Übersicht über die API von Cisco AMP für Endgeräte

Inhalt

Einführung

Dieses Dokument beschreibt Cisco Advanced Malware Protection (AMP) für Endgeräte. Cisco AMP für Endgeräte ist mit einer API (Application Programming Interface) ausgestattet. Sie können Daten aus einer Bereitstellung von AMP für Endgeräte abrufen und bei Bedarf bearbeiten.

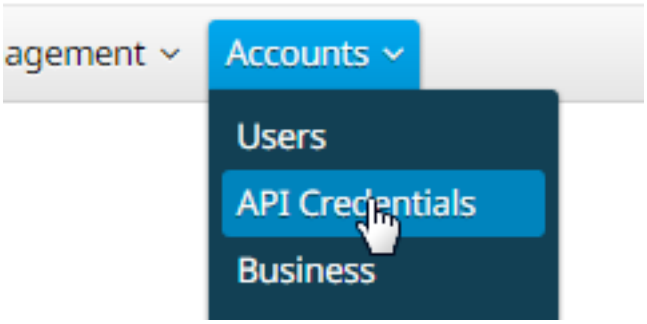
Dieser Artikel veranschaulicht einige grundlegende Funktionen der API. In den Beispielen in diesem Artikel wird ein Windows 7-Endpunkt verwendet.

Mitarbeiter: Matthew Franks, Nazmul Rajib und Cisco TAC Engineers.

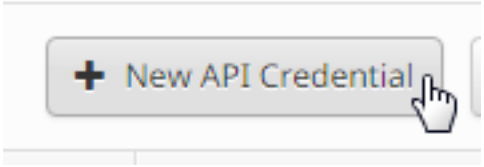
Erstellen und Löschen von API-Anmeldeinformationen

Um die AMP für Endgeräte-API zu verwenden, müssen Sie eine API-Anmeldeinformationen einrichten. Befolgen Sie die Anweisungen zum Erstellen einer Anmeldeinformationen über die AMP Console.

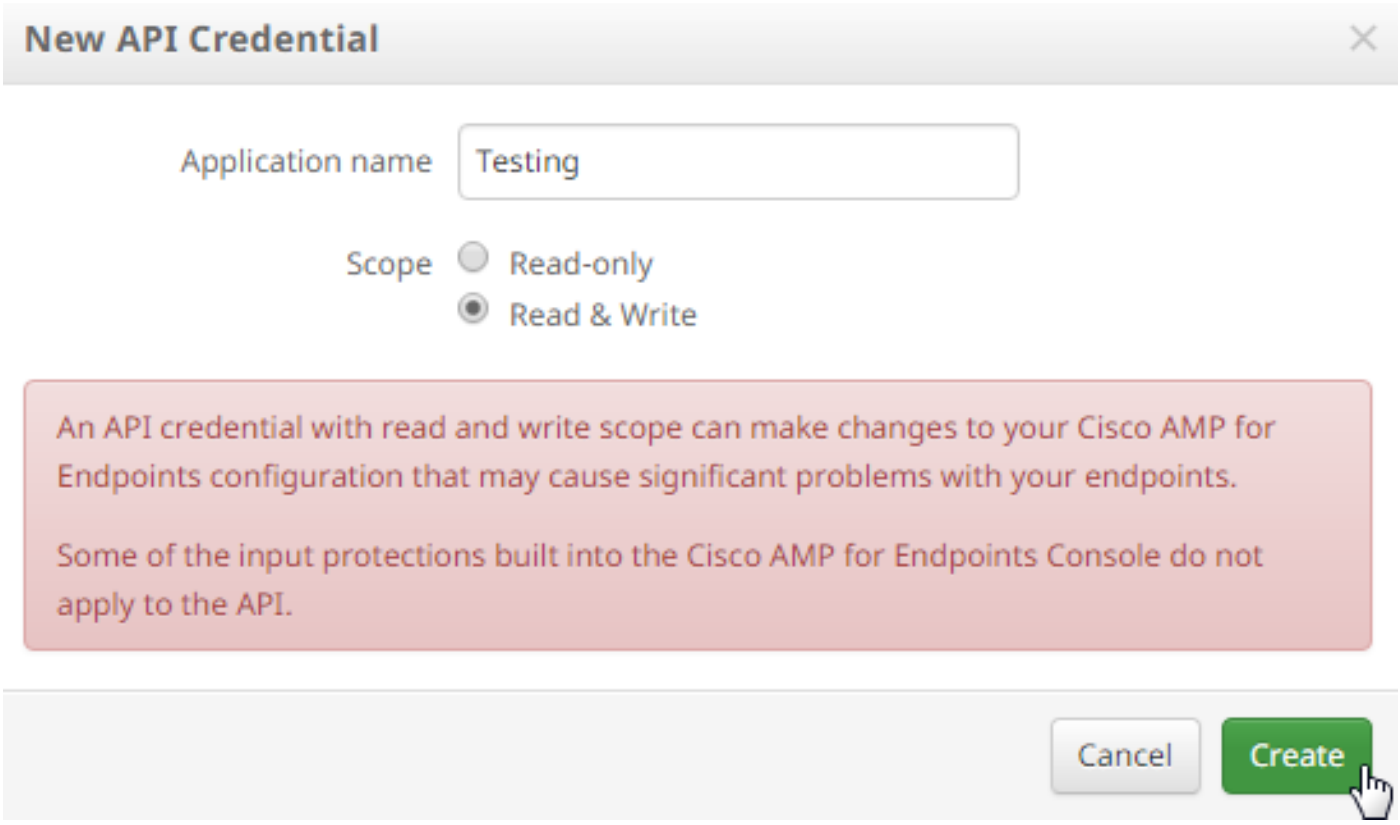
Schritt 1: Melden Sie sich bei der Konsole an, und navigieren Sie zu **Accounts > API Credentials (Konten > API-Anmeldeinformationen).**



Schritt 2: Klicken Sie auf **Neue API-Anmeldeinformationen**, um eine neue Gruppe von Schlüsseln zu erstellen.

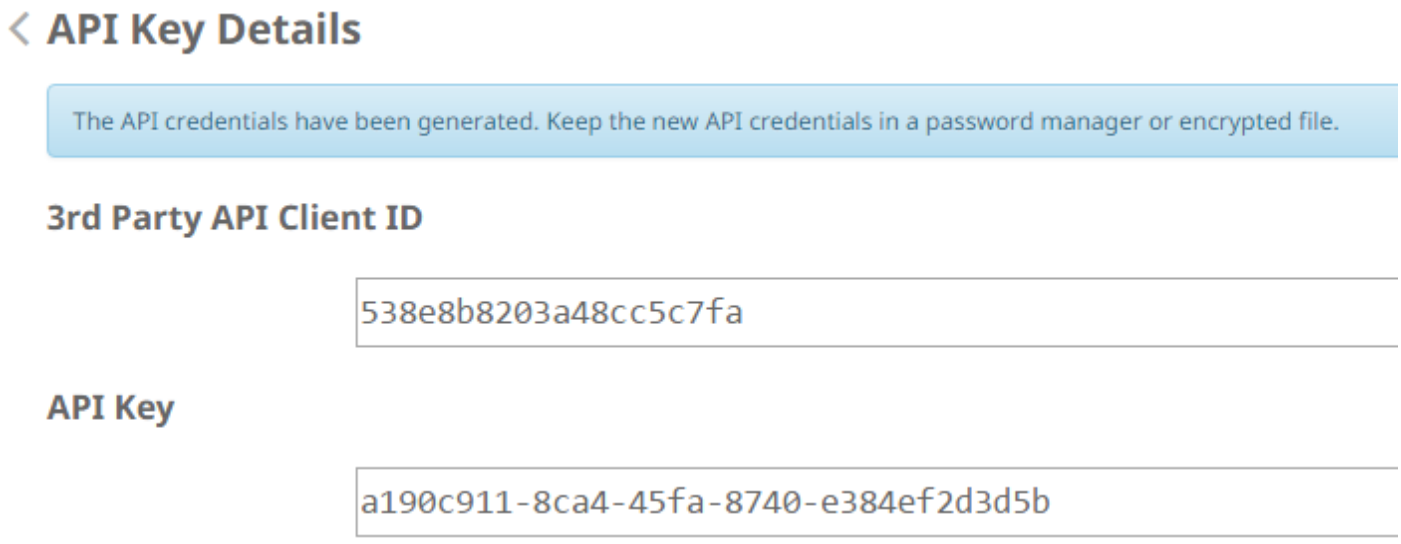


Schritt 3: Geben Sie einen **Anwendungsnamen an**. Wählen Sie den **Bereich** Schreibgeschützt oder Lesen und Schreiben aus.



> **Hinweis**: Eine API-Anmeldeinformationen mit Lese- und Schreibzugriff kann Änderungen an der Konfiguration von Cisco AMP für Endgeräte vornehmen, die erhebliche Probleme mit Ihren Endgeräten verursachen können. Einige der in die Cisco AMP für Endpoints-Konsole integrierten Eingabeschutzfunktionen gelten nicht für die API.

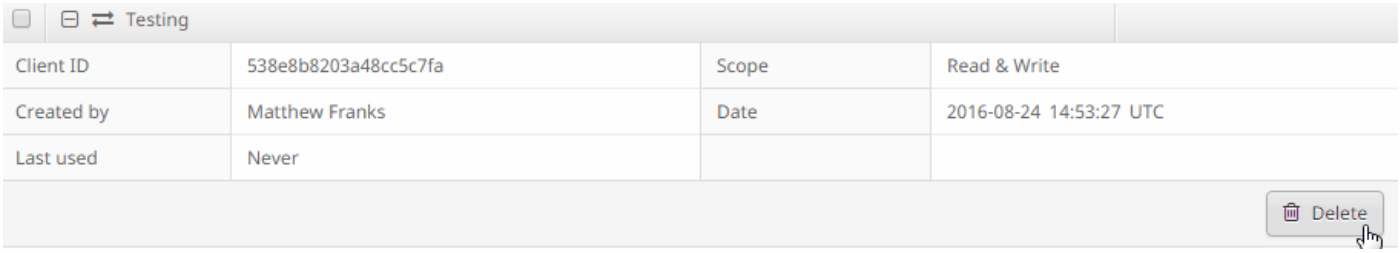
Schritt 4: Klicken Sie auf die Schaltfläche **Erstellen**. Die **API-Schlüsseldetails** werden angezeigt. Speichern Sie diese Informationen, da einige davon nach dem Verlassen des Bildschirms nicht mehr verfügbar sind.



Hinweis: API-Anmeldeinformationen (API-Client-ID und API-Schlüssel) ermöglichen es anderen Programmen, Daten von Cisco AMP für Endgeräte abzurufen und zu ändern. Sie entspricht in der Funktionalität einem Benutzernamen und einem Kennwort und sollte als solche behandelt werden.

Vorsicht: Ihre API-Anmeldeinformationen werden nur einmal angezeigt. Wenn Sie die Anmeldeinformationen verlieren, müssen Sie neue generieren.

Löschen Sie die API-Anmeldeinformationen für eine Anwendung, wenn Sie vermuten, dass sie kompromittiert wurden, und erstellen Sie eine neue. Wenn Sie eine API-Anmeldeinformationen löschen, sperrt sie den Client, der die alten verwendet. Aktualisieren Sie diese daher mit den neuen Anmeldeinformationen.



API-Versionen und aktuelle Optionen

Derzeit sind zwei Versionen der AMP für Endgeräte-API verfügbar: Version 0 und Version 1. Version 1 bietet gegenüber Version 0 zusätzliche Funktionen. Die Dokumentation für Version 1 ist hier. Sie können diese Informationen unter Verwendung von Version 1 abrufen.

- Computer
- Computeraktivität
- Veranstaltungen
- Ereignistypen
- Dateilisten
- Dateilistenelemente
- Gruppen
- Richtlinien

- Versionen

Klicken Sie auf den entsprechenden Befehl im Dokument, um Beispiele seiner Verwendung anzuzeigen.

API-Befehlsuntergliederung und Beispiel

Jeder API-Befehl enthält ähnliche Informationen und kann im Wesentlichen in einen Curl-Befehl unterteilt werden. Dieser kann wie folgt aussehen:

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

Wenn Sie den Befehl curl mit der Option -o verwenden, können Sie die Ausgabe in einer Datei speichern. In diesem Fall lautet der Dateiname "IhrDateiname.json".

> **Tipp**: Weitere Informationen zu .json-Dateien finden Sie hier.

Der nächste Schritt im Befehl **curl** besteht darin, die Adresse mit Ihren Anmeldeinformationen vor dem @-Symbol festzulegen. Wenn Sie API-Anmeldeinformationen generieren, kennen Sie die clientID und APIKey. Dieser Abschnitt des Befehls ähnelt daher dem unten angegebenen Link.

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

Fügen Sie die Versionsnummer und die gewünschten Schritte hinzu. Führen Sie in diesem Beispiel die GET /v1/computers-Optionen aus.Der vollständige Befehl sieht wie folgt aus:

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

Nachdem Sie den Befehl ausgeführt haben, sollten Sie eine **computers.json-**Datei in das Verzeichnis herunterladen, in dem Sie den Befehl initiiert haben.

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

> **Hinweis**: Curl ist online verfügbar und für viele Plattformen mit Windows kompiliert (in der Regel sollten Sie die Win32 - Generic-Version verwenden).

Wenn Sie die Datei öffnen, werden alle Daten in einer Zeile angezeigt. Wenn Sie dies im richtigen Format sehen möchten, können Sie ein Browser-Plugin installieren, um es als JSON zu formatieren und die Datei in einem Browser öffnen. Hier werden Informationen für Ihre Computer angezeigt, die Sie nach Belieben verwenden können, z. B.:

connection_guid, hostname, active, links, connection_version, operating_system, internal_ips, external_ip, group_guid, network_address, policy-GUID und Richtlinienname.


```
{
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"
}
```


Nachdem Sie ein einfaches Beispiel in Aktion gesehen haben, können Sie die verschiedenen

Befehlsoptionen verwenden, um Daten in Ihrer Umgebung abzurufen und zu bearbeiten.

Zugehörige Informationen

- API-Dokumentation für Cisco AMP für Endgeräte

Technischer Support und Dokumentation - Cisco Systems