

Panoramica dell'API Cisco AMP for Endpoints

Sommario

[Introduzione](#)

[Genera ed elimina credenziali API](#)

[Versioni API e opzioni correnti](#)

[Comando API: analisi stratificata ed esempio](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive Cisco Advanced Malware Protection (AMP) for Endpoints. Cisco AMP for Endpoints è fornito con un'API (Application Programming Interface). Consente di estrarre i dati da un'implementazione di AMP for Endpoints e di modificarli, se necessario.

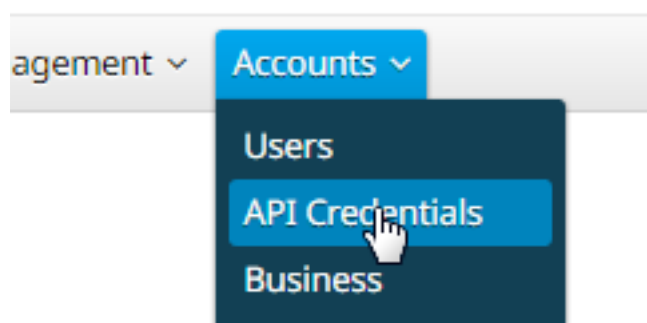
In questo articolo vengono illustrate alcune funzionalità di base dell'API. Negli esempi di questo articolo viene utilizzato un endpoint di Windows 7.

Contributo di Matthew Franks, Nazmul Rajib e Cisco TAC Engineers.

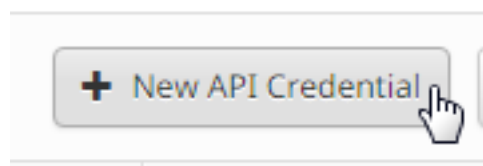
Genera ed elimina credenziali API

Per utilizzare l'API AMP for Endpoint, è necessario configurare una credenziale API. Seguire i passaggi forniti per creare una credenziale tramite AMP Console.

Passaggio 1: Accedere alla Console e selezionare **Account > Credenziali API**.



Passaggio 2: Fare clic su **Nuove credenziali API** per creare un nuovo set di chiavi.



Passaggio 3: Specificare un **nome applicazione**. Selezionare **Ambito** di sola lettura o Lettura e scrittura.

New API Credential




Application name

Scope Read-only
 Read & Write

An API credential with read and write scope can make changes to your Cisco AMP for Endpoints configuration that may cause significant problems with your endpoints.

Some of the input protections built into the Cisco AMP for Endpoints Console do not apply to the API.

Cancel

Create 

Nota: Una credenziale API con ambito di lettura e scrittura può apportare modifiche alla configurazione di Cisco AMP for Endpoints che potrebbero causare problemi significativi con gli endpoint. Alcune delle protezioni di input incorporate nella Cisco AMP for Endpoints Console non si applicano all'API.

Passaggio 4: Fare clic sul pulsante **Crea**. Viene visualizzata la finestra **API Key Details** (Dettagli chiave API). Salvare queste informazioni poiché alcune non saranno disponibili dopo aver lasciato la schermata.

< API Key Details

The API credentials have been generated. Keep the new API credentials in a password manager or encrypted file.

3rd Party API Client ID

538e8b8203a48cc5c7fa

API Key

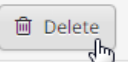
a190c911-8ca4-45fa-8740-e384ef2d3d5b

Nota: Le credenziali API (ID client API e chiave API) consentono ad altri programmi di recuperare e modificare i dati di Cisco AMP for Endpoints. Dal punto di vista funzionale, equivale a nome utente e password e deve essere considerato come tale.

Attenzione: Le credenziali API vengono visualizzate una sola volta. Se si perdono le credenziali, è necessario crearne di nuove.

Eliminare le credenziali API per un'applicazione se si sospetta che siano state compromesse e crearne una nuova. Quando si elimina una credenziale API, viene bloccato il client che utilizza le credenziali precedenti, quindi è necessario aggiornarle con le nuove credenziali.

Testing			
Client ID	538e8b8203a48cc5c7fa	Scope	Read & Write
Created by	Matthew Franks	Date	2016-08-24 14:53:27 UTC
Last used	Never		



Versioni API e opzioni correnti

Attualmente sono disponibili due versioni dell'API AMP for Endpoints: la versione 0 e la versione 1. La versione 1 presenta funzionalità aggiuntive rispetto alla versione 0. La documentazione della versione 1 è disponibile [qui](#). È possibile estrarre queste informazioni utilizzando la versione 1.

- Computer
- Attività computer
- Eventi
- Tipi di evento
- Elenchi di file
- Voci elenco file
- Gruppi
- Criteri
- Versioni

Fare clic sul comando corrispondente nel documento per visualizzare esempi di utilizzo.

Comando API: analisi stratificata ed esempio

Ciascun comando API contiene informazioni simili e può essenzialmente essere scomposto in un comando curl e può essere visualizzato nel modo seguente:

```
curl -o nomefile.json https://clientID:APIKey@api.amp.cisco.com/v1/whatyouwanttodo
```

Quando si utilizza il comando curl con l'opzione -o, è possibile salvare l'output in un file. In questo caso, il nome del file è "nomefile.json".

Suggerimento: Per ulteriori informazioni sui file con estensione json, fare clic [qui](#).

Il passaggio successivo del comando **curl** consiste nell'impostare l'indirizzo con le proprie credenziali prima del simbolo @. Quando si generano le credenziali API, si conoscono l'ID client e l'ID API, quindi questa sezione del comando sarà simile al collegamento riportato di seguito.

<https://538e8b8203a48cc5c7fa:a190c911-8ca4-45fa-8740-e384ef2d3d5b@>

Aggiungere il numero di versione e l'operazione che si desidera eseguire. Per questo esempio, eseguire le opzioni [GET /v1/computers](#). Il comando completo ha il seguente aspetto:

```
curl -o computers.json https://538e8b8203a48cc5c7fa:a190c911-8ca4-45fa-8740-e384ef2d3d5b@api.amp.cisco.com/v1/computers
```

Dopo aver eseguito il comando, dovrebbe essere visualizzato un file **computers.json** scaricato nella directory in cui è stato avviato il comando.

```
C:\Users\mafranks>curl -o computers.json https://538e8b8203a48cc5c7fa:a190c911-8ca4-45fa-8740-e384ef2d3d5b@api.amp.cisco.com/v1/computers
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           0         0     0         0          0      0      0      0
0         0     0         0          0      0      0      0  --:--:--  0:00:02  --:--:--    0
```

```
C:\Users\mafranks>dir | findstr computers
09/06/2016  02:37 PM                128 computers.json
```

Nota: Curl è disponibile [online](#) e compilato per molte piattaforme che includono Windows (generalmente si desidera utilizzare la versione Win32 - Generic).

Quando si apre il file, tutti i dati verranno visualizzati su un'unica riga. Se si desidera visualizzare questo file nel formato corretto, è possibile installare un plugin del browser per formattarlo come JSON e aprire il file in un browser. In questo modo vengono visualizzate le informazioni per i computer che è possibile utilizzare nel modo desiderato, ad esempio:

connector_guid, hostname, active, links, connector_version, operating_system, internal_ips, external_ip, group_guid, network_address, policy_guid e policy name.

```
{
  version: "v1.0.0",
  metadata: {
    links: {
      self: "https://api.amp.cisco.com/v1/computers"
    },
    results: {
      total: 4,
      current_item_count: 4,
      index: 0,
      items_per_page: 500
    }
  },
  data: [
    {
      connector_guid: "abcdef-1234-5678-9abc-def123456789",
      hostname: "test.cisco.com",
      active: true,
      links: {
        computer: "https://api.amp.cisco.com/v1/computers/abcdef-1234-5678-9abc-def123456789",
        trajectory: "https://api.amp.cisco.com/v1/computers/abcdef-1234-5678-9abc-def123456789/trajectory",
        group: "https://api.amp.cisco.com/v1/groups/abcdef-1234-5678-9abc-def123456789"
      }
    }
  ]
}
```

```
},
connector_version: "4.4.2.10200",
operating_system: "Windows 7, SP 1.0",
internal_ips: [
"10.1.1.2",
" 192.168.1.2",
" 192.168.2.2",
" 169.254.245.1"
],
external_ip: "1.1.1.1",
group_guid: "abcdef-1234-5678-9abc-def123456789",
network_addresses: [
{
mac: "ab:cd:ef:01:23:45",
ip: "10.1.1.2"
},
{
mac: "bc:de:f0:12:34:56",
ip: "192.168.1.2"
},
{
mac: "cd:ef:01:23:45:67",
ip: "192.168.2.2"
},
{
mac: "de:f0:12:34:56:78",
ip: "169.254.245.1"
}
],
policy: {
guid: "abcdef-1234-5678-9abc-def123456789",
name: "Protect Policy"
}
```

Dopo aver visto un esempio di base in azione, è possibile utilizzare le varie opzioni dei comandi per estrarre e modificare i dati nell'ambiente.

Informazioni correlate

- [Documentazione sull'API Cisco AMP for Endpoints](#)

Documentazione e supporto tecnico – Cisco Systems