagine.


### Errore: Chiave API o ID client sconosciuto [401]

Se le API non sono valide se viene eseguita un'analisi in SecureX Threat Response, come mostrato nell'immagine.




Verificare che le credenziali API siano valide o esistenti nella console AMP. In caso contrario, provare a utilizzare credenziali nuove.

Se dopo aver esaminato le informazioni di cui sopra si riscontrano ancora problemi, contattare il supporto tecnico.

## Guida video